Revelation of System and Human Vulnerabilities Across MITRE ATT&CK Techniques with Insights from ChatGPT

Jeongkeun Shin*, Geoffrey B. Dobson, L. Richard Carley*, Kathleen M. Carley

December 28th, 2023
CMU-S3D-23-107

Software and Societal Systems Department
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

*Department of Electrical and Computer
Engineering Carnegie Institute of Technology
Carnegie Mellon University
Pittsburgh, PA 15213

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research was supported in part by the Minerva Research Initiative under Grant #N00014-21-1-4012, and by the center for Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. The views and conclusions are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research or the US Government.

Center for the Computational Analysis of Social and Organizational Systems
CASOS technical report.

Keywords: Cybersecurity, MITRE ATT&CK, Enterprise Device Vulnerability, Mobile Device Vulnerability

Abstract

Cybercriminals employ a diverse range of tactics and techniques to exploit vulnerabilities in targeted computing devices. In employing each method, they actively search for weaknesses in the target device's system or capitalize on human vulnerabilities, often arising from end users' mistakes or the sophisticated deception employed by cybercriminals. Therefore, constructing a realistic model to simulate cyber attack campaigns in the virtual environments requires a thorough understanding of all possible system and human vulnerabilities that may be exploited during such campaigns. In this technical report, we have delineated the various system and human vulnerabilities associated with each MITRE ATT&CK technique. In this technical report, we comprehensively outline the system and human vulnerabilities associated with each MITRE ATT&CK technique. We have enlisted the assistance of ChatGPT 3.5 to succinctly summarize the potential vulnerabilities targeted by each technique, drawing insights from the detailed information provided for each MITRE ATT&CK technique. Furthermore, we provide cyber attack mitigation strategies and leverage reverse-engineering capabilities through ChatGPT to infer potential vulnerabilities or weaknesses.

Table of Contents

1 Introduction

Understanding the systems and human vulnerabilities targeted by cyber attack tactics and techniques is crucial for developing new cybersecurity software, establishing effective cybersecurity policies within organizations, and devising defensive tactics to counter cyber attacks. Furthermore, when developing a virtual model to simulate cyber attacks and defenses, it is essential to incorporate accurate systems and human vulnerabilities to create a realistic and precise model. This must be implemented with precision so that, during the simulation, cybercriminal agents' exploitation of vulnerabilities to achieve their objectives can be accurately assessed. This way, within the model, the extent of damage from the specific cyber attack campaign can be accurately calculated through simulation. Then, it will be possible to precisely assess how effectively specific defensive measures, cybersecurity education, and the implementation of cybersecurity software can reduce vulnerabilities and the scale of damage within the organization.

There have been numerous efforts to develop the simulation models to realistically replicate the cyber attack campaigns and defense scenarios. Dobson and Carley introduced the Cyber-FIT framework [770][774], a platform designed to simulate virtual cyber warfare involving Denial of Service (DoS), Routing Protocol Attack (RPA), and phishing attacks targeting networking, server, and user systems. Subsequently, they further refined this framework by incorporating the cyber kill chain paradigm, thereby ensuring that cyber attacker agents meticulously follow the cyber attack sequence for a heightened sense of realism [771]. Furthermore, they integrated the concept of cyber situational awareness into all agents, effectively representing the time required for these agents to become aware of the evolving cyber threat landscape [772]. However, Cyber-FIT still has a limitation in accurately capturing the vulnerabilities. While Dobson and Carley introduced the concept of vulnerabilities within the terrain agent in the Cyber-FIT framework [773], it is important to note that these conceptual vulnerabilities do not faithfully replicate real-world scenarios. During simulations, vulnerability scores ranging from 0 to 99 randomly manifest within the terrain agents. A higher score signifies a more severe vulnerability, one that can be exploited by attacker agents to craft and execute cyberattacks. Also, human vulnerabilities are not considered in this model. Shin et al. introduced the OSIRIS model [775] designed for simulating a range of cyber attack campaigns and assessing the efficacy of diverse defense strategies. They conducted experiments, including testing the effectiveness of a human firewall strategy against a spearphishing campaign for data exfiltration [776], the evaluation of the potential damage from ransomware [777], and assessment of the performance of intrusion detection systems against Denial of Service (DoS) attacks [779]. Nevertheless, despite their endeavors to capture the dynamic phishing susceptibility of each end-user agent by considering various human factors [778], the OSIRIS model does not currently incorporate other forms of human vulnerabilities and potential system vulnerabilities.

To enhance the authenticity of our current cyber attack and defense simulation models, we have compiled a comprehensive list of system and human vulnerabilities by leveraging MITRE ATT&CK tactic and technique information for both enterprises and mobile environments [1][2][3][769]. Utilizing OpenAI's ChatGPT [781], we sought to extract valuable insights into the vulnerabilities associated with each MITRE ATT&CK

technique [2][3]. Experts often implicitly refer to the system and human vulnerabilities exploited in the process of describing various cyber attack techniques. Consequently, we utilized the following script to present each MITRE ATT&CK [1] technique to ChatGPT [781], prompting it to provide succinct summaries of the corresponding system and human vulnerabilities.

> Hello. I am trying to gather the system and human vulnerability list from each MITRE ATT&CK technique information. Can you help me to summarize the high-level system and human vulnerability list from the given MITRE ATT&CK information?
>
> (Specific MITRE ATT&CK technique description)
>
> Based on this attack information, please list all vulnerabilities that come from the system's weakness or human's mistakes.
> Please don't include the vulnerability outside of this attack information, and do not generate redundant vulnerability information.
> If the vulnerability comes from the system's weakness, tell us what it is by starting the sentence with "The system's vulnerability targeted by an adversary is..."
> If the vulnerability is made by a human's mistake, please start the sentence with "The vulnerability is made by the user is..."
> Please don't list the potential for attack as a vulnerability.
> If there is no relevant system weakness, just say system weakness does not exist.
> If there is no relevant human mistake, just say human mistake does not exist.
> For each vulnerability, please summarize in one sentence.

For every Enterprise and Mobile MITRE ATT&CK technique [2][3], corresponding mitigation strategies are typically provided [782][783]. By presenting these mitigation strategies [782][783] to ChatGPT [781], we seek its assistance in reverse engineering to deduce potential system and human vulnerabilities using the following script:

> Here are the mitigation strategies for the technique mentioned above.
>
> (Descriptions of MITRE ATT&CK mitigation strategies)
>
> Based on the mitigation information, please list additional vulnerabilities that come from the system's weakness or human's mistakes.
> Please don't list the potential for attack as a vulnerability.
> If there is no relevant system weakness, just say system weakness does not exist.
> If there is no relevant human mistake, just say human mistake does not exist.
> If the vulnerability comes from the system's weakness, tell us what it is by starting the sentence with "The system's vulnerability targeted by an adversary is..."
> If the vulnerability is made by a human's mistake, please start the sentence with "The vulnerability is made by the user is..."
> For each vulnerability, please summarize in one sentence.

The technical paper on ChatGPT [781] had previously demonstrated its efficacy in elucidating vulnerabilities within the cybersecurity domain. In our experiments, ChatGPT consistently provided insightful summaries of system and human vulnerabilities related to a given MITRE ATT&CK technique, along with corresponding mitigation strategies. However, we observed that ChatGPT occasionally characterized the adversary's potential attack itself as a vulnerability, particularly when the MITRE ATT&CK technique information did not explicitly specify any clear vulnerabilities. Despite instructing ChatGPT to explicitly mention "system/human vulnerability does not exist" when no specific vulnerability information was found in the given MITRE ATT&CK technique, this directive did not consistently produce the desired results. In such instances, inspection of ChatGPT's responses was necessary, and we manually filter out irrelevant vulnerability information and clarify ambiguous responses. We also observed that the quantity of vulnerabilities presented by ChatGPT is frequently influenced by the number of vulnerabilities it previously provided in connection with specific MITRE ATT&CK techniques. To prevent ChatGPT to overlook particular vulnerability details or generate irrelevant information, initiating a new chat for each MITRE ATT&CK technique is essential.

As an alternative candidate, the MITRE CVE (Common Vulnerabilities and Exposures) [780] was considered, which provides a documented list of system vulnerabilities. However, this list goes too deeply into technical aspects. Within the simulation model, there was a need for high-level vulnerability descriptions that could be more intuitively understood. Additionally, MITRE CVE [780] does not cover human vulnerabilities. As social engineering techniques continue to advance and the significance of social cybersecurity [784] continues to escalate, it becomes imperative to uncover and consider the list of human vulnerabilities. Analyzing each technique in MITRE ATT&CK [1] to derive vulnerabilities proves advantageous, as it facilitates matching between MITRE ATT&CK techniques and vulnerabilities. This consideration allows for the implementation of which MITRE ATT&CK techniques [2][3] target specific vulnerabilities within the model.

In the subsequent chapters, our findings are presented. Chapter 2 provides a comprehensive compilation of system and human vulnerabilities corresponding to each enterprise MITRE ATT&CK technique [2]. Chapter 3 provides a comprehensive compilation of system and human vulnerabilities associated with each mobile MITRE ATT&CK technique [3]. For ease of reference, enterprise vulnerabilities are coded as 'EV,' while mobile vulnerability codes begin with 'MV.' The numerical MITRE ATT&CK code (e.g., 1595) is then appended, followed by 'S' for system vulnerabilities and 'H' for human vulnerabilities. Here are examples to illustrate this coding system:

- EV1595-S1: The first system vulnerability related to enterprise technique T1595.
- MV1561-H2: The second human vulnerability linked to mobile technique T1541.

2 Enterprise Device Vulnerability [2]

2.1 Reconnaissance (TA0043) [4]

2.1.1 Active Scanning (T1595) [65]

EV Code	Vulnerability Description
EV1595-S1	A lack of proper network traffic filtering, allowing adversaries to execute active reconnaissance scans, potentially leading to the identification of exploitable weaknesses.
EV1595-H1	Insufficient configuration of network protocols, particularly ICMP, creating opportunities for adversaries to perform active scanning and gather sensitive information about the system.

2.1.2 Active Scanning: Scanning IP Blocks (T1595.001) [66]

EV Code	Vulnerability Description
EV1595.001-S1	Inadequate network security measures, allowing the scanning of IP blocks and disclosure of active IP addresses, potentially leading to further reconnaissance and exploitation.
EV1595.001-S2	Insufficient filtering of ICMP requests and responses, leaving the network susceptible to simple ping scans that can disclose the existence of active IP addresses.
EV1595.001-H1	Poor configuration management, enabling the exposure of detailed host information through server banners and network artifacts during IP block scans, facilitating potential avenues for exploitation.
EV1595.001-H2	Neglecting to update and patch server software, as revealed by server banners during IP block scans, exposing the system to potential exploits targeting known software vulnerabilities.

2.1.3 Active Scanning: Vulnerability Scanning (T1595.002) **[67]**

EV Code	Vulnerability Description
EV1595.002-S1	The potential misconfiguration of the target host/application, including outdated or insecure software versions, which could align with specific exploits sought by the adversary during vulnerability scanning.

2.1.4 Active Scanning: Wordlist Scanning (T1595.003) **[68]**

EV Code	Vulnerability Description
EV1595.003-S1	The lack of proper access controls and security measures on web servers, allowing enumeration of website pages and directories through tools like Dirb, DirBuster, and GoBuster, potentially revealing old, vulnerable pages or hidden administrative portals.
EV1595.003-S2	The insufficient configuration of cloud storage solutions, leading to the exposure of globally unique names and allowing enumeration of public and private buckets using tools like s3recon and GCPBucketBrute, potentially exposing sensitive data.
EV1595.003-H1	The inadequate management of cloud storage permissions, as adversaries may leverage discovered storage objects to access valuable information, leading to potential data exfiltration or privilege escalation.
EV1595.003-H2	The failure to remove or secure unnecessary and sensitive information, as adversaries may capitalize on exposed data during wordlist scans, potentially leading to unauthorized access or information leakage.
EV1595.003-H3	The oversight in not conducting a thorough review of external system configurations, as failure to identify and remove non-essential services or resources may result in increased attack surface and potential security risks.

2.1.5 Gather Victim Host Information (T1592) **[288]**

EV Code	Vulnerability Description
EV1592-H1	Inadequate protection of sensitive host information on online platforms or victim-owned websites, allowing adversaries to exploit human mistakes in data exposure.

2.1.6 Gather Victim Host Information: Hardware (T1592.001) **[289]**

EV Code	Vulnerability Description
EV1592.001-H1	The inadvertent disclosure of hardware-related information in publicly accessible documents, job postings, or other online data sets, potentially providing adversaries with valuable reconnaissance data.

2.1.7 Gather Victim Host Information: Software (T1592.002) **[290]**

EV Code	Vulnerability Description
EV1592.002-H1	The unintentional exposure of installed software information through online data sets, such as job postings or resumes, creating opportunities for adversaries to gather intelligence for subsequent stages of the attack lifecycle.
EV1592.002-H2	The inadvertent inclusion of host information in accessible data sets like network maps or purchase invoices, providing adversaries with valuable insights for reconnaissance and potential exploitation.

2.1.8 Gather Victim Host Information: Firmware (T1592.003) **[291]**

EV Code	Vulnerability Description
EV1592.003-H1	The exposure of host firmware details, including type and versions, which could be exploited to infer additional information about hosts in the environment, such as configuration, purpose, age/patch level, etc.

2.1.9 Gather Victim Host Information: Client Configurations (T1592.004) [292]

EV Code	Vulnerability Description
EV1592.004-H1	The exposure of client configurations through publicly accessible data sets, such as job postings, network maps, assessment reports, resumes, or purchase invoices.

2.1.10 Gather Victim Identity Information (T1589) [293]

EV Code	Vulnerability Description
EV1589-S1	The potential exposure of sensitive information due to weaknesses in authentication services that allow for probing and analyzing responses, revealing valid usernames in the system.
EV1589-H1	The inadvertent disclosure of personal and sensitive information through phishing, where adversaries exploit human mistakes by directly eliciting victim identity information.

2.1.11 Gather Victim Identity Information: Credentials (T1589.001) [294]

EV Code	Vulnerability Description
EV1589.001-S1	The compromise of a service provider when multi-factor authentication (MFA) based on out-of-band communications is in use, allowing adversaries to gain access to MFA codes and one-time passwords (OTP).
EV1589.001-H1	The tendency to reuse passwords across personal and business accounts, which adversaries exploit when gathering credentials.
EV1589.001-H2	The exposure of credential information through leaks to online or other accessible data sets, such as search engines, breach dumps, code repositories, etc.

2.1.12 Gather Victim Identity Information: Email Addresses (T1589.002) [295]

EV Code	Vulnerability Description
EV1589.002-S1	The potential exposure of email addresses in public-facing infrastructure, which may result from insufficient access controls or oversight in managing publicly accessible endpoints.
EV1589.002-S2	The risk of enumeration of email addresses in Office 365 environments due to publicly available API endpoints like autodiscover and GetCredentialType, emphasizing the need for enhanced security controls and restrictions on such endpoints.
EV1589.002-H1	The inadvertent exposure of email addresses on social media or victim-owned websites, highlighting the human mistake of oversharing sensitive information online, facilitating easy reconnaissance for adversaries.

2.1.13 Gather Victim Identity Information: Employee Names (T1589.003) [296]

EV Code	Vulnerability Description
EV1589.003-S1	The potential lack of privacy controls or security measures in place, allowing employee names to be readily available and exposed via online or other accessible datasets, such as social media or search victim-owned websites.
EV1589.003-H1	The inadvertent exposure of employee names on online platforms or search victim-owned websites, enabling adversaries to easily gather this information for malicious purposes.

2.1.14 Gather Victim Network Information (T1590) [297]

EV Code	Vulnerability Description
EV1590-H1	Unintentional exposure of network details through actions like Active Scanning or falling victim to Phishing for Information, providing adversaries with valuable insights for subsequent attacks.

2.1.15 Gather Victim Network Information: Domain Properties (T1590.001) **[298]**

EV Code	Vulnerability Description
EV1590.001-H1	The inadvertent exposure of domain-related details, including administrative data, contacts, business addresses, and name servers, through actions like Active Scanning or falling victim to Phishing for Information, providing adversaries with valuable reconnaissance opportunities.

2.1.16 Gather Victim Network Information: DNS (T1590.002) **[299]**

EV Code	Vulnerability Description
EV1590.002-H1	The inadvertent exposure of DNS information through online or accessible datasets, such as Search Open Technical Databases, potentially aiding adversaries in reconnaissance activities and providing opportunities for further exploitation.

2.1.17 Gather Victim Network Information: Network Trust Dependencies (T1590.003) **[300]**

EV Code	Vulnerability Description
EV1590.003-H1	The inadvertent disclosure of information related to network trusts through means such as Phishing for Information, providing adversaries with opportunities for reconnaissance, operational resource establishment, and initial access.

2.1.18 Gather Victim Network Information: Network Topology (T1590.004) **[301]**

EV Code	Vulnerability Description
EV1590.004-S1	The exposure of sensitive network topology details due to inadequate security measures, potentially allowing unauthorized access.

2.1.19 Gather Victim Network Information: IP Addresses (T1590.005) **[302]**

EV Code	Vulnerability Description
EV1590.005-S1	The potential exposure of organizational details, including IP addresses, due to the allocation of public IP addresses in sequential blocks, which may enable the adversary to deduce information about organizational size, physical locations, Internet service providers, and the hosting of publicly-facing infrastructure.
EV1590.005-H1	The inadvertent exposure of information about assigned IP addresses through actions such as Active Scanning or falling victim to Phishing for Information, providing adversaries with opportunities for reconnaissance, operational resource establishment, and initial access.

2.1.20 Gather Victim Network Information: Network Security Appliances (T1590.006) **[303]**

EV Code	Vulnerability Description
EV1590.006-S1	The potential exposure of network security appliances, such as firewalls, content filters, and proxies/bastion hosts, due to their existence and specifics being gathered, which may lead to subsequent reconnaissance and exploitation opportunities.
EV1590.006-H1	The inadvertent exposure of network security appliance information through actions like Active Scanning or falling victim to Phishing for Information, providing adversaries with insights into defensive cybersecurity operations and potential avenues for further attacks.

2.1.21 Gather Victim Org Information (T1591) **[304]**

EV Code	Vulnerability Description
EV1591-H1	The inadvertent disclosure of sensitive organizational information during direct elicitation via Phishing for Information.

EV1591-H2	The potential exposure of organizational details through online or accessible data sets, such as Social Media or Victim-Owned Websites.

2.1.22 Gather Victim Org Information: Determine Physical Locations (T1591.001) **[305]**

EV Code	Vulnerability Description
EV1591.001-H1	The exposure of physical location information through online or accessible data sets.
EV1591.001-H2	The exposure of physical location details through direct elicitation via Phishing for Information, potentially leading to further exploitation.

2.1.23 Gather Victim Org Information: Business Relationships (T1591.002) **[306]**

EV Code	Vulnerability Description
EV1591.002-S1	The potential exposure of sensitive business relationship information due to inadequate network access controls and monitoring, allowing adversaries to identify and exploit weaknesses in second or third-party organizations/domains connected to the victim's network.
EV1591.002-H1	The inadvertent disclosure of business relationship details on social media or victim-owned websites, facilitating adversaries in gathering valuable intelligence through online reconnaissance efforts.

2.1.24 Gather Victim Org Information: Identify Business Tempo (T1591.003) **[307]**

EV Code	Vulnerability Description
EV1591.003-S1	The lack of proper controls or restrictions on the disclosure of operational details, such as business tempo, potentially exposing sensitive information.
EV1591.003-H1	Unintentional disclosure of business tempo-related information through phishing for information, potentially aiding adversaries in subsequent stages of the attack.

2.1.25 Gather Victim Org Information: Identify Roles (T1591.004) **[308]**

EV Code	Vulnerability Description
EV1591.004-H1	The potential exposure of identifiable information about key personnel and their data/resources access due to weaknesses in how roles and identities are managed within the victim organization.
EV1591.004-H2	The inadvertent disclosure of business roles and associated details through actions such as participating in phishing for information, which exposes the organization to targeted attacks.

2.1.26 Phishing for Information (T1598) **[465]**

EV Code	Vulnerability Description
EV1598-H1	The potential for falling victim to phishing messages, either through email, instant messages, or other electronic communication means, as users may unknowingly disclose confidential information in response to deceptive requests.

2.1.27 Phishing for Information: Spearphishing Service (T1598.001) **[466]**

EV Code	Vulnerability Description
EV15998.001-H1	The potential lax security policies of non-enterprise controlled services, such as various social media services and personal webmail, making them more susceptible to spearphishing attacks.
EV15998.001-H2	User falls for social engineering techniques, including the adversary posing as a source with a reason to collect information or sending urgent messages, which can lead to the disclosure of sensitive information, including credentials.
EV15998.001-H3	User creates an opportunity for adversaries by engaging with fake social media accounts or responding to messages related to potential job opportunities, thereby inadvertently facilitating the adversary's efforts to gather information through spearphishing.

EV15998.001-H4	The potential lack of user awareness and training, leaving users susceptible to social engineering techniques and spearphishing attempts.

2.1.28 Phishing for Information: Spearphishing Attachment (T1598.002) [467]

EV Code	Vulnerability Description
EV1598.002-S1	The susceptibility to malicious attachments, which can exploit software vulnerabilities upon opening.
EV1598.002-S2	The lack of effective anti-spoofing and email authentication mechanisms, such as SPF and DKIM, leading to an increased susceptibility to spearphishing attacks.
EV1598.002-H1	The exposure of the sensitive information by populating and returning the attached file in response to the spearphishing email, facilitated by social engineering techniques.
EV1598.002-H2	The risk of users lacking adequate training to identify and resist social engineering techniques and spearphishing attempts, potentially resulting in the inadvertent opening of malicious attachments.

2.1.29 Phishing for Information: Spearphishing Link (T1598.003) [468]

EV Code	Vulnerability Description
EV1598.003-S1	The potential for bypassing anti-spoofing and email authentication mechanisms (such as SPF and DKIM) if not properly configured or enforced, allowing malicious messages to evade validation checks and reach users.
EV1598.003-H1	The inadvertent disclosure of information through web forms on fake websites, as adversaries gather data submitted by users who mistakenly believe they are interacting with legitimate platforms.
EV1598.003-H2	The risk of users lacking adequate training to identify and resist social engineering techniques and spearphishing attempts, potentially resulting in the inadvertent opening of malicious attachments.

2.1.30 Phishing for Information: Spearphishing Voice (T1598.004) [469]

EV Code	Vulnerability Description
EV1598.004-H1	User falls victim to voice phishing (vishing) attacks due to social engineering techniques, such as impersonation and creating a sense of urgency, leading them to disclose confidential information over the phone.
EV1598.004-H2	The inadequate user training programs, allowing for gaps in knowledge and awareness, which may result in users being less adept at identifying and reporting social engineering techniques and spearphishing attempts.

2.1.31 Search Closed Sources (T1597) [526]

EV Code	Vulnerability Description
EV1597-H1	The exposure of sensitive information due to the availability of victim information for purchase from closed sources, including reputable private databases, dark web, or cybercrime black markets.

2.1.32 Search Closed Sources: Threat Intel Vendors (T1597.001) [527]

EV Code	Vulnerability Description
EV1597.001-H1	The exposure of actionable information during searches in private threat intelligence vendor data, potentially revealing information about ongoing campaigns, aligned target industries, capabilities/objectives, or other operational concerns.

2.1.33 Search Closed Sources: Purchase Technical Data (T1597.002) [528]

EV Code	Vulnerability Description
EV1597.002-H1	The inadvertent disclosure of information to adversaries, as users may unknowingly contribute to the compromise of their organization's security by allowing their data to be available for purchase on the dark web or cybercrime blackmarkets.

2.1.34 Search Open Technical Databases (T1596) [529]

EV Code	Vulnerability Description
EV1596-H1	The inadvertent exposure of information in online databases, potentially aiding adversaries in activities like phishing or further reconnaissance.

2.1.35 Search Open Technical Databases: DNS/Passive DNS (T1596.001) [530]

EV Code	Vulnerability Description
EV1596.001-S1	The potential DNS misconfigurations/leaks, which may reveal information about internal networks, providing opportunities for reconnaissance, operational resource acquisition, and initial access.

2.1.36 Search Open Technical Databases: WHOIS (T1596.002) [531]

EV Code	Vulnerability Description
EV1596.002-S1	The exposure of sensitive information due to the public availability of WHOIS data, allowing for reconnaissance activities and potentially leading to further attacks.

2.1.37 Search Open Technical Databases: Digital Certificates (T1596.003) [532]

EV Code	Vulnerability Description
EV1596.003-H1	The inadvertent exposure of digital certificate data, as individuals within the organization may unintentionally reveal information through artifacts signed with certificates used for encrypted web traffic, providing threat actors with opportunities for reconnaissance and establishing operational resources.

2.1.38 Search Open Technical Databases: CDNs (T1596.004) [533]

EV Code	Vulnerability Description
EV1596.004-S1	The potential misconfigurations in the CDN that may leak sensitive information not intended to be hosted or lack the same protection mechanisms as the organization's website, such as login portals.
EV1596.004-H1	The inadvertent exposure of actionable information through online resources and lookup tools, allowing threat actors to harvest data about content servers within the CDN, thereby aiding in reconnaissance and potential exploitation.

2.1.39 Search Open Technical Databases: Scan Databases (T1596.005) [534]

EV Code	Vulnerability Description
EV1596.005-S1	The potential exposure of sensitive information due to the publication of active IP addresses, hostnames, open ports, certificates, and server banners in public scan databases.
EV1596.005-H1	The inadvertent exposure of information as threat actors may exploit the human mistake of not adequately securing or restricting access to sensitive data published in scan databases.

2.1.40 Search Open Websites/Domains (T1593) [535]

EV Code	Vulnerability Description
EV1593-H1	The potential exposure of sensitive information due to the presence of company-related details on freely available websites, such as social media, news sites, or platforms hosting business operation information.
EV1593-H2	The unintentional inclusion of sensitive information (credentials or API keys) in public code repositories, potentially leading to unauthorized access if not adequately reviewed and removed.

2.1.41 Search Open Websites/Domains: Social Media (T1593.001) **[536]**

EV Code	Vulnerability Description
EV1593.001-H1	The potential exposure of sensitive organizational information through social media due to insufficient privacy controls and security measures.

2.1.42 Search Open Websites/Domains: Search Engines (T1593.002) **[537]**

EV Code	Vulnerability Description
EV1593.002-H1	The potential exposure of sensitive information due to the search engine indexing, which may inadvertently reveal network details or credentials, leading to opportunities for further reconnaissance or initial access.

2.1.43 Search Open Websites/Domains: Code Repositories (T1593.003) **[538]**

EV Code	Vulnerability Description
EV1593.003-S1	The lack of automated checks or filters in public code repositories, allowing developers to inadvertently upload sensitive information, such as credentials and API keys.
EV1593.003-H1	The inadvertent inclusion of sensitive information, such as credentials or API keys, in publicly accessible code repositories, posing a risk of unauthorized access by adversaries.

2.1.44 Search Victim-Owned Websites (T1594) **[539]**

EV Code	Vulnerability Description
EV1594-H1	The failure to implement sufficient security controls on victim-owned websites, leading to the unintentional disclosure of valuable information that adversaries can exploit for various malicious activities, including reconnaissance and initial access.

2.2 Resource Development (TA0042) [5]

2.2.1 Acquire Access (T1650) [55]

This attack technique does not rely on a specific vulnerability for execution.

2.2.2 Acquire Infrastructure (T1583) [56]

This attack technique does not rely on a specific vulnerability for execution.

2.2.3 Acquire Infrastructure: Domains (T1583.001) [57]

This attack technique does not rely on a specific vulnerability for execution.

2.2.4 Acquire Infrastructure: DNS Server (T1583.002) [58]

This attack technique does not rely on a specific vulnerability for execution.

2.2.5 Acquire Infrastructure: Virtual Private Server (T1583.003) [59]

This attack technique does not rely on a specific vulnerability for execution.

2.2.6 Acquire Infrastructure: Server (T1583.004) [60]

This attack technique does not rely on a specific vulnerability for execution.

2.2.7 Acquire Infrastructure: Botnet (T1583.005) [61]

This attack technique does not rely on a specific vulnerability for execution.

2.2.8 Acquire Infrastructure: Web Services (T1583.006) [62]

This attack technique does not rely on a specific vulnerability for execution.

2.2.9 Acquire Infrastructure: Serverless (T1583.007) [63]

This attack technique does not rely on a specific vulnerability for execution.

2.2.10 Acquire Infrastructure: Malvertising (T1583.008) [64]

This attack technique does not rely on a specific vulnerability for execution.

2.2.11 Compromise Accounts (T1586) [135]

This attack technique does not rely on a specific vulnerability for execution.

2.2.12 Compromise Accounts: Social Media Accounts (T1586.001) [136]

This attack technique does not rely on a specific vulnerability for execution.

2.2.13 Compromise Accounts: Email Accounts (T1586.002) [137]

This attack technique does not rely on a specific vulnerability for execution.

2.2.14 Compromise Accounts: Cloud Accounts (T1586.003) [138]

This attack technique does not rely on a specific vulnerability for execution.

2.2.15 Compromise Infrastructure (T1584) [140]

This attack technique does not rely on a specific vulnerability for execution.

2.2.16 Compromise Infrastructure: Domains (T1584.001) **[141]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.17 Compromise Infrastructure: DNS Server (T1584.002) **[142]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.18 Compromise Infrastructure: Virtual Private Server (T1584.003) **[143]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.19 Compromise Infrastructure: Server (T1584.004) **[144]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.20 Compromise Infrastructure: Botnet (T1584.005) **[145]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.21 Compromise Infrastructure: Web Services (T1584.006) **[146]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.22 Compromise Infrastructure: Serverless (T1584.007) **[147]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.23 Develop Capabilities (T1587) **[201]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.24 Develop Capabilities: Malware (T1587.001) **[202]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.25 Develop Capabilities: Code Signing Certificates (T1587.002) **[203]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.26 Develop Capabilities: Digital Certificates (T1587.003) **[204]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.27 Develop Capabilities: Exploits (T1587.004) **[205]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.28 Establish Accounts (T1585) **[233]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.29 Establish Accounts: Social Media Accounts (T1585.001) **[234]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.30 Establish Accounts: Email Accounts (T1585.002) **[235]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.31 Establish Accounts: Cloud Accounts (T1585.003) **[236]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.32 Obtain Capabilities (T1588) **[431]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.33 Obtain Capabilities: Malware (T1588.001) **[432]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.34 Obtain Capabilities: Tool (T1588.002) **[433]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.35 Obtain Capabilities: Code Signing Certificates (T1588.003) **[434]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.36 Obtain Capabilities: Digital Certificates (T1588.004) **[435]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.37 Obtain Capabilities: Exploits (T1588.005) **[436]**

This attack technique does not rely on a specific vulnerability for execution.

2.2.38 Obtain Capabilities: Vulnerabilities (T1588.006) [437]

This attack technique does not rely on a specific vulnerability for execution.

2.2.39 Stage Capabilities (T1608) [552]

This attack technique does not rely on a specific vulnerability for execution.

2.2.40 Stage Capabilities: Upload Malware (T1608.001) [553]

This attack technique does not rely on a specific vulnerability for execution.

2.2.41 Stage Capabilities: Upload Tool (T1608.002) [554]

This attack technique does not rely on a specific vulnerability for execution.

2.2.42 Stage Capabilities: Install Digital Certificate (T1608.003) [555]

This attack technique does not rely on a specific vulnerability for execution.

2.2.43 Stage Capabilities: Drive-by-Target (T1608.004) [556]

This attack technique does not rely on a specific vulnerability for execution.

2.2.44 Stage Capabilities: Link Target (T1608.005) [557]

This attack technique does not rely on a specific vulnerability for execution.

2.2.45 Stage Capabilities: SEO Poisoning (T1608.006) [558]

This attack technique does not rely on a specific vulnerability for execution.

2.3 Initial Access (TA0001) [6]

2.3.1 Content Injection (T1659) [150]

EV Code	Vulnerability Description
EV1659-S1	The potential lack of encryption for sensitive information in online traffic, making it susceptible to interception, manipulation, or unauthorized access.
EV1659-S2	The potential failure to restrict web-based content adequately, allowing the download, transfer, and execution of potentially uncommon file types used in adversary campaigns.

2.3.2 Drive-by Compromise (T1189) [215]

EV Code	Vulnerability Description
EV1189-S1	The potential bypass or escape from browser sandboxes, which, although used for application isolation, may still have existing sandbox escape vulnerabilities.
EV1189-S2	The risk of additional exploits and weaknesses in implementation for virtualization and application microsegmentation, even though they may mitigate the impact of client-side exploitation.
EV1189-H1	User enables scripting or active website components and ignoring warning dialog boxes, which may be required for the exploitation process during a drive-by compromise.
EV1189-H2	User interacts with popups on legitimate websites that deliver malicious applications designed to steal Application Access Tokens.
EV1189-H3	The potential failure to use adblockers, allowing malicious code served through ads to execute, compromising the system.
EV1189-H4	The potential failure to use script blocking extensions, leading to the execution of JavaScript commonly used during the exploitation process.
EV1189-H5	The potential neglect of using modern browsers with security features turned on, leaving the system susceptible to exploitation.

EV1189-H6	The failure to keep security applications and protection mechanisms, such as Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET), updated, potentially leaving the system susceptible to exploitation behavior due to outdated or incompatible protections.

2.3.3 Exploit Public-Facing Application (T1190) [270]

EV Code	Vulnerability Description
EV1190-S1	The weaknesses in Internet-facing hosts or systems, including software bugs, temporary glitches, or misconfigurations, which may lead to unauthorized access to the network.
EV1190-S2	The common web-based vulnerabilities in websites and databases, as highlighted by the OWASP top 10 and CWE top 25, potentially allowing adversaries to exploit these weaknesses for unauthorized access.
EV1190-S3	Inadequate application isolation and sandboxing, potentially allowing unauthorized access to other processes and system features.
EV1190-S4	The absence of exploit protection, as the lack of Web Application Firewalls may expose applications to exploit traffic, enabling adversaries to compromise the system.
EV1190-S5	Insufficient network segmentation, particularly the absence of a DMZ or separate hosting infrastructure for externally facing servers and services, potentially allowing adversaries to pivot within the network.
EV1190-H1	The outdated software, as the absence of regular software updates and patch management for externally exposed applications may leave the system vulnerable to exploitation.
EV1190-H2	The inadequate management of privileged accounts, as not using least privilege for service accounts may grant exploited processes excessive permissions on the rest of the system.

EV1190-H3	The lack of vulnerability scanning practices, as not regularly scanning externally facing systems for vulnerabilities and promptly patching critical issues may expose the system to exploitation and unauthorized access.

2.3.4 External Remote Services (T1133) [276]

EV Code	Vulnerability Description
EV1133-S1	The existence of exposed services, such as Docker API, Kubernetes API server, kubelet, or web applications like the Kubernetes dashboard, in containerized environments without proper authentication, facilitating unauthorized access.
EV1133-S2	The potential failure to disable or block unnecessary remotely available services, leaving avenues for exploitation.
EV1133-S3	The potential lack of network segmentation, allowing direct remote access to internal systems and increasing the risk of compromise.
EV1133-H1	The potential failure to implement strong two-factor or multi-factor authentication for remote service accounts, allowing adversaries to exploit stolen credentials.
EV1133-H2	The potential oversight in limiting access to remote services through centrally managed concentrators, such as VPNs and other managed remote access systems.

2.3.5 Hardware Additions (T1200) [310]

EV Code	Vulnerability Description
EV1200-H1	The inadvertent use of commercial and open source products without thorough security evaluation, leading to the unintentional exposure of the system to risks associated with passive network tapping, network traffic modification, keystroke injection, kernel memory reading via DMA, and addition of new wireless access points.
EV1200-H2	Inadequate implementation of network access control policies, such as insufficient use of device certificates and the 802.1x standard, allowing unregistered devices to communicate with trusted systems.

EV1200-H3	The failure to properly configure and monitor endpoint security settings, which may result in the inability to effectively block unknown devices and accessories, leaving the system susceptible to unauthorized hardware installations and potential exploitation by adversaries.

2.3.6 Phishing (T1566) **[460]**

EV Code	Vulnerability Description
EV1566-S1	The potential failure of antivirus/antimalware to automatically quarantine suspicious files, allowing malicious code execution through phishing attachments.
EV1566-S2	The susceptibility of network intrusion prevention systems to false negatives, potentially allowing malicious email attachments or links to evade detection.
EV1566-S3	The risk associated with inadequate restriction of web-based content, particularly the failure to block access to websites or attachment types commonly used for phishing, posing a potential threat to the organization.
EV1566-S4	The potential bypass of email authentication mechanisms such as SPF and DKIM, leading to the failure of anti-spoofing measures and increasing the likelihood of successful phishing attacks.
EV1566-H1	User overlooks or ignores training on social engineering techniques and phishing emails, leading to a higher likelihood of falling victim to such attacks.
EV1566-H2	User falls for social engineering techniques, such as trusting a forged or spoofed identity, leading to the opening of malicious emails or clicking on harmful links.
EV1566-H3	User follows instructions from phishing messages to call a phone number, resulting in actions that may lead to visiting malicious URLs, downloading malware, or installing adversary-accessible remote management tools onto their computer.

2.3.7 Phishing: Spearphishing Attachment (T1566.001) [461]

EV Code	Vulnerability Description
EV1566.001-S1	The potential failure of antivirus/antimalware measures to automatically quarantine suspicious files, leaving the system exposed to malicious attachments delivered through spearphishing.
EV1566.001-S2	The potential for network intrusion prevention and email scanning systems to be ineffective, allowing malicious activity to go undetected when adversaries exploit user execution via spearphishing attachments.
EV1566.001-S3	The potential inadequacy of web-based content restrictions, as blocking unknown or unused attachments by default may not cover all vectors, leaving the system susceptible to concealed malicious attachments in various formats.
EV1566.001-S4	The potential failure of software configuration measures, such as anti-spoofing and email authentication mechanisms, leading to inadequate filtering and validation of messages, allowing malicious emails to bypass security checks.
EV1566.001-H1	The potential for falling victim to social engineering techniques, as the spearphishing email manipulates users into opening the attachment by providing a plausible reason and instructions on bypassing system protections.
EV1566.001-H2	The potential lack of awareness or training, as users may fail to identify social engineering techniques and spearphishing emails, leading to the inadvertent opening of malicious attachments despite security measures in place.

2.3.8 Phishing: Spearphishing Link (T1566.002) [462]

EV Code	Vulnerability Description
EV1566.002-S1	The potential lack of audit controls, allowing unauthorized access to data and resources due to insufficient monitoring of application permissions.

EV1566.002-S2	The potential absence of anti-spoofing and email authentication mechanisms, leading to a higher likelihood of successful spearphishing attacks through the exploitation of sender domain validity and message integrity
EV1566.002-S3	The potential lack of enforcement of browser extensions protecting against IDN and homograph attacks, leaving the system exposed to manipulation via these techniques.
EV1566.002-H1	User clicks or copy and paste a URL into a browser, leading to potential compromise through user-executed actions
EV1566.002-H2	The susceptibility of the email reader to exploitation through links, particularly those that interact directly with the reader or contain embedded images for malicious purposes.
EV1566.002-H3	The acceptance of OAuth 2.0 request URLs, leading to the unwitting provision of permissions/access for malicious applications and enabling the adversary to steal application access tokens
EV1566.002-H4	The potential risk posed by accessing certain websites necessary for business operations but lacking effective monitoring, leaving the system susceptible to spearphishing activities.
EV1566.002-H5	User grants consent to unfamiliar or unverified third-party applications due to limitations not being applied by Azure AD Administrators, enabling adversaries to exploit OAuth 2.0 consent phishing.
EV1566.002-H6	The potential failure to identify social engineering techniques and malicious links in spearphishing emails, leading to user interactions that could compromise the system's security.
EV1566.002-H7	The potential difficulty in visually checking domains due to homographs in ASCII and in IDN domains and URL schema obfuscation, increasing the risk of falling victim to spearphishing attacks despite user training efforts.

2.3.9 Phishing: Spearphishing via Service (T1566.003) **[463]**

EV Code	Vulnerability Description
EV1566.003-S1	The potential failure of antivirus/antimalware protection, as it may not automatically quarantine all suspicious files, leaving room for malicious content to go undetected.
EV1566.003-S2	The risk of inadequate web content restrictions, as the adversary could exploit the necessity of certain social media sites or personal webmail services for business operations, leading to potential spearphishing attacks.
EV1566.003-H1	The likelihood of opening malicious links or attachments sent through third-party services, such as personal webmail, due to the adversary building rapport and creating a plausible reason for interaction, making the target more susceptible to social engineering attacks.
EV1566.003-H2	The absence of a robust user training program, leaving users unaware of security best practices and more susceptible to social engineering attacks, especially through voice communications.

2.3.10 Phishing: Spearphishing Voice (T1566.004) **[464]**

EV Code	Vulnerability Description
EV1566.004-H1	The potential for users to download malware or install adversary-accessible remote management tools, relying on user interaction initiated through voice communications or phone calls.
EV1566.004-H2	The likelihood of falling for social engineering techniques, such as impersonation or the creation of a sense of urgency, leading them to provide access to systems or divulge sensitive information during voice communications or phone calls.
EV1566.004-H3	The risk of users being tricked into divulging Multi-Factor Authentication (MFA) credentials or accepting fraudulent authentication prompts during voice phishing, especially when combined with Multi-Factor Authentication Request Generation by adversaries.

EV1566.004-H4	The absence of a robust user training program, leaving users unaware of security best practices and more susceptible to social engineering attacks, especially through voice communications.

2.3.11 Replication Through Removable Media (T1091) [514]

EV Code	Vulnerability Description
EV1091-S1	The potential failure to adequately configure Windows 10 Attack Surface Reduction (ASR) rules, allowing unsigned/untrusted executable files from USB removable drives to run, if ASR is not properly enabled or configured.
EV1091-S2	The susceptibility to malware propagation through USB devices and removable media within a network, if hardware installation is not adequately limited, potentially allowing unauthorized access or infection.
EV1091-H1	The failure to disable Autorun when unnecessary, leaving the system exposed to the execution of malicious files from removable media, or neglecting to disallow/restrict removable media at an organizational policy level, which could lead to increased risk if not required for business operations.

2.3.12 Supply Chain Compromise (T1195) [574]

EV Code	Vulnerability Description
EV1195-S1	The replacement of legitimate software with modified versions, posing a risk of deploying malicious software to end consumers.
EV1195-H1	The failure to update software, leaving unused, unmaintained, or previously vulnerable dependencies unaddressed and creating opportunities for compromise.
EV1195-H2	The unintentional acceptance and deployment of modified or counterfeit products, leading to potential data or system compromise.
EV1195-H3	The unintentional use of compromised software due to the distribution of malicious additions to legitimate software in software distribution or update channels.

EV1195-H4	The potential adoption of open source projects as dependencies without thorough scrutiny, which may expose users to malicious code added by adversaries targeting popular projects.
EV1195-H5	The potential failure to establish continuous monitoring of vulnerability sources and the insufficient use of automatic and manual code review tools, resulting in a decreased ability to detect and address vulnerabilities in a timely manner, increasing the risk of compromise.

2.3.13 Supply Chain Compromise: Compromise Software Dependencies and Development Tools (T1195.001) [575]

EV Code	Vulnerability Description
EV1195.001-S1	The susceptibility of software dependencies and development tools to manipulation, allowing the injection of malicious code prior to reaching the final consumer.
EV1195.001-H1	The failure to update software, leaving unused, unmaintained, or previously vulnerable dependencies unaddressed and creating opportunities for compromise.
EV1195.001-H2	The potential failure to establish continuous monitoring of vulnerability sources and the insufficient use of automatic and manual code review tools, resulting in a decreased ability to detect and address vulnerabilities in a timely manner, increasing the risk of compromise.

2.3.14 Supply Chain Compromise: Compromise Software Supply Chain (T1195.002) [576]

EV Code	Vulnerability Description
EV1195.002-H1	The potential failure to verify the integrity of received software, creating an opportunity for adversaries to exploit and compromise the system through manipulated or maliciously replaced software.
EV1195.002-H2	The failure to update software, leaving unused, unmaintained, or previously vulnerable dependencies unaddressed and creating opportunities for compromise.

EV1195.002-H3	The potential failure to establish continuous monitoring of vulnerability sources and the insufficient use of automatic and manual code review tools, resulting in a decreased ability to detect and address vulnerabilities in a timely manner, increasing the risk of compromise.

2.3.15 Supply Chain Compromise: Compromise Hardware Supply Chain (T1195.003) [577]

EV Code	Vulnerability Description
EV1195.003-S1	The susceptibility of hardware components to unauthorized modification in the supply chain, enabling the insertion of undetected backdoors into consumer networks.
EV1195.003-S2	The absence of Trusted Platform Module technology or an insecure boot process, allowing unauthorized modifications during the supply chain.
EV1195.003-H1	The failure to regularly check and ensure the integrity of the BIOS or EFI, creating an opportunity for adversaries to exploit and modify these components.

2.3.16 Trusted Relationship (T1199) [616]

EV Code	Vulnerability Description
EV1199-S1	Inadequate network segmentation, leading to potential compromise of infrastructure components that do not require broad network access.
EV1199-H1	The absence of Multi-factor Authentication (MFA) on delegated administrator accounts, which could expose them to compromise.
EV1199-H2	Improper management of accounts and permissions in trusted relationships, increasing the risk of abuse if the party is compromised.

2.3.17 Valid Accounts (T1078) [636]

EV Code	Vulnerability Description
EV1078-S1	The potential lack of proper configuration and monitoring of conditional access policies, allowing non-compliant devices or logins from outside defined organization IP ranges.
EV1078-H1	The use of legacy authentication in Active Directory, which does not support multi-factor authentication (MFA), and the failure to enforce the use of modern authentication protocols.
EV1078-H2	The insecure storage of sensitive data or credentials in applications, such as storing plaintext credentials in code, publishing credentials in repositories, or leaving credentials in public cloud storage, providing opportunities for adversaries to compromise credentials.
EV1078-H3	The failure to promptly change default usernames and passwords on applications and appliances after installation, potentially leaving systems exposed to credential abuse.
EV1078-H4	The potential lack of routine audits of domain and local accounts, their permission levels, and the failure to detect situations that could allow adversaries to gain wide access by obtaining credentials of privileged accounts.
EV1078-H5	The failure to regularly audit user accounts for activity and deactivate or remove unnecessary accounts, increasing the risk of adversaries exploiting unused accounts for unauthorized access.
EV1078-H6	The lack of awareness and training regarding multi-factor authentication (MFA) push notifications, potentially leading users to accept and authenticate malicious notifications, compromising account security.

2.3.18 Valid Accounts: Default Accounts (T1078.001) **[637]**

EV Code	Vulnerability Description
EV1078.001-H1	The presence of default accounts with unchanged credentials, such as Guest or Administrator accounts on Windows systems, which can be exploited for Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.001-H2	The failure to change preset usernames and passwords for equipment like network devices and computer applications, including internal, open source, or commercial systems, which poses a serious threat if not altered post-installation.

2.3.19 Valid Accounts: Domain Accounts (T1078.002) **[638]**

EV Code	Vulnerability Description
EV1078.002-S1	Lack of multi-factor authentication (MFA) implementation, potentially allowing adversaries to gain control of valid credentials.
EV1078.002-S2	Poor design and administration of the enterprise network, potentially leading to the inappropriate inclusion of user or admin domain accounts in local administrator groups across systems, creating a security risk equivalent to having a common local administrator account password.
EV1078.002-H1	Password reuse, which can be exploited by adversaries to compromise domain accounts, posing a risk to Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.002-H2	Inadequate privileged account management, including the lack of routine audits on domain account permission levels, which could enable adversaries to exploit overly permissive access and compromise privileged accounts.
EV1078.002-H3	Insufficient user training on recognizing valid push notifications for multi-factor authentication, increasing the risk of users accepting fraudulent notifications and compromising the effectiveness of MFA.

EV1078.002-H4	Weak password management practices, resulting in credential overlap across systems and increasing the risk of unauthorized access if an adversary obtains account credentials.

2.3.20 Valid Accounts: Local Accounts (T1078.003) [639]

EV Code	Vulnerability Description
EV1078.003-H1	The inadequate enforcement of complex, unique passwords for local administrator accounts across all systems, potentially allowing unauthorized access.
EV1078.003-H2	The reuse of passwords for local accounts, enabling adversaries to abuse credentials across multiple machines on a network, facilitating Privilege Escalation and Lateral Movement.
EV1078.003-H3	The inadequate management of privileged accounts, as routine audits may be neglected, leading to situations where adversaries can exploit credentials of privileged accounts with wide access.
EV1078.003-H4	The improper use of local administrator accounts for day-to-day operations may expose user to potential adversaries, posing a security risk.

2.3.21 Valid Accounts: Cloud Accounts (T1078.004) [640]

EV Code	Vulnerability Description
EV1078.004-S1	The absence of multi-factor authentication for cloud accounts, especially privileged accounts, which could leave accounts susceptible to unauthorized access.
EV1078.004-S2	The potential for misconfigurations in conditional access policies, allowing logins from non-compliant devices or outside defined organization IP ranges.
EV1078.004-H1	Misconfigurations in role assignments or role assumption policies within cloud environments, enabling unauthorized access and privilege escalation.

EV1078.004-H2	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H3	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H4	The lack of enforcement of complex, unique passwords across all systems on the network, particularly for privileged cloud accounts, potentially allowing adversaries to exploit compromised credentials.
EV1078.004-H5	The inadequate review of privileged cloud account permission levels, which may result in the presence of high-risk roles such as Global Administrator and Privileged Role Administrator, providing adversaries with extensive access.
EV1078.004-H6	The failure to periodically review and remove inactive or unnecessary user accounts, potentially leaving dormant accounts that could be exploited by adversaries.
EV1078.004-H7	The potential for users to accept and act on invalid push notifications for multi-factor authentication, highlighting the importance of training users to recognize and report suspicious push notifications.

2.4 Execution (TA0002) [7]

2.4.1 Cloud Administration Command (T1651) [119]

EV Code	Vulnerability Description
EV1651-H1	The improper assignment of privileges, as attackers could exploit a compromise of accounts with roles like Azure Virtual Machine Contributor and above or Global and Intune administrators, emphasizing the importance of limiting the number of users with such permissions.

EV1651-H2	The improper assignment of permissions to execute the ssm:SendCommand action in AWS, with the mitigation recommending the limitation of users with this capability and the use of tags to restrict the number of machines those users can execute commands on.

2.4.2 Command and Scripting Interpreter (T1059) [124]

EV Code	Vulnerability Description
EV1059-S1	The risk of inadequate configuration and monitoring of Attack Surface Reduction (ASR) rules on Windows 10, leading to the potential bypass of behavior prevention mechanisms for Visual Basic and JavaScript scripts
EV1059-S2	The insufficient enforcement of code signing policies, allowing the execution of unsigned scripts and increasing the likelihood of malicious code execution
EV1059-S3	The existence of unnecessary or unused shells and interpreters, as the failure to disable or remove them may provide additional avenues for unauthorized command or script execution
EV1059-S4	The potential absence or inadequate implementation of application control, leaving the system vulnerable to the execution of arbitrary scripts and commands
EV1059-H1	The unintentional execution of malicious commands or scripts, facilitated by the lack of awareness or vigilance in scrutinizing and validating the content of received documents, especially lure documents delivered through Initial Access payloads.
EV1059-H2	The potential failure to implement or enforce robust antivirus/antimalware solutions, which may result in the inability to automatically quarantine suspicious files and prevent malicious execution
EV1059-H3	The insufficient management of privileged accounts, particularly in PowerShell usage, where a lack of restrictions on PowerShell execution policy may increase the risk of unauthorized script execution

EV1059-H4	The lack of awareness or implementation of PowerShell JEA (Just Enough Administration), which could lead to the unsupervised execution of commands through remote PowerShell sessions.

2.4.3 Command and Scripting Interpreter: PowerShell (T1059.001) [125]

EV Code	Vulnerability Description
EV1059.001-S1	The lack of proper updating of antivirus/antimalware solutions, leading to inadequate detection and quarantine of evolving and sophisticated malicious files.
EV1059.001-S2	The potential lack of implementation or improper configuration of application control measures, allowing the execution of malicious PowerShell commands or scripts.
EV1059.001-H1	The potential oversight in not enforcing the use of code signing for PowerShell scripts through proper execution policy configuration, allowing the execution of unsigned and potentially malicious scripts.
EV1059.001-H2	The potential failure to properly disable or restrict the WinRM Service, creating a pathway for unauthorized remote execution of PowerShell, especially if WinRM is unnecessary for legitimate administrative functions.
EV1059.001-H3	The potential misconfiguration or oversight in not effectively implementing PowerShell Constrained Language mode, allowing access to sensitive language elements and facilitating the execution of malicious commands.
EV1059.001-H4	The potential failure to appropriately restrict PowerShell execution policy to administrators, allowing non-administrative users to execute PowerShell scripts and potentially perform unauthorized actions.
EV1059.001-H5	The potential misconfiguration or lack of implementation of PowerShell JEA (Just Enough Administration), leading to inadequate sandboxing of administration and allowing unnecessary or risky commands to be executed through remote PowerShell sessions.

2.4.4 Command and Scripting Interpreter: AppleScript (T1059.002) **[126]**

EV Code	Vulnerability Description
EV1059.002-S1	The potential failure to enforce code signing requirements for AppleScript, as not mandating that all scripts be signed by a trusted developer ID could allow the execution of unsigned and potentially malicious AppleScript code.
EV1059.002-H1	The potential neglect to implement application control measures, creating a lapse in the prevention of unauthorized execution of AppleScript code and other malicious activities.

2.4.5 Command and Scripting Interpreter: Windows Command Shell (T1059.003) **[127]**

EV Code	Vulnerability Description
EV1059.003-H1	The failure to implement proper application control measures, allowing adversaries to potentially execute unauthorized commands and payloads using the Windows command shell (cmd).

2.4.6 Command and Scripting Interpreter: Unix Shell (T1059.004) **[128]**

EV Code	Vulnerability Description
EV1059.004-S1	Security weaknesses in Unix shells, including variations such as sh, bash, zsh, etc., which can grant adversaries control over various aspects of the system and may allow execution of commands with elevated privileges.
EV1059.004-H1	The potential inadequacy of application control implementation, as improper or incomplete deployment of application control measures may leave avenues for adversaries to exploit weaknesses in Unix shells for execution.

2.4.7 Command and Scripting Interpreter: Visual Basic (T1059.005) [129]

EV Code	Vulnerability Description
EV1059.005-S1	The potential reliance on antivirus/antimalware solutions, which may not always effectively detect and quarantine suspicious files, allowing for the execution of Visual Basic payloads.
EV1059.005-S2	The potential limitation of Attack Surface Reduction (ASR) rules on Windows 10, as they may not comprehensively prevent all instances of Visual Basic script execution from potentially malicious downloaded content.
EV1059.005-S3	The existence of unnecessary or unneeded VB components, which, if not disabled or access-restricted, could provide avenues for exploitation.
EV1059.005-S4	Insufficient use of application control, as VBA macros obtained from the Internet may not be adequately blocked from executing in various Office applications, even with the default blocking mechanism based on the file's Mark of the Web (MOTW) attribute.
EV1059.005-S5	The lack of script blocking extensions, which could lead to the execution of malicious scripts and HTA files commonly used during the exploitation process.
EV1059.005-H1	The absence of adblockers, leaving the system susceptible to the execution of malicious code served through ads, potentially compromising security.

2.4.8 Command and Scripting Interpreter: Python (T1059.006) [130]

EV Code	Vulnerability Description
EV1059.006-S1	Insecure file operations and device I/O functionalities in Python's built-in packages, allowing for unauthorized access and manipulation of sensitive system data.
EV1059.006-S2	The potential weakness in antivirus or antimalware configurations, as misconfigurations or outdated signatures may result in the inability to effectively quarantine suspicious Python files.

EV1059.006-H1	The failure to regularly and comprehensively audit inventory systems may lead to undetected unauthorized Python installations and potential security gaps.
EV1059.006-H2	The potential failure to denylist scripting appropriately, which may result in the execution of malicious scripts.
EV1059.006-H3	The failure to adequately restrict user permissions may result in the installation of Python in unauthorized areas, allowing adversaries to circumvent intended security measures.

2.4.9 Command and Scripting Interpreter: JavaScript (T1059.007) [131]

EV Code	Vulnerability Description
EV1059.007-S1	Security gaps in various implementations of JavaScript, including JavaScript (JS), JScript, and JavaScript for Automation (JXA), due to their platform-independent nature and runtime execution capabilities, allowing for abuse in both web browsers and non-browser environments.
EV1059.007-S2	The failure to implement Attack Surface Reduction (ASR) rules on Windows 10, exposing the system to the risk of JavaScript scripts executing potentially malicious downloaded content.
EV1059.007-H1	The risk of not turning off or restricting access to unneeded scripting components, leaving unnecessary attack surfaces open to potential exploitation by adversaries.
EV1059.007-H2	The potential failure to denylist scripting appropriately, which may result in the execution of malicious scripts.
EV1059.007-H3	The risk of not using script blocking extensions or adblockers to prevent the execution of JavaScript and HTA files, particularly during the exploitation process or when served through ads, allowing potential code execution by adversaries.

2.4.10 Command and Scripting Interpreter: Network Device CLI (T1059.008) **[132]**

EV Code	Vulnerability Description
EV1059.008-S1	The potential misconfigurations in the network device CLI, such as inadequate permission levels, allowing unauthorized access and manipulation of critical device functions.
EV1059.008-S2	The insufficient implementation of TACACS+ for authentication and command authorization, allowing adversaries to potentially bypass access controls and execute unauthorized commands on the network device CLI.
EV1059.008-S3	Insufficiently securing remote access methods like telnet or SSH to the network device CLI, facilitating unauthorized entry and potential exploitation by adversaries.
EV1059.008-H1	The misconfiguration or inadequate setup of Authentication, Authorization, and Accounting (AAA) systems, including TACACS+, leading to ineffective privileged account management and potentially allowing unauthorized actions on the network device.
EV1059.008-H2	The inadequate enforcement of least privilege principles in user account management, creating a potential avenue for unauthorized configuration changes.

2.4.11 Command and Scripting Interpreter: Cloud API (T1059.009) **[133]**

EV Code	Vulnerability Description
EV1059.009-S1	The potential misconfigurations or weak permissions in cloud API settings, allowing unauthorized administrative access to critical services such as compute, storage, IAM, networking, and security policies.
EV1059.009-S2	The lack of effective application control, potentially allowing the execution of PowerShell CmdLets or other host-based resources to access cloud API resources.

EV1059.009-H1	Inadequate management of credentials, particularly the insecure handling or sharing of Application Access Tokens and Web Session Cookies, potentially enabling adversaries to exploit cloud APIs for malicious actions.
EV1059.009-H2	Inadequate implementation of privileged account management, specifically the absence or improper configuration of Identity and Access Management (IAM) with Role-Based Access Control (RBAC) policies, which may lead to excessive permissions and increase the risk of unauthorized actions by adversaries.

2.4.12 Container Administration Command (T1609) **[148]**

EV Code	Vulnerability Description
EV1609-S1	The Docker daemon, Kubernetes API server, or kubelet may allow unauthorized remote management of containers, potentially leading to unauthorized access and control within the containerized environment.
EV1609-S2	Insufficient limitation of communications with the container service to managed and secured channels may expose vulnerabilities, providing attackers with the opportunity to intercept or manipulate communications, potentially leading to unauthorized access to container services.
EV1609-H1	Failure to disable or remove unnecessary features or programs from containers may expose additional attack surfaces, providing adversaries with opportunities to exploit unneeded functionalities and compromise container security.
EV1609-H2	Neglecting to implement read-only containers, read-only file systems, or minimal images may result in the execution of unauthorized commands, potentially leading to unauthorized access and data compromise within the containerized environment.
EV1609-H3	Inadequate use of application control and software restriction tools, such as those provided by SELinux, to restrict access to files, processes, and system calls in containers may lead to vulnerabilities, allowing adversaries to manipulate container resources and compromise security.

EV1609-H4	Failure to enforce secure port access and TLS for communication with Docker API and Kubernetes API Server may expose these interfaces to unauthorized access, increasing the risk of unauthorized control and manipulation of containers.
EV1609-H5	Neglecting to define and enforce Pod Security Standards in Kubernetes may result in containers running as root by default, posing security risks and providing adversaries with opportunities to exploit privileged containers within the cluster.
EV1609-H6	Inadequate enforcement of authentication and role-based access control on the container service may result in unauthorized users having elevated privileges, leading to potential unauthorized actions within the containerized environment.
EV1609-H7	User grants wildcard permissions or adding them to the system:masters group in Kubernetes, instead of using more restrictive RoleBindings, may lead to excessive privileges and increase the risk of unauthorized access and control within the Kubernetes environment.

2.4.13 Deploy Container (T1610) [200]

EV Code	Vulnerability Description
EV1610-S1	Lack of proper image scanning and compliance checks before deployment, allowing potentially insecure or non-compliant images to be deployed, posing a security risk.
EV1610-S2	Inadequate network segmentation, as direct remote access to internal systems is not denied effectively through network proxies, gateways, and firewalls, potentially exposing sensitive services to unauthorized access.
EV1610-S3	Insufficient restrictions on communication channels, as the use of unmanaged or insecure communication channels with the container service could lead to unauthorized access, bypassing secure channels like local Unix sockets or SSH.

EV1610-H1	Failing to enforce the principle of least privilege, as users may be granted unnecessary access to container dashboards, or users might be added to overly permissive groups like system:masters in Kubernetes, leading to unauthorized access and potential misuse.
EV1610-H2	User Neglects to implement just-in-time (JIT) access controls for the Kubernetes API, resulting in a failure to place additional restrictions on API access, potentially allowing unauthorized users to gain access to critical resources.
EV1610-H3	Failure to properly configure and restrict IP ranges in cloud environments, where the Kubernetes API server is deployed, potentially allowing unauthorized access to the API server from untrusted sources.
EV1610-H4	User Neglects to employ RoleBindings instead of ClusterRoleBindings in Kubernetes, which may result in users being granted broader privileges than necessary or intended, thereby opening the possibility of unauthorized actions within the cluster.
EV1610-H5	User Neglects to disable unauthenticated access to Docker API, Kubernetes API Server, and container orchestration web applications, leaving these interfaces exposed and vulnerable to unauthorized access or attacks on the containerized environment.

2.4.14 Exploitation for Client Execution (T1203) [271]

EV Code	Vulnerability Description
EV1203-S1	Software vulnerabilities in client applications, stemming from unsecure coding practices that can lead to unanticipated behavior, allowing for targeted exploitation and arbitrary code execution.
EV1203-S2	The susceptibility of web browsers to Drive-by Compromise and Spearphishing Link, enabling compromise through normal web browsing or spearphishing emails without user action.
EV1203-S3	The potential escape from browser sandboxes, which, while used for mitigation, may still have existing sandbox escape vulnerabilities.

EV1203-S4	Weaknesses in virtualization and application microsegmentation systems, potentially mitigating the impact of client-side exploitation but introducing new points of vulnerability.
EV1203-S5	The potential for security applications like Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET) to have risks of additional exploits and weaknesses, depending on the specific architecture and target application binary.
EV1203-H1	Weaknesses in applications like Adobe Reader and Flash, often requiring user interaction to open files or objects within documents, presenting an avenue for gaining access to systems.
EV1203-H2	The need for user interaction to open malicious documents transmitted through phishing, exploiting common office and productivity applications such as Microsoft Office for arbitrary code execution.
EV1203-H3	The potential to open malicious documents or files delivered through phishing, specifically in the context of office applications, where user actions are necessary for the exploit to run.
EV1203-H4	User do not keep security applications like Windows Defender Exploit Guard (WDEG) or Enhanced Mitigation Experience Toolkit (EMET) up to date, potentially leaving the system vulnerable to exploitation.

2.4.15 Inter-Process Communication (T1559) **[368]**

EV Code	Vulnerability Description
EV1559-S1	Insecure inter-process communication (IPC) mechanisms, such as those accessible through programming languages/libraries or native interfaces like Windows Dynamic Data Exchange or Component Object Model, which may lack proper authentication or authorization controls.
EV1559-S2	The potential misconfiguration or oversight in application development, where the inclusion of the com.apple.security.get-task-allow entitlement with the value set to any variation of true may occur, compromising the effectiveness of the Hardened Runtime capability.

EV1559-S3	The potential lack of Attack Surface Reduction (ASR) rules on Windows 10, allowing for the exploitation of inter-process communication (IPC) vulnerabilities, such as DDE attacks and spawning of child processes from Office programs.
EV1559-S4	The potential existence of insecure default Registry keys related to Microsoft Office feature control security, which could allow automatic DDE/OLE execution, compromising the security of inter-process communication (IPC) mechanisms.
EV1559-H1	The potential failure to enable COM alerts and Protected View, leaving the system susceptible to exploitation through inter-process communication (IPC) mechanisms.
EV1559-H2	The potential failure to modify Registry settings in HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{AppID_GUID} and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole using Dcomcnfg.exe, leading to inadequate management of process-wide and system-wide security settings for individual COM applications and defaults for all COM applications, respectively.
EV1559-H3	The potential oversight in disabling embedded files in Office programs, such as OneNote, that do not work with Protected View, leaving a potential avenue for exploitation through inter-process communication (IPC) mechanisms.

2.4.16 Inter-Process Communication: Component Object Model (T1559.001) [369]

EV Code	Vulnerability Description
EV1559.001-S1	Insecurely exposed Windows Component Object Model (COM) interfaces, allowing arbitrary code execution, which can be facilitated through various programming languages such as C, C++, Java, and Visual Basic.
EV1559.001-S2	Inadequate enforcement of COM alerts and Protected View, which may occur if these security measures are not consistently enabled, leaving openings for COM-based attacks due to insufficient application isolation and sandboxing.

EV1559.001-S3	The misconfiguration of Registry settings, either directly or through Dcomcnfg.exe, in HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID{AppID_GUID} and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole. This misconfiguration could lead to inadequate process-wide and system-wide security settings for COM applications, creating opportunities for unauthorized access and execution.

2.4.17 Inter-Process Communication: Dynamic Data Exchange (T1559.002) [370]

EV Code	Vulnerability Description
EV1559.002-S1	The potential enabling of Windows Dynamic Data Exchange (DDE) in Windows 10 and Microsoft Office 2016 through Registry keys, even though it has been superseded by Component Object Model (COM).
EV1559.002-S2	The risk of DDE execution being invoked remotely via Remote Services, such as Distributed Component Object Model (DCOM), allowing adversaries operating on compromised machines without direct access to a Command and Scripting Interpreter.
EV1559.002-S3	The potential oversight in not properly configuring Registry keys specific to Microsoft Office feature control security, which may result in the failure to disable automatic DDE/OLE execution and enhance overall security.
EV1559.002-S4	The potential misconfiguration or neglect in not utilizing or properly configuring the default Registry keys provided by Microsoft to completely disable DDE execution in Word and Excel, leaving these applications susceptible to exploitation.
EV1559.002-H1	The potential failure to ensure that Protected View is enabled, leaving Microsoft Office applications exposed to the risk of DDE attacks.
EV1559.002-H2	The potential misconfiguration or oversight in not enabling Attack Surface Reduction (ASR) rules on Windows 10, which could lead to the exploitation of DDE attacks and the spawning of child processes from Office programs.

EV1559.002-H3	The potential oversight in not considering the disabling of embedded files in Office programs, such as OneNote, that do not work with Protected View, creating a potential avenue for DDE attacks.

2.4.18 Inter-Process Communication: XPC Services (T1559.003) [371]

EV Code	Vulnerability Description
EV1559.003-S1	Weaknesses in the XPC service daemon, which runs with root privileges, allowing them to provide malicious content for local code execution.
EV1559.003-H1	User fails to enable the Hardened Runtime capability or improperly configure entitlements, adversaries may exploit the absence of security features, potentially leading to the inclusion of the com.apple.security.get-task-allow entitlement with a true value and increasing the risk of local code execution.

2.4.19 Native API (T1106) [407]

EV Code	Vulnerability Description
EV1106-S1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office VBA macros to call Win32 APIs and bypass behavior prevention measures.
EV1106-S2	The potential misconfiguration or neglect of application control tools such as Windows Defender Application Control, AppLocker, or Software Restriction Policies, which could lead to the execution of potentially malicious software through the described technique.

2.4.20 Scheduled Task/Job (T1053) [518]

EV Code	Vulnerability Description
EV1053-S1	The potential permission weaknesses in scheduled tasks, allowing adversaries to exploit and escalate privileges.

EV1053-H1	The failure to configure settings for scheduled tasks to force them to run under the context of the authenticated account instead of allowing them to run as SYSTEM, creating a potential avenue for privilege escalation.
EV1053-H2	The failure to restrict the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process, potentially enabling unauthorized users to manipulate task scheduling priorities.
EV1053-H3	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, allowing unauthorized administrators to create scheduled tasks on remote systems.

2.4.21 Scheduled Task/Job: At (T1053.002) [519]

EV Code	Vulnerability Description
EV1053.002-S1	The misconfiguration of the at.allow and at.deny files on Linux and macOS, as adversaries can exploit this to invoke the at utility, potentially leading to unauthorized task scheduling.
EV1053.002-S2	The potential misconfiguration of scheduled tasks in Windows environments, as they may run with elevated privileges, allowing adversaries to exploit permission weaknesses and escalate privileges.
EV1053.002-H1	The misconfiguration of scheduled tasks in Windows environments, where tasks are allowed to run as SYSTEM, creating a potential avenue for privilege escalation if not properly configured to run under the context of the authenticated account.
EV1053.002-H2	The potential misconfiguration of the Increase Scheduling Priority option in Windows environments, as it could allow non-administrative users to schedule priority processes, leading to potential abuse.
EV1053.002-H3	The mismanagement of user account privileges in Linux environments, specifically related to the at utility, where users listed in the at.deny file may not be properly restricted from invoking the at utility, potentially leading to unauthorized task scheduling.

2.4.22 Scheduled Task/Job: Cron (T1053.003) [520]

EV Code	Vulnerability Description
EV1053.003-H1	The absence of regular auditing for changes to the cron schedule, potentially allowing undetected malicious scheduling.
EV1053.003-H2	Inadequate management of cron permissions through /etc/cron.allow and /etc/cron.deny, which may result in unauthorized users gaining cron access or superfluous restrictions, impacting proper system functioning.

2.4.23 Scheduled Task/Job: Scheduled Task (T1053.005) [521]

EV Code	Vulnerability Description
EV1053.005-S1	The potential permission weaknesses in scheduled tasks, which may be exploited to escalate privileges, as highlighted by the PowerSploit framework's PowerUp modules.
EV1053.005-S2	The insufficient restriction of the Increase Scheduling Priority option, potentially allowing non-administrative users to schedule a priority process, which can be mitigated by configuring GPO settings to restrict this privilege to the Administrators group.
EV1053.005-H1	The misconfiguration of scheduled task settings, allowing tasks to run as SYSTEM, which can be mitigated by configuring settings to force tasks to run under the context of the authenticated account and adjusting associated Registry keys and Group Policy Objects (GPO).
EV1053.005-H2	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, leading to unauthorized creation of scheduled tasks on remote systems; this can be addressed by appropriately limiting user privileges and addressing Privilege Escalation vectors through effective User Account Management.

2.4.24 Scheduled Task/Job: Systemd Timers (T1053.006) [522]

EV Code	Vulnerability Description
EV1053.006-H1	The improper implementation of privileged account management, as failure to limit access to the root account may result in unauthorized creation or modification of systemd timer unit files by users.
EV1053.006-H2	User insufficiently restricts file and directory permissions, as failure to limit access to systemd .timer unit files may allow unauthorized users to read or modify them, potentially leading to the execution of malicious code.
EV1053.006-H3	Inadequate user account management, as failure to restrict user access to system utilities may result in unauthorized use of 'systemctl' or 'systemd-run' by users, facilitating the abuse of systemd timers for malicious purposes.

2.4.25 Scheduled Task/Job: Container Orchestration Job (T1053.007) [523]

EV Code	Vulnerability Description
EV1053.007-S1	The potential for containers to run with root privileges by default, creating a security weakness that can be exploited for malicious activities.
EV1053.007-H1	User misconfigures or allows unauthorized access to CronJobs within Kubernetes, enabling the scheduling of jobs that execute malicious code in various nodes within a cluster.
EV1053.007-H2	The improper configuration and lack of adherence to Pod Security Standards in Kubernetes environments, allowing containers to run as privileged, which undermines the intended security measures and facilitates unauthorized activities.

2.4.26 Serverless Execution (T1648) [546]

EV Code	Vulnerability Description
EV1648-H1	The improper configuration or granting of permissions, such as the misuse of IAM:PassRole in AWS or iam.serviceAccounts.actAs in Google Cloud, enabling adversaries to add Additional Cloud Roles to serverless functions and perform unauthorized actions in the cloud environment.

2.4.27 Shared Modules (T1129) [548]

EV Code	Vulnerability Description
EV1129-S1	The Windows module loader's capability to load DLLs from arbitrary local paths and Universal Naming Convention (UNC) network paths, facilitated by NTDLL.dll and the Windows Native API, introduces a vulnerability that adversaries can leverage.
EV1129-S2	The ability of Linux and macOS module loaders to load and execute shared objects from arbitrary local paths, as well as the common practice of executing .dylib files on macOS, poses a vulnerability that adversaries can exploit.
EV1129-S3	The potential failure or misconfiguration of application control tools, which may allow the execution of potentially malicious software through the mentioned technique if these tools are not properly configured or if their capabilities are circumvented.

2.4.28 Software Deployment Tools (T1072) [549]

EV Code	Vulnerability Description
EV1072-S1	Inadequate Active Directory configuration, potentially leading to unauthorized access to critical network systems
EV1072-S2	The absence of restrictions on the installation of third-party software within the enterprise network, creating a potential avenue for unauthorized access

EV1072-S3	The insecure configuration of remote data storage, potentially allowing unauthorized access to the application deployment system
EV1072-H1	The inadequate management of user accounts used by third-party providers, potentially leading to unauthorized access
EV1072-H2	The insufficient management of privileged accounts, potentially leading to unauthorized access to application deployment systems
EV1072-H3	Mismanagement of password policies, such as using non-unique credentials across the enterprise network, posing a risk of unauthorized access to deployment systems
EV1072-H4	Insufficient implementation of multi-factor authentication, which may expose critical network systems to unauthorized access
EV1072-H5	Inadequate network segmentation, potentially allowing unauthorized access to critical network systems
EV1072-H6	The lack of regular software patching on deployment systems, creating a potential avenue for remote access through exploitation for privilege escalation
EV1072-H7	The absence of a strict approval policy for the use of deployment systems, creating a potential avenue for unauthorized access
EV1072-H8	The lack of user training, potentially leading to insecure use of deployment systems;

2.4.29 System Services (T1569) **[603]**

EV Code	Vulnerability Description
EV1569-H1	The failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing processes created by PsExec to run and potentially bypass security measures.
EV1569-H2	The misconfiguration of permissions, allowing services that run at a higher permissions level to be created or interacted with by a user with a lower permission level.
EV1569-H3	The failure to restrict file and directory permissions, potentially allowing users with lower permission levels to replace or modify high permission level service binaries.

EV1569-H4	The failure to prevent users from installing their own launch agents or launch daemons, creating opportunities for unauthorized execution of code or programs.

2.4.30 System Services: Launchctl (T1569.001) [604]

EV Code	Vulnerability Description
EV1569.001-H1	The failure to prevent users from installing their own launch agents or launch daemons, allowing for potential unauthorized execution of commands or programs and increasing the risk of exploitation.

2.4.31 System Services: Service Execution (T1569.002) [605]

EV Code	Vulnerability Description
EV1569.002-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing processes created by PsExec to run and potentially execute malicious actions.
EV1569.002-H2	The failure to appropriately configure permissions, allowing services that run at a higher permission level to be created or interacted with by users with lower permission levels, potentially leading to unauthorized access and misuse.
EV1569.002-H3	The absence of proper file and directory permission restrictions, which could enable users with lower permission levels to replace or modify high permission level service binaries, posing a risk of unauthorized changes and potential exploitation.

2.4.32 User Execution (T1204) [632]

EV Code	Vulnerability Description
EV1204-S1	The potential lack of Attack Surface Reduction (ASR) rules enabled on Windows 10, which may allow executable files to run without meeting prevalence, age, or trusted list criteria, and Office applications to create potentially malicious executable content.

EV1204-S2	The absence of effective application control, which may result in the running of executables masquerading as other files.
EV1204-S3	The lack of network intrusion prevention systems or inadequate protection against malicious downloads, potentially allowing users to visit malicious links that lead to the execution of harmful actions.
EV1204-S4	The absence of restrictions on web-based content, specifically the failure to block unknown or unused files in transit and the lack of policies to prevent the download of suspicious files from potentially malicious sites.
EV1204-H1	User's susceptibility to social engineering, leading them to execute malicious code by opening malicious document files or links.
EV1204-H2	User clicks a file placed in a shared directory or on their desktop by an adversary, especially after falling victim to internal spearphishing.
EV1204-H3	User downloads and executes malware for User Execution, particularly in scenarios like tech support scams facilitated through phishing, vishing, or other forms of user interaction.
EV1204-H4	User falls prey to spoofing and the promotion of toll-free numbers or call centers, which can lead victims to malicious websites and result in the delivery and execution of payloads containing malware or Remote Access Software.
EV1204-H5	The potential lack of awareness and training, as users may not be adequately trained to recognize and avoid common phishing and spearphishing techniques, leaving them susceptible to executing malicious code.

2.4.33 User Execution: Malicious Link (T1204.001) [633]

EV Code	Vulnerability Description
EV1204.001-S1	The potential lack of robust network intrusion prevention systems or inadequate scanning mechanisms for malicious downloads, which could result in the failure to block malicious activity effectively.

EV1204.001-S2	The absence of restrictions on web-based content, allowing the download of unknown or unused files that could be exploited, highlighting the importance of implementing effective content restriction policies.
EV1204.001-H1	The susceptibility to social engineering tactics, leading them to click on a malicious link, thereby initiating the User Execution technique and enabling further malicious activities.
EV1204.001-H2	User ignores or overlooks training on common phishing and spearphishing techniques, leading to a higher likelihood of falling victim to social engineering tactics and clicking on malicious links.

2.4.34 User Execution: Malicious File (T1204.002) **[634]**

EV Code	Vulnerability Description
EV1204.002-S1	The potential failure of Attack Surface Reduction (ASR) rules on Windows 10, particularly if cloud-delivered protection is not enabled, allowing the execution of potentially malicious executable files.
EV1204.002-S2	The potential inadequacy of application control measures in preventing the execution of executables masquerading as other files.
EV1204.002-H1	User succumbs to social engineering tactics, leading them to open malicious files, such as .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl, facilitating adversary-initiated code execution.
EV1204.002-H2	The susceptibility to masquerading and obfuscated files or information, increasing the likelihood of successful user execution by using familiar naming conventions or password-protected files with supplied instructions.
EV1204.002-H3	User overlooks or dismisses user training, diminishing user's awareness of common phishing and spearphishing techniques and reducing their ability to raise suspicion for potentially malicious events.

2.4.35 User Execution: Malicious Image (T1204.003) **[635]**

EV Code	Vulnerability Description
EV1204.003-S1	The potential for inadequate auditing practices, as the absence of regular audits of deployed images within the environment may fail to detect the presence of malicious components.
EV1204.003-S2	The absence of code signing or digital signatures in image verification processes may allow attackers to compromise the integrity and authenticity of images, undermining the effectiveness of runtime verification.
EV1204.003-S3	Insufficient network intrusion prevention measures, as systems designed to scan and remove malicious downloads may not be robust enough to effectively block all malicious activity associated with the deployment of backdoored images.
EV1204.003-H1	The likelihood of mistakenly deploying an instance or container from a malicious image due to deceptive naming conventions chosen by adversaries, such as using names that match legitimate images or locations, thereby increasing the chances of user error in deployment.
EV1204.003-H2	The likelihood of inadequate user training, as users who are not sufficiently trained may remain unaware of the existence of malicious images and lack the knowledge to avoid deploying instances and containers from them, potentially leading to unintentional execution of malicious code.

2.4.36 Windows Management Instrumentation (T1047) **[653]**

EV Code	Vulnerability Description
EV1047-S1	The potential lack of Attack Surface Reduction (ASR) rules on Windows 10, allowing processes created by WMI commands to run unchecked, unless ASR is specifically configured.
EV1047-S2	The absence of application control configurations blocking the execution of wmic.exe, leaving the system susceptible to misuse of WMI commands by adversaries.

EV1047-H1	The potential lack of privileged account management, leading to credential overlap across systems with administrator and privileged accounts, creating opportunities for adversaries.
EV1047-H2	The potential misconfiguration or oversight in securing Remote Services such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM), enabling adversaries to exploit WMI over DCOM using port 135 or WMI over WinRM using ports 5985 and 5986 for unauthorized remote access and execution.
EV1047-H3	The potential failure to restrict or disallow non-administrator users from remotely connecting to WMI, which could be exploited by adversaries for unauthorized access and malicious actions.

2.5 Persistence (TA0003) [8]

2.5.1 Account Manipulation (T1098) [48]

EV Code	Vulnerability Description
EV1098-S1	Insufficient access controls, allowing adversaries to modify credentials or permission groups.
EV1098-S2	Improper operating system configuration on domain controllers, exposing them to potential compromise through unnecessary protocols and services.
EV1098-S3	Inadequate network segmentation, potentially allowing unauthorized access to critical systems and domain controllers.
EV1098-H1	Poor password management practices, as iterative password updates may be performed to bypass password duration policies.
EV1098-H2	The absence of multi-factor authentication, which could leave user and privileged accounts susceptible to compromise.
EV1098-H3	Inappropriate use of domain administrator accounts for day-to-day operations, increasing the risk of exposure to potential adversaries on unprivileged systems.
EV1098-H4	Insufficient user account management, risking unauthorized modifications to accounts or account-related policies by low-privileged user accounts.

2.5.2 Account Manipulation: Additional Cloud Credentials (T1098.001) [49]

EV Code	Vulnerability Description
EV1098.001-S1	The insufficient control or monitoring of credential additions in cloud accounts, allowing unauthorized and adversary-controlled credentials to be added.
EV1098.001-S2	The lack of proper validation or restrictions on the addition of Service Principal and Application credentials in Azure AD, enabling adversaries to augment existing legitimate credentials.
EV1098.001-S3	The insufficient control over credential management tools such as the Azure Portal, Azure command line interface, and Azure or Az PowerShell modules, providing avenues for unauthorized credential additions
EV1098.001-S4	The lack of robust security measures in infrastructure-as-a-service (IaaS) environments, allowing adversaries to generate or import their own SSH keys, potentially leading to persistent unauthorized access
EV1098.001-H1	The inadequate management of permissions and roles, allowing adversaries in Azure AD environments to exploit the Application Administrator role and add unauthorized credentials to their application's service principal.
EV1098.001-H2	The inadequate management of permissions in AWS environments, enabling adversaries to use the sts:GetFederationToken API call and create temporary credentials tied to the permissions of the original user account, potentially leading to privilege escalation.
EV1098.001-H3	The failure to deactivate or manage API credentials properly in AWS environments, allowing temporary credentials created through sts:GetFederationToken to remain valid even after the deactivation of the original account's API credentials.
EV1098.001-H4	The absence of enforced multi-factor authentication for the CreateKeyPair and ImportKeyPair API calls, potentially allowing adversaries to bypass authentication measures and manipulate SSH keys.

EV1098.001-H5	The lack of proper network segmentation, which may result in broader access to critical systems and domain controllers, providing adversaries with an extended attack surface.
EV1098.001-H6	The inadequate privileged account management, as allowing domain administrator or root accounts to be used for day-to-day operations increases the risk of exposure to potential adversaries on unprivileged systems.
EV1098.001-H7	The lack of restrictions on users calling the sts:GetFederationToken API in AWS environments, unless explicitly required, potentially leading to unauthorized creation of temporary credentials and privilege escalation.

2.5.3 Account Manipulation: Additional Email Delegate Permissions (T1098.002) [50]

EV Code	Vulnerability Description
EV1098.002-S1	The potential misconfiguration or lack of proper access controls in email systems, such as on-premises Exchange, Office 365, or Google Workspace, allowing adversaries to use commands like Add-MailboxPermission or delegate permissions to maintain persistent access to an adversary-controlled email account.
EV1098.002-H1	The reliance on single-factor authentication, as not implementing multi-factor authentication for user and privileged accounts may expose the system to higher risks of unauthorized access in the event of compromised credentials.
EV1098.002-H2	The failure to disable or remove unnecessary features or programs, as not taking action to disable email delegation when not required may create an avenue for exploitation, allowing adversaries to misuse the feature for unauthorized access or other malicious activities.
EV1098.002-H3	The overuse of domain administrator accounts for day-to-day operations, which could expose privileged accounts to potential adversaries on unprivileged systems, increasing the likelihood of privilege escalation attacks.

2.5.4 Account Manipulation: Additional Cloud Roles (T1098.003) [51]

EV Code	Vulnerability Description
EV1098.003-S1	The lack of proper controls to prevent the use of APIs like CreatePolicyVersion and AttachUserPolicy in AWS environments, enabling the definition of new IAM policy versions or attachment of policies with additional permissions to compromised user accounts.
EV1098.003-H1	The absence of multi-factor authentication for user and privileged accounts, which could expose these accounts to compromise.
EV1098.003-H2	The failure to adequately secure IAM credentials, leading to a compromised account with sufficient permissions, potentially granting almost unlimited access to data and settings.
EV1098.003-H3	The failure to implement least privilege principles, potentially allowing accounts to have excessive permissions, and in Azure AD environments, not leveraging Privileged Identity Management (PIM) may lead to inadequate control over role assignments, risking unauthorized access.
EV1098.003-H4	The lack of restrictions on low-privileged user accounts, enabling them to have permissions to add or modify permissions on accounts or IAM policies.

2.5.5 Account Manipulation: SSH Authorized Keys (T1098.004) [52]

EV Code	Vulnerability Description
EV1098.004-S1	The misconfiguration of SSH configuration files, specifically the mismanagement of PubkeyAuthentication and RSAAuthentication directives, allowing adversaries to enable unauthorized public key and RSA authentication.
EV1098.004-H1	The inadequate restriction of file and directory permissions for the authorized_keys file, allowing unauthorized modifications and additions by adversaries.
EV1098.004-H2	The inadequate protection of network devices, specifically the failure to secure the ip ssh pubkey-chain command on network devices, enabling adversaries to add unauthorized SSH keys.

EV1098.004-H3	The failure to disable or restrict SSH access when it is unnecessary on a host, creating an avenue for unauthorized manipulation of SSH authorized_keys files.
EV1098.004-H4	The lack of proper user account management in cloud environments, specifically the failure to restrict permissions for updating instance metadata or configurations, leading to potential unauthorized modifications of SSH authorized_keys files.

2.5.6 Account Manipulation: Device Registration (T1098.005) [53]

EV Code	Vulnerability Description
EV1098.005-S1	Insecure MFA self-enrollment process that, in some cases, requires only a username and password, enabling the adversary to enroll the account's first device or register a device to an inactive account without robust authentication.
EV1098.005-S2	The risk associated with device registration in Azure AD and Microsoft Intune, as an adversary with existing network access can register a device to bypass conditional access policies and gain unauthorized access to sensitive data or resources.
EV1098.005-H1	Failure to require MFA for device registration in Azure AD or allowing device enrollment for inactive accounts may leave the system susceptible to unauthorized access.
EV1098.005-H2	The inadequate implementation of MFA policies, such as not configuring MFA systems to disallow enrolling new devices for inactive accounts or failing to use conditional access policies to restrict device enrollment to trusted locations or devices, which could result in a compromised device registration process.
EV1098.005-H3	The reliance on temporary access passes as an initial MFA solution for device enrollment, as their misuse or improper implementation may introduce a vulnerability that adversaries can exploit to register unauthorized devices.
EV1098.005-H4	The failure to enforce conditional access policies during the first enrollment of MFA, potentially allowing device registration from untrusted locations or devices and undermining the security measures intended to restrict access.

2.5.7 Account Manipulation: Additional Container Cluster Roles (T1098.006) [54]

EV Code	Vulnerability Description
EV1098.006-S1	Insufficient access controls, allowing the addition of roles or permissions to user accounts and unauthorized modifications in container orchestration systems
EV1098.006-H1	The failure to properly configure and monitor attribute-based access control (ABAC) policies in Kubernetes, enabling adversaries with sufficient permissions to manipulate access controls and grant additional privileges to targeted accounts.
EV1098.006-H2	The absence of multi-factor authentication for user accounts integrated into container clusters, allowing adversaries to potentially exploit accounts with single-factor authentication.
EV1098.006-H3	The failure to restrict low-privileged accounts from having the capability to add permissions to accounts or update container cluster roles, creating a potential avenue for unauthorized modifications and privilege escalation.

2.5.8 BITS Jobs (T1197) [87]

EV Code	Vulnerability Description
EV1197-S1	The potential oversight in network and/or host firewall rule configurations, allowing unauthorized BITS traffic if not adequately filtered, thus compromising the BITS mechanism.
EV1197-H1	The potential failure to optimize the default BITS job lifetime, as users may overlook reducing it through Group Policy or adjusting the JobInactivityTimeout and MaxDownloadTime Registry values, potentially exposing the system to prolonged malicious BITS activities.
EV1197-H2	The potential oversight in user account management, as not limiting access to the BITS interface to specific users or groups may provide adversaries with unauthorized control over BITS jobs, leading to malicious activities.

2.5.9 Boot or Logon Autostart Execution (T1547) **[88]**

EV Code	Vulnerability Description
EV1547-S1	The potential for misconfiguration or lack of proper access controls in the operating system, allowing adversaries to configure settings for automatic program execution during system boot or logon.

2.5.10 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) **[89]**

EV Code	Vulnerability Description
EV1547.001-S1	The presence of default run keys in Windows systems, such as HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, allows adversaries to achieve persistence by adding malicious programs, exploiting the system's reliance on these keys during startup.

2.5.11 Boot or Logon Autostart Execution: Authentication Package (T1547.002) **[90]**

EV Code	Vulnerability Description
EV1547.002-H1	The potential failure to enable the Protected Process Light (PPL) mode on Windows 8.1, Windows Server 2012 R2, and later versions, by neglecting to set the Registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL, which would allow unauthorized DLLs to be loaded by LSA.

2.5.12 Boot or Logon Autostart Execution: Time Providers (T1547.003) **[91]**

EV Code	Vulnerability Description
EV1547.003-H1	The potential mistake of not configuring Group Policy settings to block additions/modifications to W32Time DLLs, leaving the system exposed to unauthorized changes and manipulation by adversaries.

EV1547.003-H2	the potential mistake of not configuring Group Policy settings to block modifications to W32Time parameters in the Registry, allowing adversaries to tamper with critical time provider settings and compromise system security.

2.5.13 *Boot or Logon Autostart Execution: Winlogon Helper DLL (T1547.004)* [92]

EV Code	Vulnerability Description
EV1547.004-S1	The potential failure to implement effective execution prevention measures, allowing potentially malicious software to be executed through the Winlogon helper process, if application control tools like AppLocker are not properly configured or utilized.
EV1547.004-H1	The inadequate management of user accounts, specifically the failure to limit privileges, which may result in unauthorized users being able to perform Winlogon helper changes and potentially introduce malicious DLLs or executables during user logon.

2.5.14 *Boot or Logon Autostart Execution: Security Support Provider (T1547.005)* [93]

EV Code	Vulnerability Description
EV1547.005-S1	If the system is not configured to run the Local Security Authority (LSA) as a Protected Process Light (PPL) on Windows 8.1, Windows Server 2012 R2, and later versions, adversaries may still exploit the LSA process, potentially compromising the integrity of privileged processes.

2.5.15 *Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006)* [94]

EV Code	Vulnerability Description
EV1547.006-S1	The inherent security gap in macOS kernel extensions (kexts) arising from their exemption from macOS security policies, enabling adversaries to exploit them for persistence and privilege escalation, even with the introduction of System Extensions in macOS Catalina.

EV1547.006-S2	The potential weakness in antivirus/antimalware tools, as certain Linux rootkits may be designed to evade detection by common tools like rkhunter and chrootkit.
EV1547.006-S3	The susceptibility to kernel module loading due to inadequate execution prevention measures, where reliance solely on application control and software restriction tools may not provide comprehensive protection against all potential attacks.
EV1547.006-H1	The failure to adequately control and regulate the loading and unloading of kernel extensions (kexts) on macOS, as users without necessary privileges can sign kexts that may compromise system security, particularly when System Integrity Protection (SIP) is disabled.
EV1547.006-H2	The failure to upgrade to the latest macOS versions that deprecate kernel extensions (kexts) in favor of more secure System Extensions, leaving systems exposed to potential exploitation of legacy vulnerabilities.
EV1547.006-H3	The failure to implement proper privileged account management, allowing users to access the root account and load kernel modules, thereby increasing the risk of privilege escalation and unauthorized system modifications.
EV1547.006-H4	The inadequate management of user accounts, as the user's ability to install or approve kernel extensions is not effectively controlled through Mobile Device Management (MDM), potentially leading to the approval of malicious extensions and compromising system security.

2.5.16 Boot or Logon Autostart Execution: Re-opened Applications (T1547.007) **[95]**

EV Code	Vulnerability Description
EV1547.007-H1	The default configuration allowing the persistence feature, as it can be disabled through a terminal command, but may be overlooked, leaving the system susceptible to unauthorized autostart execution.

EV1547.007-H2	The failure to apply user training, specifically neglecting to hold the Shift key while logging in, which could result in unintentional execution of applications configured for autostart, even after the feature has been disabled, due to user oversight.

2.5.17 Boot or Logon Autostart Execution: LSASS Driver (T1547.008) [96]

EV Code	Vulnerability Description
EV1547.008-S1	The Windows security subsystem's weakness that allows adversaries to modify or add LSASS drivers, enabling them to achieve persistence on compromised systems.
EV1547.008-S2	Inadequate protection against credential access, as Windows 10 and Server 2016 may be susceptible if Windows Defender Credential Guard is not enabled, allowing lsass.exe to operate in a potentially compromised environment.
EV1547.008-S3	Lack of privileged process integrity on Windows 8.1 and Server 2012 R2, where not enabling LSA Protection by setting the Registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL to dword:00000001 could expose lsass.exe to potential compromise by loading unsigned and non-compliant LSA plug-ins and drivers.
EV1547.008-S4	Weakness in library loading security, specifically when safe DLL search mode is not enabled (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode), posing a risk of lsass.exe loading malicious code libraries.

2.5.18 Boot or Logon Autostart Execution: Shortcut Modification (T1547.009) [97]

EV Code	Vulnerability Description
EV1547.009-H1	The failure to properly configure group policies related to symbolic link creation, such as overlooking restrictions in GPO settings, leading to an increased risk of adversaries being able to exploit the autostart mechanism through shortcut modification.

2.5.19 Boot or Logon Autostart Execution: Port Monitors (T1547.010) [98]

EV Code	Vulnerability Description
EV1547.009-H2	The permission allowance for writing a fully-qualified pathname for an arbitrary DLL to HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors, enabling the loading of malicious code at startup.

2.5.20 Boot or Logon Autostart Execution: Print Processors (T1547.012) [99]

EV Code	Vulnerability Description
EV1547.012-S1	The print spooler service allows the installation of print processors with malicious DLLs during system boot, providing a potential avenue for persistence and privilege escalation.
EV1547.012-H1	Failing to limit user accounts that can load or unload device drivers by not disabling the SeLoadDriverPrivilege, providing an avenue for adversaries to abuse the print spooler service.

2.5.21 Boot or Logon Autostart Execution: XDG Autostart Entries (T1547.013) [100]

EV Code	Vulnerability Description
EV1547.013-S1	The lack of limitations on software installation, as unrestricted software installation may lead to the introduction of malicious packages, increasing the risk of compromise through the manipulation of XDG Autostart Entries.
EV1547.013-H1	The insufficient restriction of file and directory permissions, as inadequate controls on write access to XDG autostart entries may allow unauthorized users to manipulate these configurations, potentially enabling the execution of malicious programs during login.

EV1547.013-H2	The inadequate management of user accounts, as the failure to limit privileges on user accounts may result in unauthorized users creating or modifying XDG Autostart Entries, facilitating the establishment of persistence through the execution of malicious commands during user login.

2.5.22 Boot or Logon Autostart Execution: Active Setup (T1547.014) **[101]**

This attack technique does not rely on a specific vulnerability for execution.

2.5.23 Boot or Logon Autostart Execution: Login Items (T1547.015) **[102]**

EV Code	Vulnerability Description
EV1547.015-S1	Weaknesses in the Service Management Framework and shared file list methods, allowing for persistent and privileged execution.

2.5.24 Boot or Logon Initialization Scripts (T1037) **[103]**

EV Code	Vulnerability Description
EV1037-H1	The improper assignment of file and directory permissions, allowing unauthorized administrators or users to write to logon scripts, potentially leading to persistence.
EV1037-H2	The misconfiguration of registry permissions, which may enable users to modify registry keys associated with logon scripts, posing a risk of

2.5.25 Boot or Logon Initialization Scripts: Logon Script (Windows) (T1037.001) **[104]**

EV Code	Vulnerability Description
EV1037.001-S1	The potential weakness in the Windows registry configuration, specifically the HKCU\Environment\UserInitMprLogonScript Registry key, which allows the execution of logon scripts during initialization, providing an avenue for persistence.

EV1037.001-H1	The misconfiguration of registry permissions, which may enable users to modify registry keys associated with logon scripts, posing a risk of

2.5.26 Boot or Logon Initialization Scripts: Login Hook (T1037.002) [105]

EV Code	Vulnerability Description
EV1037.002-H1	The failure to restrict file and directory permissions appropriately, which can lead to unauthorized modifications of logon scripts by administrators, enabling the execution of malicious scripts upon user logon.

2.5.27 Boot or Logon Initialization Scripts: Network Logon Script (T1037.003) [106]

EV Code	Vulnerability Description
EV1037.003-H1	The failure to restrict file and directory permissions appropriately, which can lead to unauthorized modifications of logon scripts by administrators, enabling the execution of malicious scripts upon user logon.

2.5.28 Boot or Logon Initialization Scripts: RC Scripts (T1037.004) [107]

EV Code	Vulnerability Description
EV1037.004-S1	The reliance on deprecated RC scripts during startup, especially in lightweight Unix-like distributions with default root user access, such as IoT or embedded systems, and the failure to update or transition from deprecated RC scripts to modern alternatives like Systemd, leaving the system exposed to persistence methods using malicious binary paths or shell commands in RC scripts.
EV1037.004-H1	The failure to properly limit privileges of user accounts, enabling unauthorized individuals to edit critical files like rc.common and potentially facilitate persistence through the manipulation of startup scripts.

2.5.29 Boot or Logon Initialization Scripts: Startup Items (T1037.005) [108]

EV Code	Vulnerability Description
EV1037.005-S1	The potential existence of the deprecated /Library/StartupItems folder on macOS systems, which may still be present by default on macOS Sierra, providing an avenue for adversaries to establish persistence during the boot process.
EV1037.005-H1	Inadequate restriction of write permissions on the /Library/StartupItems directory, which could lead to the registration of unauthorized startup items, circumventing the mitigation strategy and allowing persistence.

2.5.30 Browser Extensions (T1176) [109]

EV Code	Vulnerability Description
EV1176-S1	Potential lack of security measures on browser app stores, allowing malicious extensions to masquerade as legitimate ones and potentially evade automated scanners.
EV1176-S2	In macOS versions prior to 11, the ability for adversaries to silently install browser extensions via the command line using the profiles tool.
EV1176-S3	Lack of robust auditing processes, allowing malicious extensions to go unnoticed by failing to verify if installed extensions are indeed the intended ones.
EV1176-S4	Insufficient controls on software installation, allowing users to install browser extensions without proper verification, creating an avenue for the installation of malicious extensions.
EV1176-H1	User susceptibility to social engineering, leading to the installation of malicious extensions through deceptive methods.
EV1176-H2	Failure to verify the authenticity of browser extensions during installation, potentially leading to the inadvertent installation of malicious extensions.
EV1176-H3	Delayed or inadequate software updates, potentially leaving operating systems and browsers vulnerable to known exploits.

EV1176-H4	Neglecting to close browser sessions after use, potentially allowing malicious extensions to persistently run in the background.
EV1176-H5	Insufficient user training on recognizing and avoiding potentially malicious extensions, leading to the inadvertent installation and execution of harmful browser extensions.

2.5.31 Compromise Client Software Binary (T1554) [139]

EV Code	Vulnerability Description
EV1554-H1	The failure to enforce code signing practices, leading to unsigned or incorrectly signed application component binaries and increasing the risk of unauthorized modifications by adversaries.

2.5.32 Create Account (T1136) [151]

EV Code	Vulnerability Description
EV1136-S1	Insufficient network segmentation, allowing unauthorized access to domain controllers and systems responsible for creating and managing accounts.
EV1136-S2	Improper security configuration of critical servers, specifically domain controllers, exposing them to potential exploitation.
EV1136-H1	The absence or inadequate implementation of multi-factor authentication, leaving user and privileged accounts susceptible to compromise through single-factor authentication methods.
EV1136-H2	The failure to limit the number of accounts with permissions to create other accounts, increasing the risk of unauthorized account creation and potential misuse.
EV1136-H3	The usage of domain administrator accounts for day-to-day operations on unprivileged systems, exposing these high-privileged accounts to potential compromise.

2.5.33 Create Account: Local Account (T1136.001) **[152]**

EV Code	Vulnerability Description
EV1136.001-H1	The absence or inadequate implementation of multi-factor authentication, leaving user and privileged accounts susceptible to compromise through single-factor authentication methods.
EV1136.001-H2	The failure to limit the number of accounts with permissions to create other accounts, increasing the risk of unauthorized account creation and potential misuse.
EV1136.001-H3	The usage of domain administrator accounts for day-to-day operations on unprivileged systems, exposing these high-privileged accounts to potential compromise.

2.5.34 Create Account: Domain Account (T1136.002) **[153]**

EV Code	Vulnerability Description
EV1136.002-S1	Insufficient network segmentation, allowing unauthorized access to domain controllers and systems responsible for creating and managing accounts.
EV1136.002-S2	Improper security configuration of critical servers, specifically domain controllers, exposing them to potential exploitation.
EV1136.002-H1	The absence or inadequate implementation of multi-factor authentication, leaving user and privileged accounts susceptible to compromise through single-factor authentication methods.
EV1136.002-H2	The failure to limit the number of accounts with permissions to create other accounts, increasing the risk of unauthorized account creation and potential misuse.
EV1136.002-H3	The usage of domain administrator accounts for day-to-day operations on unprivileged systems, exposing these high-privileged accounts to potential compromise.

2.5.35 Create Account: Cloud Account (T1136.003) **[154]**

EV Code	Vulnerability Description
EV1136.003-S1	Insufficient network segmentation, allowing unauthorized access to domain controllers and systems responsible for creating and managing accounts.
EV1136.003-H1	The absence or inadequate implementation of multi-factor authentication, leaving user and privileged accounts susceptible to compromise through single-factor authentication methods.
EV1136.003-H2	The failure to limit the number of accounts with permissions to create other accounts, increasing the risk of unauthorized account creation and potential misuse.
EV1136.003-H3	The usage of domain administrator accounts for day-to-day operations on unprivileged systems, exposing these high-privileged accounts to potential compromise.

2.5.36 Create or Modify System Process (T1543) **[155]**

EV Code	Vulnerability Description
EV1543-S1	Insufficient enforcement of software installation restrictions, posing a risk of allowing unauthorized or potentially malicious software installations from untrusted repositories.
EV1543-S2	The potential absence of properly configured Attack Surface Reduction (ASR) rules on Windows 10, which could permit applications to write signed vulnerable drivers to the system.
EV1543-S3	The lack of enabled Microsoft Vulnerable Driver Blocklist on Windows 10 and 11, leaving the system less resilient against third-party-developed drivers that may introduce vulnerabilities.
EV1543-H1	Inadequate auditing practices, potentially allowing privilege and service abuse opportunities to go undetected and uncorrected.
EV1543-H2	The failure to enforce the registration and execution of only legitimately signed service drivers, potentially leading to the acceptance of unsigned or malicious drivers.

EV1543-H3	The failure to ensure the enforcement of Driver Signature Enforcement, which could result in the installation of unsigned drivers, posing a potential security risk.
EV1543-H4	Inadequate restriction of read/write access to system-level process files, potentially allowing unauthorized users to manipulate critical system services.
EV1543-H5	Insufficient limitation of privileges for user accounts and groups, creating the risk that unauthorized individuals may interact with system-level process changes and service configurations.

2.5.37 Create or Modify System Process: Launch Agent (T1543.001) [156]

EV Code	Vulnerability Description
EV1543.001-H1	The failure to implement group policies to restrict file permissions in the ~/launchagents folder, leaving the system exposed to potential misuse by adversaries.

2.5.38 Create or Modify System Process: Systemd Service (T1543.002) [157]

EV Code	Vulnerability Description
EV1543.002-S1	The weaknesses in default initialization (init) system, systemd, which allows adversaries to create or modify services, leading to the repeated execution of malicious payloads and potential privilege escalation.
EV1543.002-H1	Inadequate software source control, as unrestricted software installation can lead to the introduction of malicious or unauthorized software packages, posing a security risk.
EV1543.002-H2	Insufficient control over privileged accounts, since the creation and modification of systemd service unit files, critical for system functionality, are not adequately restricted to authorized administrators, potentially allowing unauthorized manipulation.
EV1543.002-H3	Overly permissive file and directory permissions, as unrestricted read/write access to systemd unit files may enable unauthorized users to tamper with or disrupt critical system services.

EV1543.002-H4	Inappropriate user access management, as granting unnecessary access to system utilities like systemctl increases the attack surface and potential for misuse by users without a legitimate need.

2.5.39 Create or Modify System Process: Windows Service (T1543.003) [158]

EV Code	Vulnerability Description
EV1543.003-S1	Inadequate auditing configurations, potentially allowing privilege and service abuse opportunities to go undetected.
EV1543.003-S2	The lack of Attack Surface Reduction (ASR) rules enforcement on Windows 10, which may enable an application to write a signed vulnerable driver to the system.
EV1543.003-S3	The absence of Microsoft Vulnerable Driver Blocklist activation on Windows 10 and 11, leaving the system more susceptible to third-party-developed service drivers that could pose security risks.
EV1543.003-S4	The absence of enabled Driver Signature Enforcement, which could lead to the installation of unsigned drivers, compromising the system's integrity.
EV1543.003-H1	The failure to enforce the registration and execution of only legitimately signed service drivers, allowing for potential unauthorized or malicious drivers to be executed.
EV1543.003-H2	The failure to properly limit privileges, potentially leading to unauthorized users gaining access to service changes and configurations.

2.5.40 Create or Modify System Process: Launch Daemon (T1543.004) [159]

EV Code	Vulnerability Description
EV1543.004-S1	The poor configurations allowing globally writable folders (e.g., usr/local/bin), enabling the modification of executables referenced by current Launch Daemon's plist files.

EV1543.004-S2	The inadequate auditing practices, as the absence of effective auditing tools capable of detecting folder permissions abuse opportunities may allow malicious modifications to Launch Daemon executables to go unnoticed.
EV1543.004-H1	The failure to sufficiently limit privileges and remediate Privilege Escalation vectors, which could result in unauthorized users creating new Launch Daemons and compromising system integrity despite the recommended mitigation measures.

2.5.41 Event Triggered Execution (T1546) [237]

EV Code	Vulnerability Description
EV1546-S1	The vulnerability in the operating system event monitoring, enabling adversaries to exploit subscribed events for unauthorized execution, leading to persistent access and privilege escalation.
EV1546-S2	The vulnerability in the cloud environment functions and services related to event monitoring, allowing adversaries to leverage specific cloud events for unauthorized execution, resulting in persistent access and privilege escalation.

2.5.42 Event Triggered Execution: Change Default File Association (T1546.001) [238]

EV Code	Vulnerability Description
EV1546.001-S1	The ability for users, administrators, or programs with Registry access to edit file associations, providing an opportunity for malicious changes and persistent execution of arbitrary programs by adversaries.

2.5.43 Event Triggered Execution: Screensaver (T1546.002) [239]

EV Code	Vulnerability Description
EV1546.002-S1	The insecure storage of screensaver settings in the Registry (HKCU\Control Panel\Desktop), allowing manipulation of SCRNSAVE.exe to a malicious PE path, enabling the execution of malware upon user inactivity.
EV1546.002-H1	User configure setting ScreenSaverIsSecure to '0', neglecting to require a password to unlock the screensaver, potentially compromising security when the screensaver is triggered by user inactivity.
EV1546.002-H2	The potential failure to disable screensavers through Group Policy, leaving unnecessary screensavers active and susceptible to manipulation for malicious purposes.
EV1546.002-H3	The failure to block .scr files from non-standard locations, allowing adversaries to potentially execute malicious screensavers if they are stored in unconventional directories.

2.5.44 Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003) [240]

EV Code	Vulnerability Description
EV1546.003-S1	Inadequate configuration of Windows 10, allowing the potential abuse of WMI for persistence, as Attack Surface Reduction (ASR) rules are not enabled.
EV1546.003-S2	Weak remote access controls on WMI, as by default, non-administrator users are allowed to connect remotely; proper restrictions are not in place.
EV1546.003-H1	Allowing credential overlap across systems for administrator and privileged accounts, potentially exposing sensitive credentials to compromise.
EV1546.003-H2	Failure to properly configure or enforce remote access policies for WMI, leading to an increased risk of unauthorized access and potential misuse by adversaries.

2.5.45 Event Triggered Execution: Unix Shell Configuration Modification (T1546.004) **[241]**

EV Code	Vulnerability Description
EV1546.004-H1	The failure to restrict file and directory permissions adequately, which could allow adversaries to modify crucial configuration files and establish user-level persistence on the system.

2.5.46 Event Triggered Execution: Trap (T1546.005) **[242]**

This attack technique does not rely on a specific vulnerability for execution.

2.5.47 Event Triggered Execution: LC_LOAD_DYLIB Addition (T1546.006) **[243]**

EV Code	Vulnerability Description
EV1546.006-S1	The failure to adequately protect digital signatures on binaries, as removing the LC_CODE_SIGNATURE command to evade signature checks exposes the system to potential malicious alterations.
EV1546.006-S2	The potential lack of effective execution prevention, as allowing applications via known hashes may not prevent the execution of tampered binaries with modified Mach-O headers.
EV1546.006-S3	The potential lack of proper auditing practices, as failure to baseline binaries for required dynamic libraries may result in overlooking the addition of malicious libraries during updates.
EV1546.006-H1	Failure to enforce the correct Apple Developer IDs for all binaries may lead to the acceptance of unsigned or incorrectly signed binaries, compromising the system's integrity.

2.5.48 Event Triggered Execution: Netsh Helper DLL (T1546.007) [244]

EV Code	Vulnerability Description
EV1546.007-S1	The potential for arbitrary code execution through the Netsh Helper DLLs, exploiting weaknesses in the design of the netsh.exe utility and its extensibility mechanism.

2.5.49 Event Triggered Execution: Accessibility Features (T1546.008) [245]

EV Code	Vulnerability Description
EV1546.008-S1	The failure to adequately secure the accessibility feature binaries, such as C:\Windows\System32\sethc.exe and C:\Windows\System32\utilman.exe, which can be exploited by an adversary to gain unauthenticated access through actions like pressing the shift key five times or using the Windows + U key combination.
EV1546.008-S2	The susceptibility of Windows XP and later versions, as well as Windows Server 2003/R2 and later, to binary replacement attacks where a legitimate program (e.g., C:\Windows\System32\utilman.exe) may be replaced with a malicious one (e.g., "cmd.exe") for backdoor access.
EV1546.008-S3	The lack of protection measures, such as digital signatures and Windows File or Resource Protection, on replaced binaries, which are required for newer versions of Windows to prevent unauthorized execution.
EV1546.008-H1	The potential failure to implement effective application control tools (e.g., Windows Defender Application Control, AppLocker, or Software Restriction Policies), allowing the replacement of accessibility feature binaries with malicious alternatives for unauthorized execution.
EV1546.008-H2	The failure to configure and utilize a Remote Desktop Gateway, leaving RDP connections and security configurations vulnerable to exploitation through accessibility feature binaries.

EV1546.008-H3	The failure to enable Network Level Authentication (NLA) on remote desktop sessions, potentially allowing adversaries to exploit accessibility features through RDP without proper authentication.

2.5.50 Event Triggered Execution: AppCert DLLs (T1546.009) [246]

EV Code	Vulnerability Description
EV1546.009-H1	The failure to properly configure and maintain application control tools (e.g., Windows Defender Application Control, AppLocker, or Software Restriction Policies), allowing adversaries to evade detection and successfully execute malicious AppCertDLL binaries.

2.5.51 Event Triggered Execution: AppInit DLLs (T1546.010) [247]

EV Code	Vulnerability Description
EV1546.010-S1	The persistence mechanism provided by AppInit DLLs, which, when triggered by API activity, can continuously execute malicious code, exploiting a weakness in the Windows operating system's design.
EV1546.010-H1	The potential for ineffective execution prevention, as adversaries can still install new AppInit DLL binaries, bypassing application control tools like Windows Defender Application Control, AppLocker, or Software Restriction Policies if not appropriately configured or monitored.
EV1546.010-H2	The failure to update software, leaving systems vulnerable to this technique; upgrading to Windows 8 or later and enabling secure boot is crucial for mitigating the risk associated with AppInit DLLs, and neglecting this update could expose the system to exploitation.

2.5.52 Event Triggered Execution: Application Shimming (T1546.011) **[248]**

EV Code	Vulnerability Description
EV1546.011-S1	The Windows Application Compatibility Infrastructure/Framework (Application Shim) allowing certain shims (e.g., Bypass User Account Control, RedirectEXE, InjectDLL, DisableNX, DisableSEH, GetProcAddress) to be used for malicious purposes.
EV1546.011-S2	The presence of the "auto-elevate" flag within the sdbinst.exe, which, if not addressed by applying the optional patch update (KB3045645), allows for potential misuse of application shimming to bypass User Account Control (UAC).
EV1546.011-H1	User opts not to change UAC settings to "Always Notify" due to the inconvenience of frequent notifications, leaving systems more susceptible to unauthorized elevation of privileges through application shimming.

2.5.53 Event Triggered Execution: Image File Execution Options Injection (T1546.012) **[249]**

EV Code	Vulnerability Description
EV1546.012-S1	The misconfiguration of IFEO via Registry settings, including both direct modifications and the use of Global Flags, which can lead to unintended privilege escalation and persistent execution of malicious code.
EV1546.012-S2	The configuration of "cmd.exe" or another backdoor program as a "debugger" for an accessibility program through Registry key modification, leading to unauthorized execution with SYSTEM privileges by triggering the specified program at the login screen.

2.5.54 Event Triggered Execution: PowerShell Profile (T1546.013) **[250]**

EV Code	Vulnerability Description
EV1546.013-S1	The lack of enforcement in code signing for PowerShell scripts, allowing the execution of unsigned scripts and potential compromise.

EV1546.013-H1	The lack of proper configuration to restrict file and directory permissions on PowerShell profiles, allowing unauthorized modifications and persistence by adversaries.
EV1546.013-H2	The inappropriate use of PowerShell profiles when not needed and the failure to consistently use the -NoProfile flag when executing scripts remotely, exposing the system to unnecessary risks of customization and potential exploitation.

2.5.55 Event Triggered Execution: Emond (T1546.014) [251]

EV Code	Vulnerability Description
EV1546.014-H1	The potential failure to disable or remove the emond feature, as adversaries could exploit its presence and associated Launch Daemon plist file to execute malicious content, gain persistence, and potentially escalate privileges.

2.5.56 Event Triggered Execution: Component Object Model Hijacking (T1546.015) [252]

EV Code	Vulnerability Description
EV1546.015-H1	Inadequate monitoring and control over changes to the Registry, enabling adversaries to modify references to legitimate system components without detection, leading to the execution of malicious code during normal system operation.

2.5.57 Event Triggered Execution: Installer Packages (T1546.016) [253]

EV Code	Vulnerability Description
EV1546.016-H1	The granting of administrative permissions to installer packages during the installation of applications, facilitating the execution of malicious content by adversaries.

2.5.58 External Remote Services (T1133) **[276]**

EV Code	Vulnerability Description
EV1133-S1	The existence of exposed services, such as Docker API, Kubernetes API server, kubelet, or web applications like the Kubernetes dashboard, in containerized environments without proper authentication, facilitating unauthorized access.
EV1133-S2	The potential failure to disable or block unnecessary remotely available services, leaving avenues for exploitation.
EV1133-S3	The potential lack of network segmentation, allowing direct remote access to internal systems and increasing the risk of compromise.
EV1133-H1	The potential failure to implement strong two-factor or multi-factor authentication for remote service accounts, allowing adversaries to exploit stolen credentials.
EV1133-H2	The potential oversight in limiting access to remote services through centrally managed concentrators, such as VPNs and other managed remote access systems.

2.5.59 Hijack Execution Flow (T1574) **[323]**

EV Code	Vulnerability Description
EV1574-S1	Inadequate control and protection of locations where the operating system looks for programs/resources, such as file directories and the Windows Registry, which could be manipulated by adversaries to include malicious payloads.
EV1574-S2	The absence of hash values in manifest files, allowing for potential side-loading of malicious libraries, which could compromise the integrity of program execution.
EV1574-S3	Inadequate auditing configurations, allowing the adversary to exploit hijacking opportunities on systems within the enterprise.
EV1574-S4	Manifest files with side-loading vulnerabilities, as they may be exploited by adversaries to compromise the integrity of software.

EV1574-S5	Path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and shortcuts, which could be exploited to execute or load malicious binaries.
EV1574-S6	Lingering Windows Registry keys from uninstalled software, providing opportunities for adversaries to exploit keys with no associated legitimate binaries.
EV1574-S7	Inadequate configuration of endpoint security solutions, which may allow adversaries to bypass behavior prevention measures and successfully execute process injection or memory tampering.
EV1574-S8	Insufficient application control solutions, leading to the potential execution of malicious software through payload hijacking and exploitation of libraries loaded by legitimate software.
EV1574-S9	Insecure file and directory permissions, as the absence of write protection in software installation locations and inadequate access controls on directories could enable unauthorized file writes in critical application and library folders.
EV1574-S10	Inadequate restriction of library loading, which could lead to the loading of malicious or unauthorized DLLs, compromising system integrity.
EV1574-S11	Improper registry permissions, which may allow unauthorized modification of keys, leading to potential privilege escalation.
EV1574-H1	Failure to use quotation marks around PATH variables in configurations, scripts, or shortcuts, potentially exposing the system to path interception attacks.
EV1574-H2	User Neglects to use fully qualified paths wherever appropriate, leaving the system susceptible to the search order Windows uses for executing or loading binaries.
EV1574-H3	User overlooks the need to periodically search for and address path interception weaknesses introduced by custom or available tools, potentially leaving the system exposed to insecure path configurations.

EV1574-H4	The failure to enable Safe DLL Search Mode, exposing the system to the risk of loading DLLs from less secure directories before searching in system directories, potentially allowing for the execution of malicious code.
EV1574-H5	Inadequate software updates, exposing the system to known DLL side-loading vulnerabilities and increasing the risk of exploitation by attackers.
EV1574-H6	Failure to turn off UAC's privilege elevation for standard users ("ConsentPromptBehaviorUser"=dword:00000000) may expose the system to unauthorized privilege elevation, allowing attackers to execute malicious actions without user consent.
EV1574-H7	Failure to enable installer detection ("EnableInstallerDetection"=dword:00000001) for all users can result in a lack of password prompts during installation, potentially facilitating unauthorized installations and compromising the system's security.
EV1574-H8	Insufficient privilege management, as unauthorized users may gain access to service changes and binary target path locations if privileges are not adequately limited.
EV1574-H9	Inadequate enforcement of proper permissions and directory access controls, potentially allowing users to write files to critical directories, such as C:\ and C:\Windows, leading to an increased risk of malicious file execution.

2.5.60 Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) **[324]**

EV Code	Vulnerability Description
EV1574.001-S1	Weakness in DLL search order, allowing adversaries to hijack the loading of DLLs and execute malicious payloads, potentially leading to unauthorized persistence, privilege escalation, and evasion of file execution restrictions.
EV1574.001-S2	The absence of proactive auditing practices, as enterprises may overlook DLL search order hijacking opportunities without utilizing tools like the PowerSploit framework or sxstrace.exe to detect and correct these weaknesses.

EV1574.001-S3	Failure to disallow loading of remote DLLs, especially on systems running versions prior to Windows Server 2012 or those that have not been patched, which may expose the system to DLL search order hijacking vulnerabilities.
EV1574.001-H1	The failure to implement and enforce application control solutions capable of blocking DLLs loaded by legitimate software, allowing potentially malicious DLLs to be executed through search order hijacking.
EV1574.001-H2	Misconfiguring the Safe DLL Search Mode settings, as incorrect Group Policy configurations or alterations to the Windows Registry key (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode) could compromise the intended security measures.

2.5.61 Hijack Execution Flow: DLL Side-Loading (T1574.002) **[325]**

EV Code	Vulnerability Description
EV1574.002-S1	DLL search order used by the loader, which can be exploited through side-loading by positioning both the victim application and malicious payload alongside each other.
EV1574.002-S2	The absence of hash values in manifest files, potentially allowing for the side-loading of malicious libraries due to a lack of integrity verification.
EV1574.002-H1	The failure to regularly update software, leading to the persistence of DLL side-loading vulnerabilities and an increased risk of exploitation.

2.5.62 Hijack Execution Flow: Dylib Hijacking (T1574.004) **[326]**

EV Code	Vulnerability Description
EV1574.004-S1	The sequential order of search paths for dynamic libraries in macOS, which allows adversaries to exploit the system's search mechanism and execute malicious code by placing a dylib with an expected name in a victim application's runtime path.

EV1574.004-S2	The use of weak linking, such as the LC_LOAD_WEAK_DYLIB function, which enables adversaries to execute an application even if the expected dylib is not present, potentially leading to unintended execution of malicious code.
EV1574.004-H1	Inadequate file and directory permissions, allowing potential unauthorized write access, which can lead to unauthorized modifications or deletions of critical files, compromising system integrity.

2.5.63 Hijack Execution Flow: Executable Installer File Permissions Weakness (T1574.005) [327]

EV Code	Vulnerability Description
EV1574.005-S1	Improper file system and binary permissions on the executable installer, allowing the adversary to overwrite legitimate binaries with malicious ones, potentially leading to code execution at a higher permissions level, including SYSTEM.
EV1574.005-S2	The lack of effective implementation of auditing tools, as the absence of tools capable of detecting file system permissions abuse opportunities may result in inadequate identification and correction of vulnerabilities in systems within an enterprise.
EV1574.005-H1	Inadequate permission settings on subdirectories and files created during the installation process, specifically within the %TEMP% directory, enabling the execution of untrusted code and the potential overwriting of binaries, leading to privilege escalation and code execution at elevated permissions.
EV1574.005-H2	Improper configuration of User Account Control (UAC), as failure to disable UAC's privilege elevation for standard users and appropriately configure installer detection may lead to unauthorized privilege escalation and undocumented installation attempts, potentially compromising system security.

EV1574.005-H3	Insufficient user account management practices, as the failure to appropriately limit privileges of user accounts and groups, especially in relation to service changes and service binary target path locations, may expose systems to unauthorized interactions and executions, potentially leading to privilege escalation and unauthorized code execution.

2.5.64 Hijack Execution Flow: Dynamic Linker Hijacking (T1574.006) **[328]**

EV Code	Vulnerability Description
EV1574.006-S1	The potential failure to implement effective execution prevention measures, allowing adversaries to use new payloads and execute dynamic linker hijacking attacks if application control solutions are not properly configured or lack the capability to block malicious software effectively.
EV1574.006-H1	The failure to enable or properly configure System Integrity Protection (SIP) on macOS systems, leaving the environment variables susceptible to exploitation; neglecting SIP increases the risk of dynamic linker hijacking.
EV1574.006-H2	The inadequate application of security measures, such as not leveraging Apple's Hardened Runtime or imposing restrictions on applications; this allows adversaries to exploit environment variables and conduct dynamic linker hijacking on macOS systems.

2.5.65 Hijack Execution Flow: Path Interception by PATH Environment Variable (T1574.007) **[329]**

EV Code	Vulnerability Description
EV1574.007-S1	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.007-S2	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.

EV1574.007-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.007-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.5.66 Hijack Execution Flow: Path Interception by Search Order Hijacking (T1574.008) [330]

EV Code	Vulnerability Description
EV1574.008-S1	The lack of explicit path specification in some programs, allowing adversaries to perform Search Order Hijacking and execute their malicious payloads by placing files in the directory where the calling program is located.
EV1574.008-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.008-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.008-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.008-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.5.67 Hijack Execution Flow: Path Interception by Unquoted Path (T1574.009) [331]

EV Code	Vulnerability Description
EV1574.009-S1	The lack of proper quoting in file paths, allowing for path interception and execution of malicious payloads by placing executables in higher-level directories.
EV1574.009-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.009-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.009-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.009-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.5.68 Hijack Execution Flow: Services File Permissions Weakness (T1574.010) [332]

EV Code	Vulnerability Description
EV1574.010-S1	Flaws in Windows service file permissions, which allow the replacement of legitimate binaries, leading to the execution of malicious payloads with potentially elevated permissions, including SYSTEM.
EV1574.010-S2	Lack of auditing tools capable of detecting file system permissions abuse opportunities, allowing adversaries to exploit weaknesses in service file permissions.
EV1574.010-H1	Improperly setting permissions on the file system directory containing the target binary or on the binary itself, enabling adversaries to overwrite the target binary with a malicious one using user-level permissions.

EV1574.010-H2	Failure to turn off User Account Control's (UAC) privilege elevation for standard users or properly configure UAC settings, potentially allowing elevation of privileges through exploitation during the UAC detection process.
EV1574.010-H3	Allowing execution from user directories, file download directories, and temp directories, potentially providing adversaries with the ability to exploit service binary vulnerabilities and execute malicious code.

2.5.69 Hijack Execution Flow: Services Registry Permissions Weakness (T1574.011) [333]

EV Code	Vulnerability Description
EV1574.011-S1	The weakness in Registry permissions for service-related keys (HKLM\SYSTEM\CurrentControlSet\Services), allowing unauthorized modification of a service's execution parameters, potentially leading to the execution of adversary-controlled code during service startup.
EV1574.011-H1	The failure to set appropriate access controls for the service's Registry keys, allowing adversaries to manipulate keys such as FailureCommand or create custom subkeys, facilitating elevated execution and persistence.
EV1574.011-H2	The lack of proper access controls on the Performance key, enabling adversaries to create or modify it to point to a malicious DLL, potentially leading to the execution of adversary-controlled code during the operation of a driver service.
EV1574.011-H3	The failure to set proper access controls on the Parameters key or custom subkeys, allowing adversaries to add malicious data, establish persistence, or enable other malicious activities associated with their services.
EV1574.011-H4	The failure to secure the service's file identification process using HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll, potentially leading to misidentification of the service's file when launched through svchost.exe.

2.5.70 Hijack Execution Flow: COR_PROFILER (T1574.012) [334]

EV Code	Vulnerability Description
EV1574.012-S1	Insufficient control over DLL execution, as the system lacks robust mechanisms to identify and block potentially malicious unmanaged COR_PROFILER profiling DLLs.
EV1574.012-S2	Inadequate registry permission management, leaving the system exposed to potential modifications of keys associated with COR_PROFILER due to improper permissions on Registry hives.
EV1574.012-H1	Mismanagement of user privileges, allowing unauthorized individuals to edit system environment variables and potentially compromise the system's security.

2.5.71 Hijack Execution Flow: KernelCallbackTable (T1574.013) [335]

EV Code	Vulnerability Description
EV1574.013-S1	The vulnerability in the initialization process of the KernelCallbackTable within the Process Environment Block (PEB), which can be exploited to hijack the execution flow of a process.
EV1574.013-S2	Potential weaknesses in the endpoint security solution's configuration that may allow the adversary to evade behavior prevention mechanisms, specifically related to blocking process injection and memory tampering behaviors.
EV1574.013-H1	Allowing unauthorized access to the Process Environment Block (PEB) memory, potentially through inadequate access controls or permissions, enabling the adversary to obtain a pointer to the KernelCallbackTable.

2.5.72 Implant Internal Image (T1525) [349]

EV Code	Vulnerability Description
EV1525-S1	Inadequate periodic integrity checks on images and containers in cloud deployments, which may result in a failure to detect modifications introducing malicious software.

EV1525-H1	Insufficiently implementing code signing practices, as not leveraging content trust models or signing container images by trusted sources may lead to the acceptance of unsigned or unverified images, compromising the integrity of the deployment.
EV1525-H2	Excessive permissions associated with creating and modifying platform images or containers, violating the principle of least privilege and increasing the risk of unauthorized implantation of malicious code.

2.5.73 Modify Authentication Process (T1556) **[385]**

EV Code	Vulnerability Description
EV1556-S1	Weaknesses in the authentication mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, allowing for the modification of these processes to reveal or bypass credentials.
EV1556-S2	The potential for misconfigurations in authentication logs, such as the lack of proper enforcement of Multi-Factor Authentication (MFA), which could allow adversaries to exploit authentication weaknesses.
EV1556-S3	The potential for unsigned or improperly signed Dynamic Link Libraries (DLLs) and executable files within the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, which could be exploited to introduce malicious components into the authentication process.
EV1556-S4	The existence of new and unknown network provider DLLs within the Registry, specifically at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services <NetworkProviderName>\NetworkProvider\ProviderPath, which, if not periodically reviewed, could introduce unauthorized components affecting authentication.

EV1556-S5	The potential misconfigurations in the implementation of multi-factor authentication (MFA), such as weak settings or insufficient monitoring, which could be exploited to bypass the intended security measures.
EV1556-S6	The potential compromise of password filters due to improper registration, as the absence of filter DLLs in the designated Windows installation directory or missing registry entries may allow unauthorized manipulation, undermining the intended security measures.
EV1556-S7	The potential misconfiguration or oversight in the implementation of Protected Process Light (PPL) for LSA, which may lead to a compromise of privileged process integrity.
EV1556-S8	The risk of unauthorized write access to the /Library/Security/SecurityAgentPlugins directory, posing a threat to the integrity and security of the system.
EV1556-S9	The inadequate restriction on Registry permissions, allowing unauthorized modifications to sensitive Registry keys, specifically HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order, which could lead to system instability or compromise.
EV1556-H1	The unintentional misconfiguration or lack of secure practices in the authentication process, leading to the persistence of compromised credentials for remote access to systems and externally available services like VPNs, Outlook Web Access, and remote desktop.
EV1556-H2	The inadvertent failure to periodically review the hybrid identity solution for discrepancies, including unauthorized Pass Through Authentication (PTA) agents in the Azure Management Portal, potentially leading to undetected compromises of authentication mechanisms.
EV1556-H3	The inadvertent failure to verify the validity of binaries catalog-signed in some cases, potentially causing discrepancies in authentication logs and leading to the exploitation of authentication weaknesses.

EV1556-H4	The failure to disable the EnableMPRNotifications policy through Group Policy or a configuration service provider in Windows 11 22H2, thereby exposing the system to the risk of unauthorized credential transmission by Winlogon to network providers.
EV1556-H5	Inadequate password policies, which could expose sensitive information if the AllowReversiblePasswordEncryption property is improperly configured, allowing reversible password encryption.
EV1556-H6	Insufficient auditing of domain and local accounts, potentially leading to unauthorized access if privilege levels are not routinely reviewed, default accounts are enabled, or unauthorized local accounts are created without proper authorization.
EV1556-H7	Unrestricted access to the root account, which poses a risk of modifying protected components, unless proper privilege separation mechanisms (e.g., SELinux, grsecurity, AppArmor) are implemented to limit Privilege Escalation opportunities.
EV1556-H8	Failure to follow best practices for the design and administration of an enterprise network, potentially allowing excessive privileged account use across administrative tiers, increasing the risk of unauthorized access.
EV1556-H9	Failure to limit Azure AD Global Administrator accounts to only those required and not using dedicated cloud-only accounts, potentially exposing the hybrid identity solution to increased risk of compromise.
EV1556-H10	The potential failure to enforce or adhere to proper user account management policies, leading to insecure enrollment or deactivation of authentication mechanisms, such as MFA, for user accounts and compromising the overall security posture of the system.

2.5.74 Modify Authentication Process: Domain Controller Authentication (T1556.001) [386]

EV Code	Vulnerability Description
EV1556.001-S1	The susceptibility of the domain controller's authentication process to patching, allowing the bypass of typical authentication mechanisms and unauthorized access to user accounts.

EV1556.001-S2	The lack of enabled features, such as Protected Process Light (PPL), for Local Security Authority (LSA), which may contribute to compromised privileged processes
EV1556.001-H1	The absence of multi-factor authentication (MFA), which could potentially allow adversaries to gain control of valid credentials and exploit them for unauthorized access
EV1556.001-H2	Insufficient privileged account management, as auditing domain and local accounts irregularly may result in overlooking situations that could grant adversaries wide access through privileged account credentials.

2.5.75 Modify Authentication Process: Password Filter DLL (T1556.002) [387]

EV Code	Vulnerability Description
EV1556.002-H1	User fails to ensure that filter DLLs are present in the correct Windows installation directory (C:\Windows\System32\ by default) and appropriately registered in the system registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages), which can lead to ineffective password filtering and security risks.

2.5.76 Modify Authentication Process: Pluggable Authentication Modules (T1556.003) [388]

EV Code	Vulnerability Description
EV1556.003-S1	The risk of user credentials being harvested due to plain-text exchange of values with PAM components, as PAM does not store passwords.
EV1556.003-H1	The inadequate implementation of multi-factor authentication (MFA), which could expose accounts to compromise due to the reliance on single-factor authentication.
EV1556.003-H2	The risk of inadequate privileged account management, potentially allowing unauthorized modification of Pluggable Authentication Modules (PAM) components and increasing the likelihood of privilege escalation opportunities.

2.5.77 Modify Authentication Process: Network Device Authentication (T1556.004) [389]

EV Code	Vulnerability Description
EV1556.004-H1	The potential lack of multi-factor authentication for user and privileged accounts on network devices, which could leave these accounts more susceptible to compromise.
EV1556.004-H1	The inadequate implementation of privileged account management practices, such as not restricting administrator accounts to as few individuals as possible and not following least privilege principles, which may result in increased attack surface and potential credential overlap across systems.

2.5.78 Modify Authentication Process: Reversible Encryption (T1556.005) [390]

EV Code	Vulnerability Description
EV1556.005-H1	The potential enabling of reversible password encryption in Active Directory, allowing the decryption of passwords through abuse of the AllowReversiblePasswordEncryption property.
EV1556.005-H2	The potential misconfiguration of the AllowReversiblePasswordEncryption property, which can occur if administrators fail to ensure that it is set to disabled, except when necessary for specific applications.
EV1556.005-H3	The inadequate auditing of domain and local accounts, potentially allowing an adversary to exploit situations where credentials of privileged accounts are obtained, emphasizing the importance of routine audits to detect and address such security risks.

2.5.79 Modify Authentication Process: Multi-Factor Authentication (T1556.006) **[391]**

EV Code	Vulnerability Description
EV1556.006-S1	Insecure configuration of the Windows hosts file (C:\windows\system32\drivers\etc\hosts), allowing adversaries to redirect MFA calls to localhost and causing the MFA process to fail.
EV1556.006-S2	Lack of proper auditing and review processes for MFA actions alongside authentication logs, potentially allowing adversaries to manipulate MFA without detection.
EV1556.006-H1	Failure to enforce a "fail closed" policy for MFA, allowing otherwise successful authentication attempts to be granted access without enforcing multi-factor authentication.
EV1556.006-H2	Failure to ensure that all user accounts have MFA enabled, leaving some accounts without the additional security provided by multi-factor authentication.
EV1556.006-H3	Inadequate implementation of MFA policies and requirements for existing, deactivated, or dormant accounts and devices, allowing adversaries to exploit gaps in MFA coverage.

2.5.80 Modify Authentication Process: Hybrid Identity (T1556.007) **[392]**

EV Code	Vulnerability Description
EV1556.007-S1	Weakness in the on-premises server running a Pass Through Authentication (PTA) agent, allowing adversaries to inject a malicious DLL into the AzureADConnectAuthenticationAgentService process, enabling unauthorized authentication attempts and credential recording.
EV1556.007-S2	In environments using Active Directory Federation Services (AD FS), adversaries can exploit a weakness by editing the Microsoft.IdentityServer.Servicehost configuration file to load a malicious DLL, generating authentication tokens for any user and bypassing multi-factor authentication and defined AD FS policies.

EV1556.007-S3	Lack of verification of the integrity of DLLs and executable files in the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, creating a potential avenue for adversaries to introduce malicious code if files are not properly signed by Microsoft.
EV1556.007-H1	Failure to periodically review the hybrid identity solution for discrepancies, such as unwanted or unapproved Pass Through Authentication (PTA) agents in the Azure Management Portal, leading to potential unauthorized access.
EV1556.007-H2	Inadequate privileged account management, as organizations may fail to limit on-premises accounts with access to the hybrid identity solution, potentially allowing unauthorized access if Azure AD Global Administrator accounts are not properly restricted and dedicated for cloud-only use.
EV1556.007-H3	Failure to integrate multi-factor authentication (MFA) as part of organizational policy, increasing the risk of adversaries gaining control of valid credentials that could be exploited for various tactics, including initial access, lateral movement, and information collection.

2.5.81 Modify Authentication Process: Network Provider DLL (T1556.008) **[393]**

EV Code	Vulnerability Description
EV1556.008-S1	The insecure transmission of credentials during the logon process, as Winlogon sends credentials to the local mpnotify.exe process via RPC without encryption.
EV1556.008-S2	The insecure sharing of credentials in cleartext by the mpnotify.exe process with registered credential managers during logon events, potentially exposing sensitive information.
EV1556.008-H1	The failure to consistently review and identify new or unknown network provider DLLs within the Registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services<NetworkProviderName>\NetworkProvider\ProviderPath) could allow malicious DLLs to go unnoticed.

EV1556.008-H2	The failure to ensure that only valid DLLs are registered and listed in the Registry key at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order may lead to the registration of malicious DLLs.
EV1556.008-H3	The potential for misconfiguration, as the EnableMPRNotifications policy in Windows 11 22H2 can be disabled to prevent Winlogon from sending credentials to network providers, and a failure to apply this configuration could expose credentials during the logon process.
EV1556.008-H4	The mismanagement of Registry permissions, as failure to restrict permissions to sensitive Registry keys, such as HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order, may allow unauthorized modification and compromise the integrity of network provider configurations.

2.5.82 Office Application Startup (T1137) **[438]**

EV Code	Vulnerability Description
EV1137-S1	The inadequate software configuration related to the Office Test method, where the absence of proper Registry key permissions may allow unauthorized access without administrator permissions or privilege escalation during Office application startup.
EV1137-H1	the improper handling of Office add-ins, either not disabling them or not following best practices for securing them, potentially providing adversaries with an avenue to exploit these add-ins for persistence during Office application startup.
EV1137-H2	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.
EV1137-H3	The lack of applying necessary software updates, specifically failing to apply patches such as KB3191938, KB4011091, and KB4011162, leaving systems exposed to known vulnerabilities associated with Outlook methods during Office application startup.

EV1137-H4	The improper configuration and security of Office VBA macros, as well as the failure to disable or properly secure Office add-ins, leaving a potential avenue for adversaries to exploit these features for persistence during Office application startup.

2.5.83 Office Application Startup: Office Template Macros (T1137.001) [439]

EV Code	Vulnerability Description
EV1137.001-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.
EV1137.001-H2	The improper configuration and security of Office VBA macros, as well as the failure to disable or properly secure Office add-ins, leaving a potential avenue for adversaries to exploit these features for persistence during Office application startup.

2.5.84 Office Application Startup: Office Test (T1137.002) [440]

EV Code	Vulnerability Description
EV1137.002-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.
EV1137.002-H2	The inadequate configuration of the Registry key used to execute DLLs, as improper settings or permissions may still allow unauthorized access, necessitating proper configuration and permission settings to prevent easy exploitation.

2.5.85 Office Application Startup: Outlook Forms (T1137.003) **[441]**

EV Code	Vulnerability Description
EV1137.003-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.
EV1137.003-H2	The lack of applying necessary software updates, specifically failing to apply patches such as KB3191938, KB4011091, and KB4011162, leaving systems exposed to known vulnerabilities associated with Outlook methods during Office application startup.

2.5.86 Office Application Startup: Outlook Home Page (T1137.004) **[442]**

EV Code	Vulnerability Description
EV1137.004-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.
EV1137.004-H2	The lack of applying necessary software updates, specifically failing to apply patches such as KB3191938, KB4011091, and KB4011162, leaving systems exposed to known vulnerabilities associated with Outlook methods during Office application startup.

2.5.87 Office Application Startup: Outlook Rules (T1137.005) **[443]**

EV Code	Vulnerability Description
EV1137.005-H1	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.

EV1137.005-H2	The lack of applying necessary software updates, specifically failing to apply patches such as KB3191938, KB4011091, and KB4011162, leaving systems exposed to known vulnerabilities associated with Outlook methods during Office application startup.

2.5.88 Office Application Startup: Add-ins (T1137.006) [444]

EV Code	Vulnerability Description
EV1137.006-H1	The failure to adequately control and restrict the execution of code within Office add-ins, allowing adversaries to exploit the user's configuration and potentially achieve persistence on the compromised system.
EV1137.006-H2	The potential failure to enable Attack Surface Reduction (ASR) rules on Windows 10, allowing Office applications to create child processes and write potentially malicious executable content to disk during Office application startup.

2.5.89 Power Settings (T1653) [471]

EV Code	Vulnerability Description
EV1653-H1	The potential oversight or neglect in conducting regular system audits to identify abnormal power settings, introducing a gap in the detection and response to malicious activities.

2.5.90 Pre-OS Boot (T1542) [472]

EV Code	Vulnerability Description
EV1542-S1	The absence or inadequate implementation of Trusted Platform Module (TPM) technology and a secure or trusted boot process, which could allow unauthorized modifications to BIOS or EFI during pre-OS boot.
EV1542-H2	The risk of BIOS or EFI not being patched and updated, potentially leaving the system exposed to known vulnerabilities that adversaries could exploit during the pre-OS boot process.

EV1542-H3	The potential failure to ensure proper permissions for privileged accounts, allowing adversaries to gain unauthorized access to critical system components, such as boot drivers or firmware, and compromise system integrity during the pre-OS boot process.

2.5.91 Pre-OS Boot: System Firmware (T1542.001) [473]

EV Code	Vulnerability Description
EV1542.001-S1	The potential lack of integrity verification for the BIOS or EFI, allowing for vulnerability to modification and compromise.
EV1542.001-S2	The reliance on software-based root of trust, making the SPI flash memory susceptible to tampering.
EV1542.001-S3	The absence of protective technologies like Intel Boot Guard, leaving the system exposed to potential firmware modifications.
EV1542.001-H1	The risk of BIOS or EFI not being patched and updated, potentially leaving the system exposed to known vulnerabilities that adversaries could exploit during the pre-OS boot process.
EV1542.001-H2	The potential failure to ensure proper permissions for privileged accounts, allowing adversaries to gain unauthorized access to critical system components, such as boot drivers or firmware, and compromise system integrity during the pre-OS boot process.

2.5.92 Pre-OS Boot: Component Firmware (T1542.002) [474]

EV Code	Vulnerability Description
EV1542.002-H1	The failure to implement robust integrity checking mechanisms for computer components, facilitating the installation of malicious firmware and providing a persistent level of access to systems.
EV1542.002-H2	The failure to perform regular firmware updates, exposing the system to increased risks of exploitation and abuse by adversaries due to outdated firmware.

2.5.93 Pre-OS Boot: Bootkit (T1542.003) [475]

EV Code	Vulnerability Description
EV1542.003-S1	The susceptibility of the Master Boot Record (MBR) and Volume Boot Record (VBR) to unauthorized modification, allowing adversaries with raw access to the boot drive to divert execution during startup to malicious code.
EV1542.003-S2	The absence of Trusted Platform Module (TPM) technology or a secure/trusted boot process, leaving the system exposed to potential compromise of boot integrity.
EV1542.003-H1	Inadequate privileged account management, allowing adversaries to potentially gain unauthorized access to accounts necessary for installing a bootkit, emphasizing the importance of ensuring proper permissions to prevent such access.

2.5.94 Pre-OS Boot: ROMMONkit (T1542.004) [476]

EV Code	Vulnerability Description
EV1542.004-S1	The potential lack of periodic integrity checks on the system image, which could result in the failure to detect unauthorized modifications.
EV1542.004-S2	The absence of secure boot features, leaving the device susceptible to unauthorized firmware upgrades in the ROM Monitor (ROMMON) of Cisco network devices.
EV1542.004-H1	The failure to enable secure boot features, which could result in the inability to validate the digital signature of the boot environment and system image, allowing for potential unauthorized software loading.
EV1542.004-H2	The failure to enable and configure network intrusion detection and prevention systems specifically for protocols like TFTP, leaving the network susceptible to unauthorized firmware updates and potential compromise by adversaries.

2.5.95 Pre-OS Boot: TFTP Boot (T1542.005) [477]

EV Code	Vulnerability Description
EV1542.005-S1	The potential lack of periodic integrity checks on the system image, which could result in the failure to detect unauthorized modifications.
EV1542.005-S2	The unrestricted use of protocols without encryption or authentication mechanisms, posing a risk of unauthorized manipulation during the netbooting process.
EV1542.005-S3	The inadequate use of Authentication, Authorization, and Accounting (AAA) systems for privileged account management, potentially allowing unauthorized actions by administrators and hindering the detection of abuse through a lack of comprehensive user action history.
EV1542.005-H1	The failure to enable secure boot features, which could result in the inability to validate the digital signature of the boot environment and system image, allowing for potential unauthorized software loading.
EV1542.005-H2	The failure to enable and configure network intrusion detection and prevention systems specifically for protocols like TFTP, leaving the network susceptible to unauthorized firmware updates and potential compromise by adversaries.
EV1542.005-H3	The lack of adherence to vendor device hardening best practices, potentially leading to the presence of unnecessary and unused features and services, default configurations, and passwords that could be exploited by adversaries.

2.5.96 Scheduled Task/Job (T1053) [518]

EV Code	Vulnerability Description
EV1053-S1	The potential permission weaknesses in scheduled tasks, allowing adversaries to exploit and escalate privileges.

EV1053-H1	The failure to configure settings for scheduled tasks to force them to run under the context of the authenticated account instead of allowing them to run as SYSTEM, creating a potential avenue for privilege escalation.
EV1053-H2	The failure to restrict the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process, potentially enabling unauthorized users to manipulate task scheduling priorities.
EV1053-H3	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, allowing unauthorized administrators to create scheduled tasks on remote systems.

2.5.97 Scheduled Task/Job: At (T1053.002) [519]

EV Code	Vulnerability Description
EV1053.002-S1	The misconfiguration of the at.allow and at.deny files on Linux and macOS, as adversaries can exploit this to invoke the at utility, potentially leading to unauthorized task scheduling.
EV1053.002-S2	The potential misconfiguration of scheduled tasks in Windows environments, as they may run with elevated privileges, allowing adversaries to exploit permission weaknesses and escalate privileges.
EV1053.002-H1	The misconfiguration of scheduled tasks in Windows environments, where tasks are allowed to run as SYSTEM, creating a potential avenue for privilege escalation if not properly configured to run under the context of the authenticated account.
EV1053.002-H2	The potential misconfiguration of the Increase Scheduling Priority option in Windows environments, as it could allow non-administrative users to schedule priority processes, leading to potential abuse.
EV1053.002-H3	The mismanagement of user account privileges in Linux environments, specifically related to the at utility, where users listed in the at.deny file may not be properly restricted from invoking the at utility, potentially leading to unauthorized task scheduling.

2.5.98 Scheduled Task/Job: Cron (T1053.003) [520]

EV Code	Vulnerability Description
EV1053.003-H1	The absence of regular auditing for changes to the cron schedule, potentially allowing undetected malicious scheduling.
EV1053.003-H2	Inadequate management of cron permissions through /etc/cron.allow and /etc/cron.deny, which may result in unauthorized users gaining cron access or superfluous restrictions, impacting proper system functioning.

2.5.99 Scheduled Task/Job: Scheduled Task (T1053.005) [521]

EV Code	Vulnerability Description
EV1053.005-S1	The potential permission weaknesses in scheduled tasks, which may be exploited to escalate privileges, as highlighted by the PowerSploit framework's PowerUp modules.
EV1053.005-S2	The insufficient restriction of the Increase Scheduling Priority option, potentially allowing non-administrative users to schedule a priority process, which can be mitigated by configuring GPO settings to restrict this privilege to the Administrators group.
EV1053.005-H1	The misconfiguration of scheduled task settings, allowing tasks to run as SYSTEM, which can be mitigated by configuring settings to force tasks to run under the context of the authenticated account and adjusting associated Registry keys and Group Policy Objects (GPO).
EV1053.005-H2	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, leading to unauthorized creation of scheduled tasks on remote systems; this can be addressed by appropriately limiting user privileges and addressing Privilege Escalation vectors through effective User Account Management.

2.5.100 Scheduled Task/Job: Systemd Timers (T1053.006) [522]

EV Code	Vulnerability Description
EV1053.006-H1	The improper implementation of privileged account management, as failure to limit access to the root account may result in unauthorized creation or modification of systemd timer unit files by users.
EV1053.006-H2	User insufficiently restricts file and directory permissions, as failure to limit access to systemd .timer unit files may allow unauthorized users to read or modify them, potentially leading to the execution of malicious code.
EV1053.006-H3	Inadequate user account management, as failure to restrict user access to system utilities may result in unauthorized use of 'systemctl' or 'systemd-run' by users, facilitating the abuse of systemd timers for malicious purposes.

2.5.101 Scheduled Task/Job: Container Orchestration Job (T1053.007) [523]

EV Code	Vulnerability Description
EV1053.007-S1	The potential for containers to run with root privileges by default, creating a security weakness that can be exploited for malicious activities.
EV1053.007-H1	User misconfigures or allows unauthorized access to CronJobs within Kubernetes, enabling the scheduling of jobs that execute malicious code in various nodes within a cluster.
EV1053.007-H2	The improper configuration and lack of adherence to Pod Security Standards in Kubernetes environments, allowing containers to run as privileged, which undermines the intended security measures and facilitates unauthorized activities.

2.5.102 Server Software Component (T1505) **[540]**

EV Code	Vulnerability Description
EV1505-S1	The potential weakness in legitimate extensible development features in server applications, allowing adversaries to install and abuse malicious components for persistent access.
EV1505-S2	Insufficient regular checks on critical services, potentially allowing adversaries to exploit unverified and compromised components for persistence.
EV1505-S3	The absence of code signing for application component binaries, exposing the system to the risk of unauthorized or tampered software execution.
EV1505-H1	The failure to disable or remove unnecessary software components, providing adversaries with opportunities to abuse these components for malicious purposes.
EV1505-H2	User utilize administrator accounts with permissions to add component software for day-to-day operations, potentially exposing these high-privilege accounts to adversaries on less secure systems.
EV1505-H3	Inadequately restricted registry permissions, creating a potential avenue for adversaries to modify critical server parameters and compromise system integrity.
EV1505-H4	Insufficient enforcement of the principle of least privilege, allowing user accounts to possess privileges that enable unauthorized modification or addition of server software components.

2.5.103 Server Software Component: SQL Stored Procedures (T1505.001) **[541]**

EV Code	Vulnerability Description
EV1505.001-S1	The potential weakness in the Microsoft SQL Server's CLR integration, as adversaries can craft or modify CLR assemblies linked to stored procedures, enabling the execution of arbitrary commands.

EV1505.001-S2	Insufficient regular checks on critical services, potentially allowing adversaries to exploit unverified and compromised components for persistence.
EV1505.001-S3	The absence of code signing for application component binaries, exposing the system to the risk of unauthorized or tampered software execution.
EV1505.001-H1	User utilize administrator accounts with permissions to add component software for day-to-day operations, potentially exposing these high-privilege accounts to adversaries on less secure systems.

2.5.104 Server Software Component: Transport Agent (T1505.002) [542]

EV Code	Vulnerability Description
EV1505.002-S1	Potential weaknesses in Microsoft Exchange transport agents, which can be exploited by adversaries to establish persistent access to systems.
EV1505.002-S2	Insufficient regular checks on critical services, potentially allowing adversaries to exploit unverified and compromised components for persistence.
EV1505.002-S3	The absence of code signing for application component binaries, exposing the system to the risk of unauthorized or tampered software execution.
EV1505.002-H1	User utilize administrator accounts with permissions to add component software for day-to-day operations, potentially exposing these high-privilege accounts to adversaries on less secure systems.

2.5.105 Server Software Component: Web Shell (T1505.003) [543]

EV Code	Vulnerability Description
EV1505.003-S1	The potential oversight in not disabling or removing insecure features, such as PHP's eval(), which could be abused for web shell attacks.

EV1505.003-H1	The failure to enforce the principle of least privilege in user account management, allowing unauthorized accounts to potentially modify the web directory and introduce web shells.

2.5.106 Server Software Component: IIS Components (T1505.004) [544]

EV Code	Vulnerability Description
EV1505.004-S1	The lack of regular integrity checks on installed IIS components, which may allow the persistence of malicious components on the web server.
EV1505.004-S2	The absence of code signing for IIS DLLs and binaries, potentially enabling the execution of unauthorized or tampered code on the web server.
EV1505.004-S3	The potential oversight in restricting unallowed ISAPI extensions and filters, leading to the execution of unauthorized code and manipulation of IIS web requests and responses.
EV1505.004-H1	The potential mismanagement of privileged accounts, allowing administrator accounts with permissions to add IIS components to be used for day-to-day operations, exposing these elevated permissions to potential adversaries and other unprivileged systems.

2.5.107 Server Software Component: Terminal Services DLL (T1505.005) [545]

EV Code	Vulnerability Description
EV1505.005-S1	The weakness in the Microsoft Terminal Services, particularly the ability to modify and replace the default Terminal Services DLL (termsrv.dll) to facilitate persistent access to victimized hosts.
EV1505.005-S2	The failure to adequately secure Windows Services that run as "generic" processes (e.g., svchost.exe), allowing adversaries to exploit the ServiceDll Registry entry, potentially leading to unauthorized modifications of the Terminal Services DLL.
EV1505.005-S3	The potential lack of regular integrity checks on critical services' component software, allowing adversaries to persistently manipulate Terminal Services components without detection.

EV1505.005-H1	The failure to implement Group Policy restrictions effectively, leading to an inability to block modifications to Terminal Services parameters in the Registry, thereby exposing the system to potential unauthorized changes.

2.5.108 Traffic Signaling (T1205) [610]

EV Code	Vulnerability Description
EV1205-H1	Failure to disable or remove the Wake-on-LAN feature when not needed within an environment, which could expose systems to unauthorized activation and subsequent lateral movement.
EV1205-H2	The potential failure to implement stateful firewalls effectively, allowing some variants of traffic signaling to bypass network defenses.

2.5.109 Traffic Signaling: Port Knocking (T1205.001) [611]

EV Code	Vulnerability Description
EV1205.001-H1	The potential failure to implement or configure stateful firewalls effectively, leaving the system susceptible to variants of the port knocking technique and associated adversarial activities.

2.5.110 Traffic Signaling: Socket Filters (T1205.002) [612]

EV Code	Vulnerability Description
EV1205.001-H1	The potential misconfiguration or improper implementation of stateful firewalls, introducing the risk of ineffective mitigation and leaving the system susceptible to network traffic filtering manipulations by adversaries.

2.5.111 Valid Accounts (T1078) [636]

EV Code	Vulnerability Description
EV1078-S1	The potential lack of proper configuration and monitoring of conditional access policies, allowing non-compliant devices or logins from outside defined organization IP ranges.
EV1078-H1	The use of legacy authentication in Active Directory, which does not support multi-factor authentication (MFA), and the failure to enforce the use of modern authentication protocols.
EV1078-H2	The insecure storage of sensitive data or credentials in applications, such as storing plaintext credentials in code, publishing credentials in repositories, or leaving credentials in public cloud storage, providing opportunities for adversaries to compromise credentials.
EV1078-H3	The failure to promptly change default usernames and passwords on applications and appliances after installation, potentially leaving systems exposed to credential abuse.
EV1078-H4	The potential lack of routine audits of domain and local accounts, their permission levels, and the failure to detect situations that could allow adversaries to gain wide access by obtaining credentials of privileged accounts.
EV1078-H5	The failure to regularly audit user accounts for activity and deactivate or remove unnecessary accounts, increasing the risk of adversaries exploiting unused accounts for unauthorized access.
EV1078-H6	The lack of awareness and training regarding multi-factor authentication (MFA) push notifications, potentially leading users to accept and authenticate malicious notifications, compromising account security.

2.5.112 Valid Accounts: Default Accounts (T1078.001) [637]

EV Code	Vulnerability Description
EV1078.001-H1	The presence of default accounts with unchanged credentials, such as Guest or Administrator accounts on Windows systems, which can be exploited for Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.001-H2	The failure to change preset usernames and passwords for equipment like network devices and computer applications, including internal, open source, or commercial systems, which poses a serious threat if not altered post-installation.

2.5.113 Valid Accounts: Domain Accounts (T1078.002) [638]

EV Code	Vulnerability Description
EV1078.002-S1	Lack of multi-factor authentication (MFA) implementation, potentially allowing adversaries to gain control of valid credentials.
EV1078.002-S2	Poor design and administration of the enterprise network, potentially leading to the inappropriate inclusion of user or admin domain accounts in local administrator groups across systems, creating a security risk equivalent to having a common local administrator account password.
EV1078.002-H1	Password reuse, which can be exploited by adversaries to compromise domain accounts, posing a risk to Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.002-H2	Inadequate privileged account management, including the lack of routine audits on domain account permission levels, which could enable adversaries to exploit overly permissive access and compromise privileged accounts.
EV1078.002-H3	Insufficient user training on recognizing valid push notifications for multi-factor authentication, increasing the risk of users accepting fraudulent notifications and compromising the effectiveness of MFA.

EV1078.002-H4	Weak password management practices, resulting in credential overlap across systems and increasing the risk of unauthorized access if an adversary obtains account credentials.

2.5.114 Valid Accounts: Local Accounts (T1078.003) [639]

EV Code	Vulnerability Description
EV1078.003-H1	The inadequate enforcement of complex, unique passwords for local administrator accounts across all systems, potentially allowing unauthorized access.
EV1078.003-H2	The reuse of passwords for local accounts, enabling adversaries to abuse credentials across multiple machines on a network, facilitating Privilege Escalation and Lateral Movement.
EV1078.003-H3	The inadequate management of privileged accounts, as routine audits may be neglected, leading to situations where adversaries can exploit credentials of privileged accounts with wide access.
EV1078.003-H4	The improper use of local administrator accounts for day-to-day operations may expose user to potential adversaries, posing a security risk.

2.5.115 Valid Accounts: Cloud Accounts (T1078.004) [640]

EV Code	Vulnerability Description
EV1078.004-S1	The absence of multi-factor authentication for cloud accounts, especially privileged accounts, which could leave accounts susceptible to unauthorized access.
EV1078.004-S2	The potential for misconfigurations in conditional access policies, allowing logins from non-compliant devices or outside defined organization IP ranges.
EV1078.004-H1	Misconfigurations in role assignments or role assumption policies within cloud environments, enabling unauthorized access and privilege escalation.

EV1078.004-H2	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H3	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H4	The lack of enforcement of complex, unique passwords across all systems on the network, particularly for privileged cloud accounts, potentially allowing adversaries to exploit compromised credentials.
EV1078.004-H5	The inadequate review of privileged cloud account permission levels, which may result in the presence of high-risk roles such as Global Administrator and Privileged Role Administrator, providing adversaries with extensive access.
EV1078.004-H6	The failure to periodically review and remove inactive or unnecessary user accounts, potentially leaving dormant accounts that could be exploited by adversaries.
EV1078.004-H7	The potential for users to accept and act on invalid push notifications for multi-factor authentication, highlighting the importance of training users to recognize and report suspicious push notifications.

2.6 Privilege Escalation (TA0004) [9]

2.6.1 Abuse Elevation Control Mechanism (T1548) [30]

EV Code	Vulnerability Description
EV1548-S1	Misconfiguration of setuid and setgid bits on applications with known vulnerabilities or shell escapes, potentially allowing adversaries to compromise the system.
EV1548-S2	Suboptimal User Account Control (UAC) enforcement, providing opportunities for UAC bypass techniques and DLL Search Order Hijacking.

EV1548-H1	The failure to appropriately configure and manage authorization, leading to the potential for adversaries to exploit and elevate privileges on the system.
EV1548-H2	Inadequate auditing practices, potentially allowing attackers to exploit common User Account Control (UAC) bypass weaknesses on Windows systems.
EV1548-H3	Failure to implement proper execution prevention measures, such as allowing applications from only legitimate repositories or restricting the execution of unsigned applications, which could expose the system to increased risk.
EV1548-H4	Retaining unnecessary users in the local administrator group, creating opportunities for adversaries to exploit privileged accounts and escalate privileges.
EV1548-H5	Improper configuration of the sudoers file, including not strictly requiring passwords or allowing users to spawn risky processes with higher privileges, potentially enabling unauthorized activities.
EV1548-H6	Granting excessive privileges to cloud accounts, increasing the risk of unauthorized access and privilege escalation in cloud environments.
EV1548-H7	Failure to enforce just-in-time access with manual approval for temporary elevation of privileges, potentially allowing unauthorized elevation of permissions.

2.6.2 Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001) [31]

EV Code	Vulnerability Description
EV1548.001-H1	The improper application of setuid and setgid flags to their own applications using the chmod command, enabling the user to execute programs in elevated contexts without the necessary privileges and bypassing execution environment restrictions.
EV1548.001-H2	The failure to properly configure applications, as not removing setuid or setgid bits from programs with known vulnerabilities or shell escapes could result in an increased attack surface and potential compromise of the system.

2.6.3 Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) [32]

EV Code	Vulnerability Description
EV1548.002-S1	Due to a UAC protection level set below the highest, certain Windows programs may elevate privileges or execute elevated Component Object Model objects without triggering a user prompt.
EV1548.002-S2	The potential for common UAC bypass weaknesses on Windows systems, which may be overlooked during audits, leading to an unaware risk posture.
EV1548.002-S3	The potential suboptimal enforcement level for UAC, which may allow for the exploitation of UAC bypass techniques and unauthorized access to the system.
EV1548.002-H1	The inclusion of unnecessary users in the local administrator group on systems, increasing the risk of privilege abuse and compromise.
EV1548.002-H2	The outdated Windows version and patch level, which can be exploited to bypass UAC and compromise the system.

2.6.4 Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003) [33]

EV Code	Vulnerability Description
EV1548.003-S1	Inadequate configuration of the tty_tickets setting, allowing potential leakage across tty sessions, compromising the security of the operating system.
EV1548.003-H1	The absence of a password requirement for executing commands in the sudoers file, making it easier for adversaries who gain terminal access to execute privileged commands without authentication.
EV1548.003-H2	The failure to strictly edit the sudoers file to always require passwords and prevent users from spawning risky processes, leaving the system exposed to potential misuse or unauthorized access.

2.6.5 *Abuse Elevation Control Mechanism: Elevated Execution with Prompt (T1548.004)* [34]

EV Code	Vulnerability Description
EV1548.004-S1	The deprecated AuthorizationExecuteWithPrivileges API still being fully functional in the latest releases of macOS, providing an exploitable mechanism for privilege escalation.
EV1548.004-H1	User is tricked into granting escalated privileges by entering credentials when prompted, as the AuthorizationExecuteWithPrivileges API does not perform checks on the legitimacy of the requesting program.
EV1548.004-H2	User inadvertently downloads and runs unsigned applications, which could bypass the execution prevention measures and introduce security risks to the system.

2.6.6 *Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)* [35]

EV Code	Vulnerability Description
EV1548.005-H1	The failure to appropriately limit privileges for cloud accounts, allowing them to assume, create, or impersonate additional roles, policies, and permissions beyond what is necessary.
EV1548.005-H2	The failure to implement proper access controls and manual approval processes for just-in-time access, potentially leading to unauthorized temporary elevation of privileges in cloud environments.

2.6.7 *Access Token Manipulation (T1134)* [36]

EV Code	Vulnerability Description
EV1134-S1	The susceptibility of Windows access tokens to manipulation, allowing unauthorized users to modify tokens and operate under a different security context, potentially bypassing access controls.

EV1134-S2	The inherent weakness in Windows API functions that allows token stealing, enabling adversaries in a privileged user context to elevate their security level from administrator to SYSTEM.
EV1134-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.6.8 Access Token Manipulation: Token Impersonation/Theft (T1134.001) [37]

EV Code	Vulnerability Description
EV1134.001-S1	The potential weakness in access token handling mechanisms, allowing duplication and subsequent impersonation of another user's token.
EV1134.001-S2	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.001-H1	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.6.9 Access Token Manipulation: Create Process with Token (T1134.002) [38]

EV Code	Vulnerability Description
EV1134.002-S1	Insufficient access controls on token creation mechanisms, allowing adversaries to create new processes with existing tokens and escalate privileges.

EV1134.002-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.002-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.6.10 Access Token Manipulation: Make and Impersonate Token (T1134.003) [39]

EV Code	Vulnerability Description
EV1134.003-S1	Weak or easily guessable usernames and passwords, enabling adversaries to utilize the LogonUser function for token creation.
EV1134.003-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.003-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.6.11 Access Token Manipulation: Parent PID Spoofing (T1134.004) [40]

EV Code	Vulnerability Description
EV1134.004-S1	The lack of robust process monitoring defenses, allowing adversaries to spoof the Parent Process Identifier (PPID) and evade detection.

2.6.12 Access Token Manipulation: SID-History Injection (T1134.005) **[41]**

EV Code	Vulnerability Description
EV1134.005-S1	The possibility of SID Filtering not being automatically applied to legacy trusts or intentionally disabled for inter-domain access, creating a security gap that could be exploited for unauthorized activities.
EV1134.005-S2	The incorrect application of SID Filter Quarantining to external trusts, potentially leading to misconfigurations that could be exploited by adversaries for unauthorized access or privilege escalation.
EV1134.005-S3	The unsupported configuration of applying SID Filtering to domain trusts within a single forest, risking breaking changes and potential security issues that may arise due to this configuration.
EV1134.005-H1	The failure to clean up SID-History attributes after legitimate account migration, leaving potential traces that could be exploited by adversaries for unauthorized access or privilege escalation.

2.6.13 Account Manipulation (T1098) **[48]**

EV Code	Vulnerability Description
EV1098-S1	Insufficient access controls, allowing adversaries to modify credentials or permission groups.
EV1098-S2	Improper operating system configuration on domain controllers, exposing them to potential compromise through unnecessary protocols and services.
EV1098-S3	Inadequate network segmentation, potentially allowing unauthorized access to critical systems and domain controllers.
EV1098-H1	Poor password management practices, as iterative password updates may be performed to bypass password duration policies.
EV1098-H2	The absence of multi-factor authentication, which could leave user and privileged accounts susceptible to compromise.

EV1098-H3	Inappropriate use of domain administrator accounts for day-to-day operations, increasing the risk of exposure to potential adversaries on unprivileged systems.
EV1098-H4	Insufficient user account management, risking unauthorized modifications to accounts or account-related policies by low-privileged user accounts.

2.6.14 Account Manipulation: Additional Cloud Credentials (T1098.001) [49]

EV Code	Vulnerability Description
EV1098.001-S1	The insufficient control or monitoring of credential additions in cloud accounts, allowing unauthorized and adversary-controlled credentials to be added.
EV1098.001-S2	The lack of proper validation or restrictions on the addition of Service Principal and Application credentials in Azure AD, enabling adversaries to augment existing legitimate credentials.
EV1098.001-S3	The insufficient control over credential management tools such as the Azure Portal, Azure command line interface, and Azure or Az PowerShell modules, providing avenues for unauthorized credential additions
EV1098.001-S4	The lack of robust security measures in infrastructure-as-a-service (IaaS) environments, allowing adversaries to generate or import their own SSH keys, potentially leading to persistent unauthorized access
EV1098.001-H1	The inadequate management of permissions and roles, allowing adversaries in Azure AD environments to exploit the Application Administrator role and add unauthorized credentials to their application's service principal.
EV1098.001-H2	The inadequate management of permissions in AWS environments, enabling adversaries to use the sts:GetFederationToken API call and create temporary credentials tied to the permissions of the original user account, potentially leading to privilege escalation.

EV1098.001-H3	The failure to deactivate or manage API credentials properly in AWS environments, allowing temporary credentials created through sts:GetFederationToken to remain valid even after the deactivation of the original account's API credentials.
EV1098.001-H4	The absence of enforced multi-factor authentication for the CreateKeyPair and ImportKeyPair API calls, potentially allowing adversaries to bypass authentication measures and manipulate SSH keys.
EV1098.001-H5	The lack of proper network segmentation, which may result in broader access to critical systems and domain controllers, providing adversaries with an extended attack surface.
EV1098.001-H6	The inadequate privileged account management, as allowing domain administrator or root accounts to be used for day-to-day operations increases the risk of exposure to potential adversaries on unprivileged systems.
EV1098.001-H7	The lack of restrictions on users calling the sts:GetFederationToken API in AWS environments, unless explicitly required, potentially leading to unauthorized creation of temporary credentials and privilege escalation.

2.6.15 Account Manipulation: Additional Email Delegate Permissions (T1098.002) [50]

EV Code	Vulnerability Description
EV1098.002-S1	The potential misconfiguration or lack of proper access controls in email systems, such as on-premises Exchange, Office 365, or Google Workspace, allowing adversaries to use commands like Add-MailboxPermission or delegate permissions to maintain persistent access to an adversary-controlled email account.
EV1098.002-H1	The reliance on single-factor authentication, as not implementing multi-factor authentication for user and privileged accounts may expose the system to higher risks of unauthorized access in the event of compromised credentials.

EV1098.002-H2	The failure to disable or remove unnecessary features or programs, as not taking action to disable email delegation when not required may create an avenue for exploitation, allowing adversaries to misuse the feature for unauthorized access or other malicious activities.
EV1098.002-H3	The overuse of domain administrator accounts for day-to-day operations, which could expose privileged accounts to potential adversaries on unprivileged systems, increasing the likelihood of privilege escalation attacks.

2.6.16 Account Manipulation: Additional Cloud Roles (T1098.003) [51]

EV Code	Vulnerability Description
EV1098.003-S1	The lack of proper controls to prevent the use of APIs like CreatePolicyVersion and AttachUserPolicy in AWS environments, enabling the definition of new IAM policy versions or attachment of policies with additional permissions to compromised user accounts.
EV1098.003-H1	The absence of multi-factor authentication for user and privileged accounts, which could expose these accounts to compromise.
EV1098.003-H2	The failure to adequately secure IAM credentials, leading to a compromised account with sufficient permissions, potentially granting almost unlimited access to data and settings.
EV1098.003-H3	The failure to implement least privilege principles, potentially allowing accounts to have excessive permissions, and in Azure AD environments, not leveraging Privileged Identity Management (PIM) may lead to inadequate control over role assignments, risking unauthorized access.
EV1098.003-H4	The lack of restrictions on low-privileged user accounts, enabling them to have permissions to add or modify permissions on accounts or IAM policies.

2.6.17 Account Manipulation: SSH Authorized Keys (T1098.004) [52]

EV Code	Vulnerability Description
EV1098.004-S1	The misconfiguration of SSH configuration files, specifically the mismanagement of PubkeyAuthentication and RSAAuthentication directives, allowing adversaries to enable unauthorized public key and RSA authentication.
EV1098.004-H1	The inadequate restriction of file and directory permissions for the authorized_keys file, allowing unauthorized modifications and additions by adversaries.
EV1098.004-H2	The inadequate protection of network devices, specifically the failure to secure the ip ssh pubkey-chain command on network devices, enabling adversaries to add unauthorized SSH keys.
EV1098.004-H3	The failure to disable or restrict SSH access when it is unnecessary on a host, creating an avenue for unauthorized manipulation of SSH authorized_keys files.
EV1098.004-H4	The lack of proper user account management in cloud environments, specifically the failure to restrict permissions for updating instance metadata or configurations, leading to potential unauthorized modifications of SSH authorized_keys files.

2.6.18 Account Manipulation: Device Registration (T1098.005) [53]

EV Code	Vulnerability Description
EV1098.005-S1	Insecure MFA self-enrollment process that, in some cases, requires only a username and password, enabling the adversary to enroll the account's first device or register a device to an inactive account without robust authentication.
EV1098.005-S2	The risk associated with device registration in Azure AD and Microsoft Intune, as an adversary with existing network access can register a device to bypass conditional access policies and gain unauthorized access to sensitive data or resources.

EV1098.005-H1	Failure to require MFA for device registration in Azure AD or allowing device enrollment for inactive accounts may leave the system susceptible to unauthorized access.
EV1098.005-H2	The inadequate implementation of MFA policies, such as not configuring MFA systems to disallow enrolling new devices for inactive accounts or failing to use conditional access policies to restrict device enrollment to trusted locations or devices, which could result in a compromised device registration process.
EV1098.005-H3	The reliance on temporary access passes as an initial MFA solution for device enrollment, as their misuse or improper implementation may introduce a vulnerability that adversaries can exploit to register unauthorized devices.
EV1098.005-H4	The failure to enforce conditional access policies during the first enrollment of MFA, potentially allowing device registration from untrusted locations or devices and undermining the security measures intended to restrict access.

2.6.19 Account Manipulation: Additional Container Cluster Roles (T1098.006) **[54]**

EV Code	Vulnerability Description
EV1098.006-S1	Insufficient access controls, allowing the addition of roles or permissions to user accounts and unauthorized modifications in container orchestration systems
EV1098.006-H1	The failure to properly configure and monitor attribute-based access control (ABAC) policies in Kubernetes, enabling adversaries with sufficient permissions to manipulate access controls and grant additional privileges to targeted accounts.
EV1098.006-H2	The absence of multi-factor authentication for user accounts integrated into container clusters, allowing adversaries to potentially exploit accounts with single-factor authentication.
EV1098.006-H3	The failure to restrict low-privileged accounts from having the capability to add permissions to accounts or update container cluster roles, creating a potential avenue for unauthorized modifications and privilege escalation.

2.6.20 Boot or Logon Autostart Execution (T1547) [88]

EV Code	Vulnerability Description
EV1547-S1	The potential for misconfiguration or lack of proper access controls in the operating system, allowing adversaries to configure settings for automatic program execution during system boot or logon.

2.6.21 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) [89]

EV Code	Vulnerability Description
EV1547.001-S1	The presence of default run keys in Windows systems, such as HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, allows adversaries to achieve persistence by adding malicious programs, exploiting the system's reliance on these keys during startup.

2.6.22 Boot or Logon Autostart Execution: Authentication Package (T1547.002) [90]

EV Code	Vulnerability Description
EV1547.002-H1	The potential failure to enable the Protected Process Light (PPL) mode on Windows 8.1, Windows Server 2012 R2, and later versions, by neglecting to set the Registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL, which would allow unauthorized DLLs to be loaded by LSA.

2.6.23 Boot or Logon Autostart Execution: Time Providers (T1547.003) [91]

EV Code	Vulnerability Description
EV1547.003-H1	The potential mistake of not configuring Group Policy settings to block additions/modifications to W32Time DLLs, leaving the system exposed to unauthorized changes and manipulation by adversaries.

EV1547.003-H2	the potential mistake of not configuring Group Policy settings to block modifications to W32Time parameters in the Registry, allowing adversaries to tamper with critical time provider settings and compromise system security.

2.6.24 Boot or Logon Autostart Execution: Winlogon Helper DLL (T1547.004) [92]

EV Code	Vulnerability Description
EV1547.004-S1	The potential failure to implement effective execution prevention measures, allowing potentially malicious software to be executed through the Winlogon helper process, if application control tools like AppLocker are not properly configured or utilized.
EV1547.004-H1	The inadequate management of user accounts, specifically the failure to limit privileges, which may result in unauthorized users being able to perform Winlogon helper changes and potentially introduce malicious DLLs or executables during user logon.

2.6.25 Boot or Logon Autostart Execution: Security Support Provider (T1547.005) [93]

EV Code	Vulnerability Description
EV1547.005-S1	If the system is not configured to run the Local Security Authority (LSA) as a Protected Process Light (PPL) on Windows 8.1, Windows Server 2012 R2, and later versions, adversaries may still exploit the LSA process, potentially compromising the integrity of privileged processes.

2.6.26 Boot or Logon Autostart Execution: Kernel Modules and Extensions (T1547.006) [94]

EV Code	Vulnerability Description
EV1547.006-S1	The inherent security gap in macOS kernel extensions (kexts) arising from their exemption from macOS security policies, enabling adversaries to exploit them for persistence and privilege escalation, even with the introduction of System Extensions in macOS Catalina.

EV1547.006-S2	The potential weakness in antivirus/antimalware tools, as certain Linux rootkits may be designed to evade detection by common tools like rkhunter and chrootkit.
EV1547.006-S3	The susceptibility to kernel module loading due to inadequate execution prevention measures, where reliance solely on application control and software restriction tools may not provide comprehensive protection against all potential attacks.
EV1547.006-H1	The failure to adequately control and regulate the loading and unloading of kernel extensions (kexts) on macOS, as users without necessary privileges can sign kexts that may compromise system security, particularly when System Integrity Protection (SIP) is disabled.
EV1547.006-H2	The failure to upgrade to the latest macOS versions that deprecate kernel extensions (kexts) in favor of more secure System Extensions, leaving systems exposed to potential exploitation of legacy vulnerabilities.
EV1547.006-H3	The failure to implement proper privileged account management, allowing users to access the root account and load kernel modules, thereby increasing the risk of privilege escalation and unauthorized system modifications.
EV1547.006-H4	The inadequate management of user accounts, as the user's ability to install or approve kernel extensions is not effectively controlled through Mobile Device Management (MDM), potentially leading to the approval of malicious extensions and compromising system security.

2.6.27 Boot or Logon Autostart Execution: Re-opened Applications (T1547.007) **[95]**

EV Code	Vulnerability Description
EV1547.007-H1	The default configuration allowing the persistence feature, as it can be disabled through a terminal command, but may be overlooked, leaving the system susceptible to unauthorized autostart execution.

EV1547.007-H2	The failure to apply user training, specifically neglecting to hold the Shift key while logging in, which could result in unintentional execution of applications configured for autostart, even after the feature has been disabled, due to user oversight.

2.6.28 Boot or Logon Autostart Execution: LSASS Driver (T1547.008) **[96]**

EV Code	Vulnerability Description
EV1547.008-S1	The Windows security subsystem's weakness that allows adversaries to modify or add LSASS drivers, enabling them to achieve persistence on compromised systems.
EV1547.008-S2	Inadequate protection against credential access, as Windows 10 and Server 2016 may be susceptible if Windows Defender Credential Guard is not enabled, allowing lsass.exe to operate in a potentially compromised environment.
EV1547.008-S3	Lack of privileged process integrity on Windows 8.1 and Server 2012 R2, where not enabling LSA Protection by setting the Registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL to dword:00000001 could expose lsass.exe to potential compromise by loading unsigned and non-compliant LSA plug-ins and drivers.
EV1547.008-S4	Weakness in library loading security, specifically when safe DLL search mode is not enabled (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode), posing a risk of lsass.exe loading malicious code libraries.

2.6.29 Boot or Logon Autostart Execution: Shortcut Modification (T1547.009) **[97]**

EV Code	Vulnerability Description
EV1547.009-H1	The failure to properly configure group policies related to symbolic link creation, such as overlooking restrictions in GPO settings, leading to an increased risk of adversaries being able to exploit the autostart mechanism through shortcut modification.

2.6.30 Boot or Logon Autostart Execution: Port Monitors (T1547.010) [98]

EV Code	Vulnerability Description
EV1547.010-H1	The permission allowance for writing a fully-qualified pathname for an arbitrary DLL to HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors, enabling the loading of malicious code at startup.

2.6.31 Boot or Logon Autostart Execution: Print Processors (T1547.012) [99]

EV Code	Vulnerability Description
EV1547.012-S1	The print spooler service allows the installation of print processors with malicious DLLs during system boot, providing a potential avenue for persistence and privilege escalation.
EV1547.012-H1	Failing to limit user accounts that can load or unload device drivers by not disabling the SeLoadDriverPrivilege, providing an avenue for adversaries to abuse the print spooler service.

2.6.32 Boot or Logon Autostart Execution: XDG Autostart Entries (T1547.013) [100]

EV Code	Vulnerability Description
EV1547.013-S1	The lack of limitations on software installation, as unrestricted software installation may lead to the introduction of malicious packages, increasing the risk of compromise through the manipulation of XDG Autostart Entries.
EV1547.013-H1	The insufficient restriction of file and directory permissions, as inadequate controls on write access to XDG autostart entries may allow unauthorized users to manipulate these configurations, potentially enabling the execution of malicious programs during login.

EV1547.013-H2	The inadequate management of user accounts, as the failure to limit privileges on user accounts may result in unauthorized users creating or modifying XDG Autostart Entries, facilitating the establishment of persistence through the execution of malicious commands during user login.

2.6.33 Boot or Logon Autostart Execution: Active Setup (T1547.014) [101]

This attack technique does not rely on a specific vulnerability for execution.

2.6.34 Boot or Logon Autostart Execution: Login Items (T1547.015) [102]

EV Code	Vulnerability Description
EV1547.015-S1	Weaknesses in the Service Management Framework and shared file list methods, allowing for persistent and privileged execution.

2.6.35 Boot or Logon Initialization Scripts (T1037) [103]

EV Code	Vulnerability Description
EV1037-S1	The improper assignment of file and directory permissions, allowing unauthorized administrators or users to write to logon scripts, potentially leading to persistence.
EV1037-H1	The misconfiguration of registry permissions, which may enable users to modify registry keys associated with logon scripts, posing a risk of

2.6.36 Boot or Logon Initialization Scripts: Logon Script (Windows) (T1037.001) [104]

EV Code	Vulnerability Description
EV1037.001-S1	The potential weakness in the Windows registry configuration, specifically the HKCU\Environment\UserInitMprLogonScript Registry key, which allows the execution of logon scripts during initialization, providing an avenue for persistence.

EV1037.001-H1	The misconfiguration of registry permissions, which may enable users to modify registry keys associated with logon scripts, posing a risk of

2.6.37 Boot or Logon Initialization Scripts: Login Hook (T1037.002) [105]

EV Code	Vulnerability Description
EV1037.002-H1	The failure to restrict file and directory permissions appropriately, which can lead to unauthorized modifications of logon scripts by administrators, enabling the execution of malicious scripts upon user logon.

2.6.38 Boot or Logon Initialization Scripts: Network Logon Script (T1037.003) [106]

EV Code	Vulnerability Description
EV1037.003-H1	The failure to restrict file and directory permissions appropriately, which can lead to unauthorized modifications of logon scripts by administrators, enabling the execution of malicious scripts upon user logon.

2.6.39 Boot or Logon Initialization Scripts: RC Scripts (T1037.004) [107]

EV Code	Vulnerability Description
EV1037.004-S1	The reliance on deprecated RC scripts during startup, especially in lightweight Unix-like distributions with default root user access, such as IoT or embedded systems, and the failure to update or transition from deprecated RC scripts to modern alternatives like Systemd, leaving the system exposed to persistence methods using malicious binary paths or shell commands in RC scripts.
EV1037.004-H1	The failure to properly limit privileges of user accounts, enabling unauthorized individuals to edit critical files like rc.common and potentially facilitate persistence through the manipulation of startup scripts.

2.6.40 Boot or Logon Initialization Scripts: Startup Items (T1037.005) **[108]**

EV Code	Vulnerability Description
EV1037.005-S1	The potential existence of the deprecated /Library/StartupItems folder on macOS systems, which may still be present by default on macOS Sierra, providing an avenue for adversaries to establish persistence during the boot process.
EV1037.005-H1	Inadequate restriction of write permissions on the /Library/StartupItems directory, which could lead to the registration of unauthorized startup items, circumventing the mitigation strategy and allowing persistence.

2.6.41 Create or Modify System Process (T1543) **[155]**

EV Code	Vulnerability Description
EV1543-S1	Insufficient enforcement of software installation restrictions, posing a risk of allowing unauthorized or potentially malicious software installations from untrusted repositories.
EV1543-S2	The potential absence of properly configured Attack Surface Reduction (ASR) rules on Windows 10, which could permit applications to write signed vulnerable drivers to the system.
EV1543-S3	The lack of enabled Microsoft Vulnerable Driver Blocklist on Windows 10 and 11, leaving the system less resilient against third-party-developed drivers that may introduce vulnerabilities.
EV1543-H1	Inadequate auditing practices, potentially allowing privilege and service abuse opportunities to go undetected and uncorrected.
EV1543-H2	The failure to enforce the registration and execution of only legitimately signed service drivers, potentially leading to the acceptance of unsigned or malicious drivers.
EV1543-H3	The failure to ensure the enforcement of Driver Signature Enforcement, which could result in the installation of unsigned drivers, posing a potential security risk.

EV1543-H4	Inadequate restriction of read/write access to system-level process files, potentially allowing unauthorized users to manipulate critical system services.
EV1543-H5	Insufficient limitation of privileges for user accounts and groups, creating the risk that unauthorized individuals may interact with system-level process changes and service configurations.

2.6.42 Create or Modify System Process: Launch Agent (T1543.001) [156]

EV Code	Vulnerability Description
EV1543.001-H1	The failure to implement group policies to restrict file permissions in the ~/launchagents folder, leaving the system exposed to potential misuse by adversaries.

2.6.43 Create or Modify System Process: Systemd Service (T1543.002) [157]

EV Code	Vulnerability Description
EV1543.002-S1	The weaknesses in default initialization (init) system, systemd, which allows adversaries to create or modify services, leading to the repeated execution of malicious payloads and potential privilege escalation.
EV1543.002-H1	Inadequate software source control, as unrestricted software installation can lead to the introduction of malicious or unauthorized software packages, posing a security risk.
EV1543.002-H2	Insufficient control over privileged accounts, since the creation and modification of systemd service unit files, critical for system functionality, are not adequately restricted to authorized administrators, potentially allowing unauthorized manipulation.
EV1543.002-H3	Overly permissive file and directory permissions, as unrestricted read/write access to systemd unit files may enable unauthorized users to tamper with or disrupt critical system services.
EV1543.002-H4	Inappropriate user access management, as granting unnecessary access to system utilities like systemctl increases the attack surface and potential for misuse by users without a legitimate need.

2.6.44 Create or Modify System Process: Windows Service (T1543.003) [158]

EV Code	Vulnerability Description
EV1543.003-S1	Inadequate auditing configurations, potentially allowing privilege and service abuse opportunities to go undetected.
EV1543.003-S2	The lack of Attack Surface Reduction (ASR) rules enforcement on Windows 10, which may enable an application to write a signed vulnerable driver to the system.
EV1543.003-S3	The absence of Microsoft Vulnerable Driver Blocklist activation on Windows 10 and 11, leaving the system more susceptible to third-party-developed service drivers that could pose security risks.
EV1543.003-S4	The absence of enabled Driver Signature Enforcement, which could lead to the installation of unsigned drivers, compromising the system's integrity.
EV1543.003-H1	The failure to enforce the registration and execution of only legitimately signed service drivers, allowing for potential unauthorized or malicious drivers to be executed.
EV1543.003-H2	The failure to properly limit privileges, potentially leading to unauthorized users gaining access to service changes and configurations.

2.6.45 Create or Modify System Process: Launch Daemon (T1543.004) [159]

EV Code	Vulnerability Description
EV1543.004-S1	The poor configurations allowing globally writable folders (e.g., usr/local/bin), enabling the modification of executables referenced by current Launch Daemon's plist files.
EV1543.004-S2	The inadequate auditing practices, as the absence of effective auditing tools capable of detecting folder permissions abuse opportunities may allow malicious modifications to Launch Daemon executables to go unnoticed.

EV1543.004-H1	The failure to sufficiently limit privileges and remediate Privilege Escalation vectors, which could result in unauthorized users creating new Launch Daemons and compromising system integrity despite the recommended mitigation measures.

2.6.46 Domain Policy Modification (T1484) **[211]**

EV Code	Vulnerability Description
EV1484-H1	The inadequate auditing and correction of Group Policy Object (GPO) permissions abuse opportunities, allowing adversaries to potentially exploit GPO modification privileges undetected.
EV1484-H2	The creation of service accounts with administrative privileges on the Domain Controller and Active Directory Federation Services (AD FS) server, increasing the risk of unauthorized modifications to domain policy settings.
EV1484-H3	User grants adversaries sufficient permissions to modify domain policy settings, enabling them to execute malicious actions such as pushing a malicious Scheduled Task or modifying domain trusts to control access tokens in the domain environment.
EV1484-H4	The failure to implement additional controls like WMI and security filtering to tailor the application of GPOs, allowing adversaries to potentially manipulate GPO settings by exploiting broader application scenarios.

2.6.47 Domain Policy Modification: Group Policy Modification (T1484.001) **[212]**

EV Code	Vulnerability Description
EV1484.001-H1	Inadequate access control configuration on Group Policy Objects (GPOs), as default permissions grant all user accounts in the domain the ability to read GPOs, potentially leading to unauthorized modifications.

EV1484.001-H2	the failure to implement WMI and security filtering for GPOs, leading to a lack of tailored application of GPOs to specific users and computers, which could be exploited by adversaries seeking unauthorized modifications.

2.6.48 Domain Policy Modification: Domain Trust Modification (T1484.002) [213]

EV Code	Vulnerability Description
EV1484.002-H1	The failure to enforce the principle of least privilege in administrative access to domain trusts, potentially resulting in elevated access levels that could be exploited by adversaries seeking to manipulate trust properties.
EV1484.002-H2	Insufficient scrutiny of domain trust details, such as whether a domain is federated, potentially leading to oversight in recognizing and addressing unauthorized changes that could compromise authentication and authorization integrity.

2.6.49 Escape to Host (T1611) [232]

EV Code	Vulnerability Description
EV1611-S1	The lack of seccomp, seccomp-bpf, or similar solutions, allowing unrestricted system calls such as mount and increasing the risk of container breakout in Kubernetes environments.
EV1611-S2	The presence of unnecessary tools and software in containers, which can be exploited to facilitate unauthorized access or execution of malicious commands.
EV1611-S3	The absence of read-only containers, read-only file systems, and minimal images, potentially enabling the running of unauthorized commands within containers.
EV1611-H1	The use of containers running as root by default or with unnecessary privileges, increasing the likelihood of successful privilege escalation and unauthorized access to host resources in Kubernetes environments.

EV1611-H2	The failure to define and implement Pod Security Standards in Kubernetes environments, allowing the running of privileged containers and exposing the host to potential compromise.

2.6.50 Event Triggered Execution (T1546) [237]

EV Code	Vulnerability Description
EV1546-S1	The vulnerability in the operating system event monitoring, enabling adversaries to exploit subscribed events for unauthorized execution, leading to persistent access and privilege escalation.
EV1546-S2	The vulnerability in the cloud environment functions and services related to event monitoring, allowing adversaries to leverage specific cloud events for unauthorized execution, resulting in persistent access and privilege escalation.

2.6.51 Event Triggered Execution: Change Default File Association (T1546.001) [238]

EV Code	Vulnerability Description
EV1546.001-S1	The ability for users, administrators, or programs with Registry access to edit file associations, providing an opportunity for malicious changes and persistent execution of arbitrary programs by adversaries.

2.6.52 Event Triggered Execution: Screensaver (T1546.002) [239]

EV Code	Vulnerability Description
EV1546.002-S1	The insecure storage of screensaver settings in the Registry (HKCU\Control Panel\Desktop), allowing manipulation of SCRNSAVE.exe to a malicious PE path, enabling the execution of malware upon user inactivity.
EV1546.002-H1	User configure setting ScreenSaverIsSecure to '0', neglecting to require a password to unlock the screensaver, potentially compromising security when the screensaver is triggered by user inactivity.

EV1546.002-H2	The potential failure to disable screensavers through Group Policy, leaving unnecessary screensavers active and susceptible to manipulation for malicious purposes.
EV1546.002-H3	The failure to block .scr files from non-standard locations, allowing adversaries to potentially execute malicious screensavers if they are stored in unconventional directories.

2.6.53 Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003) [240]

EV Code	Vulnerability Description
EV1546.003-S1	Inadequate configuration of Windows 10, allowing the potential abuse of WMI for persistence, as Attack Surface Reduction (ASR) rules are not enabled.
EV1546.003-S2	Weak remote access controls on WMI, as by default, non-administrator users are allowed to connect remotely; proper restrictions are not in place.
EV1546.003-H1	Allowing credential overlap across systems for administrator and privileged accounts, potentially exposing sensitive credentials to compromise.
EV1546.003-H2	Failure to properly configure or enforce remote access policies for WMI, leading to an increased risk of unauthorized access and potential misuse by adversaries.

2.6.54 Event Triggered Execution: Unix Shell Configuration Modification (T1546.004) [241]

EV Code	Vulnerability Description
EV1546.004-H1	The failure to restrict file and directory permissions adequately, which could allow adversaries to modify crucial configuration files and establish user-level persistence on the system.

2.6.55 Event Triggered Execution: Trap (T1546.005) [242]

This attack technique does not rely on a specific vulnerability for execution.

2.6.56 Event Triggered Execution: LC_LOAD_DYLID Addition (T1546.006) [243]

EV Code	Vulnerability Description
EV1546.006-S1	The failure to adequately protect digital signatures on binaries, as removing the LC_CODE_SIGNATURE command to evade signature checks exposes the system to potential malicious alterations.
EV1546.006-S2	The potential lack of effective execution prevention, as allowing applications via known hashes may not prevent the execution of tampered binaries with modified Mach-O headers.
EV1546.006-S3	The potential lack of proper auditing practices, as failure to baseline binaries for required dynamic libraries may result in overlooking the addition of malicious libraries during updates.
EV1546.006-H1	Failure to enforce the correct Apple Developer IDs for all binaries may lead to the acceptance of unsigned or incorrectly signed binaries, compromising the system's integrity.

2.6.57 Event Triggered Execution: Netsh Helper DLL (T1546.007) [244]

EV Code	Vulnerability Description
EV1546.007-S1	The potential for arbitrary code execution through the Netsh Helper DLLs, exploiting weaknesses in the design of the netsh.exe utility and its extensibility mechanism.

2.6.58 Event Triggered Execution: Accessibility Features (T1546.008) [245]

EV Code	Vulnerability Description
EV1546.008-S1	The failure to adequately secure the accessibility feature binaries, such as C:\Windows\System32\sethc.exe and C:\Windows\System32\utilman.exe, which can be exploited by an adversary to gain unauthenticated access through actions like pressing the shift key five times or using the Windows + U key combination.
EV1546.008-S2	The susceptibility of Windows XP and later versions, as well as Windows Server 2003/R2 and later, to binary replacement attacks where a legitimate program (e.g., C:\Windows\System32\utilman.exe) may be replaced with a malicious one (e.g., "cmd.exe") for backdoor access.
EV1546.008-S3	The lack of protection measures, such as digital signatures and Windows File or Resource Protection, on replaced binaries, which are required for newer versions of Windows to prevent unauthorized execution.
EV1546.008-H1	The potential failure to implement effective application control tools (e.g., Windows Defender Application Control, AppLocker, or Software Restriction Policies), allowing the replacement of accessibility feature binaries with malicious alternatives for unauthorized execution.
EV1546.008-H2	The failure to configure and utilize a Remote Desktop Gateway, leaving RDP connections and security configurations vulnerable to exploitation through accessibility feature binaries.
EV1546.008-H3	The failure to enable Network Level Authentication (NLA) on remote desktop sessions, potentially allowing adversaries to exploit accessibility features through RDP without proper authentication.

2.6.59 Event Triggered Execution: AppCert DLLs (T1546.009) [246]

EV Code	Vulnerability Description
EV1546.009-H1	The failure to properly configure and maintain application control tools (e.g., Windows Defender Application Control, AppLocker, or Software Restriction Policies), allowing adversaries to evade detection and successfully execute malicious AppCertDLL binaries.

2.6.60 Event Triggered Execution: AppInit DLLs (T1546.010) [247]

EV Code	Vulnerability Description
EV1546.010-S1	The persistence mechanism provided by AppInit DLLs, which, when triggered by API activity, can continuously execute malicious code, exploiting a weakness in the Windows operating system's design.
EV1546.010-H1	The potential for ineffective execution prevention, as adversaries can still install new AppInit DLL binaries, bypassing application control tools like Windows Defender Application Control, AppLocker, or Software Restriction Policies if not appropriately configured or monitored.
EV1546.010-H2	The failure to update software, leaving systems vulnerable to this technique; upgrading to Windows 8 or later and enabling secure boot is crucial for mitigating the risk associated with AppInit DLLs, and neglecting this update could expose the system to exploitation.

2.6.61 Event Triggered Execution: Application Shimming (T1546.011) [248]

EV Code	Vulnerability Description
EV1546.011-S1	The Windows Application Compatibility Infrastructure/Framework (Application Shim) allowing certain shims (e.g., Bypass User Account Control, RedirectEXE, InjectDLL, DisableNX, DisableSEH, GetProcAddress) to be used for malicious purposes.

EV1546.011-S2	The presence of the "auto-elevate" flag within the sdbinst.exe, which, if not addressed by applying the optional patch update (KB3045645), allows for potential misuse of application shimming to bypass User Account Control (UAC).
EV1546.011-H1	User opts not to change UAC settings to "Always Notify" due to the inconvenience of frequent notifications, leaving systems more susceptible to unauthorized elevation of privileges through application shimming.

2.6.62 *Event Triggered Execution: Image File Execution Options Injection (T1546.012)* [249]

EV Code	Vulnerability Description
EV1546.012-S1	The misconfiguration of IFEO via Registry settings, including both direct modifications and the use of Global Flags, which can lead to unintended privilege escalation and persistent execution of malicious code.
EV1546.012-S2	The configuration of "cmd.exe" or another backdoor program as a "debugger" for an accessibility program through Registry key modification, leading to unauthorized execution with SYSTEM privileges by triggering the specified program at the login screen.

2.6.63 *Event Triggered Execution: PowerShell Profile (T1546.013)* [250]

EV Code	Vulnerability Description
EV1546.013-S1	The lack of enforcement in code signing for PowerShell scripts, allowing the execution of unsigned scripts and potential compromise.
EV1546.013-H1	The lack of proper configuration to restrict file and directory permissions on PowerShell profiles, allowing unauthorized modifications and persistence by adversaries.
EV1546.013-H2	The inappropriate use of PowerShell profiles when not needed and the failure to consistently use the -NoProfile flag when executing scripts remotely, exposing the system to unnecessary risks of customization and potential exploitation.

2.6.64 Event Triggered Execution: Emond (T1546.014) **[251]**

EV Code	Vulnerability Description
EV1546.014-H1	The potential failure to disable or remove the emond feature, as adversaries could exploit its presence and associated Launch Daemon plist file to execute malicious content, gain persistence, and potentially escalate privileges.

2.6.65 Event Triggered Execution: Component Object Model Hijacking (T1546.015) **[252]**

EV Code	Vulnerability Description
EV1546.015-H1	Inadequate monitoring and control over changes to the Registry, enabling adversaries to modify references to legitimate system components without detection, leading to the execution of malicious code during normal system operation.

2.6.66 Event Triggered Execution: Installer Packages (T1546.016) **[253]**

EV Code	Vulnerability Description
EV1546.016-H1	The granting of administrative permissions to installer packages during the installation of applications, facilitating the execution of malicious content by adversaries.

2.6.67 Exploitation for Privilege Escalation (T1068) **[274]**

EV Code	Vulnerability Description
EV1068-S1	Exploitable software vulnerabilities in operating system components and higher-privileged software, allowing adversaries to elevate privileges and execute adversary-controlled code.
EV1068-S2	Lack of robust application isolation and sandboxing, which may expose the system to exploitation of undiscovered or unpatched vulnerabilities, allowing adversaries to advance their operations.

EV1068-S3	The Absence of execution prevention measures for known vulnerable drivers, enabling adversaries to exploit these drivers to execute code in kernel mode, posing a risk to system stability.
EV1068-S4	The absence of a robust cyber threat intelligence program, hindering the organization's ability to proactively identify and address potential threats that may use software exploits and 0-days.
EV1068-S5	The lack of control flow integrity checking, potentially allowing adversaries to successfully execute software exploits for privilege escalation.
EV1068-S6	The potential incompatibility of security applications like Windows Defender Exploit Guard and Enhanced Mitigation Experience Toolkit with certain architectures and target application binaries, limiting their effectiveness for privilege escalation protection.
EV1068-H1	The failure to regularly update software, leaving the system exposed to potential exploitation of undiscovered or unpatched vulnerabilities.
EV1068-H2	Inadequate validation of driver block rules, posing a risk of destabilizing the system if not thoroughly tested in audit mode before production deployment.

2.6.68 Hijack Execution Flow (T1574) **[323]**

EV Code	Vulnerability Description
EV1574-S1	Inadequate control and protection of locations where the operating system looks for programs/resources, such as file directories and the Windows Registry, which could be manipulated by adversaries to include malicious payloads.
EV1574-S2	The absence of hash values in manifest files, allowing for potential side-loading of malicious libraries, which could compromise the integrity of program execution.
EV1574-S3	Inadequate auditing configurations, allowing the adversary to exploit hijacking opportunities on systems within the enterprise.
EV1574-S4	Manifest files with side-loading vulnerabilities, as they may be exploited by adversaries to compromise the integrity of software.

EV1574-S5	Path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and shortcuts, which could be exploited to execute or load malicious binaries.
EV1574-S6	Lingering Windows Registry keys from uninstalled software, providing opportunities for adversaries to exploit keys with no associated legitimate binaries.
EV1574-S7	Inadequate configuration of endpoint security solutions, which may allow adversaries to bypass behavior prevention measures and successfully execute process injection or memory tampering.
EV1574-S8	Insufficient application control solutions, leading to the potential execution of malicious software through payload hijacking and exploitation of libraries loaded by legitimate software.
EV1574-S9	Insecure file and directory permissions, as the absence of write protection in software installation locations and inadequate access controls on directories could enable unauthorized file writes in critical application and library folders.
EV1574-S10	Inadequate restriction of library loading, which could lead to the loading of malicious or unauthorized DLLs, compromising system integrity.
EV1574-S11	Improper registry permissions, which may allow unauthorized modification of keys, leading to potential privilege escalation.
EV1574-H1	Failure to use quotation marks around PATH variables in configurations, scripts, or shortcuts, potentially exposing the system to path interception attacks.
EV1574-H2	User Neglects to use fully qualified paths wherever appropriate, leaving the system susceptible to the search order Windows uses for executing or loading binaries.
EV1574-H3	User overlooks the need to periodically search for and address path interception weaknesses introduced by custom or available tools, potentially leaving the system exposed to insecure path configurations.

EV1574-H4	The failure to enable Safe DLL Search Mode, exposing the system to the risk of loading DLLs from less secure directories before searching in system directories, potentially allowing for the execution of malicious code.
EV1574-H5	Inadequate software updates, exposing the system to known DLL side-loading vulnerabilities and increasing the risk of exploitation by attackers.
EV1574-H6	Failure to turn off UAC's privilege elevation for standard users ("ConsentPromptBehaviorUser"=dword:00000000) may expose the system to unauthorized privilege elevation, allowing attackers to execute malicious actions without user consent.
EV1574-H7	Failure to enable installer detection ("EnableInstallerDetection"=dword:00000001) for all users can result in a lack of password prompts during installation, potentially facilitating unauthorized installations and compromising the system's security.
EV1574-H8	Insufficient privilege management, as unauthorized users may gain access to service changes and binary target path locations if privileges are not adequately limited.
EV1574-H9	Inadequate enforcement of proper permissions and directory access controls, potentially allowing users to write files to critical directories, such as C:\ and C:\Windows, leading to an increased risk of malicious file execution.

2.6.69 Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) [324]

EV Code	Vulnerability Description
EV1574.001-S1	Weakness in DLL search order, allowing adversaries to hijack the loading of DLLs and execute malicious payloads, potentially leading to unauthorized persistence, privilege escalation, and evasion of file execution restrictions.
EV1574.001-S2	The absence of proactive auditing practices, as enterprises may overlook DLL search order hijacking opportunities without utilizing tools like the PowerSploit framework or sxstrace.exe to detect and correct these weaknesses.

EV1574.001-S3	Failure to disallow loading of remote DLLs, especially on systems running versions prior to Windows Server 2012 or those that have not been patched, which may expose the system to DLL search order hijacking vulnerabilities.
EV1574.001-H1	The failure to implement and enforce application control solutions capable of blocking DLLs loaded by legitimate software, allowing potentially malicious DLLs to be executed through search order hijacking.
EV1574.001-H2	Misconfiguring the Safe DLL Search Mode settings, as incorrect Group Policy configurations or alterations to the Windows Registry key (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode) could compromise the intended security measures.

2.6.70 Hijack Execution Flow: DLL Side-Loading (T1574.002) **[325]**

EV Code	Vulnerability Description
EV1574.002-S1	DLL search order used by the loader, which can be exploited through side-loading by positioning both the victim application and malicious payload alongside each other.
EV1574.002-S2	The absence of hash values in manifest files, potentially allowing for the side-loading of malicious libraries due to a lack of integrity verification.
EV1574.002-H1	The failure to regularly update software, leading to the persistence of DLL side-loading vulnerabilities and an increased risk of exploitation.

2.6.71 Hijack Execution Flow: Dylib Hijacking (T1574.004) **[326]**

EV Code	Vulnerability Description
EV1574.004-S1	The sequential order of search paths for dynamic libraries in macOS, which allows adversaries to exploit the system's search mechanism and execute malicious code by placing a dylib with an expected name in a victim application's runtime path.

EV1574.004-S2	The use of weak linking, such as the LC_LOAD_WEAK_DYLIB function, which enables adversaries to execute an application even if the expected dylib is not present, potentially leading to unintended execution of malicious code.
EV1574.004-H1	Inadequate file and directory permissions, allowing potential unauthorized write access, which can lead to unauthorized modifications or deletions of critical files, compromising system integrity.

2.6.72 Hijack Execution Flow: Executable Installer File Permissions Weakness (T1574.005) **[327]**

EV Code	Vulnerability Description
EV1574.005-S1	Improper file system and binary permissions on the executable installer, allowing the adversary to overwrite legitimate binaries with malicious ones, potentially leading to code execution at a higher permissions level, including SYSTEM.
EV1574.005-S2	The lack of effective implementation of auditing tools, as the absence of tools capable of detecting file system permissions abuse opportunities may result in inadequate identification and correction of vulnerabilities in systems within an enterprise.
EV1574.005-H1	Inadequate permission settings on subdirectories and files created during the installation process, specifically within the %TEMP% directory, enabling the execution of untrusted code and the potential overwriting of binaries, leading to privilege escalation and code execution at elevated permissions.
EV1574.005-H2	Improper configuration of User Account Control (UAC), as failure to disable UAC's privilege elevation for standard users and appropriately configure installer detection may lead to unauthorized privilege escalation and undocumented installation attempts, potentially compromising system security.

EV1574.005-H3	Insufficient user account management practices, as the failure to appropriately limit privileges of user accounts and groups, especially in relation to service changes and service binary target path locations, may expose systems to unauthorized interactions and executions, potentially leading to privilege escalation and unauthorized code execution.

2.6.73 Hijack Execution Flow: Dynamic Linker Hijacking (T1574.006) **[328]**

EV Code	Vulnerability Description
EV1574.006-S1	The potential failure to implement effective execution prevention measures, allowing adversaries to use new payloads and execute dynamic linker hijacking attacks if application control solutions are not properly configured or lack the capability to block malicious software effectively.
EV1574.006-H1	The failure to enable or properly configure System Integrity Protection (SIP) on macOS systems, leaving the environment variables susceptible to exploitation; neglecting SIP increases the risk of dynamic linker hijacking.
EV1574.006-H2	The inadequate application of security measures, such as not leveraging Apple's Hardened Runtime or imposing restrictions on applications; this allows adversaries to exploit environment variables and conduct dynamic linker hijacking on macOS systems.

2.6.74 Hijack Execution Flow: Path Interception by PATH Environment Variable (T1574.007) **[329]**

EV Code	Vulnerability Description
EV1574.007-S1	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.007-S2	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.

EV1574.007-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.007-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.6.75 Hijack Execution Flow: Path Interception by Search Order Hijacking (T1574.008) [330]

EV Code	Vulnerability Description
EV1574.008-S1	The lack of explicit path specification in some programs, allowing adversaries to perform Search Order Hijacking and execute their malicious payloads by placing files in the directory where the calling program is located.
EV1574.008-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.008-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.008-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.008-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.6.76 Hijack Execution Flow: Path Interception by Unquoted Path (T1574.009) [331]

EV Code	Vulnerability Description
EV1574.009-S1	The lack of proper quoting in file paths, allowing for path interception and execution of malicious payloads by placing executables in higher-level directories.
EV1574.009-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.009-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.009-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.009-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.6.77 Hijack Execution Flow: Services File Permissions Weakness (T1574.010) [332]

EV Code	Vulnerability Description
EV1574.010-S1	Flaws in Windows service file permissions, which allow the replacement of legitimate binaries, leading to the execution of malicious payloads with potentially elevated permissions, including SYSTEM.
EV1574.010-S2	Lack of auditing tools capable of detecting file system permissions abuse opportunities, allowing adversaries to exploit weaknesses in service file permissions.
EV1574.010-H1	Improperly setting permissions on the file system directory containing the target binary or on the binary itself, enabling adversaries to overwrite the target binary with a malicious one using user-level permissions.

EV1574.010-H2	Failure to turn off User Account Control's (UAC) privilege elevation for standard users or properly configure UAC settings, potentially allowing elevation of privileges through exploitation during the UAC detection process.
EV1574.010-H3	Allowing execution from user directories, file download directories, and temp directories, potentially providing adversaries with the ability to exploit service binary vulnerabilities and execute malicious code.

2.6.78 Hijack Execution Flow: Services Registry Permissions Weakness (T1574.011) [333]

EV Code	Vulnerability Description
EV1574.011-S1	The weakness in Registry permissions for service-related keys (HKLM\SYSTEM\CurrentControlSet\Services), allowing unauthorized modification of a service's execution parameters, potentially leading to the execution of adversary-controlled code during service startup.
EV1574.011-H1	The failure to set appropriate access controls for the service's Registry keys, allowing adversaries to manipulate keys such as FailureCommand or create custom subkeys, facilitating elevated execution and persistence.
EV1574.011-H2	The lack of proper access controls on the Performance key, enabling adversaries to create or modify it to point to a malicious DLL, potentially leading to the execution of adversary-controlled code during the operation of a driver service.
EV1574.011-H3	The failure to set proper access controls on the Parameters key or custom subkeys, allowing adversaries to add malicious data, establish persistence, or enable other malicious activities associated with their services.
EV1574.011-H4	The failure to secure the service's file identification process using HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll, potentially leading to misidentification of the service's file when launched through svchost.exe.

2.6.79 Hijack Execution Flow: COR_PROFILER (T1574.012) [334]

EV Code	Vulnerability Description
EV1574.012-S1	Insufficient control over DLL execution, as the system lacks robust mechanisms to identify and block potentially malicious unmanaged COR_PROFILER profiling DLLs.
EV1574.012-S2	Inadequate registry permission management, leaving the system exposed to potential modifications of keys associated with COR_PROFILER due to improper permissions on Registry hives.
EV1574.012-H1	Mismanagement of user privileges, allowing unauthorized individuals to edit system environment variables and potentially compromise the system's security.

2.6.80 Hijack Execution Flow: KernelCallbackTable (T1574.013) [335]

EV Code	Vulnerability Description
EV1574.013-S1	The vulnerability in the initialization process of the KernelCallbackTable within the Process Environment Block (PEB), which can be exploited to hijack the execution flow of a process.
EV1574.013-S2	Potential weaknesses in the endpoint security solution's configuration that may allow the adversary to evade behavior prevention mechanisms, specifically related to blocking process injection and memory tampering behaviors.
EV1574.013-H1	Allowing unauthorized access to the Process Environment Block (PEB) memory, potentially through inadequate access controls or permissions, enabling the adversary to obtain a pointer to the KernelCallbackTable.

2.6.81 Process Injection (T1055) **[479]**

EV Code	Vulnerability Description
EV1055-S1	The susceptibility to code injection, enabling unauthorized access to a process's memory, system/network resources, and potential elevation of privileges, thereby compromising the integrity of the system.
EV1055-S2	Inadequate configuration of endpoint security solutions, allowing for the bypassing of behavior prevention measures and enabling certain types of process injection.
EV1055-H1	The failure to implement robust privileged account management practices, such as not utilizing Yama or similar controls effectively, leading to the exploitation of ptrace-based process injection by non-privileged users.

2.6.82 Process Injection: Dynamic-link Library Injection (T1055.001) **[480]**

EV Code	Vulnerability Description
EV1055.001-S1	Weaknesses in memory management and specific Windows API functions, namely VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread. This creates an avenue for arbitrary code execution through DLL injection, thereby enabling unauthorized access, data compromise, or privilege escalation.
EV1055.001-H1	The possibility of misconfiguring or underutilizing endpoint security solutions, which could result in inadequate protection against process injection techniques, leading to the compromise of system integrity and data.

2.6.83 Process Injection: Portable Executable Injection (T1055.002) **[481]**

EV Code	Vulnerability Description
EV1055.002-S1	The susceptibility to code injection due to insufficient process-based defenses, allowing adversaries to inject portable executables (PE) into processes.

EV1055.002-S2	The potential misconfiguration or inadequacy of endpoint security solutions, allowing certain types of process injection to bypass behavior prevention measures.

2.6.84 Process Injection: Thread Execution Hijacking (T1055.003) [482]

EV Code	Vulnerability Description
EV1055.003-S1	The susceptibility of processes to Thread Execution Hijacking, which allows the injection of malicious code into existing processes, potentially leading to unauthorized access, memory compromise, and evasion of process-based defenses.
EV1055.003-H1	The potential reliance on endpoint security solutions alone, which, if improperly configured or not regularly updated, may fail to effectively block all types of process injection techniques, including Thread Execution Hijacking.

2.6.85 Process Injection: Asynchronous Procedure Call (T1055.004) [483]

EV Code	Vulnerability Description
EV1055.004-S1	The susceptibility of the Windows operating system to process injection through the asynchronous procedure call (APC) queue, enabling unauthorized code execution in the context of another process.
EV1055.004-S2	The potential inadequacy of endpoint security solutions configured to block process injection, as certain injection methods may evade detection due to variations in behavior, leading to a false sense of security.

2.6.86 Process Injection: Thread Local Storage (T1055.005) [484]

EV Code	Vulnerability Description
EV1055.005-S1	The potential inadequacy of endpoint security solutions configured to block process injection, as certain injection methods may evade detection due to variations in behavior, leading to a false sense of security.

2.6.87 Process Injection: Ptrace System Calls (T1055.008) [485]

EV Code	Vulnerability Description
EV1055.008-S1	The potential lack of configuration or ineffective deployment of endpoint security solutions, allowing process injection based on common sequences of behavior to bypass behavioral prevention measures.
EV1055.008-S2	The potential misconfiguration or lack of implementation of Yama (e.g., /proc/sys/kernel/yama/ptrace_scope), which could lead to unauthorized use of ptrace by non-privileged users for process injection.
EV1055.008-H1	The inadequate deployment of advanced access control and process restriction mechanisms such as SELinux, grsecurity, and AppArmor, which could allow adversaries to exploit process injection techniques by circumventing these security controls.

2.6.88 Process Injection: Proc Memory (T1055.009) [486]

EV Code	Vulnerability Description
EV1055.009-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.
EV1055.009-S2	Inadequate restriction of file and directory permissions, specifically on critical files such as /proc/[pid]/maps or /proc/[pid]/mem, potentially enabling unauthorized access and manipulation by adversaries.

2.6.89 Process Injection: Extra Window Memory Injection (T1055.011) [487]

EV Code	Vulnerability Description
EV1055.011-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.6.90 Process Injection: Process Hollowing (T1055.012) [488]

EV Code	Vulnerability Description
EV1055.012-S1	The susceptibility of processes to process hollowing, exploiting the ability to create a process in a suspended state and subsequently unmapping its memory, allowing the injection of malicious code undetected.
EV1055.012-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.6.91 Process Injection: Process Doppelganging (T1055.013) [489]

EV Code	Vulnerability Description
EV1055.013-S1	The reliance on Windows Transactional NTFS (TxF) in the system, introduced in Vista and still enabled as of Windows 10, allows adversaries to abuse TxF for a file-less variation of Process Injection, potentially evading detection and defenses.
EV1055.013-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.6.92 Process Injection: VDSO Hijacking (T1055.014) [490]

EV Code	Vulnerability Description
EV1055.014-S1	The potential weakness in memory protections, allowing the injection of malicious code into processes through VDSO hijacking, potentially evading process-based defenses and enabling privilege escalation.
EV1055.014-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.6.93 Process Injection: ListPlanting (T1055.015) [491]

EV Code	Vulnerability Description
EV1055.015-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.6.94 Scheduled Task/Job (T1053) [518]

EV Code	Vulnerability Description
EV1053-S1	The potential permission weaknesses in scheduled tasks, allowing adversaries to exploit and escalate privileges.
EV1053-H1	The failure to configure settings for scheduled tasks to force them to run under the context of the authenticated account instead of allowing them to run as SYSTEM, creating a potential avenue for privilege escalation.
EV1053-H2	The failure to restrict the Increase Scheduling Priority option to only allow the Administrators group the rights to schedule a priority process, potentially enabling unauthorized users to manipulate task scheduling priorities.
EV1053-H3	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, allowing unauthorized administrators to create scheduled tasks on remote systems.

2.6.95 Scheduled Task/Job: At (T1053.002) [519]

EV Code	Vulnerability Description
EV1053.002-S1	The misconfiguration of the at.allow and at.deny files on Linux and macOS, as adversaries can exploit this to invoke the at utility, potentially leading to unauthorized task scheduling.
EV1053.002-S2	The potential misconfiguration of scheduled tasks in Windows environments, as they may run with elevated privileges, allowing adversaries to exploit permission weaknesses and escalate privileges.
EV1053.002-H1	The misconfiguration of scheduled tasks in Windows environments, where tasks are allowed to run as SYSTEM, creating a potential avenue for privilege escalation if not properly configured to run under the context of the authenticated account.
EV1053.002-H2	The potential misconfiguration of the Increase Scheduling Priority option in Windows environments, as it could allow non-administrative users to schedule priority processes, leading to potential abuse.
EV1053.002-H3	The mismanagement of user account privileges in Linux environments, specifically related to the at utility, where users listed in the at.deny file may not be properly restricted from invoking the at utility, potentially leading to unauthorized task scheduling.

2.6.96 Scheduled Task/Job: Cron (T1053.003) [520]

EV Code	Vulnerability Description
EV1053.003-H1	The absence of regular auditing for changes to the cron schedule, potentially allowing undetected malicious scheduling.
EV1053.003-H2	Inadequate management of cron permissions through /etc/cron.allow and /etc/cron.deny, which may result in unauthorized users gaining cron access or superfluous restrictions, impacting proper system functioning.

2.6.97 Scheduled Task/Job: Scheduled Task (T1053.005) [521]

EV Code	Vulnerability Description
EV1053.005-S1	The potential permission weaknesses in scheduled tasks, which may be exploited to escalate privileges, as highlighted by the PowerSploit framework's PowerUp modules.
EV1053.005-S2	The insufficient restriction of the Increase Scheduling Priority option, potentially allowing non-administrative users to schedule a priority process, which can be mitigated by configuring GPO settings to restrict this privilege to the Administrators group.
EV1053.005-H1	The misconfiguration of scheduled task settings, allowing tasks to run as SYSTEM, which can be mitigated by configuring settings to force tasks to run under the context of the authenticated account and adjusting associated Registry keys and Group Policy Objects (GPO).
EV1053.005-H2	The failure to limit the privileges of user accounts and remediate Privilege Escalation vectors, leading to unauthorized creation of scheduled tasks on remote systems; this can be addressed by appropriately limiting user privileges and addressing Privilege Escalation vectors through effective User Account Management.

2.6.98 Scheduled Task/Job: Systemd Timers (T1053.006) [522]

EV Code	Vulnerability Description
EV1053.006-H1	The improper implementation of privileged account management, as failure to limit access to the root account may result in unauthorized creation or modification of systemd timer unit files by users.
EV1053.006-H2	User insufficiently restricts file and directory permissions, as failure to limit access to systemd .timer unit files may allow unauthorized users to read or modify them, potentially leading to the execution of malicious code.
EV1053.006-H3	Inadequate user account management, as failure to restrict user access to system utilities may result in unauthorized use of 'systemctl' or 'systemd-run' by users, facilitating the abuse of systemd timers for malicious purposes.

2.6.99 Scheduled Task/Job: Container Orchestration Job (T1053.007) [523]

EV Code	Vulnerability Description
EV1053.007-S1	The potential for containers to run with root privileges by default, creating a security weakness that can be exploited for malicious activities.
EV1053.007-H1	User misconfigures or allows unauthorized access to CronJobs within Kubernetes, enabling the scheduling of jobs that execute malicious code in various nodes within a cluster.
EV1053.007-H2	The improper configuration and lack of adherence to Pod Security Standards in Kubernetes environments, allowing containers to run as privileged, which undermines the intended security measures and facilitates unauthorized activities.

2.6.100 Valid Accounts (T1078) [636]

EV Code	Vulnerability Description
EV1078-S1	The potential lack of proper configuration and monitoring of conditional access policies, allowing non-compliant devices or logins from outside defined organization IP ranges.
EV1078-H1	The use of legacy authentication in Active Directory, which does not support multi-factor authentication (MFA), and the failure to enforce the use of modern authentication protocols.
EV1078-H2	The insecure storage of sensitive data or credentials in applications, such as storing plaintext credentials in code, publishing credentials in repositories, or leaving credentials in public cloud storage, providing opportunities for adversaries to compromise credentials.
EV1078-H3	The failure to promptly change default usernames and passwords on applications and appliances after installation, potentially leaving systems exposed to credential abuse.
EV1078-H4	The potential lack of routine audits of domain and local accounts, their permission levels, and the failure to detect situations that could allow adversaries to gain wide access by obtaining credentials of privileged accounts.

EV1078-H5	The failure to regularly audit user accounts for activity and deactivate or remove unnecessary accounts, increasing the risk of adversaries exploiting unused accounts for unauthorized access.
EV1078-H6	The lack of awareness and training regarding multi-factor authentication (MFA) push notifications, potentially leading users to accept and authenticate malicious notifications, compromising account security.

2.6.101 Valid Accounts: Default Accounts (T1078.001) [637]

EV Code	Vulnerability Description
EV1078.001-H1	The presence of default accounts with unchanged credentials, such as Guest or Administrator accounts on Windows systems, which can be exploited for Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.001-H2	The failure to change preset usernames and passwords for equipment like network devices and computer applications, including internal, open source, or commercial systems, which poses a serious threat if not altered post-installation.

2.6.102 Valid Accounts: Domain Accounts (T1078.002) [638]

EV Code	Vulnerability Description
EV1078.002-S1	Lack of multi-factor authentication (MFA) implementation, potentially allowing adversaries to gain control of valid credentials.
EV1078.002-S2	Poor design and administration of the enterprise network, potentially leading to the inappropriate inclusion of user or admin domain accounts in local administrator groups across systems, creating a security risk equivalent to having a common local administrator account password.
EV1078.002-H1	Password reuse, which can be exploited by adversaries to compromise domain accounts, posing a risk to Initial Access, Persistence, Privilege Escalation, or Defense Evasion.

EV1078.002-H2	Inadequate privileged account management, including the lack of routine audits on domain account permission levels, which could enable adversaries to exploit overly permissive access and compromise privileged accounts.
EV1078.002-H3	Insufficient user training on recognizing valid push notifications for multi-factor authentication, increasing the risk of users accepting fraudulent notifications and compromising the effectiveness of MFA.
EV1078.002-H4	Weak password management practices, resulting in credential overlap across systems and increasing the risk of unauthorized access if an adversary obtains account credentials.

2.6.103 Valid Accounts: Local Accounts (T1078.003) [639]

EV Code	Vulnerability Description
EV1078.003-H1	The inadequate enforcement of complex, unique passwords for local administrator accounts across all systems, potentially allowing unauthorized access.
EV1078.003-H2	The reuse of passwords for local accounts, enabling adversaries to abuse credentials across multiple machines on a network, facilitating Privilege Escalation and Lateral Movement.
EV1078.003-H3	The inadequate management of privileged accounts, as routine audits may be neglected, leading to situations where adversaries can exploit credentials of privileged accounts with wide access.
EV1078.003-H4	The improper use of local administrator accounts for day-to-day operations may expose user to potential adversaries, posing a security risk.

2.6.104 Valid Accounts: Cloud Accounts (T1078.004) [640]

EV Code	Vulnerability Description
EV1078.004-S1	The absence of multi-factor authentication for cloud accounts, especially privileged accounts, which could leave accounts susceptible to unauthorized access.

EV1078.004-S2	The potential for misconfigurations in conditional access policies, allowing logins from non-compliant devices or outside defined organization IP ranges.
EV1078.004-H1	Misconfigurations in role assignments or role assumption policies within cloud environments, enabling unauthorized access and privilege escalation.
EV1078.004-H2	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H3	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H4	The lack of enforcement of complex, unique passwords across all systems on the network, particularly for privileged cloud accounts, potentially allowing adversaries to exploit compromised credentials.
EV1078.004-H5	The inadequate review of privileged cloud account permission levels, which may result in the presence of high-risk roles such as Global Administrator and Privileged Role Administrator, providing adversaries with extensive access.
EV1078.004-H6	The failure to periodically review and remove inactive or unnecessary user accounts, potentially leaving dormant accounts that could be exploited by adversaries.
EV1078.004-H7	The potential for users to accept and act on invalid push notifications for multi-factor authentication, highlighting the importance of training users to recognize and report suspicious push notifications.

2.7 Defense Evasion (TA0005) [10]

2.7.1 Abuse Elevation Control Mechanism (T1548) [30]

EV Code	Vulnerability Description
EV1548-S1	Misconfiguration of setuid and setgid bits on applications with known vulnerabilities or shell escapes, potentially allowing adversaries to compromise the system.
EV1548-S2	Suboptimal User Account Control (UAC) enforcement, providing opportunities for UAC bypass techniques and DLL Search Order Hijacking.
EV1548-H1	The failure to appropriately configure and manage authorization, leading to the potential for adversaries to exploit and elevate privileges on the system.
EV1548-H2	Inadequate auditing practices, potentially allowing attackers to exploit common User Account Control (UAC) bypass weaknesses on Windows systems.
EV1548-H3	Failure to implement proper execution prevention measures, such as allowing applications from only legitimate repositories or restricting the execution of unsigned applications, which could expose the system to increased risk.
EV1548-H4	Retaining unnecessary users in the local administrator group, creating opportunities for adversaries to exploit privileged accounts and escalate privileges.
EV1548-H5	Improper configuration of the sudoers file, including not strictly requiring passwords or allowing users to spawn risky processes with higher privileges, potentially enabling unauthorized activities.
EV1548-H6	Granting excessive privileges to cloud accounts, increasing the risk of unauthorized access and privilege escalation in cloud environments.
EV1548-H7	Failure to enforce just-in-time access with manual approval for temporary elevation of privileges, potentially allowing unauthorized elevation of permissions.

2.7.2 *Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001)* [31]

EV Code	Vulnerability Description
EV1548.001-H1	The improper application of setuid and setgid flags to their own applications using the chmod command, enabling the user to execute programs in elevated contexts without the necessary privileges and bypassing execution environment restrictions.
EV1548.001-H2	The failure to properly configure applications, as not removing setuid or setgid bits from programs with known vulnerabilities or shell escapes could result in an increased attack surface and potential compromise of the system.

2.7.3 *Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002)* [32]

EV Code	Vulnerability Description
EV1548.002-S1	Due to a UAC protection level set below the highest, certain Windows programs may elevate privileges or execute elevated Component Object Model objects without triggering a user prompt.
EV1548.002-S2	The potential for common UAC bypass weaknesses on Windows systems, which may be overlooked during audits, leading to an unaware risk posture.
EV1548.002-S3	The potential suboptimal enforcement level for UAC, which may allow for the exploitation of UAC bypass techniques and unauthorized access to the system.
EV1548.002-H1	The inclusion of unnecessary users in the local administrator group on systems, increasing the risk of privilege abuse and compromise.
EV1548.002-H2	The outdated Windows version and patch level, which can be exploited to bypass UAC and compromise the system.

2.7.4 *Abuse Elevation Control Mechanism: Sudo and Sudo Caching (T1548.003)* [33]

EV Code	Vulnerability Description
EV1548.003-S1	Inadequate configuration of the tty_tickets setting, allowing potential leakage across tty sessions, compromising the security of the operating system.
EV1548.003-H1	The absence of a password requirement for executing commands in the sudoers file, making it easier for adversaries who gain terminal access to execute privileged commands without authentication.
EV1548.003-H2	The failure to strictly edit the sudoers file to always require passwords and prevent users from spawning risky processes, leaving the system exposed to potential misuse or unauthorized access.

2.7.5 *Abuse Elevation Control Mechanism: Elevated Execution with Prompt (T1548.004)* [34]

EV Code	Vulnerability Description
EV1548.004-S1	The deprecated AuthorizationExecuteWithPrivileges API still being fully functional in the latest releases of macOS, providing an exploitable mechanism for privilege escalation.
EV1548.004-H1	User is tricked into granting escalated privileges by entering credentials when prompted, as the AuthorizationExecuteWithPrivileges API does not perform checks on the legitimacy of the requesting program.
EV1548.004-H2	User inadvertently downloads and runs unsigned applications, which could bypass the execution prevention measures and introduce security risks to the system.

2.7.6 *Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access (T1548.005)* [35]

EV Code	Vulnerability Description
EV1548.005-H1	The failure to appropriately limit privileges for cloud accounts, allowing them to assume, create, or impersonate additional roles, policies, and permissions beyond what is necessary.
EV1548.005-H2	The failure to implement proper access controls and manual approval processes for just-in-time access, potentially leading to unauthorized temporary elevation of privileges in cloud environments.

2.7.7 *Access Token Manipulation (T1134)* [36]

EV Code	Vulnerability Description
EV1134-S1	The susceptibility of Windows access tokens to manipulation, allowing unauthorized users to modify tokens and operate under a different security context, potentially bypassing access controls.
EV1134-S2	The inherent weakness in Windows API functions that allows token stealing, enabling adversaries in a privileged user context to elevate their security level from administrator to SYSTEM.
EV1134-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.7.8 Access Token Manipulation: Token Impersonation/Theft (T1134.001) [37]

EV Code	Vulnerability Description
EV1134.001-S1	The potential weakness in access token handling mechanisms, allowing duplication and subsequent impersonation of another user's token.
EV1134.001-S2	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.001-H1	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.7.9 Access Token Manipulation: Create Process with Token (T1134.002) [38]

EV Code	Vulnerability Description
EV1134.002-S1	Insufficient access controls on token creation mechanisms, allowing adversaries to create new processes with existing tokens and escalate privileges.
EV1134.002-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.002-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.7.10 Access Token Manipulation: Make and Impersonate Token (T1134.003) [39]

EV Code	Vulnerability Description
EV1134.003-S1	Weak or easily guessable usernames and passwords, enabling adversaries to utilize the LogonUser function for token creation.
EV1134.003-H1	The failure to properly configure group policies (GPO) related to token creation and replacement, which may result in users or user groups having unnecessary permissions, potentially allowing adversaries to exploit this misconfiguration.
EV1134.003-H2	The failure to adhere to security best practices and routinely log in as standard users, relying on runas for elevated privileges, which can be a risk of accidentally performing privileged actions under their administrator accounts, exposing the system to potential exploitation.

2.7.11 Access Token Manipulation: Parent PID Spoofing (T1134.004) [40]

EV Code	Vulnerability Description
EV1134.004-S1	The lack of robust process monitoring defenses, allowing adversaries to spoof the Parent Process Identifier (PPID) and evade detection.

2.7.12 Access Token Manipulation: SID-History Injection (T1134.005) [41]

EV Code	Vulnerability Description
EV1134.005-S1	The possibility of SID Filtering not being automatically applied to legacy trusts or intentionally disabled for inter-domain access, creating a security gap that could be exploited for unauthorized activities.
EV1134.005-S2	The incorrect application of SID Filter Quarantining to external trusts, potentially leading to misconfigurations that could be exploited by adversaries for unauthorized access or privilege escalation.
EV1134.005-S3	The unsupported configuration of applying SID Filtering to domain trusts within a single forest, risking breaking changes and potential security issues that may arise due to this configuration.

EV1134.005-H1	The failure to clean up SID-History attributes after legitimate account migration, leaving potential traces that could be exploited by adversaries for unauthorized access or privilege escalation.

2.7.13 BITS Jobs (T1197) [87]

EV Code	Vulnerability Description
EV1197-S1	The potential oversight in network and/or host firewall rule configurations, allowing unauthorized BITS traffic if not adequately filtered, thus compromising the BITS mechanism.
EV1197-H1	The potential failure to optimize the default BITS job lifetime, as users may overlook reducing it through Group Policy or adjusting the JobInactivityTimeout and MaxDownloadTime Registry values, potentially exposing the system to prolonged malicious BITS activities.
EV1197-H2	The potential oversight in user account management, as not limiting access to the BITS interface to specific users or groups may provide adversaries with unauthorized control over BITS jobs, leading to malicious activities.

2.7.14 Build Image on Host (T1612) [117]

EV Code	Vulnerability Description
EV1612-S1	Failure to detect the malicious content in a custom image when it is based on a vanilla image pulled from a public registry, potentially allowing adversaries to evade detection.
EV1612-S2	Failure to secure the Docker API and implement restrictions on remote build requests, enabling adversaries to exploit the API to build and deploy malicious custom images on the host.
EV1612-H1	User allows unauthenticated access to the Docker API on port 2375, creating a security gap that adversaries could exploit to send remote build requests and deploy custom images.

EV1612-H2	Failure to implement proper network segmentation, which could lead to direct remote access to internal systems, providing adversaries with an opportunity to exploit the Docker API and build custom images.
EV1612-H3	User allows containers to run as root by default, potentially providing adversaries with escalated privileges to compromise the host system.
EV1612-H4	Failure to adhere to privileged account management practices, such as defining Pod Security Standards in Kubernetes environments, allowing the running of privileged containers and increasing the risk of compromise.

2.7.15 Debugger Evasion (T1622) [195]

EV Code	Vulnerability Description
EV1622-H1	Human oversight or error, such as failing to adequately secure and monitor debug logs, allowing adversaries to flood them with meaningless data through looping Native API function calls (e.g., OutputDebugStringW()), thereby concealing malicious activities.

2.7.16 Deobfuscate/Decode Files of Information (T1140) [199]

EV Code	Vulnerability Description
EV1140-S1	The lack of robust file decoding and deobfuscation detection mechanisms, allowing adversaries to hide malicious artifacts using methods such as certutil or the Windows copy /b command.
EV1140-H1	The potential for falling victim to User Execution tactics, as adversaries may trick users into taking actions that trigger deobfuscation or decryption processes, facilitating the intrusion.
EV1140-H2	The risk of providing a password to open password-protected files received from adversaries, which could be part of a social engineering tactic to gain unauthorized access to sensitive information.

2.7.17 Deploy Container (T1610) [200]

EV Code	Vulnerability Description
EV1610-S1	Lack of proper image scanning and compliance checks before deployment, allowing potentially insecure or non-compliant images to be deployed, posing a security risk.
EV1610-S2	Inadequate network segmentation, as direct remote access to internal systems is not denied effectively through network proxies, gateways, and firewalls, potentially exposing sensitive services to unauthorized access.
EV1610-S3	Insufficient restrictions on communication channels, as the use of unmanaged or insecure communication channels with the container service could lead to unauthorized access, bypassing secure channels like local Unix sockets or SSH.
EV1610-H1	Failing to enforce the principle of least privilege, as users may be granted unnecessary access to container dashboards, or users might be added to overly permissive groups like system:masters in Kubernetes, leading to unauthorized access and potential misuse.
EV1610-H2	User Neglects to implement just-in-time (JIT) access controls for the Kubernetes API, resulting in a failure to place additional restrictions on API access, potentially allowing unauthorized users to gain access to critical resources.
EV1610-H3	Failure to properly configure and restrict IP ranges in cloud environments, where the Kubernetes API server is deployed, potentially allowing unauthorized access to the API server from untrusted sources.
EV1610-H4	User Neglects to employ RoleBindings instead of ClusterRoleBindings in Kubernetes, which may result in users being granted broader privileges than necessary or intended, thereby opening the possibility of unauthorized actions within the cluster.
EV1610-H5	User Neglects to disable unauthenticated access to Docker API, Kubernetes API Server, and container orchestration web applications, leaving these interfaces exposed and vulnerable to unauthorized access or attacks on the containerized environment.

2.7.18 Direct Volume Access (T1006) [207]

EV Code	Vulnerability Description
EV1006-S1	The potential for misconfigurations in endpoint security solutions, allowing the adversary to bypass behavior prevention measures and execute commands or make API calls related to backup creation.
EV1006-H1	The mismanagement of user accounts, potentially granting unnecessary privileges to configure and manage backups, which could lead to unauthorized backup activity.

2.7.19 Domain Policy Modification (T1484) [211]

EV Code	Vulnerability Description
EV1484-H1	The inadequate auditing and correction of Group Policy Object (GPO) permissions abuse opportunities, allowing adversaries to potentially exploit GPO modification privileges undetected.
EV1484-H2	The creation of service accounts with administrative privileges on the Domain Controller and Active Directory Federation Services (AD FS) server, increasing the risk of unauthorized modifications to domain policy settings.
EV1484-H3	User grants adversaries sufficient permissions to modify domain policy settings, enabling them to execute malicious actions such as pushing a malicious Scheduled Task or modifying domain trusts to control access tokens in the domain environment.
EV1484-H4	The failure to implement additional controls like WMI and security filtering to tailor the application of GPOs, allowing adversaries to potentially manipulate GPO settings by exploiting broader application scenarios.

2.7.20 Domain Policy Modification: Group Policy Modification (T1484.001) [212]

EV Code	Vulnerability Description
EV1484.001-H1	Inadequate access control configuration on Group Policy Objects (GPOs), as default permissions grant all user accounts in the domain the ability to read GPOs, potentially leading to unauthorized modifications.
EV1484.001-H2	the failure to implement WMI and security filtering for GPOs, leading to a lack of tailored application of GPOs to specific users and computers, which could be exploited by adversaries seeking unauthorized modifications.

2.7.21 Domain Policy Modification: Domain Trust Modification (T1484.002) [213]

EV Code	Vulnerability Description
EV1484.002-H1	The failure to enforce the principle of least privilege in administrative access to domain trusts, potentially resulting in elevated access levels that could be exploited by adversaries seeking to manipulate trust properties.
EV1484.002-H2	Insufficient scrutiny of domain trust details, such as whether a domain is federated, potentially leading to oversight in recognizing and addressing unauthorized changes that could compromise authentication and authorization integrity.

2.7.22 Execution Guardrails (T1480) [254]

This attack technique does not rely on a specific vulnerability for execution.

2.7.23 Execution Guardrails: Environmental Keying (T1480.001) [255]

This attack technique does not rely on a specific vulnerability for execution.

2.7.24 Exploitation for Defense Evasion (T1211) [273]

EV Code	Vulnerability Description
EV1211-S1	The existence of exploitable vulnerabilities in the system or application, allowing them to bypass security features and execute adversary-controlled code.
EV1211-S2	The potential existence of programming errors within defensive security software, which can be exploited to disable or circumvent these security measures.
EV1211-S3	The presence of vulnerabilities in public cloud infrastructure or SaaS applications, enabling them to bypass defense boundaries, evade security logs, or deploy hidden infrastructure.
EV1211-S4	The potential inadequacy of application isolation and sandboxing measures, as these may not completely prevent the exploitation of undiscovered or unpatched vulnerabilities, and additional risks may still exist in these systems.
EV1211-S5	The potential limitations of security applications, such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET), in mitigating exploitation behavior, as they may not be universally compatible with all architectures and target application binaries.
EV1211-H1	The potential lack of awareness or diligence in maintaining and updating defensive security software, leading to the existence of vulnerabilities that adversaries can exploit.
EV1211-H2	The lack of awareness or oversight regarding security software within the environment, allowing adversaries to gather prior knowledge through reconnaissance and target the security software directly for exploitation.
EV1211-H3	The potential lack of a robust cyber threat intelligence capability, which may result in a failure to determine the types and levels of threats that may use software exploits and 0-days against a particular organization.

2.7.25 File and Directory Permissions Modification (T1222) [279]

EV Code	Vulnerability Description
EV1222-S1	Inadequate privileged account management, allowing critical system files to have overly permissive permissions and potentially being owned by accounts lacking the necessary privileges.
EV1222-S2	Insufficient monitoring and control over changes to file and directory permissions, potentially enabling malicious actors to manipulate access rights without detection.
EV1222-H1	The failure to apply more restrictive permissions to files and directories, as well as not ensuring proper configuration of user settings related to local and remote symbolic links, creating opportunities for adversaries to manipulate access controls and compromise system integrity.

2.7.26 File and Directory Permissions Modification: Windows File and Directory Permissions Modification (T1222.001) [280]

EV Code	Vulnerability Description
EV1222.001-S1	Weaknesses in Windows Discretionary Access Control Lists (DACLs) and their management, allowing adversaries to manipulate access control entries and gain elevated permissions on specific files and folders.
EV1222.001-H1	Inadequate management of privileged accounts, leading to critical system files having less restrictive permissions, which may be exploited by adversaries.
EV1222.001-H2	The failure to implement more restrictive file and directory permissions, as users may neglect to apply appropriate access controls, allowing adversaries the opportunity to modify access control lists and potentially compromise critical system files.

2.7.27 File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification (T1222.002) [281]

EV Code	Vulnerability Description
EV1222.002-S1	Inadequate file and directory permission management, allowing unauthorized modification by exploiting weaknesses in ACL configurations on Linux and Mac systems.
EV1222.002-H1	The mismanagement of file and directory permissions, potentially allowing adversaries to become owners, change modes, and lock others out, relying on users with appropriate permissions to configure ACLs securely.
EV1222.002-H2	The failure to implement privileged account management, allowing critical system files to have inadequate permissions, potentially facilitating unauthorized modifications by adversaries.

2.7.28 Hide Artifacts (T1564) [311]

EV Code	Vulnerability Description
EV1564-S1	The operating system features designed to hide artifacts, enabling the evasion of detection by concealing files, directories, user accounts, or other system activities.

2.7.29 Hide Artifacts: Hidden Files and Directories (T1564.001) [312]

EV Code	Vulnerability Description
EV1564.001-S1	The lack of visibility and default concealment of files and directories, allowing adversaries to hide malicious artifacts easily.

2.7.30 Hide Artifacts: Hidden Users (T1564.002) [313]

EV Code	Vulnerability Description
EV1564.002-S1	Process command-line arguments stored in the process environment block (PEB) can be overwritten, allowing adversaries to hide malicious activities by manipulating the information referenced during process execution.
EV1564.002-S2	Defensive tools/sensors may fail to prevent manipulation if they solely rely on retrieving process arguments from the PEB during process creation, overlooking potential alterations after initialization.

2.7.31 Hide Artifacts: Hidden Window (T1564.003) [314]

EV Code	Vulnerability Description
EV1564.003-S1	The potential for scripting languages in Windows, such as PowerShell, Jscript, and Visual Basic, to hide windows through features like powershell.exe -WindowStyle Hidden, enabling malicious activity to go unnoticed by users.
EV1564.003-S2	The configuration settings in macOS property list (plist) files, specifically the apple.awt.UIElement tag, which allows Java applications to hide their icons from the Dock, providing a mechanism for adversaries to conceal their activities on the system.
EV1564.003-H1	The mismanagement of program allowlisting on macOS, specifically in relation to the plist tag, as failure to properly allowlist trusted programs can leave the system susceptible to unauthorized and potentially malicious applications.

2.7.32 Hide Artifacts: NTFS File Attributes (T1564.004) **[315]**

EV Code	Vulnerability Description
EV1564.004-S1	The susceptibility in the NTFS file attributes, such as Extended Attributes (EA) and Alternate Data Streams (ADSs), enables adversaries to exploit these features to hide malicious data in file attribute metadata within the Master File Table (MFT), evading detection by some defenses like static indicator scanning tools and anti-virus.
EV1564.004-H1	The possibility of misconfiguring NTFS file and directory permissions, as improper adjustments may inadvertently impede routine operating system operations while attempting to restrict access to EA.

2.7.33 Hide Artifacts: Hidden File System (T1564.005) **[316]**

EV Code	Vulnerability Description
EV1564.005-S1	The weaknesses in standard file systems like FAT, NTFS, ext4, and APFS, enabling adversaries to abstract their file system structures and evade detection by security tools.

2.7.34 Hide Artifacts: Run Virtual Instance (T1564.006) **[317]**

EV Code	Vulnerability Description
EV1564.006-S1	The potential lack of monitoring capabilities within security tools to detect and analyze activities occurring inside virtual instances, allowing adversaries to hide artifacts associated with their malicious behavior.
EV1564.006-S2	The risk of unapproved virtualization software installation and use due to insufficient application control measures, potentially allowing adversaries to carry out malicious activities using virtual instances.
EV1564006-H1	The potential failure to disable Hyper-V when not necessary, which could occur due to oversight or misconfiguration, leaving the system open to malicious operations using virtual instances.

2.7.35 Hide Artifacts: VBA Stomping (T1564.007) [318]

EV Code	Vulnerability Description
EV1564.007-S1	The susceptibility of MS Office documents to have malicious Visual Basic for Applications (VBA) payloads hidden within by overwriting the VBA source code location, leaving the compiled p-code intact, thus evading detection by tools scanning for malicious VBA source code.
EV1564.007-S2	The lack of protection against overwriting VBA source code in MS Office documents, allowing adversaries to replace it with benign data, hiding malicious payloads within the compiled p-code.
EV1564.007-H1	Failure to disable or restrict access to unneeded VB components, leaving the system susceptible to the hiding of malicious VBA payloads within MS Office documents.

2.7.36 Hide Artifacts: Email Hiding Rules (T1564.008) [319]

EV Code	Vulnerability Description
EV1564.008-S1	The susceptibility of email clients and systems to allow users or adversaries with valid credentials to create, modify, or abuse inbox rules, including the use of PowerShell cmdlets like New-InboxRule or Set-InboxRule on Windows systems.
EV1564.009-H1	The potential for administrators to fail to regularly use auditing mechanisms, such as Get-InboxRule/Remove-InboxRule and Get-TransportRule/Remove-TransportRule in an Exchange environment, leading to a failure in discovering and removing potentially malicious inbox and transport rules.

2.7.37 Hide Artifacts: Resource Forking (T1564.009) [320]

EV Code	Vulnerability Description
EV1564.009-H1	The misconfiguration of applications, failing to adopt the application bundle structure and utilize the /Resources folder, which could result in security gaps and potential exploitation by adversaries due to inadequate protective measures.

2.7.38 Hide Artifacts: Process Argument Spoofing (T1564.010) [321]

EV Code	Vulnerability Description
EV1564.010-S1	The susceptibility to process manipulation, where adversaries can employ techniques like Process Hollowing to spawn a process with benign arguments and later modify them with malicious ones, exploiting potential weaknesses in memory protection.

2.7.39 Hide Artifacts: Ignore Process Interrupts (T1564.011) [322]

EV Code	Vulnerability Description
EV1564.011-S1	The susceptibility of operating systems to process interrupt signals, which can be exploited by executing commands like nohup or PowerShell -ErrorAction SilentlyContinue, allowing malicious commands and malware to persist through events that would otherwise terminate their execution.
EV1564.011-S2	The reliance on process interrupt signals for controlling process behavior, which can be exploited by executing commands that hide from these signals, allowing malicious commands and malware to continue execution even during system events like user logoff or termination of C2 network connection.

2.7.40 Hijack Execution Flow (T1574) [323]

EV Code	Vulnerability Description
EV1574-S1	Inadequate control and protection of locations where the operating system looks for programs/resources, such as file directories and the Windows Registry, which could be manipulated by adversaries to include malicious payloads.
EV1574-S2	The absence of hash values in manifest files, allowing for potential side-loading of malicious libraries, which could compromise the integrity of program execution.
EV1574-S3	Inadequate auditing configurations, allowing the adversary to exploit hijacking opportunities on systems within the enterprise.
EV1574-S4	Manifest files with side-loading vulnerabilities, as they may be exploited by adversaries to compromise the integrity of software.
EV1574-S5	Path interception weaknesses in program configuration files, scripts, the PATH environment variable, services, and shortcuts, which could be exploited to execute or load malicious binaries.
EV1574-S6	Lingering Windows Registry keys from uninstalled software, providing opportunities for adversaries to exploit keys with no associated legitimate binaries.
EV1574-S7	Inadequate configuration of endpoint security solutions, which may allow adversaries to bypass behavior prevention measures and successfully execute process injection or memory tampering.
EV1574-S8	Insufficient application control solutions, leading to the potential execution of malicious software through payload hijacking and exploitation of libraries loaded by legitimate software.
EV1574-S9	Insecure file and directory permissions, as the absence of write protection in software installation locations and inadequate access controls on directories could enable unauthorized file writes in critical application and library folders.
EV1574-S10	Inadequate restriction of library loading, which could lead to the loading of malicious or unauthorized DLLs, compromising system integrity.

EV1574-S11	Improper registry permissions, which may allow unauthorized modification of keys, leading to potential privilege escalation.
EV1574-H1	Failure to use quotation marks around PATH variables in configurations, scripts, or shortcuts, potentially exposing the system to path interception attacks.
EV1574-H2	User Neglects to use fully qualified paths wherever appropriate, leaving the system susceptible to the search order Windows uses for executing or loading binaries.
EV1574-H3	User overlooks the need to periodically search for and address path interception weaknesses introduced by custom or available tools, potentially leaving the system exposed to insecure path configurations.
EV1574-H4	The failure to enable Safe DLL Search Mode, exposing the system to the risk of loading DLLs from less secure directories before searching in system directories, potentially allowing for the execution of malicious code.
EV1574-H5	Inadequate software updates, exposing the system to known DLL side-loading vulnerabilities and increasing the risk of exploitation by attackers.
EV1574-H6	Failure to turn off UAC's privilege elevation for standard users ("ConsentPromptBehaviorUser"=dword:00000000) may expose the system to unauthorized privilege elevation, allowing attackers to execute malicious actions without user consent.
EV1574-H7	Failure to enable installer detection ("EnableInstallerDetection"=dword:00000001) for all users can result in a lack of password prompts during installation, potentially facilitating unauthorized installations and compromising the system's security.
EV1574-H8	Insufficient privilege management, as unauthorized users may gain access to service changes and binary target path locations if privileges are not adequately limited.
EV1574-H9	Inadequate enforcement of proper permissions and directory access controls, potentially allowing users to write files to critical directories, such as C:\ and C:\Windows, leading to an increased risk of malicious file execution.

2.7.41 Hijack Execution Flow: DLL Search Order Hijacking (T1574.001) **[324]**

EV Code	Vulnerability Description
EV1574.001-S1	Weakness in DLL search order, allowing adversaries to hijack the loading of DLLs and execute malicious payloads, potentially leading to unauthorized persistence, privilege escalation, and evasion of file execution restrictions.
EV1574.001-S2	The absence of proactive auditing practices, as enterprises may overlook DLL search order hijacking opportunities without utilizing tools like the PowerSploit framework or sxstrace.exe to detect and correct these weaknesses.
EV1574.001-S3	Failure to disallow loading of remote DLLs, especially on systems running versions prior to Windows Server 2012 or those that have not been patched, which may expose the system to DLL search order hijacking vulnerabilities.
EV1574.001-H1	The failure to implement and enforce application control solutions capable of blocking DLLs loaded by legitimate software, allowing potentially malicious DLLs to be executed through search order hijacking.
EV1574.001-H2	Misconfiguring the Safe DLL Search Mode settings, as incorrect Group Policy configurations or alterations to the Windows Registry key (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode) could compromise the intended security measures.

2.7.42 Hijack Execution Flow: DLL Side-Loading (T1574.002) **[325]**

EV Code	Vulnerability Description
EV1574.002-S1	DLL search order used by the loader, which can be exploited through side-loading by positioning both the victim application and malicious payload alongside each other.

EV1574.002-S2	The absence of hash values in manifest files, potentially allowing for the side-loading of malicious libraries due to a lack of integrity verification.
EV1574.002-H1	The failure to regularly update software, leading to the persistence of DLL side-loading vulnerabilities and an increased risk of exploitation.

2.7.43 Hijack Execution Flow: Dylib Hijacking (T1574.004) [326]

EV Code	Vulnerability Description
EV1574.004-S1	The sequential order of search paths for dynamic libraries in macOS, which allows adversaries to exploit the system's search mechanism and execute malicious code by placing a dylib with an expected name in a victim application's runtime path.
EV1574.004-S2	The use of weak linking, such as the LC_LOAD_WEAK_DYLIB function, which enables adversaries to execute an application even if the expected dylib is not present, potentially leading to unintended execution of malicious code.
EV1574.004-H1	Inadequate file and directory permissions, allowing potential unauthorized write access, which can lead to unauthorized modifications or deletions of critical files, compromising system integrity.

2.7.44 Hijack Execution Flow: Executable Installer File Permissions Weakness (T1574.005) [327]

EV Code	Vulnerability Description
EV1574.005-S1	Improper file system and binary permissions on the executable installer, allowing the adversary to overwrite legitimate binaries with malicious ones, potentially leading to code execution at a higher permissions level, including SYSTEM.
EV1574.005-S2	The lack of effective implementation of auditing tools, as the absence of tools capable of detecting file system permissions abuse opportunities may result in inadequate identification and correction of vulnerabilities in systems within an enterprise.

EV1574.005-H1	Inadequate permission settings on subdirectories and files created during the installation process, specifically within the %TEMP% directory, enabling the execution of untrusted code and the potential overwriting of binaries, leading to privilege escalation and code execution at elevated permissions.
EV1574.005-H2	Improper configuration of User Account Control (UAC), as failure to disable UAC's privilege elevation for standard users and appropriately configure installer detection may lead to unauthorized privilege escalation and undocumented installation attempts, potentially compromising system security.
EV1574.005-H3	Insufficient user account management practices, as the failure to appropriately limit privileges of user accounts and groups, especially in relation to service changes and service binary target path locations, may expose systems to unauthorized interactions and executions, potentially leading to privilege escalation and unauthorized code execution.

2.7.45 Hijack Execution Flow: Dynamic Linker Hijacking (T1574.006) **[328]**

EV Code	Vulnerability Description
EV1574.006-S1	The potential failure to implement effective execution prevention measures, allowing adversaries to use new payloads and execute dynamic linker hijacking attacks if application control solutions are not properly configured or lack the capability to block malicious software effectively.
EV1574.006-H1	The failure to enable or properly configure System Integrity Protection (SIP) on macOS systems, leaving the environment variables susceptible to exploitation; neglecting SIP increases the risk of dynamic linker hijacking.
EV1574.006-H2	The inadequate application of security measures, such as not leveraging Apple's Hardened Runtime or imposing restrictions on applications; this allows adversaries to exploit environment variables and conduct dynamic linker hijacking on macOS systems.

2.7.46 *Hijack Execution Flow: Path Interception by PATH Environment Variable (T1574.007)* [329]

EV Code	Vulnerability Description
EV1574.007-S1	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.007-S2	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.007-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.007-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.7.47 *Hijack Execution Flow: Path Interception by Search Order Hijacking (T1574.008)* [330]

EV Code	Vulnerability Description
EV1574.008-S1	The lack of explicit path specification in some programs, allowing adversaries to perform Search Order Hijacking and execute their malicious payloads by placing files in the directory where the calling program is located.
EV1574.008-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.008-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.

EV1574.008-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.008-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.7.48 Hijack Execution Flow: Path Interception by Unquoted Path (T1574.009) [331]

EV Code	Vulnerability Description
EV1574.009-S1	The lack of proper quoting in file paths, allowing for path interception and execution of malicious payloads by placing executables in higher-level directories.
EV1574.009-S2	The inadequate configuration of program files, scripts, the PATH environment variable, services, and shortcuts, as they may lack proper quoting in PATH variables, enabling path interception.
EV1574.009-S3	The potential existence of old Windows Registry keys with no associated legitimate binaries, which can be exploited for path interception if not cleaned up after software uninstallation.
EV1574.009-H1	The failure to properly configure file and directory permissions, allowing users to write files to critical system directories like C:\Windows, increasing the risk of malicious file placement for execution.
EV1574.009-H2	User places executables in inadequately protected directories, as not requiring all executables to be located in write-protected directories may expose the system to unauthorized execution.

2.7.49 Hijack Execution Flow: Services File Permissions Weakness (T1574.010) [332]

EV Code	Vulnerability Description
EV1574.010-S1	Flaws in Windows service file permissions, which allow the replacement of legitimate binaries, leading to the execution of malicious payloads with potentially elevated permissions, including SYSTEM.
EV1574.010-S2	Lack of auditing tools capable of detecting file system permissions abuse opportunities, allowing adversaries to exploit weaknesses in service file permissions.
EV1574.010-H1	Improperly setting permissions on the file system directory containing the target binary or on the binary itself, enabling adversaries to overwrite the target binary with a malicious one using user-level permissions.
EV1574.010-H2	Failure to turn off User Account Control's (UAC) privilege elevation for standard users or properly configure UAC settings, potentially allowing elevation of privileges through exploitation during the UAC detection process.
EV1574.010-H3	Allowing execution from user directories, file download directories, and temp directories, potentially providing adversaries with the ability to exploit service binary vulnerabilities and execute malicious code.

2.7.50 Hijack Execution Flow: Services Registry Permissions Weakness (T1574.011) [333]

EV Code	Vulnerability Description
EV1574.011-S1	The weakness in Registry permissions for service-related keys (HKLM\SYSTEM\CurrentControlSet\Services), allowing unauthorized modification of a service's execution parameters, potentially leading to the execution of adversary-controlled code during service startup.

EV1574.011-H1	The failure to set appropriate access controls for the service's Registry keys, allowing adversaries to manipulate keys such as FailureCommand or create custom subkeys, facilitating elevated execution and persistence.
EV1574.011-H2	The lack of proper access controls on the Performance key, enabling adversaries to create or modify it to point to a malicious DLL, potentially leading to the execution of adversary-controlled code during the operation of a driver service.
EV1574.011-H3	The failure to set proper access controls on the Parameters key or custom subkeys, allowing adversaries to add malicious data, establish persistence, or enable other malicious activities associated with their services.
EV1574.011-H4	The failure to secure the service's file identification process using HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll, potentially leading to misidentification of the service's file when launched through svchost.exe.

2.7.51 Hijack Execution Flow: COR_PROFILER (T1574.012) **[334]**

EV Code	Vulnerability Description
EV1574.012-S1	Insufficient control over DLL execution, as the system lacks robust mechanisms to identify and block potentially malicious unmanaged COR_PROFILER profiling DLLs.
EV1574.012-S2	Inadequate registry permission management, leaving the system exposed to potential modifications of keys associated with COR_PROFILER due to improper permissions on Registry hives.
EV1574.012-H1	Mismanagement of user privileges, allowing unauthorized individuals to edit system environment variables and potentially compromise the system's security.

2.7.52 Hijack Execution Flow: KernelCallbackTable (T1574.013) **[335]**

EV Code	Vulnerability Description
EV1574.013-S1	The vulnerability in the initialization process of the KernelCallbackTable within the Process Environment Block (PEB), which can be exploited to hijack the execution flow of a process.
EV1574.013-S2	Potential weaknesses in the endpoint security solution's configuration that may allow the adversary to evade behavior prevention mechanisms, specifically related to blocking process injection and memory tampering behaviors.
EV1574.013-H1	Allowing unauthorized access to the Process Environment Block (PEB) memory, potentially through inadequate access controls or permissions, enabling the adversary to obtain a pointer to the KernelCallbackTable.

2.7.53 Impair Defenses (T1562) **[336]**

EV Code	Vulnerability Description
EV1562-S1	The inadequate audit practices, as routine checks on account role permissions may not be conducted, allowing unexpected users and roles to gain permission to modify defensive tools and settings.
EV1562-S2	The absence of robust application control may permit the execution of tools outside of security policies, potentially enabling adversaries to abuse them for impairing system defenses.
EV1562-S3	The insufficient restriction of file and directory permissions, potentially allowing adversaries to disable or interfere with security/logging services due to improper process and file permissions.
EV1562-S4	The inadequate restriction of registry permissions, which could allow adversaries to disable or interfere with security/logging services by exploiting improper Registry permissions.

EV1562-H1	The absence of software configuration policies on internal web servers, potentially exposing insecure connections and enabling adversaries to exploit vulnerabilities such as the lack of HTTP Strict Transport Security.
EV1562-H2	The improper user account management, as the absence of proper user permissions may allow adversaries to disable or interfere with security/logging services.

2.7.54 Impair Defenses: Disable or Modify Tools (T1562.001) [337]

EV Code	Vulnerability Description
EV1562.001-S1	The susceptibility of security tools to modification or disabling, including killing processes, modifying Registry keys, and preventing updates, compromising the overall effectiveness of the security infrastructure.
EV1562.001-S2	The specific vulnerability within applications like Sysmon, where adversaries may tamper with registry values (e.g., "Start" and "Enable" in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational) to potentially disable Sysmon logging and avoid detection.
EV1562.001-S3	The absence of robust application control may permit the execution of tools outside of security policies, potentially enabling adversaries to abuse them for impairing system defenses.
EV1562.001-S4	The insufficient restriction of file and directory permissions, potentially allowing adversaries to disable or interfere with security/logging services due to improper process and file permissions.
EV1562.001-S5	The inadequate restriction of registry permissions, which could allow adversaries to disable or interfere with security/logging services by exploiting improper Registry permissions.
EV1562.001-H1	The improper user account management, where inadequate user permissions could enable adversaries to disable or interfere with security services, compromising system integrity.

2.7.55 Impair Defenses: Disable Windows Event Logging (T1562.002) [338]

EV Code	Vulnerability Description
EV1562.002-S1	The misconfiguration or inadequate protection of administrative privileges, enabling adversaries to execute commands like Set-Service and sc config to stop or disable the EventLog service, compromising the integrity of Windows event logging.
EV1562.002-S2	The potential misconfiguration of auditpol settings for Administrator accounts, leading to a failure in periodic review and dynamic baselining, which may allow malicious activity to go undetected.
EV1562.002-S3	The absence of proper Registry permissions, enabling adversaries to disable logging by adding the MiniNT registry key, subsequently disabling Event Viewer.
EV1562.002-H1	The failure to establish and maintain proper file and directory permissions for .evtx logging files, located at C:\Windows\system32\Winevt\Logs, allowing adversaries to potentially interfere with logging by modifying or deleting these files.
EV1562.002-H2	The inadequate management of user permissions, which may allow adversaries to interfere with logging by disabling or modifying EventLog service settings.

2.7.56 Impair Defenses: Impair Command History Logging (T1562.003) [339]

EV Code	Vulnerability Description
EV1562.003-S1	The lack of restrictions to change the HISTCONTROL, HISTFILE, and HISTFILESIZE environment variables, which introduces the risk of intentional or accidental misconfigurations, potentially impacting the system's logging and history functionality.
EV1562.003-H1	Inadequate configuration of PowerShell command history logging on Windows systems, as adversaries can change the log file path or disable logging altogether using PowerShell commands, enabling adversaries to hide their activities.

EV1562.003-H2	Lack of proper configuration and monitoring of Network Device CLI on network devices, allowing adversaries to disable historical command logging (e.g., no logging) and potentially cover their tracks.
EV1562.003-H3	User incorrectly change setting of the HISTCONTROL environment variable to "ignoreboth" or "ignorespace" instead of "ignoredups", which may result in unintended behavior in command history, potentially leading to overlooked or repeated commands with security implications.

2.7.57 Impair Defenses: Disable or Modify System Firewall (T1562.004) [340]

EV Code	Vulnerability Description
EV1562.004-H1	Insufficient monitoring of account role permissions, allowing unauthorized users or roles to potentially modify system firewalls.
EV1562.004-H2	Inadequate enforcement of proper process and file permissions, which could enable adversaries to disable or modify firewall settings by exploiting file and directory vulnerabilities.
EV1562.004-H3	Insufficient control over Registry permissions, exposing the system to the risk of adversaries disabling or modifying firewall settings through unauthorized Registry access.
EV1562.004-H4	The mismanagement of user permissions, creating opportunities for adversaries to exploit and manipulate firewall settings due to inadequate user account management.

2.7.58 Impair Defenses: Indicator Blocking (T1562.006) [341]

EV Code	Vulnerability Description
EV1562.006-S1	Inadequate protection of event tracers/forwarders, firewall policies, and associated mechanisms due to inappropriate permissions and access controls, potentially allowing unauthorized access or manipulation.

EV1562.006-H1	The lack of automated relaunching mechanisms for forwarding mechanisms, leaving the system exposed during intervals between manual relaunches and potentially leading to service disruptions.
EV1562.006-H2	The failure to secure event tracers/forwarders and associated mechanisms adequately, potentially allowing user accounts to manipulate these components and compromise system security.

2.7.59 Impair Defenses: Disable or Modify Cloud Firewall (T1562.007) [342]

EV Code	Vulnerability Description
EV1562.007-H1	The potential weakness in routine account role permission audits, as failure to regularly check and update permissions may result in unauthorized users or roles having the ability to modify cloud firewalls.
EV1562.007-H2	The failure to apply the principle of least privilege in Identity and Access Management (IAM) security policies, which could result in excessive permissions for users and roles, increasing the risk of unauthorized access and modifications.

2.7.60 Impair Defenses: Disable or Modify Cloud Logs (T1562.008) [343]

EV Code	Vulnerability Description
EV1562.008-H1	The failure to manage policies effectively to ensure that only necessary users have permissions to make changes to logging policies, thereby leaving the system exposed to unauthorized modifications.

2.7.61 Impair Defenses: Safe Mode Boot (T1562.009) [344]

EV Code	Vulnerability Description
EV1562.009-S1	The absence of proper configuration controls on endpoint defenses, which may fail to operate effectively in safe mode, leaving the system exposed to malicious activities.

EV1562.009-H1	Inadequate restriction of administrator accounts, potentially allowing unauthorized individuals access to privileged functions and the ability to remotely boot a machine in safe mode.

2.7.62 Impair Defenses: Downgrade Attack (T1562.010) [345]

EV Code	Vulnerability Description
EV1562.010-S1	The presence of outdated or vulnerable versions of Command and Scripting Interpreters, such as PowerShell, lacking security features like Script Block Logging (SBL), enabling the execution of malicious scripts without detection.
EV1562.010-S2	The absence of software configurations, such as the implementation of HTTP Strict Transport Security (HSTS) on internal web servers, which could prevent the enforcement of HTTPS/network traffic encryption policies and lead to insecure connections

2.7.63 Impair Defenses: Spoof Security Alerting (T1562.011) [346]

EV Code	Vulnerability Description
EV1562.011-H1	Inadequate implementation or configuration of application controls, allowing adversaries to bypass execution prevention measures and successfully install and utilize payloads for spoofing security alerting.

2.7.64 Impair Defenses: Disable or Modify Linux Audit System (T1562.012) [347]

EV Code	Vulnerability Description
EV1562.012-S1	Inadequate monitoring and control of account role permissions, which can potentially lead to unauthorized modification of logging settings, allowing adversaries to manipulate audit trails and cover their tracks.

EV1562.012-H1	The failure to implement the recommended mitigation of adding "auditctl -e 2" as the last command in the audit.rules files, which could leave the system susceptible to unauthorized configuration changes at runtime, enabling adversaries to manipulate logging settings without detection.
EV1562.012-H2	The failure to restrict user accounts to the least privileges they require, which increases the risk of unauthorized access and misuse by an adversary with root level access.

2.7.65 Impersonation (T1656) [348]

EV Code	Vulnerability Description
EV1656-H1	The susceptibility to social engineering techniques, including manipulative and persuasive language in emails, which can prompt individuals to act quickly without proper verification, leading to financial theft or information disclosure.
EV1656-H2	The potential lack of an effective threat intelligence program, making defenders and users unaware of common impersonation tactics and active campaigns, thereby increasing the risk of successful attacks.
EV1656-H3	The failure to undergo adequate training, leaving individuals unaware of impersonation tricks and less likely to employ countermeasures such as confirming requests through independent platforms, leading to an increased susceptibility to impersonation attacks.

2.7.66 Indicator Removal (T1070) [350]

EV Code	Vulnerability Description
EV1070-S1	The absence of robust encryption measures, allowing potential unauthorized access to sensitive information.
EV1070-S2	The lack of automatic and secure forwarding of events to a log server or data repository, creating opportunities for adversaries to locate and manipulate data on the local system.

EV1070-H1	The insufficient safeguarding of generated event files stored locally, lacking proper permissions and authentication, thereby creating opportunities for adversaries to exploit and potentially escalate privileges.

2.7.67 Indicator Removal: Clear Windows Event Logs (T1070.001) [351]

EV Code	Vulnerability Description
EV1070.001-S1	The absence of robust encryption measures, allowing potential unauthorized access to sensitive information.
EV1070.001-S2	The lack of automatic and secure forwarding of events to a log server or data repository, creating opportunities for adversaries to locate and manipulate data on the local system.
EV1070.001-H1	The insufficient safeguarding of generated event files stored locally, lacking proper permissions and authentication, thereby creating opportunities for adversaries to exploit and potentially escalate privileges.

2.7.68 Indicator Removal: Clear Linux or Mac System Logs (T1070.002) [352]

EV Code	Vulnerability Description
EV1070.002-S1	The lack of proper access controls or monitoring mechanisms for system logs in macOS and Linux, allowing for unauthorized clearing of critical logs, including authentication, login, kernel, and web server logs, thus concealing evidence of intrusion.
EV1070.002-S2	The absence of robust encryption measures, allowing potential unauthorized access to sensitive information.
EV1070.002-H1	The lack of automatic and secure forwarding of events to a log server or data repository, creating opportunities for adversaries to locate and manipulate data on the local system.
EV1070.002-H2	The insufficient safeguarding of generated event files stored locally, lacking proper permissions and authentication, thereby creating opportunities for adversaries to exploit and potentially escalate privileges.

2.7.69 Indicator Removal: Clear Command History (T1070.003) [353]

EV Code	Vulnerability Description
EV1070.003-S1	The retention of command history logs in Linux and macOS systems, as the adversary can manually clear the history (history -c) or delete the ~/.bash_history file, allowing them to conceal their actions during an intrusion.
EV1070.003-S2	The presence of command history logs in Network Device CLIs on network devices, which can be cleared by executing commands such as clear logging and/or clear history, enabling adversaries to hide their activities.
EV1070.003-S3	The lack of implementation of remote data storage and centralized logging solutions, exposing historical command line log data to local tampering or deletion by adversaries.
EV1070.003-H1	The failure to enforce read-only permissions on environment variables associated with command history, as this oversight may enable adversaries to manipulate or delete historical command data.
EV1070.003-H2	The inadequate enforcement of file and directory permissions, as users may have the ability to modify or delete their ~/.bash_history or ConsoleHost_history.txt files, compromising the accuracy of historical command records.

2.7.70 Indicator Removal: File Deletion (T1070.004) [354]

EV Code	Vulnerability Description
EV1070.004-S1	The insufficient access controls on file deletion operations, allowing unauthorized removal of critical files and potential disruption of system functionality.

2.7.71 Indicator Removal: Network Share Connection Removal (T1070.005) [355]

EV Code	Vulnerability Description
EV1070.005-S1	The potential weakness in Windows shared drive and SMB/Windows Admin Shares connections, allowing removal of share connections, which may compromise traceability and hinder detection of malicious activity.

2.7.72 Indicator Removal: Timestomp (T1070.006) [356]

EV Code	Vulnerability Description
EV1070.006-S1	The susceptibility to file timestamp modification, allowing adversaries to manipulate modify, access, create, and change times to conceal new or altered files and evade detection by forensic investigators or file analysis tools.

2.7.73 Indicator Removal: Clear Network Connection History and Configurations (T1070.007) [357]

EV Code	Vulnerability Description
EV1070.007-S1	The storage of network connection history in easily accessible locations, such as Windows Registry values, files like Default.rdp, and system logs on macOS and Linux hosts, providing opportunities for attackers to manipulate or erase evidence.
EV1070.007-S2	Inadequate implementation of remote data storage configurations, where failure to automatically forward events to a log server or data repository may expose the system to the risk of adversaries locating and manipulating data on the local system.
EV1070.007-H1	The potential oversight in not adequately securing or monitoring third-party applications and network configuration settings, allowing adversaries to exploit and tamper with system firewall settings or enable proxies to facilitate malicious network connections.

EV1070.007-H2	Failure to properly configure and restrict registry permissions on generated event files and logs stored locally, potentially allowing adversaries to exploit weak permissions and escalate privileges, leading to unauthorized system access.
EV1070.007-H3	Delays in event reporting and forwarding mechanisms, as human oversight or misconfiguration may lead to prolonged storage of events on the local system, providing adversaries with an extended window of opportunity for data manipulation.

2.7.74 Indicator Removal: Clear Mailbox Data (T1070.008) [358]

EV Code	Vulnerability Description
EV1070.008-S1	The ability of email applications to allow users and programs to export and delete mailbox data via command line tools or APIs.
EV1070.008-S2	The specific weakness in Exchange servers, exploited through the ExchangePowerShell PowerShell module, including the use of Remove-MailboxExportRequest to eliminate evidence of mailbox exports.
EV1070.008-S3	The susceptibility of Linux and macOS systems to email deletion through command line utilities like 'mail' or the use of AppleScript to interact with APIs on macOS.
EV1070.008-S4	Lack of timely reporting and forwarding mechanisms for mail data and events to a log server or data repository, exposing the system to extended periods of local storage and increasing the risk of unauthorized access or manipulation by adversaries.
EV1070.008-H1	User Neglects to implement proper authentication measures and permissions on the log server or data repository, potentially leading to unauthorized access and manipulation of forwarded mail data and events by adversaries.
EV1070.008-H2	The failure to appropriately configure organization-wide transport rules, leading to the unintentional removal of emails and metadata/headers indicative of spam or suspicious activity.

EV1070.008-H3	Inadequate control over transport rules in the Exchange environment, potentially allowing malicious rules to be created, leading to unauthorized actions.
EV1070.008-H4	The improper configuration of file and directory permissions, risking the exposure of generated event files to unauthorized access and potential privilege escalation opportunities.

2.7.75 Indicator Removal: Clear Persistence (T1070.009) [359]

EV Code	Vulnerability Description
EV1070.009-S1	Inadequate event forwarding configuration could lead to delayed or incomplete transmission of events, providing adversaries with opportunities to locate and manipulate data on the local system during gaps in monitoring.
EV1070.009-H1	Improper configuration of file and directory permissions by users may expose generated event files, stored locally, to unauthorized access, potentially compromising the integrity and confidentiality of the logged information.

2.7.76 Indirect Command Execution (T1202) [360]

EV Code	Vulnerability Description
EV1202-H1	The failure to implement effective restrictions or monitoring for specific Windows utilities, such as Forfiles, Program Compatibility Assistant (pcalua.exe), and components of the Windows Subsystem for Linux (WSL), which enables adversaries to exploit these utilities for arbitrary command execution, evading defenses.

2.7.77 Masquerading (T1036) [375]

EV Code	Vulnerability Description
EV1036-S1	The lack of effective antivirus/antimalware protection, allowing suspicious files to potentially go unnoticed and unquarantined.

EV1036-S2	The absence of behavior prevention on endpoints, such as a Host Intrusion Prevention System (HIPS), which could result in the execution of potentially malicious files.
EV1036-S3	The lack of code signing enforcement, leaving the system open to the execution of unsigned binaries that may be manipulated by adversaries.
EV1036-S4	The insufficient use of execution prevention tools, allowing the execution of potentially malicious files with common operating system utility names.
EV1036-H1	The inadequate restriction of file and directory permissions, leaving critical system folders, such as C:\Windows\System32, vulnerable to manipulation by adversaries.
EV1036-H2	The lack of awareness and training, leading users to open email attachments or click on unknown links, potentially introducing malicious content into the system.

2.7.78 Masquerading: Invalid Code Signature (T1036.001) [376]

EV Code	Vulnerability Description
EV1036.001-S1	The susceptibility to invalid code signatures, which can be exploited to deceive users and security tools, as files with invalid code signatures may appear more legitimate despite failing digital signature validation checks.
EV1036.001-S2	The lack of code signing enforcement, leaving the system open to the execution of unsigned binaries that may be manipulated by adversaries.

2.7.79 Masquerading: Right-to-Left Override (T1036.002) [377]

EV Code	Vulnerability Description
EV1036.002-H1	The susceptibility to spearphishing attacks or execution of malicious files, as users may be tricked into believing that a file is harmless based on its displayed name, which is manipulated using the right-to-left override (RTLO) character.

2.7.80 Masquerading: Rename System Utilities (T1036.003) [378]

EV Code	Vulnerability Description
EV1036.003-S1	Inadequate file and directory permissions on critical folders, such as C:\Windows\System32, allowing adversaries to easily manipulate and rename system utilities.

2.7.81 Masquerading: Masquerade Task or Service (T1036.004) [379]

EV Code	Vulnerability Description
EV1036.004-S1	The lack of strict validation or authentication mechanisms for task or service names and descriptions, enabling adversaries to manipulate these identifiers and potentially compromise the system.

2.7.82 Masquerading: Match Legitimate Name of Location (T1036.005) [380]

EV Code	Vulnerability Description
EV1036.005-H1	User trusts files or resources based solely on their name or location, allowing the adversary to evade defenses and observation by placing malicious executables in commonly trusted directories or giving them names of legitimate programs.
EV1036.005-H2	The tendency to rely on visual cues, such as file icons, for legitimacy verification, which could lead to overlooking malicious files that mimic the appearance of legitimate ones.

2.7.83 Masquerading: Space after Filename (T1036.006) [381]

EV Code	Vulnerability Description
EV1036.006-H1	The tendency to be deceived by benign-looking files, as adversaries exploit the visual similarity of filenames with appended spaces to trick users into double-clicking and executing potentially malicious content.

2.7.84 Masquerading: Double File Extension (T1036.007) [382]

EV Code	Vulnerability Description
EV1036.007-S1	The default configuration in Windows OS that hides file extensions for known file types, allowing attackers to exploit this behavior for double file extension-based masquerading.
EV1036.007-H1	User opens email attachments without verifying the true file type, as users may be deceived by the displayed benign file extension, leading to the inadvertent execution of hidden malware.
EV1036.007-H2	The lack of awareness or training to disable the default setting of hiding file extensions, as users may not take proactive measures to enhance their system's security by modifying this configuration.

2.7.85 Masquerading: Masquerade File Type (T1036.008) [383]

EV Code	Vulnerability Description
EV1036.008-S1	The susceptibility to file-based attacks due to the lack of robust file validation checks and input sanitization mechanisms, allowing adversaries to manipulate file headers and extensions during activities like Ingress Tool Transfer or Upload Malware.
EV1036.008-S2	The potential weakness in the antivirus/antimalware system, as it may fail to automatically quarantine certain types of suspicious files, leaving the system exposed to malware threats.
EV1036.008-S3	The absence of a Host Intrusion Prevention System (HIPS) or similar security controls on the endpoint, leaving the system more susceptible to behavioral attacks that could go undetected.
EV1036.008-S4	Inadequate input validation, potentially allowing malicious files to bypass security measures if the input is not properly sanitized or validated before execution.
EV1036.008-H1	User overlooks malicious intent, as adversaries can exploit the benign appearance and file extension of common non-executable file types (e.g., text files, image files) to disguise malware, leading users to unknowingly interact with malicious content, such as a PHP backdoor code named as test.gif.

2.7.86 Masquerading: Break Process Trees (T1036.009) [384]

EV Code	Vulnerability Description
EV1036.009-S1	The reliance on the parent-child relationship by endpoint protection software for process tree-based detection, allowing the adversary to evade analysis by modifying the executed malware's parent process ID (PPID).
EV1036.009-S2	The susceptibility to Native API calls manipulation, allowing the adversary to alter the malware's process tree, such as executing the payload without arguments, calling fork() twice, and exiting the parent process, resulting in a disconnected grandchild process adopted by the init system process.

2.7.87 Modify Authentication Process (T1556) [385]

EV Code	Vulnerability Description
EV1556-S1	Weaknesses in the authentication mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, allowing for the modification of these processes to reveal or bypass credentials.
EV1556-S2	The potential for misconfigurations in authentication logs, such as the lack of proper enforcement of Multi-Factor Authentication (MFA), which could allow adversaries to exploit authentication weaknesses.
EV1556-S3	The potential for unsigned or improperly signed Dynamic Link Libraries (DLLs) and executable files within the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, which could be exploited to introduce malicious components into the authentication process.

EV1556-S4	The existence of new and unknown network provider DLLs within the Registry, specifically at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services <NetworkProviderName>\NetworkProvider\ProviderPath, which, if not periodically reviewed, could introduce unauthorized components affecting authentication.
EV1556-S5	The potential misconfigurations in the implementation of multi-factor authentication (MFA), such as weak settings or insufficient monitoring, which could be exploited to bypass the intended security measures.
EV1556-S6	The potential compromise of password filters due to improper registration, as the absence of filter DLLs in the designated Windows installation directory or missing registry entries may allow unauthorized manipulation, undermining the intended security measures.
EV1556-S7	The potential misconfiguration or oversight in the implementation of Protected Process Light (PPL) for LSA, which may lead to a compromise of privileged process integrity.
EV1556-S8	The risk of unauthorized write access to the /Library/Security/SecurityAgentPlugins directory, posing a threat to the integrity and security of the system.
EV1556-S9	The inadequate restriction on Registry permissions, allowing unauthorized modifications to sensitive Registry keys, specifically HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order, which could lead to system instability or compromise.
EV1556-H1	The unintentional misconfiguration or lack of secure practices in the authentication process, leading to the persistence of compromised credentials for remote access to systems and externally available services like VPNs, Outlook Web Access, and remote desktop.
EV1556-H2	The inadvertent failure to periodically review the hybrid identity solution for discrepancies, including unauthorized Pass Through Authentication (PTA) agents in the Azure Management Portal, potentially leading to undetected compromises of authentication mechanisms.

EV1556-H3	The inadvertent failure to verify the validity of binaries catalog-signed in some cases, potentially causing discrepancies in authentication logs and leading to the exploitation of authentication weaknesses.
EV1556-H4	The failure to disable the EnableMPRNotifications policy through Group Policy or a configuration service provider in Windows 11 22H2, thereby exposing the system to the risk of unauthorized credential transmission by Winlogon to network providers.
EV1556-H5	Inadequate password policies, which could expose sensitive information if the AllowReversiblePasswordEncryption property is improperly configured, allowing reversible password encryption.
EV1556-H6	Insufficient auditing of domain and local accounts, potentially leading to unauthorized access if privilege levels are not routinely reviewed, default accounts are enabled, or unauthorized local accounts are created without proper authorization.
EV1556-H7	Unrestricted access to the root account, which poses a risk of modifying protected components, unless proper privilege separation mechanisms (e.g., SELinux, grsecurity, AppArmor) are implemented to limit Privilege Escalation opportunities.
EV1556-H8	Failure to follow best practices for the design and administration of an enterprise network, potentially allowing excessive privileged account use across administrative tiers, increasing the risk of unauthorized access.
EV1556-H9	Failure to limit Azure AD Global Administrator accounts to only those required and not using dedicated cloud-only accounts, potentially exposing the hybrid identity solution to increased risk of compromise.
EV1556-H10	The potential failure to enforce or adhere to proper user account management policies, leading to insecure enrollment or deactivation of authentication mechanisms, such as MFA, for user accounts and compromising the overall security posture of the system.

2.7.88 Modify Authentication Process: Domain Controller Authentication (T1556.001) [386]

EV Code	Vulnerability Description
EV1556.001-S1	The susceptibility of the domain controller's authentication process to patching, allowing the bypass of typical authentication mechanisms and unauthorized access to user accounts.
EV1556.001-S2	The lack of enabled features, such as Protected Process Light (PPL), for Local Security Authority (LSA), which may contribute to compromised privileged processes
EV1556.001-H1	The absence of multi-factor authentication (MFA), which could potentially allow adversaries to gain control of valid credentials and exploit them for unauthorized access
EV1556.001-H2	Insufficient privileged account management, as auditing domain and local accounts irregularly may result in overlooking situations that could grant adversaries wide access through privileged account credentials.

2.7.89 Modify Authentication Process: Password Filter DLL (T1556.002) [387]

EV Code	Vulnerability Description
EV1556.002-H1	User fails to ensure that filter DLLs are present in the correct Windows installation directory (C:\Windows\System32\ by default) and appropriately registered in the system registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages), which can lead to ineffective password filtering and security risks.

2.7.90 *Modify Authentication Process: Pluggable Authentication Modules (T1556.003)* [388]

EV Code	Vulnerability Description
EV1556.003-S1	The risk of user credentials being harvested due to plain-text exchange of values with PAM components, as PAM does not store passwords.
EV1556.003-H1	The inadequate implementation of multi-factor authentication (MFA), which could expose accounts to compromise due to the reliance on single-factor authentication.
EV1556.003-H2	The risk of inadequate privileged account management, potentially allowing unauthorized modification of Pluggable Authentication Modules (PAM) components and increasing the likelihood of privilege escalation opportunities.

2.7.91 *Modify Authentication Process: Network Device Authentication (T1556.004)* [389]

EV Code	Vulnerability Description
EV1556.004-H1	The potential lack of multi-factor authentication for user and privileged accounts on network devices, which could leave these accounts more susceptible to compromise.
EV1556.004-H2	The inadequate implementation of privileged account management practices, such as not restricting administrator accounts to as few individuals as possible and not following least privilege principles, which may result in increased attack surface and potential credential overlap across systems.

2.7.92 *Modify Authentication Process: Reversible Encryption (T1556.005)* [390]

EV Code	Vulnerability Description
EV1556.005-H1	The potential enabling of reversible password encryption in Active Directory, allowing the decryption of passwords through abuse of the AllowReversiblePasswordEncryption property.

EV1556.005-H2	The potential misconfiguration of the AllowReversiblePasswordEncryption property, which can occur if administrators fail to ensure that it is set to disabled, except when necessary for specific applications.
EV1556.005-H3	The inadequate auditing of domain and local accounts, potentially allowing an adversary to exploit situations where credentials of privileged accounts are obtained, emphasizing the importance of routine audits to detect and address such security risks.

2.7.93 Modify Authentication Process: Multi-Factor Authentication (T1556.006) **[391]**

EV Code	Vulnerability Description
EV1556.006-S1	Insecure configuration of the Windows hosts file (C:\windows\system32\drivers\etc\hosts), allowing adversaries to redirect MFA calls to localhost and causing the MFA process to fail.
EV1556.006-S2	Lack of proper auditing and review processes for MFA actions alongside authentication logs, potentially allowing adversaries to manipulate MFA without detection.
EV1556.006-H1	Failure to enforce a "fail closed" policy for MFA, allowing otherwise successful authentication attempts to be granted access without enforcing multi-factor authentication.
EV1556.006-H2	Failure to ensure that all user accounts have MFA enabled, leaving some accounts without the additional security provided by multi-factor authentication.
EV1556.006-H3	Inadequate implementation of MFA policies and requirements for existing, deactivated, or dormant accounts and devices, allowing adversaries to exploit gaps in MFA coverage.

2.7.94 Modify Authentication Process: Hybrid Identity (T1556.007) [392]

EV Code	Vulnerability Description
EV1556.007-S1	Weakness in the on-premises server running a Pass Through Authentication (PTA) agent, allowing adversaries to inject a malicious DLL into the AzureADConnectAuthenticationAgentService process, enabling unauthorized authentication attempts and credential recording.
EV1556.007-S2	In environments using Active Directory Federation Services (AD FS), adversaries can exploit a weakness by editing the Microsoft.IdentityServer.Servicehost configuration file to load a malicious DLL, generating authentication tokens for any user and bypassing multi-factor authentication and defined AD FS policies.
EV1556.007-S3	Lack of verification of the integrity of DLLs and executable files in the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, creating a potential avenue for adversaries to introduce malicious code if files are not properly signed by Microsoft.
EV1556.007-H1	Failure to periodically review the hybrid identity solution for discrepancies, such as unwanted or unapproved Pass Through Authentication (PTA) agents in the Azure Management Portal, leading to potential unauthorized access.
EV1556.007-H2	Inadequate privileged account management, as organizations may fail to limit on-premises accounts with access to the hybrid identity solution, potentially allowing unauthorized access if Azure AD Global Administrator accounts are not properly restricted and dedicated for cloud-only use.
EV1556.007-H3	Failure to integrate multi-factor authentication (MFA) as part of organizational policy, increasing the risk of adversaries gaining control of valid credentials that could be exploited for various tactics, including initial access, lateral movement, and information collection.

2.7.95 Modify Authentication Process: Network Provider DLL (T1556.008) [393]

EV Code	Vulnerability Description
EV1556.008-S1	The insecure transmission of credentials during the logon process, as Winlogon sends credentials to the local mpnotify.exe process via RPC without encryption.
EV1556.008-S2	The insecure sharing of credentials in cleartext by the mpnotify.exe process with registered credential managers during logon events, potentially exposing sensitive information.
EV1556.008-H1	The failure to consistently review and identify new or unknown network provider DLLs within the Registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services <NetworkProviderName>\NetworkProvider\ProviderPath) could allow malicious DLLs to go unnoticed.
EV1556.008-H2	The failure to ensure that only valid DLLs are registered and listed in the Registry key at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order may lead to the registration of malicious DLLs.
EV1556.008-H3	The potential for misconfiguration, as the EnableMPRNotifications policy in Windows 11 22H2 can be disabled to prevent Winlogon from sending credentials to network providers, and a failure to apply this configuration could expose credentials during the logon process.
EV1556.008-H4	The mismanagement of Registry permissions, as failure to restrict permissions to sensitive Registry keys, such as HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order, may allow unauthorized modification and compromise the integrity of network provider configurations.

2.7.96 Modify Cloud Compute Infrastructure (T1578) [394]

EV Code	Vulnerability Description
EV1578-H1	The absence of routine monitoring of user permissions, allowing unexpected users to potentially exploit and modify cloud compute infrastructure components.

EV1578-H2	Insufficient user account management practices, including inadequate limitation of permissions for creating, deleting, and altering compute components, potentially resulting in excessive privileges and increased attack surface.
EV1578-H3	Assigning excessive IAM roles with administrative privileges to a larger number of users within the organization, increasing the risk of unauthorized alterations to compute components.

2.7.97 Modify Cloud Compute Infrastructure: Create Snapshot (T1578.001) [395]

EV Code	Vulnerability Description
EV1578.001-H1	The lack of proper controls or restrictions on snapshot creation permissions, allowing the adversary to create snapshots within a cloud account and potentially evade defenses.
EV1578.001-H2	User applies insecure policies, such as a firewall policy that grants the adversary inbound and outbound SSH access, thereby providing unauthorized access to the created cloud instance.
EV1578.001-H3	The lack of regular auditing of user permissions, potentially allowing unintended users to retain the capability to create snapshots and backups.
EV1578.001-H4	The failure to limit administrative privileges, conduct periodic entitlement reviews, and reduce permanent privileged role assignments, leading to an increased likelihood of unauthorized snapshot creation.

2.7.98 Modify Cloud Compute Infrastructure: Create Cloud Instance (T1578.002) [396]

EV Code	Vulnerability Description
EV1578.002-S1	The lack of robust controls in the cloud compute infrastructure, allowing the adversary to create new instances and evade defenses by bypassing existing firewall rules and permissions.

EV1578.002-H1	The lack of regular audit procedures may result in overlooking user permissions, allowing unexpected users to retain the capability to create new instances.
EV1578.002-H2	The failure to limit permissions for creating new instances based on the principle of least privilege, leading to an increased risk of unauthorized instance creation.
EV1578.002-H3	Organization fails to conduct periodic entitlement reviews on IAM users, roles, and policies, contributing to the persistence of unnecessary privileges and the potential for unauthorized instance creation.

2.7.99 Modify Cloud Compute Infrastructure: Delete Cloud Instance (T1578.003) [397]

EV Code	Vulnerability Description
EV1578.003-S1	The lack of robust access controls and monitoring in cloud compute infrastructure, allowing them to delete a cloud instance and erase forensic artifacts to evade detection.
EV1578.003-H1	The inadequate routine checking of user permissions, allowing unexpected users to retain the capability to delete new instances.
EV1578.003-H2	The failure to implement proper user account management practices, such as limiting permissions and conducting periodic entitlement reviews, leading to an increased risk of unauthorized deletion of cloud instances.
EV1578.003-H3	Organization fails to conduct periodic entitlement reviews on IAM users, roles, and policies, contributing to the persistence of unnecessary privileges and the potential for unauthorized instance creation.

2.7.100 Modify Cloud Compute Infrastructure: Revert Cloud Instance (T1578.004) [398]

EV Code	Vulnerability Description
EV1578.004-S1	The potential weakness in cloud infrastructure allowing an adversary to revert changes is the reliance on virtual machine (VM) or data storage snapshots, which can be exploited through the cloud management dashboard or cloud APIs.
EV1578.004-S2	The lack of robust access controls could allow adversaries to gain unauthorized access to the cloud management dashboard or APIs, facilitating the reversion of cloud instance changes.
EV1578.004-S3	The susceptibility of the cloud infrastructure lies in the use of temporary storage attached to compute instances, particularly ephemeral types that reset upon stop/restart of the VM, providing an avenue for adversaries to erase traces of malicious activities.

2.7.101 Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations (T1578.005) [399]

EV Code	Vulnerability Description
EV1578.005-S1	The ability to enable unused/unsupported cloud regions, providing avenues for unauthorized deployment of resources and evasion of detection.
EV1578.005-H1	Lack of regular monitoring of user permissions, allowing potential unauthorized users to request quota adjustments or modify tenant-level compute settings.
EV1578.005-H2	Granting excessive permissions to users, beyond what is necessary for their roles, enabling them to request quota adjustments or modify tenant-level compute settings.

2.7.102 Modify Registry (T1112) [400]

EV Code	Vulnerability Description
EV1112-S1	Inadequate Registry permissions, stemming from misconfigurations, allowing unauthorized users to modify keys for system components and potentially leading to privilege escalation.

2.7.103 Modify System Image (T1601) [401]

EV Code	Vulnerability Description
EV1601-S1	The monolithic nature of the operating system on embedded network devices, making it susceptible to modification through changes to a single file, enabling the weakening of defenses and the introduction of new capabilities.
EV1601-S2	The lack of boot integrity measures, as some embedded network devices may not implement cryptographic signing to ensure the integrity of operating system images at boot time, allowing adversaries to potentially compromise the boot process.
EV1601-S3	The absence of code signing practices, as not all vendors provide digitally signed operating system images, leaving the system susceptible to unauthorized modifications by adversaries.
EV1601-S4	The storage of passwords for local accounts in plain-text or weakly encrypted formats on some embedded network devices, potentially facilitating unauthorized access if proper encryption measures are not implemented.
EV1601-H1	The failure to implement proper access controls or monitoring mechanisms, allowing unauthorized modification of the operating system file, either live in memory or on storage, leading to potential compromise of the network device.
EV1601-H2	The inadequate use of multi-factor authentication, as not employing this security measure for user and privileged accounts on embedded network devices may expose the system to credential compromise.

EV1601-H3	The failure to adhere to recommended password policies, as not following NIST guidelines when creating password policies for embedded network devices can result in weak passwords, increasing the risk of unauthorized access.
EV1601-H4	The insufficient management of privileged accounts, as not restricting administrator accounts and preventing credential overlap across systems may lead to a higher risk of unauthorized access, particularly between network and non-network platforms.

2.7.104 Modify System Image: Patch System Image (T1601.001) [402]

EV Code	Vulnerability Description
EV1601.001-S1	The monolithic architecture of some network devices, where the entire operating system and functionality are contained within a single file, making it susceptible to modification.
EV1601.001-S2	The presence of malicious code in the boot loader, such as the ROMMONkit method, providing the capability for direct memory manipulation and enabling the patching of the live operating system during runtime.
EV1601.001-S3	The insufficient protection of the boot loader, allowing the implantation of malicious code that facilitates direct manipulation of running operating system code in memory during the boot process.
EV1601.001-S4	The lack of boot integrity measures, as some embedded network devices may not implement cryptographic signing to ensure the integrity of operating system images at boot time, allowing adversaries to potentially compromise the boot process.
EV1601.001-S5	The absence of code signing practices, as not all vendors provide digitally signed operating system images, leaving the system susceptible to unauthorized modifications by adversaries.
EV1601.001-S6	The storage of passwords for local accounts in plain-text or weakly encrypted formats on some embedded network devices, potentially facilitating unauthorized access if proper encryption measures are not implemented.

EV1601.001-H1	The lack of adequate access controls, allowing adversaries with administrative-level access to exploit native debug commands and directly modify memory addresses containing the running operating system.
EV1601.001-H2	The inadequate use of multi-factor authentication, as not employing this security measure for user and privileged accounts on embedded network devices may expose the system to credential compromise.
EV1601.001-H3	The failure to adhere to recommended password policies, as not following NIST guidelines when creating password policies for embedded network devices can result in weak passwords, increasing the risk of unauthorized access.
EV1601.001-H4	The insufficient management of privileged accounts, as not restricting administrator accounts and preventing credential overlap across systems may lead to a higher risk of unauthorized access, particularly between network and non-network platforms.

2.7.105 Modify System Image: Downgrade System Image (T1601.002) [403]

EV Code	Vulnerability Description
EV1601.002-S1	Weaker encryption ciphers and fewer/less updated defensive features in older versions of the operating system on network devices.
EV1601.002-S2	Inherent vulnerabilities in older operating system versions that may not be patched or updated, making them susceptible to exploitation.
EV1601.002-S3	The lack of boot integrity measures, as some embedded network devices may not implement cryptographic signing to ensure the integrity of operating system images at boot time, allowing adversaries to potentially compromise the boot process.
EV1601.002-S4	The absence of code signing practices, as not all vendors provide digitally signed operating system images, leaving the system susceptible to unauthorized modifications by adversaries.
EV1601.002-S5	The storage of passwords for local accounts in plain-text or weakly encrypted formats on some embedded network devices, potentially facilitating unauthorized access if proper encryption measures are not implemented.

EV1601.002-H1	The failure to restrict access or implement secure configurations that would prevent unauthorized changes to the operating system on embedded devices.
EV1601.002-H2	The inadequate use of multi-factor authentication, as not employing this security measure for user and privileged accounts on embedded network devices may expose the system to credential compromise.
EV1601.002-H3	The failure to adhere to recommended password policies, as not following NIST guidelines when creating password policies for embedded network devices can result in weak passwords, increasing the risk of unauthorized access.
EV1601.002-H4	The insufficient management of privileged accounts, as not restricting administrator accounts and preventing credential overlap across systems may lead to a higher risk of unauthorized access, particularly between network and non-network platforms.

2.7.106 Network Boundary Bridging (T1599) [408]

EV Code	Vulnerability Description
EV1599-S1	The inadequate configuration or insufficient security measures on boundary devices, enabling adversaries to exploit and compromise them.
EV1599-S2	The storage of passwords for local accounts in plain-text or weakly encrypted formats on some embedded network devices, potentially facilitating unauthorized access if proper encryption measures are not implemented.
EV1599-S3	Inadequate implementation of network traffic filtering, particularly in scenarios where compromised network devices are not promptly identified and blocked, leading to potential unauthorized access and data compromise.
EV1599-H1	The failure to implement proper access controls or permissions on boundary devices, allowing adversaries to gain sufficient rights for reconfiguring and bypassing policy enforcement.

EV1599-H2	The failure to adhere to recommended password policies, as not following NIST guidelines when creating password policies for embedded network devices can result in weak passwords, increasing the risk of unauthorized access.
EV1599-H3	The insufficient management of privileged accounts, as not restricting administrator accounts and preventing credential overlap across systems may lead to a higher risk of unauthorized access, particularly between network and non-network platforms.

2.7.107 Network Boundary Bridging: Network Address Translation Traversal (T1599.001) **[409]**

EV Code	Vulnerability Description
EV1599.001-S1	The inadequate control or protection of network boundary devices, enabling adversaries to gain control and manipulate NAT configurations, either leveraging existing settings or implementing their own custom NAT mechanisms to obscure their activities.
EV1599.001-S2	The storage of passwords for local accounts in plain-text or weakly encrypted formats on some embedded network devices, potentially facilitating unauthorized access if proper encryption measures are not implemented.
EV1599.001-S3	Inadequate implementation of network traffic filtering, particularly in scenarios where compromised network devices are not promptly identified and blocked, leading to potential unauthorized access and data compromise.
EV1599.001-H1	The failure to implement proper access controls or permissions on boundary devices, allowing adversaries to gain sufficient rights for reconfiguring and bypassing policy enforcement.
EV1599.001-H2	The failure to adhere to recommended password policies, as not following NIST guidelines when creating password policies for embedded network devices can result in weak passwords, increasing the risk of unauthorized access.

EV1599.001-H3	The insufficient management of privileged accounts, as not restricting administrator accounts and preventing credential overlap across systems may lead to a higher risk of unauthorized access, particularly between network and non-network platforms.

2.7.108 Obfuscated Files or Information (T1027) **[418]**

EV Code	Vulnerability Description
EV1027-S1	The capacity for portions of files to be encoded, concealing plain-text strings and hindering defenders' ability to recognize malicious activity.
EV1027-S2	The lack of implementation or improper configuration of Attack Surface Reduction (ASR) rules on Windows 10+, leaving the system exposed to the execution of potentially obfuscated payloads.
EV1027-H1	Inadequate configuration of the Antivirus/Antimalware software, leading to potential bypass or evasion if not properly tuned or updated.
EV1027-H2	Insufficient monitoring and auditing of common fileless storage locations, such as the Registry or WMI repository, which may allow malicious activities to go unnoticed for extended periods.
EV1027-H3	The failure to restrict and control access to software deployment system ingress points, which may result in unauthorized individuals gaining access and enabling the deployment of malicious software.

2.7.109 Obfuscated Files or Information: Binary Padding (T1027.001) **[419]**

EV Code	Vulnerability Description
EV1027.001-S1	The potential inability of certain security tools to handle large files, resulting in decreased effectiveness and detection capabilities when binary padding is employed to increase the size of malware files beyond file size limitations.

2.7.110 Obfuscated Files or Information: Software Packing (T1027.002) [420]

EV Code	Vulnerability Description
EV1027.002-S1	Inherent weakness in executable compression or encryption methods, as adversaries leverage software packing to obfuscate code and change file signatures, aiming to evade signature-based detection.
EV1027.002-H1	Failure to update antivirus/antimalware definitions regularly or not creating custom signatures for observed malware, which could result in the system being inadequately protected against evolving and customized packing techniques used by adversaries.

2.7.111 Obfuscated Files or Information: Steganography (T1027.003) [421]

This attack technique does not rely on a specific vulnerability for execution.

2.7.112 Obfuscated Files or Information: Compile After Delivery (T1027.004) [422]

EV Code	Vulnerability Description
EV1027.004-S1	The potential weakness in security measures against uncompiled code, as text-based source code files can subvert analysis and evade protections targeting executables/binaries.
EV1027.004-S2	Inherent weakness in the native OS recognition, allowing payloads to be delivered in formats unrecognizable and inherently benign, creating an opportunity for later (re)compilation into proper executable binaries.
EV1027.004-H1	Failure to detect and prevent phishing attacks, as users may unknowingly open files containing obfuscated or encrypted source code payloads.
EV1027.004-H2	Lack of awareness or caution, leading users to execute payloads that appear benign on the surface but may later transform into malicious executables through (re)compilation with a bundled compiler and execution framework.

2.7.113 Obfuscated Files or Information: Indicator Removal from Tools (T1027.005) **[423]**

EV Code	Vulnerability Description
EV1027.005-S1	The reliance on a single indicator (e.g. file signatures) for malware detection, as adversaries can evade detection by modifying malware files to explicitly avoid known indicators.

2.7.114 Obfuscated Files or Information: HTML Smuggling (T1027.006) **[424]**

EV Code	Vulnerability Description
EV1027.005-S1	JavaScript Blobs and/or HTML5 download attributes, which allows malicious files to go undetected by content filters, helping adversaries to bypass security controls through HTML Smuggling.
EV1027.005-S2	The potential limitation of browser sandboxes in mitigating the impact of HTML Smuggling, as sandbox escapes may still exist, allowing adversaries to evade isolation mechanisms.

2.7.115 Obfuscated Files or Information: Dynamic API Resolution (T1027.007) **[425]**

EV Code	Vulnerability Description
EV1027.007-S1	The reliance on static artifacts such as strings and import address tables (IAT) in payload files, which provides adversaries with the opportunity to conceal malware characteristics and functionalities by using dynamic API resolution

2.7.116 Obfuscated Files or Information: Stripped Payloads (T1027.008) **[426]**

EV Code	Vulnerability Description
EV1027.008-S1	The reliance on symbols, strings, and other human-readable information within payloads, which, when stripped or obfuscated, hinders reverse engineers' ability to analyze code and identify functionality, thereby impeding detection and analysis of malicious payloads.

2.7.117 Obfuscated Files or Information: Embedded Payloads (T1027.009) **[427]**

EV Code	Vulnerability Description
EV1027.009-H1	User misconfigures or disables the antivirus/antimalware software, leaving the system exposed to malicious files that may not be automatically detected and quarantined.
EV1027.009-H2	The failure to regularly update and configure Attack Surface Reduction (ASR) rules on Windows 10, which may lead to inadequate prevention of potentially obfuscated script executions.

2.7.118 Obfuscated Files or Information: Command Obfuscation (T1027.010) **[428]**

EV Code	Vulnerability Description
EV1027.010-H1	The failure to keep the operating system (Windows 10+) and antivirus/antimalware software up-to-date, potentially leaving the system exposed to known vulnerabilities that could be exploited by attackers.
EV1027.010-H2	The improper configuration or disabling of the Attack Surface Reduction (ASR) rules on Windows 10+, allowing the execution of potentially malicious or obfuscated scripts and undermining the effectiveness of the behavior prevention mechanism.

2.7.119 Obfuscated Files or Information: Fileless Storage (T1027.011) **[429]**

EV Code	Vulnerability Description
EV1027.011-S1	The susceptibility to data concealment through fileless storage in non-volatile formats such as the Windows Registry, event logs, or WMI repository, which may go undetected by anti-virus and endpoint security tools accessing specific file formats from disk storage.

EV1027.011-H1	The lack of periodic review of common fileless storage locations (such as the Registry or WMI repository), leaving the system more susceptible to the persistence of abnormal and malicious data.

2.7.120 Obfuscated Files or Information: LNK Icon Smuggling (T1027.012) [430]

EV Code	Vulnerability Description
EV1027.012-H1	The potential failure of antivirus/antimalware signatures or heuristics to effectively detect newly emerging or sophisticated malicious LNK files and downloaded payloads, leading to a gap in threat detection.
EV1027.012-H2	The potential oversight or failure to enable Attack Surface Reduction (ASR) rules on Windows 10, which could allow the execution of potentially obfuscated scripts or payloads, undermining the effectiveness of behavior prevention on the endpoint.

2.7.121 Plist File Modification (T1647) [470]

EV Code	Vulnerability Description
EV1647-H1	The potential failure to implement Apple's developer guidance for enabling the hardened runtime in applications, leaving the system susceptible to exploitation through plist file modifications.

2.7.122 Pre-OS Boot (T1542) [472]

EV Code	Vulnerability Description
EV1542-S1	The absence or inadequate implementation of Trusted Platform Module (TPM) technology and a secure or trusted boot process, which could allow unauthorized modifications to BIOS or EFI during pre-OS boot.
EV1542-H1	The risk of BIOS or EFI not being patched and updated, potentially leaving the system exposed to known vulnerabilities that adversaries could exploit during the pre-OS boot process.

EV1542-H2	The potential failure to ensure proper permissions for privileged accounts, allowing adversaries to gain unauthorized access to critical system components, such as boot drivers or firmware, and compromise system integrity during the pre-OS boot process.

2.7.123 Pre-OS Boot: System Firmware (T1542.001) **[473]**

EV Code	Vulnerability Description
EV1542.001-S1	The potential lack of integrity verification for the BIOS or EFI, allowing for vulnerability to modification and compromise.
EV1542.001-S2	The reliance on software-based root of trust, making the SPI flash memory susceptible to tampering.
EV1542.001-S3	The absence of protective technologies like Intel Boot Guard, leaving the system exposed to potential firmware modifications.
EV1542.001-H1	The risk of BIOS or EFI not being patched and updated, potentially leaving the system exposed to known vulnerabilities that adversaries could exploit during the pre-OS boot process.
EV1542.001-H2	The potential failure to ensure proper permissions for privileged accounts, allowing adversaries to gain unauthorized access to critical system components, such as boot drivers or firmware, and compromise system integrity during the pre-OS boot process.

2.7.124 Pre-OS Boot: Component Firmware (T1542.002) **[474]**

EV Code	Vulnerability Description
EV1542.002-H1	The failure to implement robust integrity checking mechanisms for computer components, facilitating the installation of malicious firmware and providing a persistent level of access to systems.
EV1542.002-H2	The failure to perform regular firmware updates, exposing the system to increased risks of exploitation and abuse by adversaries due to outdated firmware.

2.7.125 Pre-OS Boot: Bootkit (T1542.003) [475]

EV Code	Vulnerability Description
EV1542.003-S1	The susceptibility of the Master Boot Record (MBR) and Volume Boot Record (VBR) to unauthorized modification, allowing adversaries with raw access to the boot drive to divert execution during startup to malicious code.
EV1542.003-S2	The absence of Trusted Platform Module (TPM) technology or a secure/trusted boot process, leaving the system exposed to potential compromise of boot integrity.
EV1542.003-H1	Inadequate privileged account management, allowing adversaries to potentially gain unauthorized access to accounts necessary for installing a bootkit, emphasizing the importance of ensuring proper permissions to prevent such access.

2.7.126 Pre-OS Boot: ROMMONkit (T1542.004) [476]

EV Code	Vulnerability Description
EV1542.004-S1	The potential lack of periodic integrity checks on the system image, which could result in the failure to detect unauthorized modifications.
EV1542.004-S2	The absence of secure boot features, leaving the device susceptible to unauthorized firmware upgrades in the ROM Monitor (ROMMON) of Cisco network devices.
EV1542.004-H1	The failure to enable secure boot features, which could result in the inability to validate the digital signature of the boot environment and system image, allowing for potential unauthorized software loading.
EV1542.004-H2	The failure to enable and configure network intrusion detection and prevention systems specifically for protocols like TFTP, leaving the network susceptible to unauthorized firmware updates and potential compromise by adversaries.

2.7.127 Pre-OS Boot: TFTP Boot (T1542.005) [477]

EV Code	Vulnerability Description
EV1542.005-S1	The potential lack of periodic integrity checks on the system image, which could result in the failure to detect unauthorized modifications.
EV1542.005-S2	The unrestricted use of protocols without encryption or authentication mechanisms, posing a risk of unauthorized manipulation during the netbooting process.
EV1542.005-S3	The inadequate use of Authentication, Authorization, and Accounting (AAA) systems for privileged account management, potentially allowing unauthorized actions by administrators and hindering the detection of abuse through a lack of comprehensive user action history.
EV1542.005-H1	The failure to enable secure boot features, which could result in the inability to validate the digital signature of the boot environment and system image, allowing for potential unauthorized software loading.
EV1542.005-H2	The failure to enable and configure network intrusion detection and prevention systems specifically for protocols like TFTP, leaving the network susceptible to unauthorized firmware updates and potential compromise by adversaries.
EV1542.005-H3	The lack of adherence to vendor device hardening best practices, potentially leading to the presence of unnecessary and unused features and services, default configurations, and passwords that could be exploited by adversaries.

2.7.128 Process Injection (T1055) [479]

EV Code	Vulnerability Description
EV1055-S1	The susceptibility to code injection, enabling unauthorized access to a process's memory, system/network resources, and potential elevation of privileges, thereby compromising the integrity of the system.

EV1055-S2	Inadequate configuration of endpoint security solutions, allowing for the bypassing of behavior prevention measures and enabling certain types of process injection.
EV1055-H1	The failure to implement robust privileged account management practices, such as not utilizing Yama or similar controls effectively, leading to the exploitation of ptrace-based process injection by non-privileged users.

2.7.129 Process Injection: Dynamic-link Library Injection (T1055.001) [480]

EV Code	Vulnerability Description
EV1055.001-S1	Weaknesses in memory management and specific Windows API functions, namely VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread. This creates an avenue for arbitrary code execution through DLL injection, thereby enabling unauthorized access, data compromise, or privilege escalation.
EV1055.001-H1	The possibility of misconfiguring or underutilizing endpoint security solutions, which could result in inadequate protection against process injection techniques, leading to the compromise of system integrity and data.

2.7.130 Process Injection: Portable Executable Injection (T1055.002) [481]

EV Code	Vulnerability Description
EV1055.002-S1	The susceptibility to code injection due to insufficient process-based defenses, allowing adversaries to inject portable executables (PE) into processes.
EV1055.002-S2	The potential misconfiguration or inadequacy of endpoint security solutions, allowing certain types of process injection to bypass behavior prevention measures.

2.7.131 Process Injection: Thread Execution Hijacking (T1055.003) [482]

EV Code	Vulnerability Description
EV1055.003-S1	The susceptibility of processes to Thread Execution Hijacking, which allows the injection of malicious code into existing processes, potentially leading to unauthorized access, memory compromise, and evasion of process-based defenses.
EV1055.003-H1	The potential reliance on endpoint security solutions alone, which, if improperly configured or not regularly updated, may fail to effectively block all types of process injection techniques, including Thread Execution Hijacking.

2.7.132 Process Injection: Asynchronous Procedure Call (T1055.004) [483]

EV Code	Vulnerability Description
EV1055.004-S1	The susceptibility of the Windows operating system to process injection through the asynchronous procedure call (APC) queue, enabling unauthorized code execution in the context of another process.
EV1055.004-S2	The potential inadequacy of endpoint security solutions configured to block process injection, as certain injection methods may evade detection due to variations in behavior, leading to a false sense of security.

2.7.133 Process Injection: Thread Local Storage (T1055.005) [484]

EV Code	Vulnerability Description
EV1055.005-S1	The potential inadequacy of endpoint security solutions configured to block process injection, as certain injection methods may evade detection due to variations in behavior, leading to a false sense of security.

2.7.134 Process Injection: Ptrace System Calls (T1055.008) [485]

EV Code	Vulnerability Description
EV1055.008-S1	The potential lack of configuration or ineffective deployment of endpoint security solutions, allowing process injection based on common sequences of behavior to bypass behavioral prevention measures.
EV1055.008-S2	The potential misconfiguration or lack of implementation of Yama (e.g., /proc/sys/kernel/yama/ptrace_scope), which could lead to unauthorized use of ptrace by non-privileged users for process injection.
EV1055.008-H1	The inadequate deployment of advanced access control and process restriction mechanisms such as SELinux, grsecurity, and AppArmor, which could allow adversaries to exploit process injection techniques by circumventing these security controls.

2.7.135 Process Injection: Proc Memory (T1055.009) [486]

EV Code	Vulnerability Description
EV1055.009-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.
EV1055.009-S2	Inadequate restriction of file and directory permissions, specifically on critical files such as /proc/[pid]/maps or /proc/[pid]/mem, potentially enabling unauthorized access and manipulation by adversaries.

2.7.136 Process Injection: Extra Window Memory Injection (T1055.011) [487]

EV Code	Vulnerability Description
EV1055.011-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.7.137 Process Injection: Process Hollowing (T1055.012) [488]

EV Code	Vulnerability Description
EV1055.012-S1	The susceptibility of processes to process hollowing, exploiting the ability to create a process in a suspended state and subsequently unmapping its memory, allowing the injection of malicious code undetected.
EV1055.012-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.7.138 Process Injection: Process Doppelganging (T1055.013) [489]

EV Code	Vulnerability Description
EV1055.013-S1	The reliance on Windows Transactional NTFS (TxF) in the system, introduced in Vista and still enabled as of Windows 10, allows adversaries to abuse TxF for a file-less variation of Process Injection, potentially evading detection and defenses.
EV1055.013-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.7.139 Process Injection: VDSO Hijacking (T1055.014) [490]

EV Code	Vulnerability Description
EV1055.014-S1	The potential weakness in memory protections, allowing the injection of malicious code into processes through VDSO hijacking, potentially evading process-based defenses and enabling privilege escalation.
EV1055.014-S2	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.7.140 Process Injection: ListPlanting (T1055.015) [491]

EV Code	Vulnerability Description
EV1055.015-S1	Insufficient configuration of endpoint security solutions, which may fail to effectively block process injection based on common behavioral sequences, leaving the system susceptible to exploitation.

2.7.141 Reflective Code Loading (T1620) [499]

This attack technique does not rely on a specific vulnerability for execution.

2.7.142 Rogue Domain Controller (T1207) [516]

EV Code	Vulnerability Description
EV1207-S1	Insufficient protection of Administrator privileges, either at the domain or local level, or the exposure of the KRBTGT hash, required for registering a rogue Domain Controller, leading to unauthorized access and manipulation of Active Directory.
EV1207-S2	Inadequate monitoring and response mechanisms, allowing the adversary to use the technique to alter, delete replication, and associated metadata, hindering forensic analysis.

2.7.143 Rootkit (T1014) [517]

EV Code	Vulnerability Description
EV1014-S1	The weaknesses in the operating system's design, allowing adversaries to intercept and modify system API calls to hide the presence of malware effectively.

2.7.144 Subvert Trust Controls (T1553) [567]

EV Code	Vulnerability Description
EV1553-S1	Inadequate application control settings, as the system allows the execution of applications not obtained from legitimate repositories, potentially enabling malicious content to run.
EV1553-S2	Lack of proper enforcement of the Flags value in the Registry (HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots), allowing non-administrator users to potentially make unauthorized root installations in their own HKCU certificate store.
EV1553-S3	Absence of restrictions on software configuration, as the system does not employ HTTP Public Key Pinning (HPKP), leaving it vulnerable to potential interception of encrypted communications through mis-issued or fraudulent certificates.
EV1553-H1	Failure to configure Windows Group Policy to manage root certificates, leaving the system susceptible to unauthorized root installations by non-administrator users.
EV1553-H2	Insufficient restrictions on Registry permissions, exposing the system to potential hijacking of components related to SIP and trust providers through unauthorized modifications to Registry keys.

2.7.145 Subvert Trust Controls: Gatekeeper Bypass (T1553.001) [568]

EV Code	Vulnerability Description
EV1553.001-S1	The limited scope of code signing and notarization checks in Gatekeeper, specifically the fact that these checks were only conducted on first launch prior to macOS 13 Ventura, enabling adversaries to bypass security controls.
EV1553.001-S2	The possibility of not setting the quarantine flag on applications and files loaded onto the system from certain sources, such as USB flash drives, optical disks, external hard drives, local network shares, or using the curl command, which can bypass Gatekeeper security checks.

EV1553.001-H1	User overrides notarization, resulting in the execution of an "unauthorized app" and modification of the security policy, allowing adversaries to bypass Gatekeeper controls.
EV1553.001-H2	The failure to configure system settings to restrict the execution of applications solely to those downloaded through the Apple Store, leading to an increased risk of malicious program execution.

2.7.146 Subvert Trust Controls: Code Signing (T1553.002) **[569]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.147 Subvert Trust Controls: SIP and Trust Provider Hijacking (T1553.003) **[570]**

EV Code	Vulnerability Description
EV1553.003-S1	Failure to properly secure and control Registry values in HKLM\SOFTWARE[\WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{SIP_GUID} may lead to unauthorized modifications by an adversary, exploiting the user's failure to secure critical system configurations.
EV1553.003-S2	Inadequate control over Registry values in HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{SIP_GUID} can allow an adversary to manipulate validation processes, exploiting the user's failure to enforce proper access controls.
EV1553.003-S3	Insufficient safeguards on Registry values in HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\Providers\Trust\FinalPolicy{trust provider GUID} may result in an adversary exploiting the user's failure to secure critical trust provider configurations, potentially leading to trust decisions based on manipulated DLLs.
EV1553.003-H1	Failure to implement proper application control solutions like AppLocker and/or Device Guard may expose the system to the loading of malicious SIP DLLs, allowing adversaries to execute unauthorized code.

EV1553.003-H2	Insufficient restriction of file and directory permissions, potentially leading to the storage and execution of SIP DLLs in user directories, rather than restricting them to protected directories like C:\Windows.
EV1553.003-H3	Inadequate registry permissions, which could allow users to modify keys related to SIP and trust provider components, potentially leading to the hijacking of components for malicious purposes if proper permissions are not enforced.

2.7.148 Subvert Trust Controls: Install Root Certificate (T1553.004) [571]

EV Code	Vulnerability Description
EV1553.004-S1	Misconfiguration of Windows Group Policy, as non-administrator users can potentially compromise the system by making unauthorized root installations into their HKCU certificate store, circumventing the ProtectedRoots setting.
EV1553.004-H1	The failure to implement HTTP Public Key Pinning (HPKP), which could lead to Adversary-in-the-Middle situations where an adversary exploits mis-issued or fraudulent certificates to intercept encrypted communications
EV1553.004-H2	The failure to adhere to recommended security measures, such as failing to configuring the Flags value of HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots as 1, allowing unauthorized root installations.

2.7.149 Subvert Trust Controls: Mark-of-the-Web Bypass (T1553.005) [572]

EV Code	Vulnerability Description
EV1553.005-S1	The potential failure to recognize the limitations of MOTW controls, as extracting or mounting container files can lead to the loss of MOTW protection for files within, allowing them to be treated as local files on disk and executed without safeguards.
EV1553.005-S2	The misconfiguration of web and email gateways, which may allow the passage of container file types and compromise the execution prevention measures.

EV1553.005-H1	The failure to disable or remove the automatic mounting of disk image files, leaving the system exposed to potential exploitation.
EV1553.005-H2	The failure to properly unregister container file extensions in Windows File Explorer, leaving the system susceptible to the execution of malicious containers despite the intended prevention measures.

2.7.150 Subvert Trust Controls: Code Signing Policy Modification (T1553.006) [573]

EV Code	Vulnerability Description
EV1553.006-S1	The exploitable weakness in kernel memory that allows modification of variables, such as g_CiOptions, leading to the disabling of Driver Signature Enforcement
EV1553.006-S2	The potential weakness in Secure Boot implementations that may not fully prevent all modifications to code signing policies, leaving room for exploitation.
EV1553.006-S3	Insufficiently restricted registry permissions, enabling adversaries to modify keys related to code signing policies and compromising the integrity of the system.
EV1553.006-H1	Misconfiguration of user privileges, where improper assignment of administrative accounts for day-to-day operations increases the risk of exposure to potential adversaries.

2.7.151 System Binary Proxy Execution (T1218) [578]

EV Code	Vulnerability Description
EV1218-S1	The reliance on signed, trusted binaries, specifically Microsoft-signed files, which can be abused to proxy execution of malicious content, bypassing process and signature-based defenses.
EV1218-S2	The lack of exploit protection mechanisms, specifically the absence of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature, allowing methods that use trusted binaries to bypass application control.

EV1218-H1	The potential oversight or failure to disable unnecessary native binaries within a given environment, which could be exploited for proxy execution.
EV1218-H2	The failure to implement proper execution prevention measures, such as application control, leading to the potential abuse of binaries susceptible to exploitation for malicious purposes.
EV1218-H3	The inadequate privileged account management, allowing the unrestricted execution of particularly vulnerable binaries by non-privileged accounts, increasing the risk of malicious usage.

2.7.152 System Binary Proxy Execution: Compiled HTML File (T1218.001) **[579]**

EV Code	**Vulnerability Description**
EV1218.001-S1	The potential for inadequate application control, as hh.exe may not be restricted, allowing adversaries to exploit it for execution purposes.
EV1218.001-H1	Inadequate web content restriction, exposing the system to potential threats through the download, transfer, and execution of uncommon file types, such as CHM files.

2.7.153 System Binary Proxy Execution: Control Panel (T1218.002) **[580]**

EV Code	**Vulnerability Description**
EV1218.002-S1	Misconfigurations in application control tools, such as Windows Defender Application Control, AppLocker, or Software Restriction Policies, which could allow an attacker to bypass execution prevention measures.
EV1218.002-H1	The inadequate restriction of file and directory permissions, as storing and executing Control Panel items in user directories instead of protected directories like C:\Windows can expose the system to potential security risks.

2.7.154 System Binary Proxy Execution: CMSTP (T1218.003) [581]

EV Code	Vulnerability Description
EV1218.003-S1	The legitimate binary's functionality of CMSTP.exe, which enables adversaries to load and execute DLLs and/or COM scriptlets (SCT) from remote servers, potentially bypassing AppLocker and other application control defenses.
EV1218.003-H1	The failure to disable or remove the CMSTP.exe feature when it is not required, leaving the system exposed to potential attacks that leverage this unnecessary functionality.

2.7.155 System Binary Proxy Execution: InstallUtil (T1218.004) [582]

EV Code	Vulnerability Description
EV1218.004-S1	The absence of execution prevention measures, such as application control configured to block the execution of InstallUtil.exe when not required, thereby allowing adversaries to exploit the utility for malicious purposes.
EV1218.004-H1	The failure to disable or remove unnecessary features or programs, such as InstallUtil, within an environment, leaving an avenue for misuse and unauthorized execution of code.

2.7.156 System Binary Proxy Execution: Mshta (T1218.005) [583]

EV Code	Vulnerability Description
EV1218.005-S1	The ability of mshta.exe to bypass application control solutions that do not account for its use, enabling the circumvention of security measures.
EV1218.005-H1	The failure to implement or configure application control to block the execution of mshta.exe when it is not required for a given system or network, allowing adversaries to potentially exploit this oversight and misuse the utility for malicious purposes.

EV1218.005-H2	The failure to disable or remove the mshta.exe feature, leaving the system exposed to potential exploitation, especially in environments where its functionality is not necessary.

2.7.157 System Binary Proxy Execution: Msiexec (T1218.007) [584]

EV Code	Vulnerability Description
EV1218.007-S1	The potential oversight in application control solutions that do not account for the abuse of msiexec.exe, particularly if it is signed and native on Windows systems, allowing adversaries to bypass these security measures.
EV1218.007-H1	The failure to disable the AlwaysInstallElevated policy, leaving the system exposed to potential misuse by allowing elevated execution of Windows Installer packages without necessary restrictions.
EV1218.007-H2	The inadequate restriction on the execution of Msiexec.exe, as it is not limited to privileged accounts or groups, providing more opportunities for malicious usage by unauthorized individuals.

2.7.158 System Binary Proxy Execution: Odbcconf (T1218.008) [585]

EV Code	Vulnerability Description
EV1218.008-H1	The potential failure to disable or remove Odbcconf.exe when it is not necessary for a given system, which could result in adversaries exploiting its functionality for malicious purposes.
EV1218.008-H2	User fails to configure application control to block the execution of Odbcconf.exe when not required, exposing the system to potential misuse by adversaries.

2.7.159 System Binary Proxy Execution: Regsvcs/Regasm (T1218.009) [586]

EV Code	Vulnerability Description
EV1218.009-S1	The inadequate implementation of application control, as both Regsvcs and Regasm can be utilized to bypass application control by specifying code execution through attributes within the binary, such as [ComRegisterFunction] or [ComUnregisterFunction], even when the process runs with insufficient privileges, resulting in the execution of the specified code.
EV1218.009-H1	The potential failure to disable or remove unnecessary features or programs like Regsvcs and Regasm, leaving avenues for exploitation.
EV1218.009-H2	The failure to implement execution prevention measures, such as blocking the execution of Regsvcs.exe and Regasm.exe when not required, allowing adversaries to potentially misuse these utilities for proxy code execution.

2.7.160 System Binary Proxy Execution: Regsvr32 (T1218.010) [587]

EV Code	Vulnerability Description
EV1218.010-S1	The limited monitoring of Regsvr32.exe execution and loaded modules, often resulting from allowlists or false positives, helping adversaries to evade security tools
EV1218.010-S2	The potential failure of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) Attack Surface Reduction (ASR) feature, leading to a bypass of application control and exploitation of regsvr32.exe.
EV1218.010-S3	The ability of Regsvr32.exe to bypass application control and execute DLLs under user permissions using COM scriptlets.
EV1218.010-S4	The network and proxy awareness of Regsvr32.exe, allowing the loading of scripts from external web servers, as demonstrated in the "Squiblydoo" technique.

EV1218.010-S5	The misconfiguration or inadequate implementation of application control tools, such as Windows Defender Application Control, AppLocker, or Software Restriction Policies, which may allow the execution of potentially malicious software through regsvr32 functionality.

2.7.161 System Binary Proxy Execution: Rundll32 (T1218.011) **[588]**

EV Code	Vulnerability Description
EV1218.011-S1	The system's weakness in monitoring rundll32.exe processes due to allowlists or false positives from normal operations, allowing adversaries to proxy execute malicious code
EV1218.011-S2	The capability of rundll32.exe to execute Control Panel Item files (.cpl) and scripts, providing avenues for launching malicious activities.
EV1218.011-S3	The capability of rundll32.exe to execute JavaScript, such as rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")", allowing for the execution of malicious scripts and exploited by malware like Poweliks.
EV1218.011-S4	The wide/Unicode and ANSI character-supported functions behavior of rundll32.exe, where adversaries may obscure malicious code by creating multiple identical exported function names and appending W and/or A to harmless ones, thus evading detection.
EV1218.011-S5	The absence of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar exploit protection mechanisms, leaving the system susceptible to methods of using rundll32.exe to bypass application control.

2.7.162 System Binary Proxy Execution: Verclsid (T1218.012) [589]

EV Code	Vulnerability Description
EV1218.012-S1	The verclsid.exe is a signed and/or native binary on Windows systems responsible for verifying shell extensions, allowing for the execution of malicious payloads and bypassing application control solutions that do not account for this specific abuse.
EV1218.012-H1	The failure to appropriately configure application control, allowing for potential misuse of verclsid.exe, indicating a lapse in user-defined execution prevention measures.
EV1218.012-H2	The insufficient modification of host firewall rules, leaving verclsid.exe susceptible to egress traffic and highlighting a user oversight in network traffic filtering.
EV1218.012-H3	Inadequate access control, as the presence of unnecessary features or programs like verclsid.exe may provide an avenue for exploitation if not properly managed.

2.7.163 System Binary Proxy Execution: Mavinject (T1218.013) [590]

EV Code	Vulnerability Description
EV1218.013-S1	The mavinject.exe is digitally signed by Microsoft, thus adversaries can exploit this to mask the execution of malicious code under a legitimate process, leading to the possible evasion of security product detection.
EV1218.013-H1	The failure to disable or remove mavinject.exe when Microsoft App-V is not utilized, creating an unnecessary and exploitable feature that could be targeted by adversaries.
EV1218.013-H2	The failure to implement execution prevention measures, such as application control, which could lead to unauthorized execution of mavinject.exe and compromise system security.

2.7.164 System Binary Proxy Execution: MMC (T1218.014) [591]

EV Code	Vulnerability Description
EV1218.014-S1	Microsoft Management Console's (MMC) functionality for creating, opening, and saving custom consoles, where adversaries may abust this functionality to proxy execution of malicious .msc files, compromising system integrity and security.
EV1218.014-H1	The failure to disable or remove the MMC feature, leaving it accessible to regular users or clients and increasing the risk of potential misuse by adversaries.
EV1218.014-H2	The misconfiguration of application control, such as failing to properly block the execution of MMC when it is not necessary, leading to a potential avenue for adversaries to misuse the tool.

2.7.165 System Script Proxy Execution (T1216) [600]

EV Code	Vulnerability Description
EV1216-S1	The vulnerabilities from trusted Microsoft-signed scripts, downloaded from Microsoft or default on Windows installations, allowing the proxy execution of malicious files, thereby bypassing application control and signature validation on systems.
EV1216-H1	The failure to appropriately configure and maintain application control settings, leading to the continued availability of signed scripts that are not essential for the system or network, thereby increasing the risk of misuse by adversaries.

2.7.166 System Script Proxy Execution: PubPrn (T1216.001) [601]

EV Code	Vulnerability Description
EV1216.001-S1	The vulnerability of PubPrn.vbs, specifically in versions prior to Windows 10, allowing proxy execution of malicious remote files by referencing scriptlet files hosted on remote sites.

EV1216.001-H1	The potential failure to update Windows Defender Application Control policies on Windows 10, leaving the system susceptible to exploitation by adversaries leveraging older, vulnerable versions of PubPrn.
EV1216.001-H2	The failure to implement application control to block the execution of unnecessary signed scripts, which could lead to the misuse of these scripts by adversaries if not properly restricted based on system requirements.

2.7.167 Template Injection (T1221) **[609]**

EV Code	Vulnerability Description
EV1221-S1	The weaknesses in Microsoft Office Open XML (OOXML) file parsing, which may allow adversaries to inject and conceal malicious code within user document templates.
EV1221-S2	The potential failure or misconfiguration of network/host intrusion prevention systems, antivirus, or detonation chambers, which may allow malicious documents to evade detection and execution prevention.
EV1221-H1	The failure of users to identify and avoid social engineering techniques and spearphishing emails, leading to the inadvertent opening and execution of malicious documents, bypassing training efforts.
EV1221-H2	The potential failure to disable or remove Microsoft Office macros/active content, leaving the system exposed to the execution of malicious payloads in documents.

2.7.168 Traffic Signaling (T1205) **[610]**

EV Code	Vulnerability Description
EV1205-H1	Failure to disable or remove the Wake-on-LAN feature when not needed within an environment, which could expose systems to unauthorized activation and subsequent lateral movement.

EV1205-H2	The potential failure to implement stateful firewalls effectively, allowing some variants of traffic signaling to bypass network defenses.

2.7.169 Traffic Signaling: Port Knocking (T1205.001) [611]

EV Code	Vulnerability Description
EV1205.001-H1	The potential failure to implement or configure stateful firewalls effectively, leaving the system susceptible to variants of the port knocking technique and associated adversarial activities.

2.7.170 Traffic Signaling: Socket Filters (T1205.002) [612]

EV Code	Vulnerability Description
EV1205.002-H1	The potential misconfiguration or improper implementation of stateful firewalls, introducing the risk of ineffective mitigation and leaving the system susceptible to network traffic filtering manipulations by adversaries.

2.7.171 Trusted Developer Utilities Proxy Execution (T1127) [614]

EV Code	Vulnerability Description
EV1127-H1	The potential oversight or failure to disable or remove unnecessary developer utilities within a given environment, leaving avenues for malicious actors to exploit these utilities for proxy execution of code.
EV1127-H2	The potential neglect to implement execution prevention measures, such as blocking or restricting specific developer utilities that are not required, thereby exposing the system to exploitation by adversaries leveraging trusted processes for malicious code execution.

2.7.172 Trusted Developer Utilities Proxy Execution: MSBuild (T1127.001) [615]

EV Code	Vulnerability Description
EV1127.001-H1	The potential oversight or neglect to disable or remove MSBuild.exe, as it may not be necessary within an environment and should be removed if not being used.
EV1127.001-H2	The failure to implement execution prevention measures, such as not configuring application control to block the execution of msbuild.exe when it is not required, leaving the system susceptible to potential misuse by adversaries.

2.7.173 Unused/Unsupported Cloud Regions (T1535) [626]

EV Code	Vulnerability Description
EV1535-H1	The failure to deactivate unused regions, which is a crucial step in implementing the mitigation strategy provided by cloud service providers, potentially allowing adversaries to exploit these regions for malicious activities.

2.7.174 Use Alternate Authentication Material (T1550) [627]

EV Code	Vulnerability Description
EV1550-S1	The potential for credential overlap across systems, which could result in the compromise of privileged accounts and increase the risk of lateral movement.
EV1550-H1	The potential mismanagement of user accounts, specifically allowing domain users to be members of the local administrator group on multiple systems, violating the principle of least privilege and creating a security risk.

2.7.175 Use Alternate Authentication Material: Application Access Token (T1550.001) **[628]**

EV Code	Vulnerability Description
EV1550.001-H1	The failure to enforce file encryption for email communications containing sensitive information, leaving the data exposed to potential compromise through unauthorized access to email services.
EV1550.001-H2	The absence of measures to block end-user consent through administrative portals, such as the Azure Portal, leading to the potential for users to authorize third-party apps through OAuth without administrative oversight, resulting in unauthorized access.
EV1550.001-H3	The potential oversight in auditing cloud and container accounts, allowing unnecessary accounts or inappropriate permissions, and the failure to disable the ability to request temporary account tokens on behalf of other accounts, which could lead to unauthorized access.
EV1550.001-H4	The lack of specific and detailed corporate policies to restrict the types of third-party applications added to online services or tools, potentially allowing the introduction of malicious applications and unauthorized access to company information, accounts, or network.

2.7.176 Use Alternate Authentication Material: Pass the Hash (T1550.002) **[629]**

EV Code	Vulnerability Description
EV1550.002-S1	The excessive credential overlap across systems, which can amplify the impact of credential compromise and increase the adversary's ability to perform lateral movement.
EV1550.002-S2	The absence of pass-the-hash mitigations, particularly the failure to enable UAC restrictions on local accounts during network logon, potentially facilitating unauthorized access and lateral movement.
EV1550.002-H1	The failure to apply necessary software updates, specifically patch KB2871997 on Windows 7 and higher systems, which could leave systems exposed to known vulnerabilities and exploitation.

EV1550.002-H2	The risk of domain users being assigned to the local administrator group on multiple systems, creating a potential avenue for credential compromise and privilege escalation.
EV1550.002-H3	The failure to implement recommended pass-the-hash mitigations through Group Policy, leaving systems susceptible to pass-the-hash attacks due to insufficient UAC restrictions on local accounts during network logons.

2.7.177 Use Alternate Authentication Material: Pass the Ticket (T1550.003) [630]

EV Code	Vulnerability Description
EV1550.003-S1	The inadequate configuration of Active Directory, allowing the persistence of golden tickets
EV1550.003-H1	The over-assignment of domain admin account permissions, leaving domain controllers and limited servers vulnerable
EV1550.003-H2	The failure to ensure complex, unique passwords for local administrator accounts, potentially compromising the security of the system.
EV1550.003-H3	The allowance of a user to be a local administrator for multiple systems, posing a security risk

2.7.178 Use Alternate Authentication Material: Web Session Cookie (T1550.004) [631]

EV Code	Vulnerability Description
EV1550.004-S1	The extended validity period of authentication cookies in web applications, which allows for the stealing and use of session cookies to bypass multi-factor authentication, gaining unauthorized access to sensitive information.
EV1550.004-H1	The failure to configure browsers or tasks to regularly delete persistent cookies, increasing the risk of unauthorized access to web applications and services by adversaries through the exploitation of stolen session cookies.

2.7.179 Valid Accounts (T1078) [636]

EV Code	Vulnerability Description
EV1078-S1	The potential lack of proper configuration and monitoring of conditional access policies, allowing non-compliant devices or logins from outside defined organization IP ranges.
EV1078-H1	The use of legacy authentication in Active Directory, which does not support multi-factor authentication (MFA), and the failure to enforce the use of modern authentication protocols.
EV1078-H2	The insecure storage of sensitive data or credentials in applications, such as storing plaintext credentials in code, publishing credentials in repositories, or leaving credentials in public cloud storage, providing opportunities for adversaries to compromise credentials.
EV1078-H3	The failure to promptly change default usernames and passwords on applications and appliances after installation, potentially leaving systems exposed to credential abuse.
EV1078-H4	The potential lack of routine audits of domain and local accounts, their permission levels, and the failure to detect situations that could allow adversaries to gain wide access by obtaining credentials of privileged accounts.
EV1078-H5	The failure to regularly audit user accounts for activity and deactivate or remove unnecessary accounts, increasing the risk of adversaries exploiting unused accounts for unauthorized access.
EV1078-H6	The lack of awareness and training regarding multi-factor authentication (MFA) push notifications, potentially leading users to accept and authenticate malicious notifications, compromising account security.

2.7.180 Valid Accounts: Default Accounts (T1078.001) [637]

EV Code	Vulnerability Description
EV1078.001-H1	The presence of default accounts with unchanged credentials, such as Guest or Administrator accounts on Windows systems, which can be exploited for Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.001-H2	The failure to change preset usernames and passwords for equipment like network devices and computer applications, including internal, open source, or commercial systems, which poses a serious threat if not altered post-installation.

2.7.181 Valid Accounts: Domain Accounts (T1078.002) [638]

EV Code	Vulnerability Description
EV1078.002-S1	Lack of multi-factor authentication (MFA) implementation, potentially allowing adversaries to gain control of valid credentials.
EV1078.002-S2	Poor design and administration of the enterprise network, potentially leading to the inappropriate inclusion of user or admin domain accounts in local administrator groups across systems, creating a security risk equivalent to having a common local administrator account password.
EV1078.002-H1	Password reuse, which can be exploited by adversaries to compromise domain accounts, posing a risk to Initial Access, Persistence, Privilege Escalation, or Defense Evasion.
EV1078.002-H2	Inadequate privileged account management, including the lack of routine audits on domain account permission levels, which could enable adversaries to exploit overly permissive access and compromise privileged accounts.
EV1078.002-H3	Insufficient user training on recognizing valid push notifications for multi-factor authentication, increasing the risk of users accepting fraudulent notifications and compromising the effectiveness of MFA.

EV1078.002-H4	Weak password management practices, resulting in credential overlap across systems and increasing the risk of unauthorized access if an adversary obtains account credentials.

2.7.182 Valid Accounts: Local Accounts (T1078.003) **[639]**

EV Code	Vulnerability Description
EV1078.003-H1	The inadequate enforcement of complex, unique passwords for local administrator accounts across all systems, potentially allowing unauthorized access.
EV1078.003-H2	The reuse of passwords for local accounts, enabling adversaries to abuse credentials across multiple machines on a network, facilitating Privilege Escalation and Lateral Movement.
EV1078.003-H3	The inadequate management of privileged accounts, as routine audits may be neglected, leading to situations where adversaries can exploit credentials of privileged accounts with wide access.
EV1078.003-H4	The improper use of local administrator accounts for day-to-day operations may expose user to potential adversaries, posing a security risk.

2.7.183 Valid Accounts: Cloud Accounts (T1078.004) **[640]**

EV Code	Vulnerability Description
EV1078.004-S1	The absence of multi-factor authentication for cloud accounts, especially privileged accounts, which could leave accounts susceptible to unauthorized access.
EV1078.004-S2	The potential for misconfigurations in conditional access policies, allowing logins from non-compliant devices or outside defined organization IP ranges.
EV1078.004-H1	Misconfigurations in role assignments or role assumption policies within cloud environments, enabling unauthorized access and privilege escalation.

EV1078.004-H2	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H3	The failure to disable legacy authentication, which does not support multi-factor authentication (MFA), and not requiring the use of modern authentication protocols, potentially leaving accounts vulnerable to compromise.
EV1078.004-H4	The lack of enforcement of complex, unique passwords across all systems on the network, particularly for privileged cloud accounts, potentially allowing adversaries to exploit compromised credentials.
EV1078.004-H5	The inadequate review of privileged cloud account permission levels, which may result in the presence of high-risk roles such as Global Administrator and Privileged Role Administrator, providing adversaries with extensive access.
EV1078.004-H6	The failure to periodically review and remove inactive or unnecessary user accounts, potentially leaving dormant accounts that could be exploited by adversaries.
EV1078.004-H7	The potential for users to accept and act on invalid push notifications for multi-factor authentication, highlighting the importance of training users to recognize and report suspicious push notifications.

2.7.184 Virtualization/Sandbox Evasion (T1497) **[642]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.185 Virtualization/Sandbox Evasion: System Checks (T1497.001) **[643]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.186 Virtualization/Sandbox Evasion: User Activity Based Checks (T1497.002) **[644]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.187 Virtualization/Sandbox Evasion: Time Based Evasion (T1497.003) **[645]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.188 Weaken Encryption (T1600) **[646]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.189 Weaken Encryption: Reduce Key Space (T1600.001) **[647]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.190 Weaken Encryption: Disable Crypto Hardware (T1600.002) **[648]**

This attack technique does not rely on a specific vulnerability for execution.

2.7.191 XSL Script Processing (T1220) **[654]**

EV Code	Vulnerability Description
EV1220-S1	The reliance on default configurations, as not blocking the execution of unnecessary msxsl.exe increases the risk of adversaries exploiting this utility for malicious purposes.

2.8 Credential Access (TA0006) [11]

2.8.1 Adversary-in-the-Middle (T1557) [69]

EV Code	Vulnerability Description
EV1557-S1	The weaknesses in common networking protocols (e.g., ARP, DNS, LLMNR) to manipulate network traffic flow and force communication through an adversary-controlled system, allowing for information collection and additional actions.
EV1557-S2	The susceptibility to Downgrade Attacks, where adversaries negotiate a less secure, deprecated, or weaker version of communication protocols (e.g., SSL/TLS) or encryption algorithms to establish an AiTM position.
EV1557-S3	The potential lack of disabling or removal of legacy network protocols, leaving avenues for intercepting network traffic and enabling Adversary-in-the-Middle attacks.
EV1557-S4	The potential absence of encryption for sensitive information in wired and/or wireless traffic, providing opportunities for unauthorized access and manipulation.
EV1557-S5	The lack of network traffic filtering, allowing the exploitation of unnecessary legacy protocols that could be leveraged for Adversary-in-the-Middle conditions.
EV1557-S6	The absence of access limitations to network infrastructure and resources that can be exploited to reshape traffic or produce Adversary-in-the-Middle conditions.
EV1557-S7	The potential absence of network intrusion prevention systems capable of identifying and mitigating Adversary-in-the-Middle activity by recognizing indicative traffic patterns.
EV1557-S8	The lack of network segmentation, potentially allowing broader access to infrastructure components and increasing the scope of Adversary-in-the-Middle activity.
EV1557-H1	The lack of awareness and training regarding certificate errors, potentially leading to users accepting unauthorized certificates used by adversaries attempting to intercept HTTPS traffic.

2.8.2 *Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001)* [70]

EV Code	Vulnerability Description
EV1557.001-S1	The vulnerability in LLMNR and NBT-NS protocols, allowing adversaries to spoof authoritative sources and poison name resolution, forcing communication with adversary-controlled systems.
EV1557.001-S2	The weakness in NTLMv1/v2 authentication, where adversaries can intercept and relay hashes, gaining unauthorized access and executing code on target systems.
EV1557.001-S3	The susceptibility of various protocols (LDAP, SMB, MSSQL, HTTP) to NTLMv1/v2 hash encapsulation, enabling adversaries to expand their attack surface and use multiple services with valid NTLM responses.
EV1557.001-S4	The potential lack of implementation or effectiveness of network intrusion detection and prevention systems, allowing adversaries to conduct AiTM activities without detection.
EV1557.001-S5	The absence or inadequacy of network segmentation, as failure to isolate infrastructure components increases the potential impact and scope of AiTM activity.
EV1557.001-H1	Failure to disable LLMNR and NetBIOS in their local computer security settings, providing an opportunity for adversaries to exploit these features.
EV1557.001-H2	User may neglect to implement host-based security software to filter LLMNR/NetBIOS traffic or enable SMB Signing, leaving systems susceptible to NTLMv2 relay attacks.

2.8.3 *Adversary-in-the-Middle: ARP Cache Poisoning (T1557.002)* [71]

EV Code	Vulnerability Description
EV1557.002-S1	The lack of authentication in the ARP protocol, allowing adversaries to poison ARP caches without authentication, leading to potential man-in-the-middle attacks.

EV1557.002-S2	The incorrect handling of ARP responses by network devices, where devices may wrongly add or update MAC addresses associated with IP addresses in their ARP caches, facilitating successful ARP cache poisoning by adversaries.
EV1557.002-S3	The reliance on broadcast ARP requests for IP-to-MAC address resolution, which can be exploited by adversaries to intercept and manipulate network traffic through ARP cache poisoning.
EV1557.002-S4	The lack of default measures to disable or prevent updating the ARP cache on gratuitous ARP replies, leaving the system susceptible to ARP cache poisoning attacks.
EV1557.002-S5	The absence of encryption on wired and/or wireless traffic, potentially exposing sensitive information, including credentials, to interception during ARP cache poisoning attacks.
EV1557.002-S6	The lack of filtering mechanisms for network traffic, as the absence of DHCP Snooping and Dynamic ARP Inspection on switches may allow malicious ARP replies to propagate, contributing to successful ARP cache poisoning.
EV1557.002-S7	The reliance on dynamic ARP entries, as the absence of static ARP entries for networked devices leaves the system vulnerable to ARP cache poisoning attacks.
EV1557.002-S8	The absence of network intrusion prevention systems capable of identifying patterns indicative of Adversary-in-the-Middle (AiTM) activity, which could mitigate ARP cache poisoning at the network level.
EV1557.002-H1	The potential for overlooking certificate errors, as users may not be adequately trained to be suspicious of certificate errors that could indicate attempts by adversaries to intercept HTTPS traffic during ARP cache poisoning attacks.

2.8.4 Adversary-in-the-Middle: DHCP Spoofing (T1557.003) [72]

EV Code	Vulnerability Description
EV1557.003-S1	The DHCPv6 client's capability to receive network configuration information without being assigned an IP address, creating an avenue for adversaries to respond with malicious configurations.
EV1557.003-S2	The DHCP service's susceptibility to exhaustion attacks, where adversaries can flood the network with broadcast DISCOVER messages, depleting the DHCP allocation pool and causing a denial of service.
EV1557.003-S3	The potential weakness in the network infrastructure, where failure to implement DHCP traffic filtering on ports 67 and 68 may expose the network to unauthorized DHCP servers, enabling adversaries to conduct DHCP spoofing attacks.
EV1557.003-S4	The absence of DHCP snooping on layer 2 switches, which can lead to DHCP spoofing attacks and starvation attacks by allowing adversaries to provide malicious network configurations.
EV1557.003-S5	The failure to block DHCPv6 traffic and incoming router advertisements, particularly if IPv6 is not commonly used in the network, which may expose the network to potential DHCPv6 attacks.
EV1557.003-H1	The failure to enable port security on layer switches, leaving the network susceptible to unauthorized devices connecting via DHCP and potentially facilitating DHCP spoofing attacks.
EV1557.003-H2	The lack of tracking available IP addresses through a script or a tool, making it difficult to detect and respond to DHCP exhaustion attacks that may result from the misuse of DHCP.
EV1557.003-H3	The oversight in implementing network intrusion detection and prevention systems capable of identifying AiTM activity, which may result in a delayed or ineffective response to DHCP spoofing and related attacks.

2.8.5 Brute Force (T1110) [112]

EV Code	Vulnerability Description
EV1110-S1	The absence of effective account lockout policies, potentially leading to a denial of service condition if too strict, or allowing prolonged brute force attempts if too lenient.
EV1110-H1	The lack of multi-factor authentication implementation on both internal and externally facing services, which increases the risk of successful brute force attacks.
EV1110-H2	The absence of adherence to NIST guidelines when creating password policies, potentially resulting in weak password configurations that are susceptible to brute force attacks.
EV1110-H3	The lack of proactive user account management, including the failure to reset accounts known to be part of breached credentials promptly, increasing the window of opportunity for adversaries conducting brute force attacks.
EV1110-H4	The failure to use strong and unique passwords, as well as the reuse of passwords across multiple accounts, undermining the effectiveness of password policies and increasing susceptibility to brute force attacks.

2.8.6 Brute Force: Password Guessing (T1110.001) [113]

EV Code	Vulnerability Description
EV1110.001-S1	The absence of effective account lockout policies, potentially leading to a denial of service condition if too strict, or allowing prolonged brute force attempts if too lenient.
EV1110.001-H1	The lack of multi-factor authentication implementation on both internal and externally facing services, which increases the risk of successful brute force attacks.
EV1110.001-H2	The absence of adherence to NIST guidelines when creating password policies, potentially resulting in weak password configurations that are susceptible to brute force attacks.

EV1110.001-H3	The lack of proactive user account management, including the failure to reset accounts known to be part of breached credentials promptly, increasing the window of opportunity for adversaries conducting brute force attacks.
EV1110.001-H4	The failure to use strong and unique passwords, as well as the reuse of passwords across multiple accounts, undermining the effectiveness of password policies and increasing susceptibility to brute force attacks.

2.8.7 Brute Force: Password Cracking (T1110.002) [114]

EV Code	Vulnerability Description
EV1110.002-H1	The absence or inadequacy of multi-factor authentication, making it more susceptible to password cracking attempts
EV1110.002-H2	User does not follow recommended password policies, as outlined by NIST guidelines, potentially leading to the use of weak passwords that are more susceptible to brute force attacks.

2.8.8 Brute Force: Password Spraying (T1110.003) [115]

EV Code	Vulnerability Description
EV1110.003-S1	The absence of effective account lockout policies, potentially leading to a denial of service condition if too strict, or allowing prolonged brute force attempts if too lenient.
EV1110.003-H1	The lack of multi-factor authentication implementation on both internal and externally facing services, which increases the risk of successful brute force attacks.
EV1110.003-H2	User does not follow recommended password policies, as outlined by NIST guidelines, potentially leading to the use of weak passwords that are more susceptible to brute force attacks.

2.8.9 Brute Force: Credential Stuffing (T1110.004) [116]

EV Code	Vulnerability Description
EV1110.004-S1	The absence of effective account lockout policies, potentially leading to a denial of service condition if too strict, or allowing prolonged brute force attempts if too lenient.
EV1110.004-H1	The lack of multi-factor authentication implementation on both internal and externally facing services, which increases the risk of successful brute force attacks.
EV1110.004-H2	The absence of adherence to NIST guidelines when creating password policies, potentially resulting in weak password configurations that are susceptible to brute force attacks.
EV1110.004-H3	The lack of proactive user account management, including the failure to reset accounts known to be part of breached credentials promptly, increasing the window of opportunity for adversaries conducting brute force attacks.
EV1110.004-H4	The failure to use strong and unique passwords, as well as the reuse of passwords across multiple accounts, undermining the effectiveness of password policies and increasing susceptibility to brute force attacks.
EV1110.004-H5	The reuse of passwords across personal and business accounts, increasing the risk of compromise when credentials are exposed in breach dumps.

2.8.10 Credentials from Password Stores (T1555) [160]

EV Code	Vulnerability Description
EV1555-H1	The insecure storage of passwords in common locations, such as password stores, which facilitates unauthorized access.
EV1555-H2	The failure to adhere to password policies, such as using weak passwords, which can undermine the effectiveness of security measures and contribute to the compromise of credentials stored in password stores.

EV1555-H3	The potential mismanagement of privileged accounts, leading to an increased risk of unauthorized access to sensitive information stored in password stores

2.8.11 Credentials from Password Stores: Keychain (T1555.001) [161]

EV Code	Vulnerability Description
EV1555.001-H1	The potential weakness in password policies, allowing adversaries to exploit Keychain credentials if users employ weak or easily guessable passwords

2.8.12 Credentials from Password Stores: Securityd Memory (T1555.002) [162]

EV Code	Vulnerability Description
EV1555.001-S1	The insecure caching of plaintext keychain passwords in OS X prior to El Capitan, allowing users with root access to read sensitive information.
EV1555.001-S2	The inadequate protection of securityd's memory, enabling an adversary to obtain root access and scan through memory to decrypt the user's logon keychain.

2.8.13 Credentials from Password Stores: Credentials from Web Browsers (T1555.003) [163]

EV Code	Vulnerability Description
EV1555.003-S1	The storage of encrypted credentials in web browsers, which can be exploited by extracting plaintext passwords through methods such as executing SQL queries on browser-specific database files.
EV1555.003-H1	The reuse of credentials across different systems and/or accounts after adversaries acquire them from web browsers, potentially leading to unauthorized access and privilege escalation.

2.8.14 Credentials from Password Stores: Windows Credential Manager (T1555.004) [164]

EV Code	Vulnerability Description
EV1555.004-S1	The storage of website and application credentials in encrypted .vcrd files under %Systemdrive%\Users[Username]\AppData\Local\Microsoft[Vault/ Credentials], with the encryption key retrievable from the Policy.vpol file in the same folder.
EV1555.004-H1	The failure to enable the "Network access: Do not allow storage of passwords and credentials for network authentication" setting, allowing network credentials to be stored in the Credential Manager and potentially exposed to adversaries.

2.8.15 Credentials from Password Stores: Password Managers (T1555.005) [165]

EV Code	Vulnerability Description
EV1555.005-S1	The lack of re-locking mechanisms with short timeouts for password managers, allowing adversaries more time to exploit decrypted databases.
EV1555.005-H1	The susceptibility to password manager compromise through weak master passwords or passwords that are easily guessable, thereby enabling adversaries to gain unauthorized access to stored credentials.
EV1555.005-H2	The absence of adherence to NIST guidelines when creating password policies, potentially resulting in weak password configurations that are susceptible to brute force attacks.
EV1555.005-H3	The absence of regular password manager software updates through patch management increases the risk of exploiting known vulnerabilities by adversaries.

2.8.16 *Credentials from Password Stores: Cloud Secrets Management Stores (T1555.006)* [166]

EV Code	Vulnerability Description
EV1555.006-H1	The improper configuration or insufficient protection of high-privileged Cloud Accounts or compromised services, enabling adversaries to gain sufficient privileges and request secrets from the secrets manager.
EV1555.006-H2	The failure to limit and tailor permissions for accounts and services with access to the secrets manager, creating a risk of overprivileged entities that could compromise the security of stored secrets.

2.8.17 *Exploitation for Credential Access (T1212)* [272]

EV Code	Vulnerability Description
EV1212-S1	Software vulnerabilities, which adversaries exploit to collect credentials by taking advantage of programming errors in programs, services, or the operating system software or kernel.
EV1212-S2	Credentialing and authentication mechanisms, as demonstrated by the MS14-068 attack on Kerberos, allowing the forging of tickets using domain user permissions.
EV1212-S3	The lack of proper validation of authentication requests by services, enabling replay attacks where intercepted data packets can be later replayed, potentially leading to unauthorized access or privileges.
EV1212-S4	Vulnerabilities in public cloud infrastructure, allowing unintended authentication token creation and renewal.
EV1212-S5	The absence of effective measures to validate authentication requests, such as one-time passwords, timestamps, sequence numbers, digital signatures, or random session keys, leaving the system susceptible to exploitation.
EV1212-S6	Inadequate application isolation and sandboxing, allowing adversaries to advance their operations.

EV1212-S7	The lack of exploit protection, as security applications like Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET) are not effectively deployed, leaving the system exposed to exploitation behavior.
EV1212-H1	The absence of a robust cyber threat intelligence capability, hindering the organization's ability to identify and defend against threats that may use software exploits and 0-days.
EV1212-H2	The failure to regularly update software through patch management for internal enterprise endpoints and servers, leaving the system exposed to known vulnerabilities that could be exploited by adversaries.

2.8.18 Forced Authentication (T1187) [284]

EV Code	Vulnerability Description
EV1187-S1	The lack of effective network traffic filtering, specifically the absence of controls blocking SMB and WebDAV protocol traffic, allowing adversaries to exploit automatic authentication behaviors and intercept user credential information.
EV1187-H1	The use of weak passwords, increasing the risk of successful brute force attacks on obtained credential hashes, emphasizing the importance of enforcing strong password policies to mitigate this weakness.

2.8.19 Forge Web Credentials (T1606) [285]

EV Code	Vulnerability Description
EV1606-S1	The potential lack of comprehensive access list audits and permissions review, allowing for the persistence of suspicious accounts and credentials accessing web applications and services.
EV1606-S2	The absence of advanced auditing on AD FS, leaving the system unaware of potential forged SAML token activities and hindering effective detection and response.

EV1606-S3	The possibility of browsers/applications retaining persistent web credentials, such as cookies, due to inadequate configuration, which may facilitate unauthorized access.
EV1606-H1	The potential failure to restrict permissions and access to the AD FS server exclusively from privileged access workstations, leaving the system exposed to unauthorized origins.
EV1606-H2	The potential insufficient enforcement of best practices for user accounts with administrative rights, including the use of privileged access workstations, Just in Time/Just Enough Administration (JIT/JEA), and strong authentication, possibly leading to compromised credentials and unauthorized access.
EV1606-H3	The potential failure to adhere to best practices in AWS environments, allowing users to call the sts:GetFederationToken API without explicit requirement, leading to the generation of unauthorized temporary security credentials.

2.8.20 Forge Web Credentials: Web Cookies (T1606.001) [286]

EV Code	Vulnerability Description
EV1606.001-S1	The potential lack of comprehensive access list audits and permissions review, allowing for the persistence of suspicious accounts and credentials accessing web applications and services.
EV1606.001-S2	The possibility of browsers/applications retaining persistent web credentials, such as cookies, due to inadequate configuration, which may facilitate unauthorized access.

2.8.21 Forge Web Credentials: SAML Tokens (T1606.002) [287]

EV Code	Vulnerability Description
EV1606.002-S1	The absence of advanced auditing on AD FS, leaving the system unaware of potential forged SAML token activities and hindering effective detection and response.

EV1606.002-H1	The potential failure to restrict permissions and access to the AD FS server exclusively from privileged access workstations, leaving the system exposed to unauthorized origins.
EV1606.002-H2	The potential insufficient enforcement of best practices for user accounts with administrative rights, including the use of privileged access workstations, Just in Time/Just Enough Administration (JIT/JEA), and strong authentication, possibly leading to compromised credentials and unauthorized access.
EV1606.002-H3	The risk of maintaining a high number of users with highly privileged Directory Roles, which could increase the attack surface and potential impact if adversaries successfully forge SAML tokens claiming these highly privileged accounts.

2.8.22 Input Capture (T1056) [363]

EV Code	Vulnerability Description
EV1056-H1	User may unknowingly provide sensitive information to what they believe is a legitimate service

2.8.23 Input Capture: Keylogging (T1056.001) [364]

EV Code	Vulnerability Description
EV1056.001-H1	User inadvertently exposes credentials, as keylogging relies on intercepting keystrokes over a period of time, especially when users are forced to reauthenticate due to actions like clearing browser cookies.

2.8.24 Input Capture: GUI Input Capture (T1056.002) [365]

EV Code	Vulnerability Description
EV1056.002-H1	The tendency to unknowingly input credentials into seemingly legitimate prompts initiated by the adversary, facilitating unauthorized access and potential data compromise.

EV1056.002-H2	The failure to undergo effective user training, resulting in a reduced ability to recognize and appropriately respond to suspicious events and dialog boxes, potentially leading to inadvertent disclosure of credentials.

2.8.25 Input Capture: Web Portal Capture (T1056.003) [366]

EV Code	Vulnerability Description
EV1056.003-H1	User unknowingly enters credentials on a compromised login page, leading to the disclosure of sensitive information to the adversary.

2.8.26 Input Capture: Credential API Hooking (T1056.004) [367]

EV Code	Vulnerability Description
EV1056.004-S1	Weaknesses in Windows API functions, potentially leading to the unauthorized collection of user credentials.
EV1056.005-H1	User enters sensitive information in applications susceptible to API hooking, thereby inadvertently providing access to adversaries.

2.8.27 Modify Authentication Process (T1556) [385]

EV Code	Vulnerability Description
EV1556-S1	Weaknesses in the authentication mechanisms, such as the Local Security Authentication Server (LSASS) process and the Security Accounts Manager (SAM) on Windows, pluggable authentication modules (PAM) on Unix-based systems, and authorization plugins on MacOS systems, allowing for the modification of these processes to reveal or bypass credentials.
EV1556-S2	The potential for misconfigurations in authentication logs, such as the lack of proper enforcement of Multi-Factor Authentication (MFA), which could allow adversaries to exploit authentication weaknesses.

EV1556-S3	The potential for unsigned or improperly signed Dynamic Link Libraries (DLLs) and executable files within the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, which could be exploited to introduce malicious components into the authentication process.
EV1556-S4	The existence of new and unknown network provider DLLs within the Registry, specifically at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services <NetworkProviderName>\NetworkProvider\ProviderPath, which, if not periodically reviewed, could introduce unauthorized components affecting authentication.
EV1556-S5	The potential misconfigurations in the implementation of multi-factor authentication (MFA), such as weak settings or insufficient monitoring, which could be exploited to bypass the intended security measures.
EV1556-S6	The potential compromise of password filters due to improper registration, as the absence of filter DLLs in the designated Windows installation directory or missing registry entries may allow unauthorized manipulation, undermining the intended security measures.
EV1556-S7	The potential misconfiguration or oversight in the implementation of Protected Process Light (PPL) for LSA, which may lead to a compromise of privileged process integrity.
EV1556-S8	The risk of unauthorized write access to the /Library/Security/SecurityAgentPlugins directory, posing a threat to the integrity and security of the system.
EV1556-S9	The inadequate restriction on Registry permissions, allowing unauthorized modifications to sensitive Registry keys, specifically HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order, which could lead to system instability or compromise.
EV1556-H1	The unintentional misconfiguration or lack of secure practices in the authentication process, leading to the persistence of compromised credentials for remote access to systems and externally available services like VPNs, Outlook Web Access, and remote desktop.

EV1556-H2	The inadvertent failure to periodically review the hybrid identity solution for discrepancies, including unauthorized Pass Through Authentication (PTA) agents in the Azure Management Portal, potentially leading to undetected compromises of authentication mechanisms.
EV1556-H3	The inadvertent failure to verify the validity of binaries catalog-signed in some cases, potentially causing discrepancies in authentication logs and leading to the exploitation of authentication weaknesses.
EV1556-H4	The failure to disable the EnableMPRNotifications policy through Group Policy or a configuration service provider in Windows 11 22H2, thereby exposing the system to the risk of unauthorized credential transmission by Winlogon to network providers.
EV1556-H5	Inadequate password policies, which could expose sensitive information if the AllowReversiblePasswordEncryption property is improperly configured, allowing reversible password encryption.
EV1556-H6	Insufficient auditing of domain and local accounts, potentially leading to unauthorized access if privilege levels are not routinely reviewed, default accounts are enabled, or unauthorized local accounts are created without proper authorization.
EV1556-H7	Unrestricted access to the root account, which poses a risk of modifying protected components, unless proper privilege separation mechanisms (e.g., SELinux, grsecurity, AppArmor) are implemented to limit Privilege Escalation opportunities.
EV1556-H8	Failure to follow best practices for the design and administration of an enterprise network, potentially allowing excessive privileged account use across administrative tiers, increasing the risk of unauthorized access.
EV1556-H9	Failure to limit Azure AD Global Administrator accounts to only those required and not using dedicated cloud-only accounts, potentially exposing the hybrid identity solution to increased risk of compromise.

EV1556-H10	The potential failure to enforce or adhere to proper user account management policies, leading to insecure enrollment or deactivation of authentication mechanisms, such as MFA, for user accounts and compromising the overall security posture of the system.

2.8.28 Modify Authentication Process: Domain Controller Authentication (T1556.001) [386]

EV Code	Vulnerability Description
EV1556.001-S1	The susceptibility of the domain controller's authentication process to patching, allowing the bypass of typical authentication mechanisms and unauthorized access to user accounts.
EV1556.001-S2	The lack of enabled features, such as Protected Process Light (PPL), for Local Security Authority (LSA), which may contribute to compromised privileged processes
EV1556.001-H1	The absence of multi-factor authentication (MFA), which could potentially allow adversaries to gain control of valid credentials and exploit them for unauthorized access
EV1556.001-H2	Insufficient privileged account management, as auditing domain and local accounts irregularly may result in overlooking situations that could grant adversaries wide access through privileged account credentials.

2.8.29 Modify Authentication Process: Password Filter DLL (T1556.002) [387]

EV Code	Vulnerability Description
EV1556.002-H1	User fails to ensure that filter DLLs are present in the correct Windows installation directory (C:\Windows\System32\ by default) and appropriately registered in the system registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages), which can lead to ineffective password filtering and security risks.

2.8.30 Modify Authentication Process: Pluggable Authentication Modules (T1556.003) [388]

EV Code	Vulnerability Description
EV1556.003-S1	The risk of user credentials being harvested due to plain-text exchange of values with PAM components, as PAM does not store passwords.
EV1556.003-H1	The inadequate implementation of multi-factor authentication (MFA), which could expose accounts to compromise due to the reliance on single-factor authentication.
EV1556.003-H2	The risk of inadequate privileged account management, potentially allowing unauthorized modification of Pluggable Authentication Modules (PAM) components and increasing the likelihood of privilege escalation opportunities.

2.8.31 Modify Authentication Process: Network Device Authentication (T1556.004) [389]

EV Code	Vulnerability Description
EV1556.004-H1	The potential lack of multi-factor authentication for user and privileged accounts on network devices, which could leave these accounts more susceptible to compromise.
EV1556.004-H2	The inadequate implementation of privileged account management practices, such as not restricting administrator accounts to as few individuals as possible and not following least privilege principles, which may result in increased attack surface and potential credential overlap across systems.

2.8.32 Modify Authentication Process: Reversible Encryption (T1556.005) [390]

EV Code	Vulnerability Description
EV1556.005-H1	The potential enabling of reversible password encryption in Active Directory, allowing the decryption of passwords through abuse of the AllowReversiblePasswordEncryption property.

EV1556.005-H2	The potential misconfiguration of the AllowReversiblePasswordEncryption property, which can occur if administrators fail to ensure that it is set to disabled, except when necessary for specific applications.
EV1556.005-H3	The inadequate auditing of domain and local accounts, potentially allowing an adversary to exploit situations where credentials of privileged accounts are obtained, emphasizing the importance of routine audits to detect and address such security risks.

2.8.33 Modify Authentication Process: Multi-Factor Authentication (T1556.006) [391]

EV Code	Vulnerability Description
EV1556.006-S1	Insecure configuration of the Windows hosts file (C:\windows\system32\drivers\etc\hosts), allowing adversaries to redirect MFA calls to localhost and causing the MFA process to fail.
EV1556.006-S2	Lack of proper auditing and review processes for MFA actions alongside authentication logs, potentially allowing adversaries to manipulate MFA without detection.
EV1556.006-H1	Failure to enforce a "fail closed" policy for MFA, allowing otherwise successful authentication attempts to be granted access without enforcing multi-factor authentication.
EV1556.006-H2	Failure to ensure that all user accounts have MFA enabled, leaving some accounts without the additional security provided by multi-factor authentication.
EV1556.006-H3	Inadequate implementation of MFA policies and requirements for existing, deactivated, or dormant accounts and devices, allowing adversaries to exploit gaps in MFA coverage.

2.8.34 Modify Authentication Process: Hybrid Identity (T1556.007) [392]

EV Code	Vulnerability Description
EV1556.007-S1	Weakness in the on-premises server running a Pass Through Authentication (PTA) agent, allowing adversaries to inject a malicious DLL into the AzureADConnectAuthenticationAgentService process, enabling unauthorized authentication attempts and credential recording.
EV1556.007-S2	In environments using Active Directory Federation Services (AD FS), adversaries can exploit a weakness by editing the Microsoft.IdentityServer.Servicehost configuration file to load a malicious DLL, generating authentication tokens for any user and bypassing multi-factor authentication and defined AD FS policies.
EV1556.007-S3	Lack of verification of the integrity of DLLs and executable files in the Active Directory Federation Services (AD FS) and Global Assembly Cache directories, creating a potential avenue for adversaries to introduce malicious code if files are not properly signed by Microsoft.
EV1556.007-H1	Failure to periodically review the hybrid identity solution for discrepancies, such as unwanted or unapproved Pass Through Authentication (PTA) agents in the Azure Management Portal, leading to potential unauthorized access.
EV1556.007-H2	Inadequate privileged account management, as organizations may fail to limit on-premises accounts with access to the hybrid identity solution, potentially allowing unauthorized access if Azure AD Global Administrator accounts are not properly restricted and dedicated for cloud-only use.
EV1556.007-H3	Failure to integrate multi-factor authentication (MFA) as part of organizational policy, increasing the risk of adversaries gaining control of valid credentials that could be exploited for various tactics, including initial access, lateral movement, and information collection.

2.8.35 Modify Authentication Process: Network Provider DLL (T1556.008) [393]

EV Code	Vulnerability Description
EV1556.008-S1	The insecure transmission of credentials during the logon process, as Winlogon sends credentials to the local mpnotify.exe process via RPC without encryption.
EV1556.008-S2	The insecure sharing of credentials in cleartext by the mpnotify.exe process with registered credential managers during logon events, potentially exposing sensitive information.
EV1556.008-H1	The failure to consistently review and identify new or unknown network provider DLLs within the Registry (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services <NetworkProviderName>\NetworkProvider\ProviderPath) could allow malicious DLLs to go unnoticed.
EV1556.008-H2	The failure to ensure that only valid DLLs are registered and listed in the Registry key at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ NetworkProvider\Order may lead to the registration of malicious DLLs.
EV1556.008-H3	The potential for misconfiguration, as the EnableMPRNotifications policy in Windows 11 22H2 can be disabled to prevent Winlogon from sending credentials to network providers, and a failure to apply this configuration could expose credentials during the logon process.
EV1556.008-H4	The mismanagement of Registry permissions, as failure to restrict permissions to sensitive Registry keys, such as HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ NetworkProvider\Order, may allow unauthorized modification and compromise the integrity of network provider configurations.

2.8.36 Multi-Factor Authentication Interception (T1111) [404]

EV Code	Vulnerability Description
EV1111-H1	The potential failure to remove smart cards when not in use, leaving them susceptible to unauthorized access and exploitation by adversaries.

2.8.37 Multi-Factor Authentication Request Generation (T1621) **[405]**

EV Code	Vulnerability Description
EV1621-S1	The potential weakness in account use policies, allowing login attempts and subsequent 2FA/MFA service requests to be initiated from suspicious locations or when the source of login attempts does not match the location of the 2FA/MFA smart device.
EV1621-S2	The potential insecurity of 2FA/MFA mechanisms, particularly simple push or one-click options, and the lack of secure configurations, such as default settings and limits on the maximum number of 2FA/MFA request prompts in a given time period.
EV1621-H1	The risk of falling victim to "MFA fatigue" due to continuous login attempts by adversaries, potentially leading to the user accepting malicious authentication requests.

2.8.38 Network Sniffing (T1040) **[415]**

EV Code	Vulnerability Description
EV1040-S1	The potential exposure of cleartext traffic in cloud-based environments due to TLS termination at the load balancer level, facilitating exfiltration techniques like Transfer Data to Cloud Account.
EV1040-S2	The potential lack of appropriate encryption for wired and/or wireless traffic, increasing the risk of unauthorized access and information exposure during network sniffing.
EV1040-S3	The inadequate implementation of network segmentation, allowing direct access to broadcasts and multicast sniffing and increasing the risk of attacks such as LLMNR/NBT-NS Poisoning and SMB Relay.
EV1040-H1	The potential absence of multi-factor authentication, leaving user accounts more susceptible to compromise and unauthorized access.
EV1040-H2	The failure to implement secure, encrypted protocols for transmitting user credentials, contributing to the risk of unauthorized access during network sniffing.

EV1040-H3	The lack of proper user account management in cloud environments, potentially granting unnecessary permissions for creating or modifying traffic mirrors and increasing the risk of unauthorized access to sniffed traffic.

2.8.39 OS Credential Dumping (T1003) [445]

EV Code	Vulnerability Description
EV1003-S1	The susceptibility of storing credentials in an insecure manner within the operating system and software, making them accessible for unauthorized credential dumping.
EV1003-S2	The lack of Attack Surface Reduction (ASR) rules enabled on Windows 10 to secure LSASS, potentially allowing for credential stealing and exploitation of endpoint security.
EV1003-S3	The lack of default configuration for Credential Guard in Windows 10, exposing LSA secrets and leaving the system susceptible to credential dumping attacks.
EV1003-S4	Inadequate securing of Domain Controller backups, potentially exposing sensitive information if backups are compromised.
EV1003-S5	The potential weakness associated with NTLM, which may be exploited, leading to unauthorized access if not disabled or properly restricted.
EV1003-S6	The risk associated with WDigest authentication if not disabled, posing a potential avenue for attackers to obtain sensitive information through credential-related vulnerabilities.
EV1003-S7	Insufficient design and administration of an enterprise network, potentially leading to the inappropriate use of privileged accounts across administrative tiers on Windows systems.
EV1003-S8	The absence of Protected Process Light for LSA on Windows 8.1 and Windows Server 2012 R2, potentially allowing adversaries to compromise the integrity of privileged processes.

EV1003-H1	The mismanagement of access control lists for "Replicating Directory Changes" and related permissions on Active Directory, potentially leading to unauthorized access and compromise of domain controller replication.
EV1003-H2	The failure to add relevant users to the "Protected Users" Active Directory security group, which may result in an increased risk of plaintext credential caching and potential unauthorized access.
EV1003-H3	Inadequate password policies, potentially allowing unauthorized access to systems if local administrator accounts do not have complex and unique passwords.
EV1003-H4	The failure to tightly control user or admin domain accounts placed in local administrator groups on Windows systems, risking equivalent local administrator access with shared passwords across systems.
EV1003-H5	Inadequate access restrictions to privileged accounts on Linux systems, which could expose sensitive regions of memory to hostile programs attempting to scrape passwords.
EV1003-H6	The practice of using the same password for multiple accounts, which, despite user training efforts, may persist and lead to credential overlap across accounts and systems, posing a security risk.

2.8.40 OS Credential Dumping: LSASS Memory (T1003.001) **[446]**

EV Code	Vulnerability Description
EV1003.001-S1	The storage of sensitive credential material in the process memory of the Local Security Authority Subsystem Service (LSASS), making it susceptible to unauthorized access.
EV1003.001-S2	The potential lack of Attack Surface Reduction (ASR) rules enabled on Windows 10, leaving LSASS susceptible to credential stealing.
EV1003.001-S3	The potential absence of configured Credential Guard on Windows 10, which may leave LSA secrets unprotected and susceptible to forms of credential dumping.

EV1003.001-S4	The potential absence of Protected Process Light for LSA on Windows 8.1 and Windows Server 2012 R2, leaving privileged processes susceptible to compromise.
EV1003.001-H1	The potential use of NTLM and WDigest authentication, which can be exploited for credential dumping.
EV1003.001-H2	The use of weak or non-unique passwords for local administrator accounts across systems, which could be exploited in credential-based attacks.
EV1003.001-H3	The potential inclusion of user or admin domain accounts in local administrator groups across systems without tight control, creating equivalent local administrator accounts with the same password on multiple systems.
EV1003.001-H4	The potential oversight in implementing best practices for privileged account management, leading to an increased risk of unauthorized access across administrative tiers.
EV1003.001-H5	The potential overlap of credentials across accounts and systems, indicating a need for user and administrator training to discourage the use of the same password for multiple accounts.

2.8.41 OS Credential Dumping: Security Account Manager (T1003.002) [447]

EV Code	Vulnerability Description
EV1003.002-S1	The susceptibility of the SAM database, stored in the Windows Registry, which can be exploited through in-memory techniques or registry extraction methods, requiring SYSTEM level access.
EV1003.002-S2	Inadequate NTLM configuration, which may expose the system to attacks exploiting weaknesses in NTLM, such as pass-the-hash attacks.
EV1003.002-H1	The potential misconfiguration of local administrator accounts, especially when they are included in the local administrator groups across multiple systems, creating a security weakness that could be exploited to gain widespread unauthorized access.

EV1003.002-H2	The reuse of passwords across multiple accounts and systems, potentially leading to credential overlap and increasing the risk of unauthorized access if one set of credentials is compromised.
EV1003.002-H3	The failure to follow best practices in designing and administering an enterprise network, leading to an increased risk of unauthorized access and compromise of privileged accounts across different administrative tiers.

2.8.42 OS Credential Dumping: NTDS (T1003.003) **[448]**

EV Code	Vulnerability Description
EV1003.003-S1	The potential exposure of sensitive credential information due to the default location (%SystemRoot%\NTDS\Ntds.dit) of the NTDS file (NTDS.dit) on domain controllers, making it a prime target for unauthorized access and copying.
EV1003.003-S2	Inadequately secured Domain Controller backups could lead to potential unauthorized access and compromise of sensitive information.
EV1003.003-H1	Improper handling of backups containing NTDS files, as adversaries may exploit this oversight to obtain sensitive information about domain members, including devices, users, and access rights.
EV1003.003-H2	Failure to enforce complex, unique passwords for local administrator accounts across all systems increases the risk of unauthorized access and potential compromise of the network.
EV1003.003-H3	Placing user or admin domain accounts in local administrator groups without tight controls and adherence to best practices for network design and administration may result in elevated privileges across systems, posing a security risk.
EV1003.003-H4	Credential overlap across accounts and systems due to users and administrators using the same password for multiple accounts increases the risk of unauthorized access and potential compromise of sensitive information.

2.8.43 OS Credential Dumping: LSA Secrets (T1003.004) [449]

EV Code	Vulnerability Description
EV1003.004-S1	The insecure storage of Local Security Authority (LSA) secrets in the registry at HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets, providing an exploitable avenue for SYSTEM-level access.
EV1003.004-H1	Inadequate enforcement of password complexity and uniqueness, potentially allowing attackers to exploit weak or shared passwords across local administrator accounts.
EV1003.004-H2	Insufficient implementation of privileged account management best practices, leaving the enterprise network susceptible to misuse of privileged accounts.
EV1003.004-H3	Credential overlap across accounts and systems, stemming from a lack of user training and awareness, potentially leading to unauthorized access if user credentials are compromised.

2.8.44 OS Credential Dumping: Cached Domain Credentials (T1003.005) [450]

EV Code	Vulnerability Description
EV1003.005-S1	The storage of cached domain credentials, specifically in the DCC2 hash format, which can be accessed by adversaries in the absence of a domain controller.
EV1003.005-H1	Failure to configure Active Directory settings, such as not adding users to the "Protected Users" security group, leading to a higher risk of plaintext credential caching.
EV1003.005-H2	Users and administrators using the same password for multiple accounts, potentially increasing the risk of credential overlap and compromise.
EV1003.005-H3	Allowing an excessive number of cached credentials, as the HKLM\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon\cachedlogonscountvalue setting is not properly configured, potentially facilitating credential access.

EV1003.005-H4	Inadequate privileged account management, such as placing user or admin domain accounts in local administrator groups without tight control, potentially leading to widespread compromise if the same password is used across systems.
EV1003.005-H5	Failing to follow best practices for designing and administering an enterprise network, resulting in the inappropriate use of privileged accounts across administrative tiers and increasing the risk of compromise.

2.8.45 OS Credential Dumping: DCSync (T1003.006) **[451]**

EV Code	Vulnerability Description
EV1003.006-S1	Inadequate management of access control lists for "Replicating Directory Changes" and other permissions associated with domain controller replication, which could lead to unauthorized access and compromise of sensitive information.
EV1003.006-H1	Weak password policies for local administrator accounts, posing a risk of unauthorized access and potential compromise of systems if passwords are easily guessable.
EV1003.006-H2	Placement of user or admin domain accounts in local administrator groups across systems without tight controls, which increases the risk of unauthorized access and potential compromise of systems due to the equivalent access provided on all systems.
EV1003.006-H3	Failure to follow best practices for the design and administration of an enterprise network, resulting in the excessive use of privileged accounts across administrative tiers and increasing the likelihood of unauthorized access and compromise of sensitive information.

2.8.46 OS Credential Dumping: Proc Filesystem (T1003.007) [452]

EV Code	Vulnerability Description
EV1003.007-S1	The potential exposure of credentials stored in the proc filesystem or /proc, which, when accessed with root privileges, allows searching for patterns indicative of credentials in memory structures or cached hashes.
EV1003.007-S2	The storing of credentials in clear text inside a process's memory, particularly in services or programs that may save sensitive information without proper encryption, facilitating their extraction by adversaries with or without root privileges.
EV1003.007-H1	Failure to enforce complex, unique passwords for root accounts across all systems increases the risk of unauthorized access and compromise.
EV1003.007-H2	Failure to follow best practices in restricting access to privileged accounts may result in the exposure of sensitive information due to unauthorized or unnecessary access granted to users.

2.8.47 OS Credential Dumping: /etc/passwd and /etc/shadow (T1003.008) [453]

EV Code	Vulnerability Description
EV1003.008-S1	The insecure default permissions on /etc/shadow, allowing unauthorized access to sensitive password hashes.
EV1003.008-S2	The potential exposure of sensitive user account information and password hashes due to the insecure storage of /etc/shadow and /etc/passwd files on most modern Linux operating systems.
EV1003.008-H1	The absence of robust password policies and enforcement mechanisms, potentially leading to weak or easily guessable passwords for root accounts.
EV1003.008-H2	Inadequate privileged account management, posing a risk of unauthorized access to sensitive information due to insufficient restrictions on privileged accounts.

2.8.48 Steal Application Access Token (T1528) [559]

EV Code	Vulnerability Description
EV1528-S1	The absence of restrictions on end-user consent for OAuth applications, potentially allowing unauthorized access to organizational data
EV1528-S2	The lack of control over user registration of applications, as users might register applications without proper scrutiny, introducing potential security risks that could be minimized by blocking end-user registration and using a Cloud Access Security Broker (CASB) to ban applications.
EV1528-H1	User may inadvertently grant access to malicious applications, allowing adversaries to steal OAuth access tokens and gain long-term access to user accounts through Application Access Tokens.
EV1528-H2	Inadequate auditing of cloud and container accounts, potentially leading to unnecessary accounts with inappropriate permissions, making it difficult to detect and respond to unauthorized access or activities.
EV1528-H3	Failure to recognize and scrutinize OAuth application redirect URLs, as users may inadvertently authorize third-party applications with malicious intent, exploiting the trust associated with familiar or legitimate service names.
EV1528-H4	User grants overly permissive permissions to OAuth applications, such as offline access or access to sensitive data like emails, increasing the risk of adversaries exploiting SaaS APIs to discover credentials and sensitive communications.
EV1528-H5	Insufficient enforcement of role-based access control, potentially leading to unnecessary access to application access tokens
EV1528-H6	The failure to disable unnecessary access to service account tokens in Kubernetes applications, as not setting "automountServiceAccountToken: false" in the YAML specification could expose sensitive tokens

2.8.49 Steal or Forge Authentication Certificates (T1649) [560]

EV Code	Vulnerability Description
EV1649-S1	The potential presence of old or insecure authentication protocols (e.g., NTLM) and unnecessary certificate features, such as vulnerable AD CS web and other enrollment server roles, which may expose the system to exploitation.
EV1649-H1	The improper handling or misplacement of AD CS certificates, including storing them in unsecured locations, which can facilitate unauthorized access by adversaries.
EV1649-H2	The misconfiguration of certificate settings and permissions during the enrollment process, allowing for the abuse of authentication certificates and potentially enabling Persistence by impersonation or assumption of privileged accounts.
EV1649-H3	The inadequate protection of certificates and associated private keys, as well as the neglect of utilizing additional hardware credential protections like trusted platform modules (TPM) or hardware security modules (HSM), leaving the system open to unauthorized access and compromise.
EV1649-H4	The failure to properly audit and remediate existing authentication certificates, as well as common misconfigurations of CA settings and permissions, leaving the system susceptible to unauthorized certificate issuance and abuse.
EV1649-H5	The potential lack of proper security measures for certificate authorities (CA), treating them as tier 0 assets, and not hardening abusable CA settings and attributes, leaving the CA infrastructure susceptible to compromise.

2.8.50 Steal or Forge Kerberos Tickets (T1558) [561]

EV Code	Vulnerability Description
EV1558-S1	The risk associated with cached Kerberos tickets on Windows, as the adversary can potentially exploit weaknesses in the storage and protection of these tickets using tools like the built-in klist utility, allowing unauthorized extraction for Pass the Ticket attacks.

EV1558-S2	The potential weakness in the storage and protection of Kerberos tickets on Linux systems, where unauthorized access to the System Security Services Daemon (SSSD) database and key (located in /var/lib/sss/secrets/secrets.ldb and /var/lib/sss/secrets/.secrets.mkey) could allow extraction of the credential cache Kerberos blob for use in Pass the Ticket attacks.
EV1558-S3	The potential mistake of inadequate protection of Kerberos tickets on macOS, where user actions, such as misconfiguring the /etc/krb5.conf file or mishandling the KRB5CCNAME environment variable, may lead to insecure storage or exposure of ccache entries, enabling adversaries to interact with or extract TGT or Service Tickets for malicious purposes.
EV1558-S4	The potential weakness in Active Directory configuration, where failure to regularly reset the KRBTGT account password and implement proper rotation practices may allow previously generated golden tickets to persist, enabling adversaries to maintain unauthorized access.
EV1558-H1	The potential mistake of using weak or outdated Kerberos encryption algorithms, such as RC4, instead of stronger options like AES, which could expose sensitive information to adversaries
EV1558-H2	The weakness in password policies, where inadequate enforcement of strong password length and complexity, along with infrequent password expiration for service accounts, may create opportunities for unauthorized access;
EV1558-H3	The potential mistake of granting excessive permissions to domain admin accounts and service accounts, including membership in privileged groups like Domain Administrators, which increases the attack surface

2.8.51 Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001) [562]

EV Code	Vulnerability Description
EV1558.001-S1	The potential inadequate configuration of Active Directory and insufficient protection of the KRBTGT account password hash, which may lead to unauthorized access to the Key Distribution Center, enabling the compromise and subsequent generation of golden tickets.
EV1558.001-H1	The improper management of privileged accounts, as domain admin account permissions are not adequately restricted to domain controllers and limited servers, potentially facilitating unauthorized access and misuse.

2.8.52 Steal or Forge Kerberos Tickets: Silver Ticket (T1558.002) [563]

EV Code	Vulnerability Description
EV1558.002-S1	The weaknesses in the Kerberos authentication system, allowing the forging of Kerberos Ticket Granting Service (TGS) tickets (silver tickets) when adversaries possess the password hash of a target service account.
EV1558.002-H1	The inadequate encryption implementation, as the use of RC4 instead of stronger algorithms like AES Kerberos exposes sensitive information to potential decryption.
EV1558.002-H2	The weak password policies, specifically the absence of periodic password expiration and the use of passwords with insufficient length and complexity, which increases the risk of unauthorized access.
EV1558.002-H3	Insufficient privilege management for service accounts, allowing them unnecessary access and membership in privileged groups like Domain Administrators, potentially leading to unauthorized system control and data compromise.

2.8.53 Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003) [564]

EV Code	Vulnerability Description
EV1558.003-S1	The potential exposure of plaintext credentials due to the use of the RC4 algorithm for encrypting portions of Kerberos ticket-granting service (TGS) tickets, making them susceptible to offline brute force attacks.
EV1558.003-H1	Over-privilege of service accounts, where granting excessive privileges, including membership in privileged groups like Domain Administrators, increases the risk of unauthorized access and potential misuse of system resources.
EV1558.003-H2	The association of service principal names (SPNs) with at least one service logon account, which, when compromised, enables adversaries possessing a valid Kerberos ticket-granting ticket (TGT) to request TGS service tickets and potentially execute offline brute force attacks on encrypted portions of these tickets, leading to exposure of plaintext credentials.

2.8.54 Steal or Forge Kerberos Tickets: AS-REP Roasting (T1558.004) [565]

EV Code	Vulnerability Description
EV1558.004-S1	The potential presence of accounts with disabled Kerberos preauthentication due to older protocols, which may be exploited if not audited and properly configured.
EV1558.004-H1	The failure to enable Kerberos preauthentication for certain accounts, exposing them to AS-REP Roasting attacks and subsequent credential compromise.
EV1558.004-H2	The failure to use strong encryption algorithms (e.g., AES) instead of weaker ones (e.g., RC4) for Kerberos, leaving encrypted data susceptible to attacks; mitigation involves enabling stronger encryption algorithms.
EV1558.004-H3	The establishment of weak password policies for service accounts, including insufficient length and complexity, potentially compromising the security of these accounts

2.8.55 Steal Web Session Cookie (T1539) [566]

EV Code	Vulnerability Description
EV1539-S1	The potential storage of sensitive authentication cookies in memory by other applications on the target machine, such as those authenticating to cloud services, providing an additional avenue for adversaries to steal session cookies.
EV1539-S2	The persistence of cookies, as a lack of configuration to regularly delete persistent cookies in browsers or tasks may expose session cookies to theft.
EV1539-H1	The potential lack of implementation of multi-factor authentication (MFA), as the absence of a physical second factor key in the negotiation protocol may allow session cookie theft through proxy methods.
EV1539-H2	The potential failure to recognize phishing attempts, as a lack of user training to identify incorrect domains in phishing sites may lead to inadvertent credential entry, facilitating session cookie theft.

2.8.56 Unsecured Credentials (T1552) [617]

EV Code	Vulnerability Description
EV1552-S1	The insecure storage of credentials in plaintext files (e.g., Bash History), operating system or application-specific repositories (e.g., Credentials in Registry), or other specialized files/artifacts (e.g., Private Keys), which can be exploited due to inadequate protection mechanisms.
EV1552-S2	Inadequate removal of vulnerable Group Policy Preferences, which could lead to unauthorized access or compromise of Active Directory configurations.
EV1552-S3	Inadequate limitation of access to the Instance Metadata API, making the system susceptible to Server-side Request Forgery (SSRF) attacks and potential exploitation by external adversaries.

EV1552-S4	Insufficient limitation of network access to sensitive services, such as the Instance Metadata API, creating opportunities for unauthorized access and potential exploitation.
EV1552-S5	Inadequate prevention of user command history flushing in the operating system configuration, allowing adversaries to potentially access sensitive command history information.
EV1552-S6	The lack of restrictions on file and directory permissions, especially in file shares, which could lead to unauthorized access by adversaries.
EV1552-S7	The absence of the patch KB2962486, which could allow credentials to be stored in Group Policy Preferences (GPPs), creating a potential security vulnerability.
EV1552-H1	The insecure handling or misplacement of credentials on the system, contributing to the risk of compromise, as exemplified by storing sensitive information in easily accessible or unprotected locations.
EV1552-H2	The failure to preemptively search for files containing passwords or other credentials, increasing the risk of exposure if such files exist on the system.
EV1552-H3	The storage of encryption keys on the local system instead of separate cryptographic hardware, potentially exposing sensitive information to unauthorized access.
EV1552-H4	The use of weak passphrases for private keys, which could facilitate password cracking attempts and compromise security.
EV1552-H5	The storage of credentials within the Registry due to insufficient password policies, potentially exposing sensitive information to unauthorized access.
EV1552-H6	The failure to restrict file shares to specific directories with access only to necessary users, potentially allowing unauthorized access to sensitive information.
EV1552-H7	The inclusion of plaintext passwords in software configuration files, which may be left on endpoint systems or servers, posing a security risk if not adequately protected or encrypted.

2.8.57 Unsecured Credentials: Credentials In Files (T1552.001) [618]

EV Code	Vulnerability Description
EV1552.001-S1	The insecurely stored credentials in local and remote files, including those created by users, shared credential stores, configuration files, and source code/binary files, which can be exploited to obtain sensitive information.
EV1552.001-S2	Inadequate restriction of file and directory permissions, allowing broader access to files containing sensitive credentials than necessary.
EV1552.001-H1	The lack of proactive auditing, as there may be a failure to preemptively search for files containing passwords, leading to increased exposure risk.
EV1552.001-H2	The absence of an organizational policy prohibiting password storage in files, which could result in inadequate password protection measures and increased susceptibility to unauthorized access.
EV1552.001-H3	Insufficient awareness among developers and system administrators about the risk associated with storing plaintext passwords in software configuration files, potentially leaving such files on endpoint systems or servers without proper safeguards.

2.8.58 Unsecured Credentials: Credentials In Registry (T1552.002) [619]

EV Code	Vulnerability Description
EV1552.002-S1	The insecure storage of credentials in the Windows Registry, allowing adversaries to search for and potentially obtain sensitive information.
EV1552.002-H1	The inadequate auditing practices, as the system lacks proactive search mechanisms for credentials within the Registry, making it difficult to detect and remediate potential risks effectively.
EV1552.002-H2	The failure to adhere to password policies, leading to the storage of credentials within the Registry, which increases the risk of exposure to adversaries.

EV1552.002-H3	Inadequate privileged account management, where software storing credentials in the Registry without appropriate permissions poses a risk of abuse if obtained by an adversary, potentially leading to unauthorized access and compromise.

2.8.59 Unsecured Credentials: Bash History (T1552.003) [620]

EV Code	Vulnerability Description
EV1552.003-S1	The insecure storage of credentials in the Bash history file (~/.bash_history) on compromised systems, allowing unauthorized access to sensitive information.
EV1552.003-S2	The failure to properly configure operating system settings, such as allowing a user's command history to be flushed to their .bash_history file, potentially leading to the exposure of sensitive credentials.
EV1552.003-H1	The practice of typing usernames and passwords on the command-line as parameters to programs, which get saved in the Bash history file (.bash_history) when the user logs out, potentially exposing sensitive credentials to adversaries.
EV1552.003-H2	The neglect to implement recommended mitigation measures, such as not using commands like set +o history or set -o history, forgetting to add unset HISTFILE to a user's .bash_rc file, or not using ln -s /dev/null ~/.bash_history to redirect commands to /dev/null, leaving the system susceptible to unauthorized access through the compromised Bash history file.

2.8.60 Unsecured Credentials: Private Keys (T1552.004) [621]

EV Code	Vulnerability Description
EV1552.004-S1	The insecure storage of private key certificate files on compromised systems, which may lead to unauthorized access and misuse of cryptographic keys and certificates.

EV1552.004-S2	The generation and export of device keys and transport keys during device registration to Azure AD, enabling potential impersonation of the registered device if the keys are compromised.
EV1552.004-S3	The inadequate auditing and monitoring of key access, as failure to regularly audit access lists may result in undetected unauthorized access to critical resources.
EV1552.004-S4	Improper file and directory permissions on folders containing sensitive private keys, posing a risk of unintended access if permissions are not adequately configured.
EV1552.004-H1	The use of weak passwords or passphrases for private keys, potentially allowing adversaries to perform offline brute force attacks or utilize input capture for keylogging, compromising the security of authentication mechanisms.
EV1552.004-H2	The failure to set the nonexportable flag during RSA key pair generation on Cisco devices, potentially allowing adversaries to export private keys and compromise the confidentiality and integrity of encrypted communications.

2.8.61 Unsecured Credentials: Cloud Instance Metadata API (T1552.005) **[622]**

EV Code	Vulnerability Description
EV1552.005-S1	Lack of proper access controls on the Cloud Instance Metadata API, allowing unauthorized access to sensitive information.
EV1552.005-S2	Potential exploitation of Server-Side Request Forgery (SSRF) vulnerabilities in public-facing web proxies, enabling adversaries to access sensitive information through requests to the Instance Metadata API.
EV1552.005-S3	Insufficient network traffic filtering allowing unauthorized access to the Instance Metadata API, potentially leading to data compromise.
EV1552.005-S4	Lack of limitations on access to the Instance Metadata API over the network, which could be exploited by adversaries if not properly restricted.
EV1552.005-H1	Failure to disable or remove unnecessary metadata services, leaving potential attack vectors open for adversaries to exploit.

2.8.62 Unsecured Credentials: Group Policy Preferences (T1552.006) [623]

EV Code	Vulnerability Description
EV1552.006-S1	The storage of Group Policy Preferences (GPP) containing unsecured credentials in SYSVOL on a domain controller, making it accessible to any domain user and susceptible to password decryption using the public AES key.
EV1552.006-H1	The oversight in auditing practices, leading to the presence of credentials within SYSVOL, posing a security risk.
EV1552.006-H2	The failure to remove or update vulnerable Group Policy Preferences, leaving potential avenues for unauthorized access and exploitation of stored credentials.
EV1552.006-H3	User neglects to apply patch KB2962486, leaving the system exposed to the risk of credentials being stored in Group Policy Preferences.

2.8.63 Unsecured Credentials: Container API (T1552.007) [624]

EV Code	Vulnerability Description
EV1552.007-S1	Lack of secure access controls in the Docker API, enabling unauthorized access and retrieval of logs containing sensitive credentials for cloud, container, and various resources.
EV1552.007-S2	Inadequate network security measures, as the Docker API and Kubernetes API may be accessed over unsecured channels, potentially allowing adversaries to intercept sensitive information, emphasizing the need to limit communications to managed and secured channels.
EV1552.007-S3	Lack of network segmentation, potentially enabling direct remote access to internal systems, indicating the need for the implementation of network proxies, gateways, and firewalls to deny unauthorized access.

EV1552.007-S4	Unrestricted IP range access to the Kubernetes API server in cloud environments, highlighting the need to leverage native cloud platform features to restrict permitted IP ranges, thus preventing potential unauthorized access.
EV1552.007-H1	Insufficient permissions management, allowing adversaries, potentially through a pod's service account, to exploit the Kubernetes API to retrieve credentials from the Kubernetes API server, including those necessary for Docker API authentication and secrets from Kubernetes cluster components.
EV1552.007-H2	Insufficiently restrictive permissions for privileged accounts, such as the service account in Kubernetes, posing a risk that unauthorized users or adversaries could exploit these accounts to access the Kubernetes API, highlighting the importance of implementing the principle of least privilege for such accounts.
EV1552.007-H3	Weak user account management practices, including the absence of proper authentication and role-based access control on the container API, creating a risk of unauthorized access and emphasizing the importance of enforcing these security measures to restrict users to the least privileges required.
EV1552.007-H4	Improper configuration of Kubernetes permissions, such as assigning wildcard permissions or adding users to the system:masters group, instead of using RoleBindings and limiting privileges to specific namespaces, posing a risk of elevated privileges for users and emphasizing the importance of adhering to secure configuration practices.

2.8.64 Unsecured Credentials: Chat Messages (T1552.008) **[625]**

EV Code	Vulnerability Description
EV1552.008-S1	The lack of proactive auditing and monitoring mechanisms within communication services, making it challenging to preemptively search for shared unsecured credentials and leaving the system susceptible to unauthorized access.

EV1552.008-H1	The inadvertent sharing of credentials on private or public corporate internal communication channels, allowing adversaries to directly collect and abuse these credentials for activities like lateral movement or privilege escalation.
EV1552.008-H2	The absence of comprehensive user training programs, leading to developers and system administrators being unaware of the risks associated with sharing unsecured passwords across communication services, thereby increasing the likelihood of inadvertent credential exposure.

2.9 Discovery (TA0007) [12]

2.9.1 Account Discovery (T1087) [43]

EV Code	Vulnerability Description
EV1087-H1	The failure to disable the Registry key (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators) through Group Policy Object (GPO) settings, allowing adversaries to exploit the misconfiguration and gather account information.

2.9.2 Account Discovery: Local Account (T1087.001) [44]

EV Code	Vulnerability Description
EV1087.001-H1	The failure to disable the Registry key (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators) through Group Policy Object (GPO) settings, allowing adversaries to exploit the misconfiguration and gather account information.

2.9.3 Account Discovery: Domain Account (T1087.002) **[45]**

EV Code	Vulnerability Description
EV1087.002-H1	The failure to disable the Registry key (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators) through Group Policy Object (GPO) settings, allowing adversaries to exploit the misconfiguration and gather account information.

2.9.4 Account Discovery: Email Account (T1087.003) **[46]**

EV Code	Vulnerability Description
EV1087.003-H1	The inadvertent exposure of email addresses and accounts due to the sharing of the GAL with Microsoft Outlook users through the Google Workspace Sync for Microsoft Outlook (GWSMO) service in Google Workspace, potentially leading to unauthorized information disclosure.

2.9.5 Account Discovery: Cloud Account (T1087.004) **[47]**

EV Code	Vulnerability Description
EV1087.004-S1	The lack of routine auditing, as the absence of regular checks on user permissions allows for potential unauthorized access to IAM identities or the discovery of cloud accounts.
EV1087.004-H1	The failure to implement least privilege principles in user account management, such as not adequately limiting permissions to discover cloud accounts, which could result in unnecessary exposure of sensitive information or unauthorized access to cloud resources.

2.9.6 Application Window Discovery (T1010) **[78]**

This attack technique does not rely on a specific vulnerability for execution.

2.9.7 Browser Information Discovery (T1217) [110]

This attack technique does not rely on a specific vulnerability for execution.

2.9.8 Cloud Infrastructure Discovery (T1580) [120]

EV Code	Vulnerability Description
EV1580-H1	The failure to adhere to the principle of least privilege in user account management, as organizations may not effectively limit the number of users with administrative roles, maintain permanent privileged role assignments, or conduct periodic entitlement reviews, increasing the risk of unauthorized cloud infrastructure discovery.

2.9.9 Cloud Service Dashboard (T1538) [121]

EV Code	Vulnerability Description
EV1538-H1	The potential failure to enforce the principle of least privilege, allowing broader dashboard visibility than necessary, which could result from misconfigurations or oversight in user account management.

2.9.10 Cloud Service Discovery (T1526) [122]

This attack technique does not rely on a specific vulnerability for execution.

2.9.11 Cloud Storage Object Discovery (T1619) [123]

EV Code	Vulnerability Description
EV1619-H1	The inadequate restriction of permissions related to listing objects in cloud storage for user accounts, demonstrating a lack of effective user account management practices and potentially exposing sensitive information to unauthorized access.

2.9.12 Container and Resource Discovery (T1613) [149]

EV Code	Vulnerability Description
EV1613-S1	The potential leakage of sensitive information through Docker logs, revealing details about the environment's configuration, available services, and the cloud provider in use.
EV1613-S2	Insecure communication channels, such as unmanaged or unsecured network connections, that could be exploited by adversaries to eavesdrop on or manipulate communication with the container service.
EV1613-S3	Lack of restrictions on API server access, including unauthenticated access to the Docker API and Kubernetes API Server, which could be exploited by adversaries to gather information and potentially manipulate the container environment.
EV1613-S4	Lack of network segmentation, potentially allowing direct remote access to internal systems, which could be exploited by adversaries to compromise sensitive resources.
EV1613-H1	Insufficient user account management practices, including granting excessive permissions (wildcard permissions or system:masters group) or using ClusterRoleBindings instead of RoleBindings in Kubernetes, which could lead to unauthorized access and privilege escalation.
EV1613-H2	Failure to implement just-in-time (JIT) access to the Kubernetes API, potentially allowing prolonged access and increasing the window of opportunity for adversaries to exploit vulnerabilities in the container environment.
EV1613-H3	Failure to enforce the principle of least privilege in dashboard visibility, allowing unnecessary users to access sensitive information, potentially aiding adversaries in their reconnaissance efforts.

2.9.13 Debugger Evasion (T1622) **[195]**

EV Code	Vulnerability Description
EV1622-H1	Human oversight or error, such as failing to adequately secure and monitor debug logs, allowing adversaries to flood them with meaningless data through looping Native API function calls (e.g., OutputDebugStringW()), thereby concealing malicious activities.

2.9.14 Device Driver Discovery (T1652) **[206]**

This attack technique does not rely on a specific vulnerability for execution.

2.9.15 Domain Trust Discovery (T1482) **[214]**

EV Code	Vulnerability Description
EV1482-S1	The potential weakness in domain trust relationships, allowing unauthorized access to resources based on the authentication procedures of another domain, thereby facilitating lateral movement opportunities.
EV1482-S2	The potential lack of proper mapping and auditing of trusts within existing domains/forests, which may result in an incomplete understanding of trust relationships and increase the risk of unauthorized access.
EV1482-H1	The potential failure to implement network segmentation for sensitive domains, exposing the entire network to higher risks, as segmentation is a crucial mitigation measure for limiting the impact of domain trust-related attacks.

2.9.16 File and Directory Discovery (T1083) **[278]**

This attack technique does not rely on a specific vulnerability for execution.

2.9.17 Group Policy Discovery (T1615) [309]

EV Code	Vulnerability Description
EV1615-S1	The predictable network path (<DOMAIN>\SYSVOL<DOMAIN>\Policies), which exposes Group Policy objects (GPOs) and allows adversaries to gather information on Group Policy settings, potentially leading to privilege escalation and manipulation of security measures within the Active Directory domain.

2.9.18 Log Enumeration (T1654) [374]

EV Code	Vulnerability Description
EV1654-H1	The potential oversight or failure to implement proper access controls, as users might not restrict sensitive log access to privileged accounts, thereby exposing the system to exploitation during log enumeration.

2.9.19 Network Service Discovery (T1046) [413]

EV Code	Vulnerability Description
EV1046-S1	The potential misconfiguration or oversight in allowing the native Bonjour application in macOS environments, such as using mDNS queries, which may inadvertently expose services like ssh, providing adversaries with information to identify and target specific systems within the network.
EV1046-S2	The potential ineffectiveness of network intrusion prevention measures, leading to the failure in detecting and preventing remote service scans, thereby leaving the system susceptible to reconnaissance and potential exploitation.
EV1046-H1	The failure to disable or remove unnecessary features or programs, which may result in the persistence of unnecessary ports and services, leaving the system exposed to discovery and potential exploitation by adversaries.

EV1046-H2	The lack of proper network segmentation, potentially resulting in the insufficient protection of critical servers and devices, increasing the risk of adversaries gaining unauthorized access to sensitive areas of the network.

2.9.20 Network Share Discovery (T1135) [414]

EV Code	Vulnerability Description
EV1135-H1	The misconfiguration of the Windows Group Policy, specifically the failure to enable the "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting, which could allow unauthorized users to enumerate network shares.

2.9.21 Network Sniffing (T1040) [415]

EV Code	Vulnerability Description
EV1040-S1	The potential exposure of cleartext traffic in cloud-based environments due to TLS termination at the load balancer level, facilitating exfiltration techniques like Transfer Data to Cloud Account.
EV1040-S2	The potential lack of appropriate encryption for wired and/or wireless traffic, increasing the risk of unauthorized access and information exposure during network sniffing.
EV1040-S3	The inadequate implementation of network segmentation, allowing direct access to broadcasts and multicast sniffing and increasing the risk of attacks such as LLMNR/NBT-NS Poisoning and SMB Relay.
EV1040-H1	The potential absence of multi-factor authentication, leaving user accounts more susceptible to compromise and unauthorized access.
EV1040-H2	The failure to implement secure, encrypted protocols for transmitting user credentials, contributing to the risk of unauthorized access during network sniffing.

EV1040-H3	The lack of proper user account management in cloud environments, potentially granting unnecessary permissions for creating or modifying traffic mirrors and increasing the risk of unauthorized access to sniffed traffic.

2.9.22 Password Policy Discovery (T1201) [454]

EV Code	Vulnerability Description
EV1201-H1	Failure to properly configure and maintain password filter DLLs, either by not ensuring their presence in the correct directory or neglecting to register them in the system registry, which may lead to a weakened defense against password-related attacks.

2.9.23 Peripheral Device Discovery (T1120) [455]

This attack technique does not rely on a specific vulnerability for execution.

2.9.24 Permission Groups Discovery (T1069) [456]

This attack technique does not rely on a specific vulnerability for execution.

2.9.25 Permission Groups Discovery: Local Groups (T1069.001) [457]

This attack technique does not rely on a specific vulnerability for execution.

2.9.26 Permission Groups Discovery: Domain Groups (T1069.002) [458]

This attack technique does not rely on a specific vulnerability for execution.

2.9.27 Permission Groups Discovery: Cloud Groups (T1069.003) [459]

EV Code	Vulnerability Description
EV1069.003-S1	The inadequate management of AWS policies, as demonstrated by the use of ListRolePolicies and ListAttachedRolePolicies commands, which may result in unintended exposure of role policies and increase the risk of unauthorized access to sensitive resources.

2.9.28 Process Discovery (T1057) [478]

This attack technique does not rely on a specific vulnerability for execution.

2.9.29 Query Registry (T1012) [498]

EV Code	Vulnerability Description
EV1012-S1	Insufficient access controls on the Registry, allowing adversaries to query information easily using the Reg utility or other means, potentially aiding them in furthering their operations within the network.

2.9.30 Remote System Discovery (T1018) [513]

This attack technique does not rely on a specific vulnerability for execution.

2.9.31 Software Discovery (T1518) [550]

This attack technique does not rely on a specific vulnerability for execution.

2.9.32 Software Discovery: Security Software Discovery (T1518.001) [551]

This attack technique does not rely on a specific vulnerability for execution.

2.9.33 System Information Discovery (T1082) **[592]**

This attack technique does not rely on a specific vulnerability for execution.

2.9.34 System Location Discovery (T1614) **[593]**

EV Code	Vulnerability Description
EV1614-S1	The inadvertent exposure of the victim host's geographical location through IP addressing, as adversaries may leverage online geolocation IP-lookup services, potentially revealing sensitive information about the system's location.

2.9.35 System Location Discovery: System Language Discovery (T1614.001) **[594]**

EV Code	Vulnerability Description
EV1614.001-S1	The inadvertent exposure of system language information through actions such as using default settings, keyboard layouts, or other behaviors that adversaries may exploit, leading to the disclosure of the host's geographical location.

2.9.36 System Network Configuration Discovery (T1016) **[595]**

This attack technique does not rely on a specific vulnerability for execution.

2.9.37 System Network Configuration Discovery: Internet Connection Discovery (T1016.001) **[596]**

EV Code	Vulnerability Description
EV1016.001-S1	The inadvertent storage of Wi-Fi network names and passwords in clear text on the system, as demonstrated by the availability of this information in files like /etc/NetworkManager/system-connections/ on Linux, posing a security risk.

EV1016.001-S2	The storage of Wi-Fi passwords associated with known networks on macOS without adequate protection, demonstrated by the ability to identify passwords using the command "security find-generic-password -wa wifiname," potentially leading to unauthorized access.

2.9.38 System Network Configuration Discovery: Wi-Fi Discovery (T1016.002) [597]

EV Code	Vulnerability Description
EV1016.002-S1	The potential exposure of Wi-Fi network names and passwords due to insecure storage on compromised systems, such as in plaintext files on Windows or in /etc/NetworkManager/system-connections/ on Linux.

2.9.39 System Network Connections Discovery (T1049) [598]

This attack technique does not rely on a specific vulnerability for execution.

2.9.40 System Owner/User Discovery (T1033) [599]

This attack technique does not rely on a specific vulnerability for execution.

2.9.41 System Service Discovery (T1007) [602]

This attack technique does not rely on a specific vulnerability for execution.

2.9.42 System Time Discovery (T1124) [607]

This attack technique does not rely on a specific vulnerability for execution.

2.9.43 Virtualization/Sandbox Evasion (T1497) [642]

This attack technique does not rely on a specific vulnerability for execution.

2.9.44 Virtualization/Sandbox Evasion: System Checks (T1497.001) [643]

This attack technique does not rely on a specific vulnerability for execution.

2.9.45 Virtualization/Sandbox Evasion: User Activity Based Checks (T1497.002) [644]

This attack technique does not rely on a specific vulnerability for execution.

2.9.46 Virtualization/Sandbox Evasion: Time Based Evasion (T1497.003) [645]

This attack technique does not rely on a specific vulnerability for execution.

2.10 Lateral Movement (TA0008) [13]

2.10.1 Exploitation of Remote Services (T1210) [275]

EV Code	Vulnerability Description
EV1210-S1	The existence of well-known vulnerabilities in common services such as SMB, RDP, MySQL, and web server services, which can be exploited through post-compromise exploitation of remote services for unauthorized access to internal systems.
EV1210-S2	The lack of application isolation and sandboxing, making it easier for adversaries to advance their operations through the exploitation of undiscovered or unpatched vulnerabilities,
EV1210-S3	The absence of effective exploit protection measures, such as behavior-based security applications and control flow integrity checking, leaving the system more susceptible to exploitation.
EV1210-S4	The inadequate network segmentation, allowing adversaries greater access to critical systems and services that could be exploited.

EV1210-S5	The lack of a robust threat intelligence program, making it difficult to proactively identify and defend against specific types and levels of threats that may use software exploits.
EV1210-H1	The potential lack of certain patches on the remote system, which may indicate vulnerabilities and be exploited by adversaries for lateral movement exploitation and unauthorized access.
EV1210-H2	The failure to disable or remove unnecessary features or programs, increasing the attack surface and providing adversaries with more potential avenues for exploitation.
EV1210-H3	The insufficient privileged account management, resulting in unnecessary permissions and access for service accounts, thereby increasing the impact of exploitation.
EV1210-H4	The failure to regularly update software, leaving internal enterprise endpoints and servers exposed to known vulnerabilities that could be exploited by adversaries.
EV1210-H5	The neglect of regular vulnerability scanning on the internal network, potentially missing new and vulnerable services that could be exploited by adversaries.

2.10.2 Internal Spearphishing (T1534) [372]

EV Code	Vulnerability Description
EV1534-H1	The susceptibility to falling for internal spearphishing attempts, especially when adversaries exploit trusted internal accounts, increasing the likelihood of successful phishing.

2.10.3 Lateral Tool Transfer (T1570) [373]

EV Code	Vulnerability Description
EV1570-S1	The potential lack of proper configuration or enforcement of host firewalls, allowing file sharing communications like SMB to occur, which can be mitigated by implementing host firewall rules to restrict such traffic.

EV1570-H1	The potential misconfiguration or inadequate updating of network intrusion detection and prevention system signatures, which could lead to a failure in identifying and mitigating activity related to lateral tool transfer over known tools and protocols.

2.10.4 Remote Service Session Hijacking (T1563) [501]

EV Code	Vulnerability Description
EV1563-S1	The potential weakness in remote service sessions, which can be exploited to allow unauthorized hijacking of preexisting sessions with services like telnet, SSH, and RDP.
EV1563-S2	The lack of network segmentation, which may result in the absence of effective firewall rules to block unnecessary traffic between network security zones, providing potential pathways for lateral movement.
EV1563-H1	The failure to implement proper privileged account management, allowing remote access to services with privileged accounts when not necessary, thereby increasing the risk of unauthorized session hijacking by adversaries.
EV1563-H2	The potential oversight in disabling unnecessary remote services (e.g., SSH, RDP), leaving avenues for exploitation if these services remain enabled unnecessarily.
EV1563-H3	The potential oversight in user account management, leading to excessive permissions for remote users.

2.10.5 Remote Service Session Hijacking: SSH Hijacking (T1563.001) [502]

EV Code	Vulnerability Description
EV1563.001-H1	The potential oversight of not disabling agent forwarding on systems that do not explicitly require this feature, leading to the risk of misuse.
EV1563.001-H2	The use of weak passwords for SSH key pairs, as failure to enforce strong password policies increases the likelihood of unauthorized access.

EV1563.001-H3	The risk of allowing remote access via SSH as root or other privileged accounts, which could be exploited if privileged account management practices are not strictly enforced.
EV1563.001-H4	The inadequate file permissions that may exist, creating opportunities for root privilege escalation, emphasizing the importance of restricting file and directory permissions and hardening the system.

2.10.6 Remote Service Session Hijacking: RDP Hijacking (T1563.002) [503]

EV Code	Vulnerability Description
EV1563.002-S1	The susceptibility of Remote Desktop Services (RDS) to RDP session hijacking, allowing unauthorized access to legitimate user sessions without the need for credentials or user prompts, potentially leading to Remote System Discovery and Privilege Escalation.
EV1563.002-S2	The inadequate audit of the Remote Desktop Users group membership, potentially leading to unauthorized access if unnecessary accounts and groups are not regularly removed.
EV1563.002-S3	Inadequate network segmentation, risking the compromise of network security zones if firewall rules are not configured to block RDP traffic appropriately.
EV1563.002-H1	The failure to disable the RDP service when unnecessary, leaving an exploitable attack surface for adversaries to potentially perform RDP session hijacking.
EV1563.002-H2	The failure to utilize remote desktop gateways, potentially allowing unauthorized access to resources over the network.
EV1563.002-H3	The failure to adjust GPOs to define shorter session timeouts and maximum active session durations, exposing the system to increased risk of unauthorized access or prolonged sessions.
EV1563.002-H4	User retains the local Administrators group in the list of groups allowed to log in through RDP, potentially providing elevated privileges to attackers in the event of a compromise.
EV1563.002-H5	The failure to limit remote user permissions appropriately, increasing the risk of unauthorized access and potential compromise of the system.

2.10.7 Remote Services (T1021) [504]

EV Code	Vulnerability Description
EV1021-S1	The centralization of identity management in enterprise domains, allowing unauthorized access to multiple machines upon obtaining valid domain credentials, exploiting weaknesses in the domain structure.
EV1021-S2	The potential escalation of an SSH session to an ARD session on macOS, enabling adversaries to accept TCC prompts without user interaction and gain access to data, particularly in versions prior to macOS 10.14.
EV1021-S3	Insufficient control over remote service configurations, potentially allowing unauthorized access if unnecessary connection types are not disabled or removed.
EV1021-S4	The potential lack of multi-factor authentication on remote service logons, which, if not implemented, could expose the system to credential compromise.
EV1021-H1	The potential oversight in user account management, specifically in limiting accounts that may use remote services or configuring permissions for higher-risk accounts, thereby contributing to the risk of unauthorized access.

2.10.8 Remote Services: Remote Desktop Protocol (T1021.001) [505]

EV Code	Vulnerability Description
EV1021.001-S1	Inadequate auditing of the Remote Desktop Users group, potentially leading to unauthorized access if unnecessary accounts and groups are not regularly removed.
EV1021.001-S2	The unnecessary presence of the RDP service, which, if not disabled, could provide an avenue for exploitation.
EV1021.001-S3	Insufficient network access controls, as the use of remote desktop gateways may not be enforced, leaving resources vulnerable to unauthorized access over the network.

EV1021.001-S4	The absence of multi-factor authentication, potentially enabling unauthorized access to remote logins in the absence of an additional authentication layer.
EV1021.001-S5	The lack of network segmentation and firewall rules may allow attackers to exploit vulnerabilities in RDP services.
EV1021.001-S6	The absence of defined timeouts and disconnected session limits in GPOs may increase the risk of unauthorized access and prolonged active sessions.
EV1021.001-H1	The use of weak or compromised credentials, as adversaries are likely to employ Credential Access techniques to acquire the necessary credentials for logging in through RDP.
EV1021.001-H2	Inadequate user account management, allowing remote users excessive permissions, which could be exploited for unauthorized actions.
EV1021.001-H3	Failure to remove the local Administrators group from the list of groups allowed to log in through RDP, potentially exposing privileged access.

2.10.9 Remote Services: SMB/Windows Admin Shares (T1021.002) **[506]**

EV Code	Vulnerability Description
EV1021.002-S1	The existence of hidden network shares (e.g., C$, ADMIN$, IPC$) on Windows systems, accessible to administrators, which can be exploited for remote file copy and other administrative functions.
EV1021.002-S2	The lack of network traffic filtering, as host firewalls are not configured to restrict file sharing communications like SMB, potentially allowing unauthorized access.
EV1021.002-S3	The existence of enabled Windows administrative shares, as not disabling them poses a risk of unauthorized remote access and lateral movement.
EV1021.002-H1	The use of weak or compromised Valid Accounts, allowing adversaries to interact with remote network shares using SMB and perform actions as the logged-on user.

EV1021.002-H2	The reuse of local administrator account passwords across systems, which could be exploited by adversaries if these passwords are compromised on one system.
EV1021.002-H3	The inclusion of domain user accounts in the local Administrators group on multiple systems, creating a potential security risk and enabling adversaries to escalate privileges if these accounts are compromised.

2.10.10 Remote Services: Distributed Component Object Model (T1021.003) [507]

EV Code	Vulnerability Description
EV1021.003-S1	The insecure default configuration of Distributed Component Object Model (DCOM), allowing remote activation and launch of COM objects by default for Administrators, potentially leading to arbitrary shellcode execution and unauthorized access.
EV1021.003-S2	The potential misconfiguration or oversight in ensuring that all COM alerts and Protected View are enabled, which could lead to a bypass of application isolation and sandboxing measures, allowing for exploitation.
EV1021.003-S3	The potential oversight in enabling the Windows firewall, which, if not implemented, could allow for the instantiation of DCOM and potential exploitation.
EV1021.003-S4	The misconfiguration of Registry settings in HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID{{AppID_GUID}} and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole, which, if not modified appropriately using Dcomcnfg.exe, may lead to inadequate process-wide and system-wide security defaults for COM applications, allowing for unauthorized interactions.
EV1021.003-H1	The improper management of access control lists (ACL) in the Registry, where misconfigurations could grant unintended users permissions to interact with local and remote server COM objects, compromising system security.

EV1021.003-H2	The mismanagement or failure to disable Distributed Component Object Model (DCOM) through Dcomcnfg.exe, leaving the system exposed to potential remote activation and launch of COM objects by adversaries.
EV1021.003-H3	The failure to implement proper privileged account management, specifically in modifying Registry settings associated with the security of individual COM applications, which may result in inadequate protection against privileged account misuse and potential unauthorized actions.

2.10.11 Remote Services: SSH (T1021.004) **[508]**

EV Code	Vulnerability Description
EV1021.004-H1	The use of weak or easily guessable passwords for SSH authentication, which could be exploited by adversaries to gain unauthorized access to remote machines.
EV1021.004-H2	The failure to disable or remove the SSH daemon on systems that do not require it, exposing unnecessary attack surfaces if administrators neglect to implement this mitigation.
EV1021.004-H3	The risk of not implementing multi-factor authentication for SSH connections, particularly with password-protected SSH keys, exposing systems to higher susceptibility if this additional layer of security is not enforced.
EV1021.004-H4	The failure to adequately manage user accounts for SSH, such as not limiting or properly configuring which user accounts are allowed to log in, potentially leading to unauthorized access if user permissions are not appropriately defined.

2.10.12 Remote Services: VNC (T1021.005) **[509]**

EV Code	Vulnerability Description
EV1021.005-S1	The potential oversight in auditing, allowing unauthorized VNC server software to remain undetected on workstations.

EV1021.005-S2	The reliance on default VNC ports (TCP ports 5900 for the server, 5800 for browser access, and 5500 for a viewer in listening mode), which can be exploited if not properly filtered or blocked.
EV1021.005-H1	The misuse or weak configuration of VNC, allowing adversaries to remotely control machines, perform malicious actions, and potentially pivot to other systems within the network.
EV1021.005-H2	The failure to uninstall unnecessary VNC server software, providing potential entry points for adversaries to exploit.
EV1021.005-H3	User allows unrestricted software installation, increasing the risk of manual installation of VNC server software by users or adversaries.

2.10.13 Remote Services: Windows Remote Management (T1021.006) [510]

EV Code	Vulnerability Description
EV1021.006-S1	The potential oversight or delay in disabling the WinRM service, leaving a window of opportunity for adversaries to exploit this feature.
EV1021.006-H1	The failure to implement network segmentation for WinRM, exposing critical enclaves to potential compromise if the service is deemed necessary but not properly isolated.
EV1021.006-H2	The misconfiguration of host firewalls for WinRM, allowing unintended access if best practices are not followed, potentially due to a lack of understanding or oversight.
EV1021.006-H3	Inadequate privileged account management for WinRM, where separate accounts and permissions are not established in critical enclaves, potentially leading to unauthorized access and actions.

2.10.14 Remote Services: Cloud Services (T1021.007) [511]

EV Code	Vulnerability Description
EV1021.007-S1	Potential misconfigurations or weak security controls in cloud native methods, allowing adversaries to exploit valid accounts and gain privileged access on the host with SYSTEM or root level access.

EV1021.007-H1	The potential use of weak or compromised credentials for logging into accessible cloud services, providing adversaries with unauthorized access to cloud-hosted resources.
EV1021.007-H2	The potential failure to implement multi-factor authentication on cloud services, leaving accounts susceptible to compromise due to the absence of an additional layer of security.
EV1021.007-H3	The potential oversight in privileged account management, such as maintaining an excessive number of high-privileged domain and cloud accounts for day-to-day operations, leading to an elevated risk of unauthorized access and compromise of cloud environments.

2.10.15 Remote Services: Direct Cloud VM Connections (T1021.008) [512]

EV Code	Vulnerability Description
EV1021.008-S1	Potential misconfigurations or weak security controls in cloud native methods, allowing adversaries to exploit valid accounts and gain privileged access on the host with SYSTEM or root level access.
EV1021.008-H1	The potential use of weak or compromised credentials for logging into accessible cloud services, providing adversaries with unauthorized access to cloud-hosted resources.
EV1021.008-H2	Failure to disable unnecessary virtual machine connection types, leaving potential attack vectors open if direct connections are not required for administrative use.
EV1021.008-H3	Inadequate user account management practices, such as allowing a broad range of users to access compute infrastructure via cloud native methods, increasing the risk of unauthorized access.

2.10.16 Replication Through Removable Media (T1091) [514]

EV Code	Vulnerability Description
EV1091-S1	The potential failure to adequately configure Windows 10 Attack Surface Reduction (ASR) rules, allowing unsigned/untrusted executable files from USB removable drives to run, if ASR is not properly enabled or configured.

EV1091-S2	The susceptibility to malware propagation through USB devices and removable media within a network, if hardware installation is not adequately limited, potentially allowing unauthorized access or infection.
EV1091-H1	The failure to disable Autorun when unnecessary, leaving the system exposed to the execution of malicious files from removable media, or neglecting to disallow/restrict removable media at an organizational policy level, which could lead to increased risk if not required for business operations.

2.10.17 Software Deployment Tools (T1072) [549]

EV Code	Vulnerability Description
EV1072-S1	Inadequate Active Directory configuration, potentially leading to unauthorized access to critical network systems
EV1072-S2	The absence of restrictions on the installation of third-party software within the enterprise network, creating a potential avenue for unauthorized access
EV1072-S3	The insecure configuration of remote data storage, potentially allowing unauthorized access to the application deployment system
EV1072-H1	The inadequate management of user accounts used by third-party providers, potentially leading to unauthorized access
EV1072-H2	The insufficient management of privileged accounts, potentially leading to unauthorized access to application deployment systems
EV1072-H3	Mismanagement of password policies, such as using non-unique credentials across the enterprise network, posing a risk of unauthorized access to deployment systems
EV1072-H4	Insufficient implementation of multi-factor authentication, which may expose critical network systems to unauthorized access
EV1072-H5	Inadequate network segmentation, potentially allowing unauthorized access to critical network systems

EV1072-H6	The lack of regular software patching on deployment systems, creating a potential avenue for remote access through exploitation for privilege escalation
EV1072-H7	The absence of a strict approval policy for the use of deployment systems, creating a potential avenue for unauthorized access
EV1072-H8	The lack of user training, potentially leading to insecure use of deployment systems;

2.10.18 Taint Shared Content (T1080) [608]

EV Code	Vulnerability Description
EV1080-S1	The susceptibility of both binary and non-binary formats (e.g., .EXE, .DLL, .SCR, .BAT, .VBS) to compromise through binary infections in shared network directories.
EV1080-S2	Inadequate antivirus/antimalware protection, as there is a risk of suspicious files not being automatically quarantined, allowing potential execution of malicious content.
EV1080-S3	The absence of effective exploit protection utilities, such as the Microsoft Enhanced Mitigation Experience Toolkit (EMET), leaving the system susceptible to common exploitation techniques.
EV1080-H1	The inadvertent opening of tainted shared content, allowing the execution of malicious code on a remote system, leading to potential lateral movement by adversaries.
EV1080-H2	Unintentional execution of infected files within shared network directories, leading to the spread of malware and potential compromise when accessed by remote systems.
EV1080-H3	The failure to implement proper execution prevention measures, such as application control tools like AppLocker or Software Restriction Policies, leading to the potential execution of unknown and malicious programs that could result from or taint shared content.
EV1080-H4	Inadequate restriction of file and directory permissions for shared folders, allowing a larger number of users to have unnecessary write access and potentially facilitating the manipulation of shared content.

2.10.19 Use Alternate Authentication Material (T1550) **[627]**

EV Code	Vulnerability Description
EV1550-S1	The potential for credential overlap across systems, which could result in the compromise of privileged accounts and increase the risk of lateral movement.
EV1550-H1	The potential mismanagement of user accounts, specifically allowing domain users to be members of the local administrator group on multiple systems, violating the principle of least privilege and creating a security risk.

2.10.20 Use Alternate Authentication Material: Application Access Token (T1550.001) **[628]**

EV Code	Vulnerability Description
EV1550.001-H1	The failure to enforce file encryption for email communications containing sensitive information, leaving the data exposed to potential compromise through unauthorized access to email services.
EV1550.001-H2	The absence of measures to block end-user consent through administrative portals, such as the Azure Portal, leading to the potential for users to authorize third-party apps through OAuth without administrative oversight, resulting in unauthorized access.
EV1550.001-H3	The potential oversight in auditing cloud and container accounts, allowing unnecessary accounts or inappropriate permissions, and the failure to disable the ability to request temporary account tokens on behalf of other accounts, which could lead to unauthorized access.
EV1550.001-H4	The lack of specific and detailed corporate policies to restrict the types of third-party applications added to online services or tools, potentially allowing the introduction of malicious applications and unauthorized access to company information, accounts, or network.

2.10.21 Use Alternate Authentication Material: Pass the Hash (T1550.002) [629]

EV Code	Vulnerability Description
EV1550.002-S1	The excessive credential overlap across systems, which can amplify the impact of credential compromise and increase the adversary's ability to perform lateral movement.
EV1550.002-S2	The absence of pass-the-hash mitigations, particularly the failure to enable UAC restrictions on local accounts during network logon, potentially facilitating unauthorized access and lateral movement.
EV1550.002-H1	The failure to apply necessary software updates, specifically patch KB2871997 on Windows 7 and higher systems, which could leave systems exposed to known vulnerabilities and exploitation.
EV1550.002-H2	The risk of domain users being assigned to the local administrator group on multiple systems, creating a potential avenue for credential compromise and privilege escalation.
EV1550.002-H3	The failure to implement recommended pass-the-hash mitigations through Group Policy, leaving systems susceptible to pass-the-hash attacks due to insufficient UAC restrictions on local accounts during network logons.

2.10.22 Use Alternate Authentication Material: Pass the Ticket (T1550.003) [630]

EV Code	Vulnerability Description
EV1550.003-S1	The inadequate configuration of Active Directory, allowing the persistence of golden tickets
EV1550.003-H1	The over-assignment of domain admin account permissions, leaving domain controllers and limited servers vulnerable
EV1550.003-H2	The failure to ensure complex, unique passwords for local administrator accounts, potentially compromising the security of the system.
EV1550.003-H3	The allowance of a user to be a local administrator for multiple systems, posing a security risk

2.10.23 Use Alternate Authentication Material: Web Session Cookie (T1550.004) [631]

EV Code	Vulnerability Description
EV1550.004-S1	The extended validity period of authentication cookies in web applications, which allows for the stealing and use of session cookies to bypass multi-factor authentication, gaining unauthorized access to sensitive information.
EV1550.004-H1	The failure to configure browsers or tasks to regularly delete persistent cookies, increasing the risk of unauthorized access to web applications and services by adversaries through the exploitation of stolen session cookies.

2.11 Collection (TA0009) [14]

2.11.1 Adversary-in-the-Middle (T1557) [69]

EV Code	Vulnerability Description
EV1557-S1	The weaknesses in common networking protocols (e.g., ARP, DNS, LLMNR) to manipulate network traffic flow and force communication through an adversary-controlled system, allowing for information collection and additional actions.
EV1557-S2	The susceptibility to Downgrade Attacks, where adversaries negotiate a less secure, deprecated, or weaker version of communication protocols (e.g., SSL/TLS) or encryption algorithms to establish an AiTM position.
EV1557-S3	The potential lack of disabling or removal of legacy network protocols, leaving avenues for intercepting network traffic and enabling Adversary-in-the-Middle attacks.
EV1557-S4	The potential absence of encryption for sensitive information in wired and/or wireless traffic, providing opportunities for unauthorized access and manipulation.
EV1557-S5	The lack of network traffic filtering, allowing the exploitation of unnecessary legacy protocols that could be leveraged for Adversary-in-the-Middle conditions.

EV1557-S6	The absence of access limitations to network infrastructure and resources that can be exploited to reshape traffic or produce Adversary-in-the-Middle conditions.
EV1557-S7	The potential absence of network intrusion prevention systems capable of identifying and mitigating Adversary-in-the-Middle activity by recognizing indicative traffic patterns.
EV1557-S8	The lack of network segmentation, potentially allowing broader access to infrastructure components and increasing the scope of Adversary-in-the-Middle activity.
EV1557-H1	The lack of awareness and training regarding certificate errors, potentially leading to users accepting unauthorized certificates used by adversaries attempting to intercept HTTPS traffic.

2.11.2 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay (T1557.001) [70]

EV Code	Vulnerability Description
EV1557.001-S1	The vulnerability in LLMNR and NBT-NS protocols, allowing adversaries to spoof authoritative sources and poison name resolution, forcing communication with adversary-controlled systems.
EV1557.001-S2	The weakness in NTLMv1/v2 authentication, where adversaries can intercept and relay hashes, gaining unauthorized access and executing code on target systems.
EV1557.001-S3	The susceptibility of various protocols (LDAP, SMB, MSSQL, HTTP) to NTLMv1/v2 hash encapsulation, enabling adversaries to expand their attack surface and use multiple services with valid NTLM responses.
EV1557.001-S4	The potential lack of implementation or effectiveness of network intrusion detection and prevention systems, allowing adversaries to conduct AiTM activities without detection.
EV1557.001-S5	The absence or inadequacy of network segmentation, as failure to isolate infrastructure components increases the potential impact and scope of AiTM activity.

EV1557.001-H1	Failure to disable LLMNR and NetBIOS in their local computer security settings, providing an opportunity for adversaries to exploit these features.
EV1557.001-H2	User may neglect to implement host-based security software to filter LLMNR/NetBIOS traffic or enable SMB Signing, leaving systems susceptible to NTLMv2 relay attacks.

2.11.3 Adversary-in-the-Middle: ARP Cache Poisoning (T1557.002) **[71]**

EV Code	Vulnerability Description
EV1557.002-S1	The lack of authentication in the ARP protocol, allowing adversaries to poison ARP caches without authentication, leading to potential man-in-the-middle attacks.
EV1557.002-S2	The incorrect handling of ARP responses by network devices, where devices may wrongly add or update MAC addresses associated with IP addresses in their ARP caches, facilitating successful ARP cache poisoning by adversaries.
EV1557.002-S3	The reliance on broadcast ARP requests for IP-to-MAC address resolution, which can be exploited by adversaries to intercept and manipulate network traffic through ARP cache poisoning.
EV1557.002-S4	The lack of default measures to disable or prevent updating the ARP cache on gratuitous ARP replies, leaving the system susceptible to ARP cache poisoning attacks.
EV1557.002-S5	The absence of encryption on wired and/or wireless traffic, potentially exposing sensitive information, including credentials, to interception during ARP cache poisoning attacks.
EV1557.002-S6	The lack of filtering mechanisms for network traffic, as the absence of DHCP Snooping and Dynamic ARP Inspection on switches may allow malicious ARP replies to propagate, contributing to successful ARP cache poisoning.
EV1557.002-S7	The reliance on dynamic ARP entries, as the absence of static ARP entries for networked devices leaves the system vulnerable to ARP cache poisoning attacks.

EV1557.002-S8	The absence of network intrusion prevention systems capable of identifying patterns indicative of Adversary-in-the-Middle (AiTM) activity, which could mitigate ARP cache poisoning at the network level.
EV1557.002-H1	The potential for overlooking certificate errors, as users may not be adequately trained to be suspicious of certificate errors that could indicate attempts by adversaries to intercept HTTPS traffic during ARP cache poisoning attacks.

2.11.4 Adversary-in-the-Middle: DHCP Spoofing (T1557.003) [72]

EV Code	Vulnerability Description
EV1557.003-S1	The DHCPv6 client's capability to receive network configuration information without being assigned an IP address, creating an avenue for adversaries to respond with malicious configurations.
EV1557.003-S2	The DHCP service's susceptibility to exhaustion attacks, where adversaries can flood the network with broadcast DISCOVER messages, depleting the DHCP allocation pool and causing a denial of service.
EV1557.003-S3	The potential weakness in the network infrastructure, where failure to implement DHCP traffic filtering on ports 67 and 68 may expose the network to unauthorized DHCP servers, enabling adversaries to conduct DHCP spoofing attacks.
EV1557.003-S4	The absence of DHCP snooping on layer 2 switches, which can lead to DHCP spoofing attacks and starvation attacks by allowing adversaries to provide malicious network configurations.
EV1557.003-S5	The failure to block DHCPv6 traffic and incoming router advertisements, particularly if IPv6 is not commonly used in the network, which may expose the network to potential DHCPv6 attacks.
EV1557.003-H1	The failure to enable port security on layer switches, leaving the network susceptible to unauthorized devices connecting via DHCP and potentially facilitating DHCP spoofing attacks.

EV1557.003-H2	The lack of tracking available IP addresses through a script or a tool, making it difficult to detect and respond to DHCP exhaustion attacks that may result from the misuse of DHCP.
EV1557.003-H3	The oversight in implementing network intrusion detection and prevention systems capable of identifying AiTM activity, which may result in a delayed or ineffective response to DHCP spoofing and related attacks.

2.11.5 Archive Collected Data (T1560) **[79]**

EV Code	Vulnerability Description
EV1560-H1	The failure to conduct regular and thorough system scans, leaving the system susceptible to the use of unauthorized archival utilities by not identifying them in a timely manner.

2.11.6 Archive Collected Data: Archive via Utility (T1560.001) **[80]**

EV Code	Vulnerability Description
EV1560.001-H1	The failure to conduct regular and thorough system scans, leaving the system susceptible to the use of unauthorized archival utilities by not identifying them in a timely manner.

2.11.7 Archive Collected Data: Archive via Library (T1560.002) **[81]**

EV Code	Vulnerability Description
EV1560.002-H1	The potential use of insecure archival libraries such as Python rarfile, libzip, and zlib, which may lead to compromised data due to inadequate encryption or compression mechanisms chosen by the user during the archiving process.

2.11.8 Archive Collected Data: Archive via Custom Method (T1560.003) **[82]**

This attack technique does not rely on a specific vulnerability for execution.

2.11.9 Audio Capture (T1123) **[83]**

EV Code	Vulnerability Description
EV1123-S1	The potential security gaps in the operating system or applications, allowing malware or scripts to interact with peripheral devices (such as microphones) through available APIs for unauthorized audio capture.
EV1123-H1	The inadequate control over microphone permissions, enabling adversaries to exploit human mistakes and capture sensitive audio recordings without user consent.

2.11.10 Automated Collection (T1119) **[84]**

EV Code	Vulnerability Description
EV1119-S1	The potential weakness in the implementation of encryption for sensitive information, as adversaries may still acquire data through other means if the intrusion persists over an extended period, highlighting the need for improved encryption practices.
EV1119-H1	Weak passwords on encrypted documents, allowing adversaries to conduct offline cracking through Brute Force techniques.

2.11.11 Browser Session Hijacking (T1185) **[111]**

EV Code	Vulnerability Description
EV1185-S1	The potential security vulnerabilities and inherent functionality in the browser software that can be exploited to change content, modify user behaviors, and intercept information.
EV1185-H1	The failure to regularly close all browser sessions when they are no longer needed, creating an opportunity for adversaries to exploit browser session hijacking techniques due to prolonged session exposure.

2.11.12 Clipboard Data (T1115) **[118]**

EV Code	Vulnerability Description
EV1115-S1	The potential exposure of sensitive information due to the inherent functionality of clipboard services on Windows, macOS, and Linux, allowing adversaries to access and collect data stored in the clipboard.
EV1115-S2	The risk of data exposure through Transmitted Data Manipulation, where adversaries can monitor and replace users' clipboard contents with malicious data, potentially leading to unintended information disclosure.

2.11.13 Data from Cloud Storage (T1530) **[172]**

EV Code	Vulnerability Description
EV1530-S1	The lack of regular auditing of permissions on cloud storage, potentially allowing for misconfigurations that grant open or unprivileged access to resources.
EV1530-S2	The absence of encryption for sensitive data stored at rest in cloud storage, which may expose information in the event of a storage breach, emphasizing the need for managed encryption keys and a robust incident response plan.
EV1530-S3	The failure to implement IP-based restrictions and user account management effectively, leaving data access susceptible to misuse, especially in cases of stolen credentials.
EV1530-S4	Insufficient control over file and directory permissions, emphasizing the need for access control lists on storage systems and objects to prevent unauthorized access.
EV1530-H1	The improper configuration of cloud storage security settings, which may expose sensitive data such as credit cards, personally identifiable information, or medical records due to inadequate access controls.

EV1530-H2	The inadequate configuration of user permissions groups and roles for access to cloud storage, highlighting the importance of strict Identity and Access Management (IAM) controls and the issuance of temporary access tokens instead of permanent credentials.
EV1530-H3	The lack of multi-factor authentication, which may expose cloud storage resources and APIs to unauthorized access.

2.11.14 Data from Configuration Repository (T1602) [173]

EV Code	Vulnerability Description
EV1602-S1	Due to inadequate encryption of SNMPv3 traffic, there is a system vulnerability targeted by adversaries, leading to the potential exposure of sensitive information.
EV1602-S2	As a result of inadequate filtering of network traffic through extended ACLs, there is a system vulnerability targeted by adversaries, posing a risk of unauthorized access and exposure of sensitive data.
EV1602-S3	Inadequate configuration of intrusion prevention devices may lead to the potential for unauthorized SNMP queries and commands to go undetected, presenting a system vulnerability targeted by adversaries.
EV1602-S4	Insufficient network segmentation results in a system vulnerability targeted by adversaries, creating the risk of unauthorized access to SNMP traffic and sensitive data.
EV1602-H1	Inadequate allowlisting of MIB objects and implementation of SNMP views give rise to a system vulnerability targeted by adversaries, leading to the potential for unauthorized access and data exposure.
EV1602-H2	Failure to keep update system images and software and migrate to SNMPv3.

2.11.15 Data from Configuration Repository: SNMP (MIB Dump) (T1602.001) [174]

EV Code	Vulnerability Description
EV1602.001-S1	Due to the failure to configure SNMPv3 with the highest level of security (authPriv), the system is vulnerable to potential exposure of sensitive information, allowing adversaries unauthorized access to SNMP-managed devices.
EV1602.001-S2	Due to the absence of proper network traffic filtering using extended ACLs, there is a risk of unauthorized protocols infiltrating the trusted network, compromising SNMP security.
EV1602.001-S3	The lack of intrusion prevention device configurations results in the system's vulnerability to unauthorized SNMP queries and commands, creating opportunities for adversaries to exploit SNMP-managed devices.
EV1602.001-S4	The absence of network segmentation leads to the system's vulnerability, potentially exposing SNMP traffic to unauthorized access and compromising the confidentiality of MIB contents.
EV1602.001-H1	User inadequately implements software configuration by not allowlisting MIB objects and establishing SNMP views results in the vulnerability of unauthorized access and manipulation of SNMP information.
EV1602.001-H2	User fails to keep system images and software updated, along with delayed migration to SNMPv3, increases the risk of exploiting known vulnerabilities and outdated security protocols.

2.11.16 Data from Configuration Repository: Network Device Configuration Dump (T1602.002) [175]

EV Code	Vulnerability Description
EV1602.002-S1	The lack of proper encryption configuration in SNMPv3, as it may not be configured to use the highest level of security (authPriv), exposing sensitive information.

EV1602.002-S2	The absence of effective network traffic filtering, leaving the system susceptible to unauthorized protocols outside the trusted network due to the lack of applied extended ACLs.
EV1602.002-S3	The insufficient implementation of network intrusion prevention measures for SNMP queries and Smart Install (SMI) usage, which could lead to unauthorized access if not properly configured.
EV1602.002-S4	The lack of network segmentation for SNMP traffic, posing a risk of unauthorized access if SNMP traffic is not appropriately segregated on a separate management network.
EV1602.002-H1	The inadequate software configuration, including the absence of proper whitelisting for MIB objects and the failure to disable Smart Install (SMI) when not in use, creating potential avenues for exploitation.
EV1602.002-H2	The neglect of software updates and migration to SNMPv3, leaving the system exposed to potential exploits due to the failure to keep software and system images updated and transition to SNMPv3.

2.11.17 Data from Information Repositories (T1213) [176]

EV Code	Vulnerability Description
EV1213-S1	Inadequate access controls or misconfigured external sharing features in information repositories, such as Sharepoint and Confluence, allowing unauthorized access to policies, procedures, and standards, physical/logical network diagrams, system architecture diagrams, technical system documentation, testing/development credentials, work/project schedules, source code snippets, and links to internal resources.
EV1213-S2	The absence of robust access control mechanisms, including both authentication and authorization, creating opportunities for unauthorized access and compromise of repositories.
EV1213-H1	Inadequate periodic review of accounts and privileges for critical and sensitive repositories, potentially allowing unauthorized access and exploitation due to overlooked changes.

EV1213-H2	The potential weakness in enforcing the principle of least privilege, leading to excessive access rights and increasing the risk of unauthorized activities in repositories.
EV1213-H3	The failure to adhere to user training on acceptable information stored in repositories, potentially resulting in the inclusion of sensitive data and exposing it to adversaries.
EV1213-H4	The failure to implement and follow policies defining acceptable information in repositories, increasing the likelihood of storing sensitive data and facilitating adversary exploitation.

2.11.18 Data from Information Repositories: Confluence (T1213.001) [177]

EV Code	Vulnerability Description
EV1213.001-S1	Inadequate access controls or misconfigured external sharing features in information Confluence, allowing unauthorized access to policies, procedures, and standards, physical/logical network diagrams, system architecture diagrams, technical system documentation, testing/development credentials, work/project schedules, source code snippets, and links to internal resources.
EV1213.001-H1	The lack of periodic account and privilege reviews for critical and sensitive Confluence repositories, potentially allowing unauthorized access and information compromise.
EV1213.001-H2	The failure to enforce the principle of least privilege, leading to excessive access rights within Confluence repositories and increasing the risk of unauthorized exposure of critical information.
EV1213.001-H3	The absence of well-defined and communicated policies regarding acceptable information stored in Confluence repositories, which may result in unintentional inclusion of sensitive data and compromise of critical information.

2.11.19 Data from Information Repositories: Sharepoint (T1213.002) [178]

EV Code	Vulnerability Description
EV1213.002-S1	Inadequate access controls or misconfigured external sharing features in Sharepoint, allowing unauthorized access to policies, procedures, and standards, physical/logical network diagrams, system architecture diagrams, technical system documentation, testing/development credentials, work/project schedules, source code snippets, and links to internal resources.
EV1213.002-S2	The absence of robust access control mechanisms incorporating both authentication and authorization, posing a risk of inadequate protection for SharePoint repositories and potential unauthorized access.
EV1213.002-H1	The potential lack of periodic review of accounts and privileges for critical and sensitive SharePoint repositories, which may result in outdated access permissions and increased risk of unauthorized access.
EV1213.002-H2	The potential failure to enforce the principle of least privilege, which may lead to excessive permissions, increasing the likelihood of unauthorized access and compromise of sensitive information.
EV1213.002-H3	The failure to adhere to defined policies governing acceptable information stored in SharePoint repositories, potentially resulting in the inadvertent inclusion of sensitive data and increased risk of unauthorized access.
EV1213.002-H4	The lack of awareness or training regarding user account management policies, increasing the risk of unintentional security lapses such as inappropriate access permissions or inadequate review of accounts and privileges.

2.11.20 Data from Information Repositories: Code Repositories (T1213.003) [179]

EV Code	Vulnerability Description
EV1213.003-H1	Inadequate periodic review of accounts and privileges for critical and sensitive code repositories, potentially allowing unauthorized access if proper auditing measures are not in place.

EV1213.003-H2	The inadvertent inclusion of sensitive information, such as credentials or proprietary source code, within the software's source code stored in code repositories, potentially leading to unauthorized access or exploitation by adversaries.
EV1213.003-H3	The failure to enforce the principle of least privilege, leading to excessive permissions within code repositories, which can be mitigated by implementing effective user account management strategies.
EV1213.003-H4	The absence of multi-factor authentication for logons to code repositories, which increases the risk of unauthorized access in the absence of an additional layer of authentication.
EV1213.003-H5	The lack of user training on acceptable information to be stored in code repositories, leaving room for inadvertent inclusion of sensitive data, and can be addressed by developing and publishing clear policies defining acceptable content.

2.11.21 Data from Local System (T1005) [180]

EV Code	Vulnerability Description
EV1005-S1	The lack of proper access controls on local file systems and configuration files, allowing unauthorized access to sensitive data.
EV1005-H1	The failure to properly configure and implement data loss prevention tools, leading to potential gaps in restricting access to sensitive data and detecting unencrypted information.
EV1005-H2	The failure to implement sufficient restrictions on command and scripting interpreter usage, leading to potential misuse by adversaries for searching and gathering sensitive information.

2.11.22 Data from Network Shared Drive (T1039) [181]

EV Code	Vulnerability Description
EV1039-S1	The lack of proper access controls on network shares, allowing unauthorized access to sensitive data stored on remote systems

EV1039-H1	The utilization of weak or easily guessable passwords on network shares, potentially enabling adversaries to compromise the system and access sensitive information

2.11.23 Data from Removable Media (T1025) [182]

EV Code	Vulnerability Description
EV1025-S1	The lack of adequate access controls on connected removable media, allowing unauthorized access and potential exfiltration of sensitive data.
EV1025-H1	The failure to employ proper security practices, such as not encrypting sensitive data on removable media, leading to potential exposure during exfiltration attempts.
EV1025-H2	The failure to properly configure or maintain the Data Loss Prevention (DLP) system, leading to gaps in the protection of sensitive data and potential data loss.

2.11.24 Data Staged (T1074) [191]

EV Code	Vulnerability Description
EV1074-S1	The lack of proper access controls, allowing for the staging of collected data in a central location or directory

2.11.25 Data Staged: Local Data Staging (T1074.001) [192]

EV Code	Vulnerability Description
EV1074.001-S1	The lack of proper access controls, allowing for the staging of collected data in a central location or directory on the local system.

2.11.26 Data Staged: Remote Data Staging (T1074.002) [193]

EV Code	Vulnerability Description
EV1074.002-S1	The insecure configurations and permissions in cloud environments, allowing adversaries to create and utilize instances for data staging, leading to unauthorized data access and potential exfiltration.

2.11.27 Email Collection (T1114) [220]

EV Code	Vulnerability Description
EV1114-S1	The lack of effective auditing mechanisms, allowing potentially malicious auto-forwarding rules to go undetected.
EV1114-H1	The failure to use encryption, exposing sensitive information to potential interception and unauthorized access.
EV1114-H2	The failure to enable or utilize multi-factor authentication, potentially allowing adversaries to exploit compromised usernames and passwords for email access.

2.11.28 Email Collection: Local Email Collection (T1114.001) [221]

EV Code	Vulnerability Description
EV1114.001-H1	Improper handling or storage of Outlook files in insecure locations like C:\Users<username>\Documents\Outlook Files or C:\Users<username>\AppData\Local\Microsoft\Outlook.
EV1114.001-H2	The failure to utilize encryption for sensitive information sent over email, which could result in the exposure of confidential data if an adversary gains access to the communication channel, emphasizing the importance of implementing encryption for email security.

2.11.29 Email Collection: Remote Email Collection (T1114.002) [222]

EV Code	Vulnerability Description
EV1114.002-S1	The potential weaknesses in the Exchange server, Office 365, or Google Workspace, which may include unpatched software, misconfigurations, or insufficient security measures.
EV1114.002-S2	The potential absence of encryption on sensitive information sent over email, exposing it to interception and unauthorized access.
EV1114.002-H1	The failure to implement multi-factor authentication on public-facing webmail servers, which could result in compromised usernames and passwords, potentially due to weak or easily guessable credentials.

2.11.30 Email Collection: Email Forwarding Rule (T1114.003) [223]

EV Code	Vulnerability Description
EV1114.003-S1	The lack of restrictions in most email clients, enabling users or adversaries with valid credentials to create email forwarding rules without limitations, potentially leading to unauthorized information access and persistent email access even after credential resets.
EV1114.003-H1	The risk of not disabling external email forwarding, which may expose the organization to unauthorized information access.
EV1114.003-H2	The potential failure to encrypt sensitive information, as the use of encryption is recommended for added security, and neglecting this measure may result in the compromise of sensitive data sent over email.
EV1114.003-H3	The potential for inadequate monitoring mechanisms, as enterprise email solutions may lack effective auditing of auto-forwarding rules, allowing malicious rules to go unnoticed.

2.11.31 Input Capture (T1056) [363]

EV Code	Vulnerability Description
EV1056-H1	User may unknowingly provide sensitive information to what they believe is a legitimate service

2.11.32 Input Capture: Keylogging (T1056.001) [364]

EV Code	Vulnerability Description
EV1056.001-H1	User inadvertently exposes credentials, as keylogging relies on intercepting keystrokes over a period of time, especially when users are forced to reauthenticate due to actions like clearing browser cookies.

2.11.33 Input Capture: GUI Input Capture (T1056.002) [365]

EV Code	Vulnerability Description
EV1056.002-H1	The tendency to unknowingly input credentials into seemingly legitimate prompts initiated by the adversary, facilitating unauthorized access and potential data compromise.
EV1056.002-H2	The failure to undergo effective user training, resulting in a reduced ability to recognize and appropriately respond to suspicious events and dialog boxes, potentially leading to inadvertent disclosure of credentials.

2.11.34 Input Capture: Web Portal Capture (T1056.003) [366]

EV Code	Vulnerability Description
EV1056.003-H1	User unknowingly enters credentials on a compromised login page, leading to the disclosure of sensitive information to the adversary.

2.11.35 Input Capture: Credential API Hooking (T1056.004) [367]

EV Code	Vulnerability Description
EV1056.004-S1	Weaknesses in Windows API functions, potentially leading to the unauthorized collection of user credentials.
EV0156.004-H1	User enters sensitive information in applications susceptible to API hooking, thereby inadvertently providing access to adversaries.

2.11.36 Screen Capture (T1113) [525]

This attack technique does not rely on a specific vulnerability for execution.

2.11.37 Video Capture (T1125) [641]

This attack technique does not rely on a specific vulnerability for execution.

2.12 Command and Control (TA0011) [15]

2.12.1 Application Layer Protocol (T1071) [73]

EV Code	Vulnerability Description
EV1071-S1	The weaknesses in OSI application layer protocols, allowing adversary to communicate and execute commands without detection or network filtering.
EV1071-H1	The potential mishandling of sensitive information within application layer protocols, such as web browsing, file transfer, email, or DNS, leading to inadvertent exposure of critical data.

2.12.2 Application Layer Protocol: Web Protocols (T1071.001) [74]

EV Code	Vulnerability Description
EV1071.001-S1	The weaknesses in application layer protocols such as HTTP/S and WebSocket, where the numerous fields and headers in these packets provide opportunities for data concealment, allowing the adversary to communicate with systems under their control within a victim network while masquerading as normal traffic.
EV1071.001-H1	The failure to implement or configure network intrusion detection and prevention systems, leaving the network susceptible to exploitation by adversary malware communicating through application layer protocols like HTTP/S and WebSocket.

2.12.3 Application Layer Protocol: File Transfer Protocols (T1071.002) [75]

EV Code	Vulnerability Description
EV1071.002-S1	The susceptibility of file transfer protocols such as SMB, FTP, FTPS, and TFTP to be exploited due to their common usage and the potential for concealing malicious commands and results within the protocol traffic.
EV1071.002-S2	The potential inadequacy of network intrusion detection and prevention systems to fully identify and mitigate all variations of adversary malware, leaving potential gaps in defense.

2.12.4 Application Layer Protocol: Mail Protocols (T1071.003) [76]

EV Code	Vulnerability Description
EV1071.003-S1	The weaknesses in Mail Protocols such as SMTP/S, POP3/S, and IMAP, which could be abused to conceal malicious commands and results within the protocol traffic.
EV1071.003-H1	The inadvertent inclusion of sensitive information within email messages, as users might unknowingly transmit confidential data, providing adversaries with opportunities for data exfiltration or reconnaissance.

EV1071.003-H2	Incomplete or ineffective deployment of network intrusion detection and prevention systems, allowing adversary activity to go undetected if the signatures for specific malware are not kept up to date or if the system configurations are not appropriately tuned.

2.12.5 Application Layer Protocol: DNS (T1071.004) [77]

EV Code	Vulnerability Description
EV1071.004-S1	The DNS protocol's susceptibility to abuse for DNS tunneling, allowing adversaries to conceal commands and communicate with systems under their control within a victim network while mimicking normal traffic.
EV1071.004-H1	Allowing DNS traffic even before network authentication is completed, potentially exposing the network to unauthorized communication and exploitation by adversaries.
EV1071.004-H2	Failing to implement or configure network traffic filters effectively, leaving the system exposed to malicious DNS requests and potential data exfiltration through DNS tunneling due to mismanagement of filtering rules and policies.

2.12.6 Communication Through Removable Media (T1092) [134]

EV Code	Vulnerability Description
EV1092-S1	The lack of proper network segmentation, allowing lateral movement and command and control through removable media.
EV1092-H1	The failure to adequately secure removable media, leading to the potential introduction of malicious commands and files into the system through the media transfer.
EV1092-H2	The failure to disable Autoruns when unnecessary, leaving a potential avenue for adversaries to exploit removable media and establish command and control within the system.

EV1092-H3	The failure to implement organizational policies disallowing or restricting the use of removable media, leaving the system exposed to potential command and control attacks facilitated by the media transfer.

2.12.7 Content Injection (T1659) [150]

EV Code	Vulnerability Description
EV1659-S1	The potential lack of encryption for sensitive information in online traffic, making it susceptible to interception, manipulation, or unauthorized access.
EV1659-S2	The potential failure to restrict web-based content adequately, allowing the download, transfer, and execution of potentially uncommon file types used in adversary campaigns.

2.12.8 Data Encoding (T1132) [168]

EV Code	Vulnerability Description
EV1132-S1	The weakness in the ability to detect command and control (C2) traffic due to the use of encoded data using standard encoding schemes such as ASCII, Unicode, hexadecimal, Base64, and MIME, making it challenging to identify malicious activities.
EV1132-S2	The potential limitation in the effectiveness of network intrusion detection and prevention systems, as adversaries may change tool command and control (C2) signatures over time or construct protocols to evade detection,

2.12.9 Data Encoding: Standard Encoding (T1132.001) [169]

EV Code	Vulnerability Description
EV1132.001-S1	The weakness in the ability to detect command and control (C2) traffic due to the use of encoded data using standard encoding schemes such as ASCII, Unicode, hexadecimal, Base64, and MIME, making it challenging to identify malicious activities.

EV1132.001-S2	The potential limitation in the effectiveness of network intrusion detection and prevention systems, as adversaries may change tool command and control (C2) signatures over time or construct protocols to evade detection,

2.12.10 Data Encoding: Non-Standard Encoding (T1132.002) [170]

EV Code	Vulnerability Description
EV1132.002-S1	The inadequate detection of command and control (C2) traffic due to the system's inability to recognize non-standard data encoding schemes, allowing adversaries to obfuscate their activities.
EV1132.002-S2	The potential limitation in the effectiveness of network intrusion detection and prevention systems, as adversaries may change tool command and control (C2) signatures over time or construct protocols to evade detection,

2.12.11 Data Obfuscation (T1001) [187]

EV Code	Vulnerability Description
EV1001-S1	The potential failure of network intrusion detection and prevention systems to effectively identify obfuscation activity, leaving the system susceptible to undetected command and control (C2) communications.

2.12.12 Data Obfuscation: Junk Data (T1001.001) [188]

EV Code	Vulnerability Description
EV1001.001-S1	The potential failure of network intrusion detection and prevention systems to effectively identify obfuscation activity, leaving the system susceptible to undetected command and control (C2) communications.

2.12.13 Data Obfuscation: Steganography (T1001.002) [189]

EV Code	Vulnerability Description
EV1001.002-S1	The potential failure of network intrusion detection and prevention systems to effectively identify obfuscation activity, leaving the system susceptible to undetected command and control (C2) communications.

2.12.14 Data Obfuscation: Protocol Impersonation (T1001.003) [190]

EV Code	Vulnerability Description
EV1001.003-S1	The potential failure of network intrusion detection and prevention systems to effectively identify obfuscation activity, leaving the system susceptible to undetected command and control (C2) communications.

2.12.15 Dynamic Resolution (T1568) [216]

EV Code	Vulnerability Description
EV1568-S1	The potential for inadequacies in network intrusion detection and prevention systems, which may rely on signatures to identify adversary malware and could be bypassed if the malware employs sophisticated dynamic resolution techniques, necessitating continuous updates and resource-intensive efforts for effective mitigation.
EV1568-S2	The susceptibility of local DNS sinkholes to be bypassed or rendered ineffective in preventing behaviors associated with dynamic resolution, potentially allowing adversaries to establish or reestablish command and control channels.

2.12.16 Dynamic Resolution: Fast Flux DNS (T1568.001) [217]

This attack technique does not rely on a specific vulnerability for execution.

2.12.17 Dynamic Resolution: Domain Generation Algorithms (T1568.002) [218]

EV Code	Vulnerability Description
EV1568.002-S1	The potential inability to effectively block, track, or take over the command and control channel due to the use of Domain Generation Algorithms (DGAs), which dynamically generate destination domains for malware, making it challenging for defenders.
EV1568.002-S2	The potential limitation of network intrusion detection and prevention systems, as the time and resource-intensive nature of reverse engineering malware variants using DGAs may result in delayed or incomplete identification of future domains, allowing adversaries to exploit the time gap.
EV1568.002-S3	The challenge in preemptively registering all possible command and control (C2) domains due to the impracticality and cost associated with the potentially thousands of domains generated daily by DGAs, leaving defenders with a risk of incomplete coverage.
EV1568.002-H1	The potential oversight in implementing and maintaining a local DNS sinkhole, which may lead to incomplete prevention of behaviors associated with dynamic resolution

2.12.18 Dynamic Resolution: DNS Calculation (T1568.003) [219]

EV Code	Vulnerability Description
EV1568.003-H1	The potential oversight in not adequately considering or configuring egress filtering rules, which could lead to an unintended exposure of the C2 channel through the manipulation of DNS calculations by adversaries.

2.12.19 Encrypted Channel (T1573) [224]

EV Code	Vulnerability Description
EV1573-H1	The failure to implement Network Intrusion Prevention measures, which could result in the inability to identify and prevent adversary malware activity at the network level despite available mitigation strategies like network intrusion detection and prevention systems
EV1573-H2	The failure to implement SSL/TLS inspection, potentially leading to an inability to inspect the contents of encrypted sessions and detect network-based indicators of malware communication protocols despite available mitigation strategies

2.12.20 Encrypted Channel: Symmetric Cryptography (T1573.001) [225]

EV Code	Vulnerability Description
EV1573.001-S1	The potential misconfiguration or inadequacy of network intrusion detection and prevention systems, which, if not properly set up or updated, could lead to the failure of identifying and mitigating adversary malware activity.

2.12.21 Encrypted Channel: Asymmetric Cryptography (T1573.002) [226]

EV Code	Vulnerability Description
EV1573.002-H1	The failure to implement Network Intrusion Prevention measures, which could result in the inability to identify and prevent adversary malware activity at the network level despite available mitigation strategies like network intrusion detection and prevention systems
EV1573.002-H2	The failure to implement SSL/TLS inspection, potentially leading to an inability to inspect the contents of encrypted sessions and detect network-based indicators of malware communication protocols despite available mitigation strategies

2.12.22 Fallback Channels (T1008) **[277]**

EV Code	Vulnerability Description
EV1008-S1	The potential ineffectiveness of network intrusion detection and prevention systems over time due to adversaries changing tool command and control (C2) signatures or constructing protocols to evade detection, requiring constant updates and adaptability of defensive tools.

2.12.23 Ingress Tool Transfer (T1105) **[361]**

EV Code	Vulnerability Description
EV1105-S1	The lack of proper restrictions or monitoring on external tool transfer utilities and protocols, such as copy, finger, certutil, PowerShell commands, curl, scp, sftp, tftp, rsync, wget, installers, and package managers on Windows, Linux, and macOS systems.
EV1105-S2	The potential failure of network intrusion detection and prevention systems to effectively identify and prevent tool or file transfers if adversaries change tool C2 signatures or employ obfuscation techniques not covered by existing signatures.

2.12.24 Multi-Stage Channels (T1104) **[406]**

EV Code	Vulnerability Description
EV1104-S1	Dependency on network intrusion detection and prevention systems, which may not cover all adversary malware or may have limitations in identifying sophisticated multi-stage channels.

2.12.25 Non-Application Layer Protocol (T1095) [416]

EV Code	Vulnerability Description
EV1095-S1	The lack of effective monitoring for non-application layer protocols, such as ICMP, which may be used to conceal malicious communications due to its lower visibility compared to more commonly monitored protocols like TCP or UDP.
EV1095-S2	Inadequate filtering of network traffic, which may allow the use of unnecessary protocols across the network boundary, providing potential avenues for malicious communication.
EV1095-S3	The absence of network intrusion detection and prevention systems, relying on network signatures to identify and mitigate specific adversary malware activities, leaving the network more susceptible to unauthorized communication.
EV1095-S4	Improper configuration of firewalls and proxies, potentially allowing outgoing traffic on unnecessary ports and compromising network security by not enforcing proper limitations.
EV1095-S5	The lack of network segmentation, leading to insufficient control over outgoing traffic, potentially exposing hosts to unauthorized communication and compromising network integrity.

2.12.26 Non-Standard Port (T1571) [417]

EV Code	Vulnerability Description
EV1571-S1	Inadequate configuration of network intrusion detection and prevention systems, potentially allowing adversaries to evade detection and carry out activities using non-standard ports.
EV1571-S2	Improper firewall and proxy configuration, leading to the possibility of outgoing traffic on unnecessary ports and undermining the effectiveness of network segmentation as a mitigation strategy.

2.12.27 Protocol Tunneling (T1572) [492]

EV Code	Vulnerability Description
EV1572-S1	The potential absence or inadequacy of network intrusion detection and prevention systems, relying on network signatures to identify adversary malware and mitigate malicious activity at the network level.
EV1572-S2	The potential absence or inadequacy of network intrusion detection and prevention systems, relying on network signatures to identify adversary malware and mitigate malicious activity at the network level.

2.12.28 Proxy (T1090) [493]

EV Code	Vulnerability Description
EV1090-S1	The potential limitation of network filtering strategies in blocking traffic to known anonymity networks and command and control (C2) infrastructure, as adversaries may employ techniques like domain fronting to circumvent these controls.
EV1090-S2	The reliance on network intrusion detection and prevention systems that use static signatures, as adversaries may modify C2 protocols or employ different malware versions, rendering these signatures ineffective over time.
EV1090-H1	The potential inability to inspect HTTPS traffic for domain fronting, as adversaries may exploit this limitation to hide malicious communications within seemingly legitimate connections.
EV1090-H2	The potential misconfiguration or oversight in not implementing SSL/TLS inspection, limiting the ability to analyze HTTPS traffic for signs of domain fronting and leaving the network susceptible to covert command and control activities.
EV1090-H3	The potential lack of awareness or misconfiguration in allowing the use of proxy tools like HTRAN, ZXProxy, and ZXPortMap, enabling adversaries to manipulate network traffic without detection.

2.12.29 Proxy: Internal Proxy (T1090.001) [494]

EV Code	Vulnerability Description
EV1090.001-S1	The potential weakness in internal systems that allows the installation and operation of proxy tools like HTRAN, ZXProxy, and ZXPortMap, enabling adversaries to redirect command and control traffic within a compromised environment.
EV1090.001-S2	The potential weakness in network intrusion detection and prevention systems that rely on specific C2 signatures, as adversaries may change these signatures over time or construct protocols to evade detection, posing a risk of bypassing network-level defenses.

2.12.30 Proxy: External Proxy (T1090.002) [495]

EV Code	Vulnerability Description
EV1090.002-S1	The potential reliance on network intrusion detection and prevention systems using signatures, which may become ineffective over time as adversaries change tool C2 signatures or construct protocols to evade detection, highlighting a need for continuous adaptation and updates in defensive tools.

2.12.31 Proxy: Multi-hop Proxy (T1090.003) [496]

EV Code	Vulnerability Description
EV1090.003-S1	The potential inadequacy of network filtering measures, specifically the susceptibility of traffic blocking to known anonymity networks and C2 infrastructure, as it may be circumvented by techniques like Domain Fronting.

2.12.32 Proxy: Domain Fronting (T1090.004) **[497]**

EV Code	Vulnerability Description
EV1090.004-S1	Inability to effectively mitigate domain fronting attacks when SSL/TLS inspection is not implemented, as capturing and analyzing HTTPS traffic for connections exhibiting domain fronting may be hindered.

2.12.33 Remote Access Software (T1219) **[500]**

EV Code	Vulnerability Description
EV1219-S1	Improper configuration of firewalls, application firewalls, and proxies, potentially leading to the unrestricted outgoing traffic to sites and services associated with remote access software.
EV1219-S2	The reliance on network intrusion detection and prevention systems with inadequate network signatures, potentially allowing traffic to remote access services to go undetected.
EV1219-H1	The failure to implement proper application control, which could result in the execution of unapproved software for remote access, bypassing security measures.

2.12.34 Traffic Signaling (T1205) **[610]**

EV Code	Vulnerability Description
EV1205-H1	Failure to disable or remove the Wake-on-LAN feature when not needed within an environment, which could expose systems to unauthorized activation and subsequent lateral movement.
EV1205-H2	The potential failure to implement stateful firewalls effectively, allowing some variants of traffic signaling to bypass network defenses.

2.12.35 Traffic Signaling: Port Knocking (T1205.001) **[611]**

EV Code	Vulnerability Description
EV1205.001-H1	The potential failure to implement or configure stateful firewalls effectively, leaving the system susceptible to variants of the port knocking technique and associated adversarial activities.

2.12.36 Traffic Signaling: Socket Filters (T1205.002) **[612]**

EV Code	Vulnerability Description
EV1205.002-H1	The potential misconfiguration or improper implementation of stateful firewalls, introducing the risk of ineffective mitigation and leaving the system susceptible to network traffic filtering manipulations by adversaries.

2.12.37 Web Service (T1102) **[649]**

EV Code	Vulnerability Description
EV1102-S1	The potential failure of network intrusion prevention systems to effectively identify and mitigate adversary activity, leaving the system exposed to exploitation through the use of legitimate external web services for data relay.
EV1102-H1	The inadvertent reliance on common services like Google or Twitter, providing adversaries with an opportunity to exploit expected network noise and evade detection during data relay.
EV1102-H2	The potential failure to implement or configure web proxies adequately, allowing unauthorized external services to bypass network communication policies, thereby undermining the effectiveness of the mitigation strategy.

2.12.38 Web Service: Dead Drop Resolver (T1102.001) [650]

EV Code	Vulnerability Description
EV1102.001-S1	The potential limitation or absence of effective network intrusion detection and prevention systems, allowing for the undetected hosting of malicious dead drop resolvers on external web services.
EV1102.001-H1	The potential failure to scrutinize content posted on web services, allowing for the hosting of malicious dead drop resolvers, which can lead to victims being redirected to adversarial command and control infrastructure.
EV1102.001-H2	The potential failure to implement or configure network intrusion detection and prevention systems with updated signatures, allowing malicious activity related to dead drop resolvers to go undetected.
EV1102.001-H3	The potential neglect in configuring web proxies to enforce policies restricting web-based content, leaving the network susceptible to the use of unauthorized external services for hosting malicious infrastructure.

2.12.39 Web Service: Bidirectional Communication (T1102.002) [651]

EV Code	Vulnerability Description
EV1102.002-H1	The risk of inadvertently hosting command and control instructions on popular websites or social media platforms, allowing adversaries to use these channels for malicious activities without raising suspicion.
EV1102.002-H2	The potential for misconfiguring or failing to implement network intrusion detection and prevention systems, allowing adversaries to evade detection by not triggering the configured network signatures for specific adversary malware.

2.12.40 Web Service: One-Way Communication (T1102.003) [652]

EV Code	Vulnerability Description
EV1102.003-S1	The reliance on SSL/TLS encryption by web service providers, providing adversaries with an added layer of protection to hide their malicious activities within encrypted traffic.
EV1102.003-S2	The potential for network intrusion detection and prevention systems to fail in identifying specific adversary malware if the network signatures are not regularly updated or if the system relies solely on signature-based detection.
EV1102.003-H1	The potential for individuals within the compromised system to inadvertently facilitate the attack by allowing communication over common services, such as Google or Twitter, which are more likely to be overlooked in network traffic.
EV1102.003-H2	The potential for misconfiguration or inadequate use of web proxies, allowing unauthorized external services to bypass the intended restrictions, undermining the effectiveness of the network communication policy.

2.13 Exfiltration (TA0010) [16]

2.13.1 Automated Exfiltration (T1020) [85]

EV Code	Vulnerability Description
EV1020-S1	The lack of effective controls preventing automated exfiltration, allowing sensitive data to be transferred without detection.
EV1020-H1	The failure to implement adequate data loss prevention measures, enabling automated exfiltration methods to successfully bypass security mechanisms.

2.13.2 Automated Exfiltration: Traffic Duplication (T1020.001) [86]

EV Code	Vulnerability Description
EV1020.001-S1	The potential absence or inadequacy of encryption measures for wired and/or wireless traffic, which could facilitate unauthorized access to sensitive information during automated exfiltration.
EV1020.001-S2	Misconfiguring cloud-based environments supporting traffic mirroring (e.g., AWS, GCP, Azure), which could result in unintentional exposure of sensitive data during automated exfiltration.
EV1020.001-H1	The improper management of user accounts in cloud environments, specifically the granting of unnecessary permissions to create or modify traffic mirrors, thereby increasing the risk of inadvertent exposure of sensitive data.

2.13.3 Data Transfer Size Limits (T1030) [194]

EV Code	Vulnerability Description
EV1030-S1	The absence of effective monitoring mechanisms to detect data exfiltration in fixed size chunks, allowing the adversary to avoid triggering network data transfer threshold alerts.
EV1030-H1	The lack of implementation or tuning of effective network intrusion detection and prevention systems, which may result in the failure to identify and mitigate traffic associated with adversary command and control infrastructure and malware.

2.13.4 Exfiltration Over Alternative Protocol (T1048) [256]

EV Code	Vulnerability Description
EV1048-S1	The lack of proper network monitoring and controls, allowing adversaries to exfiltrate data over alternative protocols such as FTP, SMTP, HTTP/S, DNS, SMB, or others without detection.

EV1048-S2	Inadequate implementation of network segmentation and firewall configurations, allowing unnecessary ports and traffic to enter and exit the network, providing opportunities for adversaries to exfiltrate data.
EV1048-S3	Insufficient access control lists on cloud storage systems and objects, potentially leading to unauthorized access and exfiltration of sensitive data.
EV1048-S4	Inadequate configuration and security settings on IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3), allowing direct download of sensitive information via the web console or Cloud API without proper access controls.
EV1048-H1	Poor user account management practices, such as not configuring proper permissions groups, roles, and Identity and Access Management (IAM) controls for access to cloud storage, which may result in unauthorized data access.
EV1048-H2	Issuing permanent credentials instead of temporary access tokens, especially when granting access to entities outside of the internal security boundary, increasing the risk of unauthorized access and data exfiltration.

2.13.5 *Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol (T1048.001)* **[257]**

EV Code	Vulnerability Description
EV1048.001-S1	The weakness in symmetric encryption implementations, where the use of shared or pre-arranged keys could be exploited for unauthorized data access.
EV1048.001-S2	The inadequacy in enforcing network segmentation, where improper firewall configurations may allow unnecessary ports and traffic, providing an avenue for exfiltration over alternative protocols.
EV1048.001-H1	The manual sharing of encryption keys, allowing adversaries to implement symmetric cryptographic algorithms like RC4 or AES, potentially leading to data compromise during exfiltration.

EV1048.001-H2	The failure to enforce dedicated servers for critical services, such as DNS, which could lead to a broader attack surface, enabling adversaries to exploit additional systems within the network during exfiltration attempts.

2.13.6 Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol (T1048.002) [258]

EV Code	Vulnerability Description
EV1048.002-S1	The reliance on asymmetrically encrypted network protocols, such as HTTPS/TLS/SSL, that may use symmetric encryption once keys are exchanged, providing an opportunity for adversaries to exploit weaknesses in these encryption mechanisms.
EV1048.002-S2	Inadequate implementation of Data Loss Prevention (DLP) solutions, allowing adversaries to bypass detection and blocking mechanisms, especially if DLP is not configured to effectively identify and prevent sensitive data exfiltration.
EV1048.002-S3	Weak network traffic filtering configurations, as adversaries may exploit gaps in proxy enforcement or the use of dedicated servers, potentially allowing unauthorized communication over ports and protocols not explicitly restricted.
EV1048.002-S4	Insufficient deployment of Network Intrusion Prevention Systems (NIPS) that lack updated signatures for identifying adversary command and control infrastructure and malware, leaving the network susceptible to undetected exfiltration attempts.
EV1048.002-S5	Poorly implemented network segmentation, where network firewall configurations do not adhere to best practices, enabling adversaries to move laterally and exfiltrate data between segments more easily.
EV1048.002-H1	The improper management of cryptographic keys, including inadequate protection of private keys and insecure exchange or storage of public keys, which can be exploited by adversaries engaging in exfiltration over alternative protocols.
EV1048.002-H2	Misconfiguration of network firewall rules, permitting unnecessary ports and traffic to enter and exit the network, providing adversaries with potential pathways for exfiltration.

2.13.7 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003) [259]

EV Code	Vulnerability Description
EV1048.003-S1	The lack of encryption in certain network protocols (e.g., HTTP, FTP, DNS), allowing for data exfiltration over unencrypted channels, potentially exposing sensitive information during transit.
EV1048.003-S2	The absence of effective data loss prevention measures, allowing sensitive data to be exfiltrated over unencrypted protocols; this weakness could be exploited due to inadequate detection and blocking mechanisms.
EV1048.003-H1	The failure to implement encryption for data exfiltration, enabling adversaries to easily intercept and access the transmitted information over alternative unencrypted protocols.
EV1048.003-H2	The misconfiguration or lack of enforcement of network traffic filtering rules, potentially permitting unauthorized communication over unnecessary ports/protocols and increasing the risk of data exfiltration over unencrypted channels.

2.13.8 Exfiltration Over C2 Channel (T1041) [260]

EV Code	Vulnerability Description
EV1041-S1	The lack of robustness in the command and control (C2) channel, which may enable the exfiltration of encoded stolen data due to inadequate security measures.
EV1041-S2	The weakness in data loss prevention mechanisms, as adversaries may find ways to evade or bypass these systems to exfiltrate sensitive data over unencrypted protocols.
EV1041-H1	The reliance on network signatures in network intrusion prevention systems, which may be circumvented if adversaries alter their malware or use different obfuscation techniques, leading to potential detection evasion.

2.13.9 Exfiltration Over Other Network Medium (T1011) **[261]**

EV Code	Vulnerability Description
EV1011-S1	The susceptibility of the alternative network medium (e.g., WiFi, modem, cellular data, Bluetooth) to unauthorized data exfiltration due to potential lack of security measures compared to the primary Internet-connected channel.
EV1011-S2	The risk of data exfiltration through newly created network adapters that may not be properly secured, emphasizing the importance of preventing the creation of such adapters, as suggested in the operating system configuration mitigation strategy.
EV1011-H1	Failure to implement the recommended security measures, such as disabling WiFi connections, modems, cellular data connections, Bluetooth, or other RF channels, either due to lack of awareness or oversight, allowing adversaries to exploit these active features for data exfiltration.
EV1011-H2	Neglecting to configure the operating system to prevent the creation of new network adapters, possibly due to lack of understanding or oversight, exposing the system to potential exploitation by adversaries seeking to use these adapters for data exfiltration.

2.13.10 Exfiltration Over Other Network Medium: Exfiltration Over Bluetooth (T1011.001) **[262]**

EV Code	Vulnerability Description
EV1011.001-S1	The lack of robust security measures for Bluetooth connections, which may not be as well-defended as the primary Internet-connected channel, posing a risk for data exfiltration.
EV1011.001-H1	The failure to disable Bluetooth in local computer security settings or through group policy when it is not needed within an environment.
EV1011.001-H2	The failure to prevent the creation of new network adapters where possible, which could undermine efforts to secure the system against Bluetooth exfiltration.

2.13.11 Exfiltration Over Physical Medium (T1052) **[263]**

EV Code	Vulnerability Description
EV1052-S1	The susceptibility of the air-gapped network to compromise, allowing exfiltration via a physical medium introduced by a user.
EV1052-S2	The potential failure or misconfiguration of Data Loss Prevention (DLP) systems, which may result in an inability to detect or block sensitive data exfiltration via physical mediums.
EV1052-H1	The introduction of a physical medium, such as a removable drive, USB drive, or other storage device, potentially facilitating data exfiltration in air-gapped network compromise scenarios.
EV1052-H2	The failure to disable or restrict Autorun when unnecessary, or neglecting to enforce organizational policies that disallow or restrict the use of removable media, which could undermine the effectiveness of mitigation strategies and allow unauthorized data transfers.

2.13.12 Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001) **[264]**

EV Code	Vulnerability Description
EV1052.001-S1	The susceptibility of air-gapped networks to compromise, allowing for exfiltration over a USB-connected physical device.
EV1052.001-S2	The inadequacy of data loss prevention mechanisms, allowing sensitive data to be copied to USB devices.
EV1052.001-H1	The introduction of a USB device into the secure environment, potentially facilitating data exfiltration or enabling lateral movement between disconnected systems.
EV1052.001-H2	The failure to disable or restrict unnecessary features such as Autorun, potentially leaving a pathway for adversaries to exploit USB-connected devices for exfiltration.
EV1052.001-H3	The failure to enforce organizational policies limiting the use of USB devices and removable media, increasing the risk of unauthorized data exfiltration.

2.13.13 Exfiltration Over Web Service (T1567) [265]

EV Code	Vulnerability Description
EV1567-S1	The lack of restrictions or monitoring on legitimate external Web services, allowing adversaries to leverage pre-existing communication channels for data exfiltration.
EV1567-H1	The potential failure to implement or enforce robust firewall rules, thereby permitting unauthorized traffic to external Web services, providing adversaries with a cover for exfiltration.
EV1567-H2	The potential failure to adequately monitor and inspect SSL/TLS-encrypted traffic, which may provide adversaries with an additional layer of protection during data exfiltration over Web services.
EV1567-H3	The potential failure to configure web proxies properly, allowing adversaries to circumvent restrictions on external services and facilitating data exfiltration.

2.13.14 Exfiltration Over Web Service: Exfiltration to Code Repository (T1567.001) [266]

EV Code	Vulnerability Description
EV1567.001-S1	The potential weakness in the security of code repositories accessed via APIs, such as inadequate access controls or misconfigurations, which could allow unauthorized exfiltration over HTTPS.
EV1567.001-S2	The potential inadequacy or misconfiguration of web proxies, which, if not properly implemented or monitored, may fail to effectively restrict web-based content and prevent unauthorized external services, leaving avenues for exfiltration to code repositories.
EV1567.001-H1	The inadvertent exposure of sensitive data to a code repository, potentially due to misjudgment or lack of awareness, enabling adversaries to exploit the repository's accessibility via APIs for exfiltration.

EV1567.001-H2	The failure to configure or monitor web proxies correctly, possibly due to oversight or lack of expertise, leading to the ineffective enforcement of external network communication policies and allowing adversaries to exploit unauthorized external services for exfiltration.

2.13.15 Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) **[267]**

EV Code	Vulnerability Description
EV1567.002-S1	The potential lack of effective controls or monitoring mechanisms to detect and prevent data exfiltration to cloud storage services, allowing adversaries to exploit this weakness for covert data transfer.
EV1567.002-S2	The potential absence or inadequacy of web proxies, allowing unauthorized external services and increasing the risk of data exfiltration to cloud storage services due to the lack of enforced network communication policies.

2.13.16 Exfiltration Over Web Service: Exfiltration to Text Storage Sites (T1567.003) **[268]**

EV Code	Vulnerability Description
EV1567.003-S1	The weaknesses in the system's ability to detect and prevent data exfiltration over web services, specifically to text storage sites like pastebin[.]com.
EV1567.003-H1	The inadvertent exposure of sensitive data due to human error, as adversaries may exploit users' lack of awareness or mistakes when handling data, allowing unauthorized exfiltration to text storage sites.
EV1567.003-H2	The failure to properly configure or update web proxies, leading to a weakened external network communication policy and potential exploitation by adversaries for unauthorized data exfiltration.

2.13.17 Exfiltration Over Web Service: Exfiltration Over Webhook (T1567.004) **[269]**

EV Code	Vulnerability Description
EV1567.004-S1	The weaknesses in the authentication and access control mechanisms of webhook endpoints, especially if they are not properly configured or secured.
EV1567.004-H1	The inadvertent linkage of an adversary-owned environment to a victim-owned SaaS service, enabling repeated automated exfiltration of sensitive data through webhooks without the user's awareness.
EV1567.004-H2	The failure to implement or configure data loss prevention tools properly, resulting in the inability to detect and block sensitive data uploaded to web services via web browsers.

2.13.18 Scheduled Transfer (T1029) **[524]**

EV Code	Vulnerability Description
EV1029-S1	The lack of restrictions or monitoring mechanisms in place, allowing scheduled data exfiltration to blend with normal activity or availability, potentially evading detection.
EV1029-S2	The potential inability of network intrusion detection and prevention systems to effectively identify and mitigate scheduled data exfiltration, especially when adversaries alter command and control signatures over time or employ obfuscation techniques to evade detection.
EV1029-H1	The failure to timely update network intrusion detection and prevention systems with new signatures, potentially leaving the system exposed to evolving adversary tactics and techniques.

2.13.19 Transfer Data to Cloud Account (T1537) [613]

EV Code	Vulnerability Description
EV1537-S1	The lack of monitoring for data transfers between cloud accounts within the same cloud provider, allowing exfiltration to occur undetected through existing cloud provider APIs and internal address space.
EV1537-S2	The absence of network-based filtering restrictions, allowing data transfers to untrusted Virtual Private Clouds (VPCs).
EV1537-H1	The failure to watch for data transfers to another account within the same cloud provider, as defenders may focus on monitoring external transfers and overlook internal transfers.
EV1537-H2	The failure to implement robust password policies, including regular access key rotation, increasing the risk of compromised credentials being effectively used by adversaries.
EV1537-H3	The inadequate limitation of user account and Identity and Access Management (IAM) policies, potentially granting excessive privileges that could facilitate unauthorized data transfers.
EV1537-H4	The lack of utilization of temporary credentials with limited validity periods, increasing the risk of compromised accounts being exploited by adversaries over an extended timeframe.

2.14 Impact (TA0040) [17]

2.14.1 Account Access Removal (T1531) [42]

EV Code	Vulnerability Description
EV1531-H1	The failure to implement strong access controls, allowing adversaries to exploit utilities like Net, Set-LocalUser, and Set-ADAccountPassword PowerShell cmdlets in Windows or the passwd utility in Linux to modify user accounts and compromise system security.

2.14.2 Data Destruction (T1485) [167]

EV Code	Vulnerability Description
EV1485-H1	The potential weakness in IT disaster recovery plans, as they may lack robust procedures for regular data backups, leaving the organization susceptible to data loss.

2.14.3 Data Encrypted for Impact (T1486) [171]

EV Code	Vulnerability Description
EV1486-S1	The potential weakness in the configuration of Windows 10, where the absence of enabled cloud-delivered protection and Attack Surface Reduction (ASR) rules may allow the execution of files resembling ransomware.
EV1486-H1	The failure to implement effective IT disaster recovery plans and regular data backups, exposing the organization to data loss and making it susceptible to ransomware attacks.

2.14.4 Data Manipulation (T1565) [183]

EV Code	Vulnerability Description
EV1565-S1	The potential exposure of sensitive information due to inadequate encryption, allowing adversaries to perform tailored data modifications.
EV1565-S2	The lack of proper segmentation, enabling adversaries to access and tamper with critical business and system processes.
EV1565-S3	Inadequate enforcement of least privilege principles on important information resources, exposing them to the risk of data manipulation.
EV1565-H1	The absence of secure IT disaster recovery plans, leading to vulnerabilities in data backups that adversaries may exploit to gain access and manipulate backups.

2.14.5 Data Manipulation: Stored Data Manipulation (T1565.001) [184]

EV Code	Vulnerability Description
EV1565.001-S1	The potential exposure of sensitive information due to inadequate encryption, allowing adversaries to perform tailored data modifications.
EV1565.001-S2	Inadequate enforcement of least privilege principles on important information resources, exposing them to the risk of data manipulation.
EV1565.001-H1	The absence of secure IT disaster recovery plans, leading to vulnerabilities in data backups that adversaries may exploit to gain access and manipulate backups.

2.14.6 Data Manipulation: Transmitted Data Manipulation (T1565.002) [185]

EV Code	Vulnerability Description
EV1565.002-S1	The potential exposure of sensitive information due to inadequate encryption, allowing adversaries to perform tailored data modifications.

2.14.7 Data Manipulation: Runtime Data Manipulation (T1565.003) [186]

EV Code	Vulnerability Description
EV1565.003-S1	The susceptibility of application binaries used to display data, allowing adversaries to manipulate runtime data and compromise data integrity.
EV1565.003-S2	The lack of proper segmentation, enabling adversaries to access and tamper with critical business and system processes.
EV1565.003-H1	The potential failure to restrict file and directory permissions adequately, which could lead to critical processes being replaced, overwritten, or reconfigured to load potentially malicious code.

2.14.8 Defacement (T1491) [196]

EV Code	Vulnerability Description
EV1491-H1	The failure to implement regular data backup procedures and IT disaster recovery plans, leaving the organization susceptible to permanent data loss in the event of a defacement attack.

2.14.9 Defacement: Internal Defacement (T1491.001) [197]

EV Code	Vulnerability Description
EV1491.001-H1	The failure to implement regular data backup procedures and IT disaster recovery plans, leaving the organization susceptible to permanent data loss in the event of a defacement attack.

2.14.10 Defacement: External Defacement (T1491.002) [198]

EV Code	Vulnerability Description
EV1491.002-H1	The failure to implement regular data backup procedures and IT disaster recovery plans, leaving the organization susceptible to permanent data loss in the event of a defacement attack.

2.14.11 Disk Wipe (T1561) [208]

EV Code	Vulnerability Description
EV1561-H1	The absence of robust disaster recovery planning, leaving the organization susceptible to data loss and prolonged downtime in the event of a disk wiping attack.
EV1561-H2	The failure to securely store and protect backup data, as adversaries may exploit inadequate security measures to gain access and destroy backups, hindering the organization's ability to recover from a disk wiping incident.

2.14.12 Disk Wipe: Disk Content Wipe (T1561.001) [209]

EV Code	Vulnerability Description
EV1561.001-H1	The absence of robust disaster recovery planning, leaving the organization susceptible to data loss and prolonged downtime in the event of a disk wiping attack.
EV1561.001-H2	The failure to securely store and protect backup data, as adversaries may exploit inadequate security measures to gain access and destroy backups, hindering the organization's ability to recover from a disk wiping incident.

2.14.13 Disk Wipe: Disk Structure Wipe (T1561.002) [210]

EV Code	Vulnerability Description
EV1561.002-H1	The absence of robust disaster recovery planning, leaving the organization susceptible to data loss and prolonged downtime in the event of a disk wiping attack.
EV1561.002-H2	The failure to securely store and protect backup data, as adversaries may exploit inadequate security measures to gain access and destroy backups, hindering the organization's ability to recover from a disk wiping incident.

2.14.14 Endpoint Denial of Service (T1499) [227]

EV Code	Vulnerability Description
EV1499-S1	The difficulty in distinguishing Distributed Denial of Service (DDoS) traffic from legitimate clients due to the overwhelming volume generated by large botnets, making defense challenging.
EV1499-H1	The inadvertent misconfiguration of Content Delivery Networks (CDN) or DoS mitigation services, potentially leading to inadequate filtering of malicious traffic and reduced effectiveness in defending against DoS attacks.

2.14.15 Endpoint Denial of Service: OS Exhaustion Flood (T1499.001) **[228]**

EV Code	Vulnerability Description
EV1499.001-S1	The finite capacity of the operating system to manage resources, which can be exploited through techniques like SYN floods and ACK floods, leading to a denial of service.
EV1499.001-H1	The potential for misconfigurations in the operating system, such as allowing excessive concurrent TCP connections, which can exacerbate the impact of OS exhaustion attacks.
EV1499.001-H2	The failure to adequately configure and enable SYN Cookies, leaving the system susceptible to SYN flood attacks due to the absence of this protective measure.

2.14.16 Endpoint Denial of Service: Service Exhaustion Flood (T1499.002) **[229]**

EV Code	Vulnerability Description
EV1499.002-S1	The potential lack of effective network traffic filtering mechanisms, which could result in an inability to adequately mitigate a Service Exhaustion Flood attack by leveraging services provided by Content Delivery Networks (CDN) or specialized DoS mitigation providers.
EV1499.002-H1	User enables SSL renegotiation without proper consideration, allowing adversaries to exploit the protocol feature in SSL/TLS and impact the availability of the service through a renegotiation attack.
EV1499.002-H2	Misconfiguring or failing to implement proper filtering rules, such as not effectively blocking source addresses, targeted ports, or protocols during mitigation efforts, potentially leaving the system exposed to continued or renewed Service Exhaustion Flood attacks.

2.14.17 Endpoint Denial of Service: Application Exhaustion Flood (T1499.003) **[230]**

EV Code	Vulnerability Description
EV1499.003-S1	The resource-intensive features of applications, particularly those in web applications, which may be exploited to exhaust system resources, leading to a denial of service (DoS) condition.

EV1499.003-H1	The potential lack of effective network traffic filtering mechanisms, leaving the system susceptible to application exhaustion floods and denial of service (DoS) attacks.
EV1499.003-H2	The failure to implement or configure appropriate content delivery network (CDN) services or DoS mitigation providers, which may result in ineffective filtering of network traffic and leave the system exposed to DoS attacks.

2.14.18 Endpoint Denial of Service: Application or System Exploitation (T1499.004) [231]

EV Code	Vulnerability Description
EV1499.004-S1	The potential failure to implement effective network traffic filtering measures, allowing malicious traffic to reach and exploit the targeted applications or systems.
EV1499.004-H1	The failure to promptly patch known vulnerabilities, exposing the system to exploitation by adversaries seeking to crash applications or systems and induce a DoS condition.
EV1499.004-H2	The failure to promptly leverage Content Delivery Networks (CDN) or specialized DoS mitigation providers to filter network traffic upstream, leaving the system exposed to potential DoS attacks by not effectively blocking malicious source addresses, targeted ports, or transport protocols.

2.14.19 Financial Theft (T1657) [282]

EV Code	Vulnerability Description
EV1657-H1	The susceptibility to social engineering tactics, such as impersonation of trusted entities, leading to victims being deceived into sending money to financial accounts controlled by adversaries in incidents like business email compromise or email fraud.
EV1657-H2	The reliance on insecure communication lines for authentication and approval, such as email, making it crucial to switch to more secure systems to prevent unauthorized transactions.

EV1657-H3	Users may contribute to vulnerabilities by not undergoing sufficient training and testing to identify social engineering techniques, leaving them susceptible to tactics that enable financial theft.

2.14.20 Firmware Corruption (T1495) [283]

EV Code	Vulnerability Description
EV1495-S1	The potential for insufficient boot integrity verification, allowing adversaries to manipulate or corrupt the BIOS and device firmware.
EV1495-H1	The inadequate management of privileged accounts, which could lead to unauthorized access and enable adversaries to replace system firmware, emphasizing the importance of effective privileged account management practices.
EV1495-H2	The lack of timely software updates, specifically patching the BIOS and other firmware, leaving the system exposed to known vulnerabilities that could be exploited for firmware corruption.

2.14.21 Inhibit System Recovery (T1490) [362]

EV Code	Vulnerability Description
EV1490-S1	The potential lack of implementation of technical controls to prevent the disabling of services or deletion of files involved in system recovery, allowing adversaries to compromise recovery mechanisms.
EV1490-S2	The absence of IT disaster recovery plans or procedures for regular data backups, leaving the organization without a structured approach to data recovery in the event of a compromise.
EV1490-H1	The failure to implement proper backup policies in cloud environments, including disabling versioning and backup policies and deleting snapshots, machine images, and prior versions of objects crucial for disaster recovery scenarios, providing adversaries the ability to undermine cloud-based recovery mechanisms.
EV1490-H2	The failure to adequately limit access to backup data by not implementing proper user account management, potentially granting unnecessary user accounts access to critical backup information.

EV1490-H3	The oversight in not enabling Windows Recovery Environment (WinRE) using the command "reagentc /enable," potentially leaving the system without a crucial recovery option.

2.14.22 Network Denial of Service (T1498) [410]

EV Code	Vulnerability Description
EV1498-S1	The susceptibility to network flooding due to insufficient capacity or capability to handle a high volume of incoming network traffic, potentially resulting in a denial of service (DoS) situation.
EV1498-H1	The failure to establish a proactive disaster recovery plan or business continuity plan, leaving critical resources at risk of prolonged unavailability during Network Denial of Service (DoS) incidents.

2.14.23 Network Denial of Service: Direct Network Flood (T1498.001) [411]

EV Code	Vulnerability Description
EV1498.001-S1	The susceptibility to network flooding due to insufficient capacity or capability to handle a high volume of incoming network traffic, potentially resulting in a denial of service (DoS) situation.
EV1498.001-H1	The potential for misconfigurations in network security settings, allowing adversaries to exploit weaknesses in protocols like UDP or ICMP, facilitating the success of the direct network flood attack.
EV1498.001-H2	The failure to establish a proactive disaster recovery plan or business continuity plan, leaving critical resources at risk of prolonged unavailability during Network Denial of Service (DoS) incidents.

2.14.24 Network Denial of Service: Reflection Amplification (T1498.002) [412]

EV Code	Vulnerability Description
EV1498.002-S1	The potential for misconfiguring protocols such as DNS and NTP, enabling adversaries to exploit Reflection Amplification attacks and cause a denial of service.

EV1498.002-H1	The failure to establish a proactive disaster recovery plan or business continuity plan, leaving critical resources at risk of prolonged unavailability during Network Denial of Service (DoS) incidents.

2.14.25 Resource Hijacking (T1496) [515]

EV Code	Vulnerability Description
EV1496-S1	The susceptibility of containerized environments, particularly due to exposed APIs, making them easy targets for deployment and scaling of mining activities.
EV1496-H1	The failure to secure containerized environments, allowing adversaries to compromise multiple containers and exploit them for resource hijacking.
EV1496-H2	The inadequate protection of network bandwidth, enabling adversaries to utilize it for botnet-driven Network Denial of Service campaigns or for selling to proxyware services.

2.14.26 Service Stop (T1489) [547]

EV Code	Vulnerability Description
EV1489-S1	The potential for inadequate file and directory permissions, enabling adversaries to disable or interfere with critical services by manipulating processes and files.
EV1489-S2	The potential for inadequate registry permissions, providing adversaries with the ability to disable or interfere with critical services by manipulating the registry.
EV1489-S3	The potential for inadequate user account management, allowing unauthorized users to interact with service changes and configurations, potentially leading to service disruption.

2.14.27 System Shutdown/Reboot (T1529) [606]

EV Code	Vulnerability Description
EV1529-S1	The susceptibility to unauthorized shutdowns or reboots, which can be initiated through commands in the operating system or Network Device CLI.

3 Mobile Device Vulnerability [3]

3.1 Initial Access (TA0027) [18]

3.1.1 Application Versioning (T1661) [662]

MV Code	Vulnerability Description
MV1661-H1	Inadequate enterprise policies, as enterprises may not have effective provisions in place for application allow-listing on mobile devices, leaving room for the installation of unapproved applications.
MV1661-H2	The failure to use a recent OS version, as users neglecting to upgrade to Android 11 and above may miss out on security features like application hibernation, leaving their devices susceptible to unauthorized application activities.

3.1.2 Drive-By-Compromise (T1456) [680]

MV Code	Vulnerability Description
MV1456-H1	User enables scripting or active website components and ignoring warning dialog boxes, which assists adversaries in searching for and exploiting potentially vulnerable versions of browsers and plugins.
MV1456-H2	The lack of timely application of security updates

3.1.3 Lockscreen Bypass (T1461) [722]

MV Code	Vulnerability Description
MV1461-S1	The exploitability of vulnerabilities periodically demonstrated on mobile devices, allowing adversaries to bypass the lockscreen; however, these vulnerabilities are generally patched by the device or OS vendor once disclosed.
MV1461-H1	The weak lockscreen passcodes (PIN or password), contributing to the risk of successful brute-force attacks or password guessing by adversaries.
MV1461-H2	User does not regularly update the mobile device, leaving it exposed to known vulnerabilities that could be exploited to bypass the lockscreen.
MV1461-H3	The risk of not consistently implementing or enforcing enterprise policies to wipe all data after too many incorrect passcode attempts, potentially leading to data compromise.
MV1461-H4	The possibility of neglecting to install OS security updates promptly, creating a window of exposure to known vulnerabilities that could be exploited by adversaries.

3.1.4 Phishing (T1660) [733]

MV Code	Vulnerability Description
MV1660-S1	The susceptibility of mobile devices, which, due to their smaller form factor, may make it challenging for users to discern differences between genuine and phishing websites.
MV1660-S2	The reliance on mobile security products with loopback VPNs, as these may not be foolproof in proactively blocking all traffic to phishing websites, potentially allowing some malicious activity to go undetected.
MV1660-H1	The potential to overlook minor differences between legitimate and malicious emails, as adversaries employ social engineering techniques while posing as trusted sources, contributing to successful phishing attempts.

MV1660-H2	User is falling victim to social engineering techniques, such as responding to SMS messages (smishing), interacting with QR codes (quishing), or succumbing to phone calls (vishing), potentially leading to actions like installing malware, visiting malicious websites, or enabling insecure configurations.
MV1660-H3	User overlooks or ignores the warnings from mobile security products with loopback VPNs, assuming a false sense of security, which could lead to engaging with phishing websites or content.
MV1660-H4	User does not undergo or participate in adequate training to identify and recognize social engineering techniques, which could result in a lack of awareness and an increased susceptibility to phishing attacks.

3.1.5 Replication Through Removable Media (T1458) [744]

MV Code	Vulnerability Description
MV1458-S1	Insecure bootloaders in Nexus 6 or 6P devices over USB, allowing actions such as intercepting phone calls, intercepting network traffic, and obtaining the device's physical location.
MV1458-S2	Weakly-enforced security boundaries in Android devices, exemplified by the Google Pixel 2, over USB.
MV1458-S3	The lack of bootloader lock, allowing arbitrary operating system code to be flashed onto the device
MV1458-H1	The failure to apply security updates
MV1458-H2	The use of outdated operating systems that lack USB Restricted Mode, as introduced in iOS 11.4.1
MV1458-H3	The use of public charging stations or computers to charge devices, creating a risk that can be mitigated by user guidance advising against this practice and recommending the use of chargers from trustworthy sources.

3.1.6 Supply Chain Compromise (T1474) [755]

MV Code	Vulnerability Description
MV1474-S1	The reliance on insecure third-party libraries by application developers, increasing the risk of supply chain compromise due to inadequate scrutiny during the integration process.
MV1474-H1	The inadvertent acceptance and distribution of manipulated or counterfeit products, including sales of modified items to legitimate distributors, contributing to the supply chain compromise.
MV1474-H2	The failure to promptly apply security updates, leaving devices susceptible to exploitation if compromised at the supply chain level, as security patches may not be implemented in a timely manner.

3.1.7 Supply Chain Compromise: Compromise Software Dependencies and Development Tools (T1474.001) [756]

MV Code	Vulnerability Description
MV1474.001-S1	The potential compromise of applications relying on external software dependencies, particularly open source projects, allowing for the introduction of malicious code into the users' systems.

3.1.8 Supply Chain Compromise: Compromise Hardware Supply Chain (T1474.002) [757]

MV Code	Vulnerability Description
MV1474.002-S1	The potential manipulation of hardware or firmware components in the supply chain, allowing the insertion of undetected backdoors into consumer networks.
MV1474.002-S2	The potential weakness in the integrity checking mechanisms, as security updates may not always be promptly applied, leaving systems exposed to unauthorized hardware modifications.

3.1.9 Supply Chain Compromise: Compromise Software Supply Chain (T1474.003) [758]

MV Code	Vulnerability Description
MV1474.003-S1	The susceptibility of the application source code to manipulation, allowing for unauthorized alterations that could compromise data or system integrity.
MV1474.003-S2	The potential lack of enabling Verified Boot on devices capable of it, which could compromise the integrity of the system partition
MV1474.003-H1	The potential failure to adequately verify the authenticity of received software updates, creating an opportunity for adversaries to compromise the software supply chain by manipulating the update/distribution mechanism or replacing compiled releases with a modified version.
MV1474.003-H2	The failure to promptly apply security updates, potentially leaving the system susceptible to compromises that the updates aim to patch

3.2 Execution (TA0041) [19]

3.2.1 Command and Scripting Interpreter (T1623) [668]

MV Code	Vulnerability Description
MV1623-S1	Insecure default configurations or inadequate access controls within command and script interpreters, allowing unauthorized execution of commands or scripts.
MV1623-S2	The potential failure of device attestation mechanisms to effectively detect jailbroken or rooted devices, allowing malicious actors to operate undetected.
MV1623-S3	The potential ineffectiveness of mobile security products in detecting compromised devices, which could result in a failure to identify and respond to unauthorized access.
MV1623-H1	The inadvertent execution of malicious commands or scripts through interactive terminals/shells, potentially facilitated by opening lure documents or downloading secondary payloads from a Command and Control (C2) infrastructure.

3.2.2 Command and Scripting Interpreter: Unix Shell (T1623.001) [669]

MV Code	Vulnerability Description
MV1623.001-S1	The potential failure of device attestation, allowing jailbroken or rooted devices to go undetected and potentially be exploited.
MV1623.001-H1	The inadvertent execution of malicious commands or payloads due to the misuse or compromise of Unix shells, particularly if the device has been rooted or jailbroken.
MV1623.001-H2	The failure to deploy or configure compromised device detection methods, leaving the system susceptible to unauthorized access through jailbroken or rooted devices.

3.2.3 Exploitation for Client Execution (T1658) [694]

MV Code	Vulnerability Description
MV1658-S1	An insecure coding practices in client applications, leading to exploitable software vulnerabilities that may result in arbitrary code execution.
MV1658-S2	A buffer overflow in the Apple Wireless Direct Link (AWDL) interface on iOS 13.4 and earlier, allowing unauthorized access to the device and execution of code as root without user interaction.
MV1658-S3	The absence of timely security updates, as users might not apply patches promptly, leaving the system exposed to known vulnerabilities.
MV1658-H1	The potential for opening iMessages from unknown senders, as users might inadvertently engage with malicious content, posing a risk to the system's security.
MV1658-H2	The risk of users opening unrecognized links or attachments in text messages, which can be exploited by adversaries to deliver malicious payloads or initiate attacks on the system.

3.2.4 Native API (T1575) [725]

MV Code	Vulnerability Description
MV1575-S1	The potential exploitation of weaknesses in Android's Native Development Kit (NDK), allowing them to write native code in C or C++ that bypasses higher-level language safeguards, making it harder to analyze and detect malicious behavior.
MV1575-H1	The potential misuse of the Java Native Interface (JNI) by developers, allowing Java functions in Android apps to call functions in a native library, which could inadvertently execute malicious code if not properly secured.

3.2.5 Scheduled Task/Job (T1603) [745]

MV Code	Vulnerability Description
MV1603-S1	The flexibility of APIs like WorkManager on Android and NSBackgroundActivityScheduler on iOS, which can lead to unauthorized execution of malicious code.
MV1603-H1	The potential misconfiguration or misuse of task scheduling parameters, such as specifying insecure intervals or failing to adequately constrain tasks, allowing adversaries to exploit these missteps for unauthorized code execution.

3.3 Persistence (TA0028) [20]

3.3.1 Boot or Logon Initialization Scripts (T1398) [665]

MV Code	Vulnerability Description
MV1398-S1	The potential weakness in the initialization script execution process, allowing unauthorized scripts to be automatically executed at boot or logon, leading to persistence.
MV1398-S2	The lack of device attestation, which could result in the failure to detect devices with unauthorized or unsafe modifications, allowing persistence.

MV1398-S3	The potential for an unlocked bootloader, enabling unauthorized modifications to protected operating system files and compromising system integrity.
MV1398-S4	The lack of system partition integrity mechanisms on certain systems, which could lead to an inability to detect unauthorized modifications and ensure the integrity of the operating system.
MV1398-H1	The absence of timely security updates, leaving the system exposed to known vulnerabilities that could be leveraged for unauthorized modifications to protected operating system files.

3.3.2 Compromise Application Executable (T1577) **[670]**

MV Code	Vulnerability Description
MV1577-S1	Device vulnerabilities, exemplified by the Android Janus vulnerability, allowing the addition of extra bytes to APK and DEX files without affecting the file's signature, enabling seamless injection of malicious code into legitimate executables.
MV1577-S2	Vulnerabilities allowing malicious activities to run inside a system application
MV1577-H1	Human actions, such as the decompilation, merging with malicious code, and recompilation of genuine applications, thereby facilitating the rebuilding of applications with concealed malicious modifications.
MV1577-H2	The lack of timely application of security updates
MV1577-H3	The usage of outdated operating systems

3.3.3 Compromise Client Software Binary (T1645) **[671]**

MV Code	Vulnerability Description
MV1645-S1	Insufficient device attestation, allowing for the detection of devices with unauthorized or unsafe modifications to be bypassed.

MV1645-S2	An unlocked bootloader, which could lead to unauthorized modifications of protected operating system files, circumventing the security measure of a locked bootloader.
MV1645-S3	The potential for compromised system partition integrity mechanisms, which, if bypassed, could fail to detect unauthorized modifications to the Android system partition.
MV1645-H1	The inadvertent execution of malicious binaries, as users may unknowingly trigger pre-compiled malicious binaries during routine interactions with the system, facilitating persistent access for the adversary.
MV1645-H2	The absence of timely updates may leave the system exposed to vulnerabilities that could be leveraged to modify protected operating system files.

3.3.4 Event Triggered Execution (T1624) [687]

MV Code	Vulnerability Description
MV1624-H1	The inadvertent creation or modification of event triggers by users, providing an avenue for adversaries to point to malicious content, leading to unauthorized execution upon the occurrence of specified events.
MV1624-H2	The failure of users to update their Android OS to version 8 or later, leaving their devices susceptible to the implicit intent-related vulnerabilities present in earlier OS versions.

3.3.5 Event Triggered Execution: Broadcast Receivers (T1624.001) [688]

MV Code	Vulnerability Description
MV1624.001-H1	User installs malicious applications that register for sensitive broadcast intents, enabling adversaries to manipulate the device and perform malicious actions based on system events.
MV1624.001-H2	The failure of users to update their Android OS to version 8 or later, leaving their devices susceptible to the implicit intent-related vulnerabilities present in earlier OS versions.

3.3.6 Foreground Persistence (T1541) [698]

MV Code	Vulnerability Description
MV1541-S1	The potential abuse of Android's startForeground() API method, allowing malicious applications to gain unhindered access to device sensors, such as the camera, microphone, and gyroscope, by running in the foreground with a fake notification.
MV1541-H1	User does not uninstall a source application with an unrecognized persistent notification, creating a risk of maintaining access for malicious applications and allowing continued abuse of sensor privileges.

3.3.7 Hijack Execution Flow (T1625) [703]

MV Code	Vulnerability Description
MV1625-S1	The lack of device attestation, allowing unauthorized operating system modifications that could lead to execution flow hijacking, unless detected by attestation mechanisms.
MV1625-H1	The inadvertent inclusion of malicious payloads in file directories or locations where the operating system looks for programs or resources, enabling the adversary to exploit this human mistake for hijacking execution flow.
MV1625-H2	Inadequate implementation of system partition integrity checks, as the absence of measures like Android Verified Boot could allow unauthorized modifications to the system partition, potentially leading to the hijacking of execution flow.
MV1625-H3	The omission or misconfiguration of device attestation, leading to a failure in detecting unauthorized operating system modifications and providing adversaries with opportunities to hijack execution flow without being detected.

3.3.8 *Hijack Execution Flow: System Runtime API Hijacking (T1625.001)* [704]

MV Code	Vulnerability Description
MV1625.001-S1	The susceptibility of the operating system to API library overwrites, allowing adversaries to hijack execution flow and achieve persistence through malicious alternatives.
MV1625.001-S2	The weakness in device attestation, as the failure to implement or properly configure attestation mechanisms may allow adversaries to go undetected despite unauthorized operating system modifications.
MV1625.001-S3	The susceptibility of Android Verified Boot to evasion or compromise, as adversaries may exploit weaknesses in the verification process, allowing unauthorized modifications to the system partition and facilitating execution flow hijacking.
MV1625.001-H1	The failure to adequately protect against unauthorized API library modifications on Android, enabling adversaries to overwrite the standard OS API library with a malicious alternative and compromise core functions for persistent execution.
MV1625.001-H2	The omission or misconfiguration of device attestation, leading to a failure in detecting unauthorized operating system modifications and providing adversaries with opportunities to hijack execution flow without being detected.
MV1625.001-H3	The inadequate implementation or misconfiguration of Android Verified Boot, enabling adversaries to potentially evade detection by exploiting weaknesses in the verification process and facilitating unauthorized modifications to the system partition, ultimately leading to execution flow hijacking.

3.3.9 *Scheduled Task/Job (T1603)* [745]

MV Code	Vulnerability Description
MV1603-S1	The flexibility of APIs like WorkManager on Android and NSBackgroundActivityScheduler on iOS, which can lead to unauthorized execution of malicious code.

MV1603-H1	The potential misconfiguration or misuse of task scheduling parameters, such as specifying insecure intervals or failing to adequately constrain tasks, allowing adversaries to exploit these missteps for unauthorized code execution.

3.4 Privilege Escalation (TA0029) [21]

3.4.1 Abuse Elevation Control Mechanism (T1626) [655]

MV Code	Vulnerability Description
MV1626-S1	The potential weakness in native elevation control mechanisms, allowing for unauthorized escalation of privileges on the system.
MV1626-H1	Inadequate authorization management, which may grant excessive privileges to certain users, providing an opportunity for privilege escalation by adversaries.
MV1626-H2	The potential oversight by developers in not adhering to guidance, allowing applications to unnecessarily request administrator permissions, increasing the risk of being perceived as potentially malicious.

3.4.2 Abuse Elevation Control Mechanism: Device Administrator Permissions (T1626.001) [656]

MV Code	Vulnerability Description
MV1626.001-S1	The potential abuse of Android's device administration API, allowing unauthorized elevation of control over the device.
MV1626.001-H1	The approval of device administrators at runtime without proper scrutiny, enabling adversaries to gain elevated privileges.
MV1626.001-H2	User uses outdated Android operating systems (OS) versions, as changes introduced in Android 7 aimed at mitigating abuse of device administrator permissions may not be present, exposing devices to exploitation.

3.4.3 Exploitation for Privilege Escalation (T1404) [695]

MV Code	Vulnerability Description
MV1404-S1	Software vulnerabilities within the operating system software or kernel, allowing the execution of adversary-controlled code for privilege escalation.
MV1404-S2	The potential for compromised devices, such as jailbroken or rooted devices, which can be detected through attestation methods, but this may not be foolproof.
MV1404-H1	The potential existence of programming errors in applications or services, particularly within operating system components and applications running at higher permissions, that can be exploited by adversaries to gain higher levels of access on the system.
MV1404-H2	The potential failure to deploy effective compromised device detection methods, relying on mobile security products, which may have limitations in detecting jailbroken or rooted devices.
MV1404-H3	The delay or failure in applying security updates, as security updates often contain crucial patches for vulnerabilities, leaving systems exposed to known exploits.

3.4.4 Process Injection (T1631) [735]

MV Code	Vulnerability Description
MV1631-S1	The lack of inherent mechanisms in both Android and iOS to prevent process injection, allowing adversaries to abuse existing root access or exploit vulnerabilities for unauthorized code execution.

3.4.5 Process Injection: Ptrace System Calls (T1631.001) [736]

MV Code	Vulnerability Description
MV1631.001-S1	The vulnerability in the ptrace system call, which allows adversaries to inject malicious code into processes and execute arbitrary actions in the context of another process, potentially gaining unauthorized access, manipulating memory, and evading detection from security products.
MV1631.001-H1	The improper handling of process memory, such as writing arbitrary code into a running process using malloc, and invoking that memory with PTRACE_SETREGS, which can lead to the execution of unauthorized instructions and compromise the integrity of the targeted system.

3.5 Defense Evasion (TA0030) [22]

3.5.1 Application Versioning (T1661) [662]

MV Code	Vulnerability Description
MV1661-H1	Inadequate enterprise policies, as enterprises may not have effective provisions in place for application allow-listing on mobile devices, leaving room for the installation of unapproved applications.
MV1661-H2	The failure to use a recent OS version, as users neglecting to upgrade to Android 11 and above may miss out on security features like application hibernation, leaving their devices susceptible to unauthorized application activities.

3.5.2 Download New Code at Runtime (T1407) [679]

MV Code	Vulnerability Description
MV1407-H1	The inadvertent allowance of dynamic code execution, particularly on Android, where native code, Dalvik code, or JavaScript code utilizing Android WebView's JavascriptInterface capability may be downloaded and executed, posing a risk to the system.

MV1407-H2	The potential introduction of security risks in iOS by downloading and executing dynamic code through third-party libraries such as JSPatch, thereby compromising the system's integrity.
MV1407-H3	The risk of using Android devices with operating system versions lower than API level 29, as such devices lack the protective measure against the execution of native code stored in the application's internal data storage directory, potentially facilitating the download and execution of malicious dynamic code.

3.5.3 Execution Guardrails (T1627) [689]

MV Code	Vulnerability Description
MV1627-H1	The failure to adequately configure and provide environment-specific guardrail information, leading to the potential compromise of systems not intended to be targeted, thus undermining the effectiveness of guardrails.
MV1627-H2	The use of outdated operating systems, which may lack the additional limitations or controls introduced in recent OS versions to enhance device location access security.
MV1627-H3	User overlooks or approves permission requests from applications without proper scrutiny, particularly those requesting location or sensitive phone information, undermining the effectiveness of guardrails and exposing the system to unauthorized access.

3.5.4 Execution Guardrails: Geofencing (T1627.001) [690]

MV Code	Vulnerability Description
MV1627.001-H1	The granting of unnecessary permissions, such as ACCESS_FINE_LOCATION and ACCESS_BACKGROUND_LOCATION on Android, which may be exploited by adversaries to implement geofencing and perform location-based malicious activities without the user's awareness or consent.

MV1627.001-H2	The reliance on users to update their operating systems, as not using the latest OS version may expose devices to potential limitations or controls that could be exploited by adversaries.

3.5.5 Foreground Persistence (T1541) [698]

MV Code	Vulnerability Description
MV1541-S1	The potential abuse of Android's startForeground() API method, allowing malicious applications to gain unhindered access to device sensors, such as the camera, microphone, and gyroscope, by running in the foreground with a fake notification.
MV1541-H1	User does not uninstall a source application with an unrecognized persistent notification, creating a risk of maintaining access for malicious applications and allowing continued abuse of sensor privileges.

3.5.6 Hide Artifacts (T1628) [700]

MV Code	Vulnerability Description
MV1628-S1	The legitimate APIs and features in mobile operating systems to hide application artifacts, unintentionally aiding adversaries in evading detection.

3.5.7 Hide Artifacts: Suppress Application Icon (T1628.001) [701]

MV Code	Vulnerability Description
MV1628.001-S1	The legitimate APIs and features in mobile operating systems to hide application artifacts, unintentionally aiding adversaries in evading detection.
MV1628.001-H1	The failure to detect and remove malicious applications that have suppressed their icons, potentially allowing them to persist on the device unnoticed.

3.5.8 Hide Artifacts: User Evasion (T1628.002) [702]

MV Code	Vulnerability Description
MV1628.002-S1	The lack of controls preventing unauthorized access to device sensors, allowing malicious applications to use motion sensors like accelerometer or gyroscope to detect user interactions and evade detection without requiring user permissions.
MV1628.002-H1	User grants unnecessary permissions to applications, as the adversary can exploit the transparent access to motion sensors without explicit user consent, enabling the hiding of malicious activity on the device.
MV1628.002-H2	The failure to deploy or properly configure mobile security products, such as Samsung Knox for Mobile Threat Defense, which could leave the device susceptible to undetected malicious applications that exploit the idle state, highlighting the importance of proactive security measures.

3.5.9 Hooking (T1617) [705]

MV Code	Vulnerability Description
MV1617-S1	The susceptibility to hooking techniques, which allows the modification of return values or data structures of system APIs and function calls through the use of 3rd party root frameworks, such as Xposed or Magisk, potentially leading to evasion of detection and manipulation of system functionality.
MV1617-S2	The potential inadequacy of device attestation methods, which may fail to effectively detect rooted devices, leaving a gap in the defense against hooking techniques.
MV1617-H1	Unintentional installation or misuse of 3rd party root frameworks like Xposed or Magisk, providing adversaries with the opportunity to exploit system APIs and compromise system integrity.
MV1617-H2	The failure to deploy or configure compromised device detection methods, such as mobile security products, which could result in the oversight of rooted devices and compromise the effectiveness of mitigation strategies.

3.5.10 Impair Defenses (T1629) [706]

MV Code	Vulnerability Description
MV1629-S1	Lack of a compromised device detection method, allowing adversaries to exploit rooted or jailbroken devices that may compromise defenses.
MV1629-S2	Lack of system partition integrity mechanisms, such as Verified Boot, which could allow unauthorized modification of system files, impacting defenses.
MV1629-H1	Configuration mistakes or oversights that could allow adversaries to modify or disable defensive mechanisms, compromising the effectiveness of security tools.
MV1629-H2	Inadequate enterprise policy implementation, specifically in using Android's accessibility features, which could be exploited to impair defenses.
MV1629-H3	Insufficient user awareness and education regarding the modal requests for administrator permissions, potentially leading to unwittingly allowing malicious actions that impair defenses.
MV1629-H4	Delayed or neglected application of security updates, leaving the system exposed to vulnerabilities that could be exploited for root access and impairing defenses.

3.5.11 Impair Defenses: Prevent Application Removal (T1629.001) [707]

MV Code	Vulnerability Description
MV1629.001-S1	The vulnerability in the Android device administration API, which, in earlier Android versions, required explicit deactivation of administration capabilities before uninstalling an application, allowing adversaries to prevent application removal by abusing this process.
MV1629.001-S2	The vulnerability in the Android device accessibility APIs, enabling malicious applications to programmatically monitor and manipulate the device screen, preventing the user from uninstalling the application by injecting input or emulating back button presses.

MV1629.001-S3	The inadequacy in Enterprise Policy, as an improperly configured EMM/MDM that fails to explicitly define permitted accessibility services could leave the system susceptible to abuse of Android's accessibility features by malicious applications.
MV1629.001-H1	User activates Android device administration capabilities without considering the potential consequences, allowing adversaries to exploit this human mistake to impair defenses and prevent application removal.
MV1629.001-H2	User overlooks the permissions granted to applications, enabling adversaries to abuse accessibility APIs by installing malicious applications that can monitor and manipulate the device screen to hinder the uninstallation process.
MV1629.001-H3	The reliance on outdated Android versions, as systems not using recent versions may still be vulnerable to exploitation of the Android device administrator uninstall process, posing a risk even with available OS-level improvements.
MV1629.001-H4	User grants excessive access without proper scrutiny, where user who overlooks warnings and grants access to accessibility features or device administration services may inadvertently allow malicious applications to impair defenses and interfere with the uninstallation process
MV1629.001-H5	User lacks awareness and knowledge about safe practices, as user who is not educated on booting into safe mode to uninstall malicious applications may struggle to mitigate the impact of interference with the uninstallation process by such applications.

3.5.12 Impair Defenses: Device Lockout (T1629.002) [708]

MV Code	Vulnerability Description
MV1629.002-S1	Weaknesses in the Android operating system, particularly in versions prior to Android 7, where device administrators could reset the device lock passcode, providing an avenue for unauthorized access.

MV1629.002-H1	User grants device administrator permissions to malicious applications, enabling the adversary to employ techniques such as DevicePolicyManager.lockNow() to lock the device, indicating a human mistake in granting excessive permissions without proper scrutiny.
MV1629.002-H2	User neglects to update to recent Android versions, as using an outdated version increases the likelihood of an adversary successfully employing techniques to lock the device, highlighting a human mistake in maintaining up-to-date operating systems.

3.5.13 Impair Defenses: Disable or Modify Tools (T1629.003) [709]

MV Code	Vulnerability Description
MV1629.003-S1	The potential weakness in device administrator permissions, allowing for the disabling of security tools and interference with scanning or reporting functions.
MV1629.003-S2	The potential absence or inadequate implementation of compromised device detection methods, leaving the system susceptible to exploitation by adversaries who may have rooted or jailbroken the device.
MV1629.003-S3	The absence or ineffectiveness of system partition integrity mechanisms, such as Verified Boot, which could fail to detect unauthorized modifications to system files.
MV1629.003-H1	The potential delay or omission of security updates, exposing the system to known vulnerabilities that could be exploited for root access.
MV1629.003-H2	The lack of awareness or understanding, as users may not be adequately informed about the dangers of rooting or jailbreaking their devices, potentially leading to security compromises.
MV1629.003-H3	User grants root access, enabling the modification of protected system files and compromising the effectiveness of security software.

3.5.14 Indicator Removal on Host (T1630) [710]

MV Code	Vulnerability Description
MV1630-S1	The lack of adequate file and artifact protection mechanisms, allowing for the deletion, alteration, or concealment of generated artifacts on the device.
MV1630-S2	Insufficient attestation implementation, which may result in the failure to detect unauthorized modifications to devices and hinder the effectiveness of mitigation actions by mobile security software.
MV1630-H1	The failure to implement proper access controls or monitoring configurations, potentially leading to compromised event collection, reporting, and detection of intrusion activity.
MV1630-H2	User neglects security updates, leaving the system exposed to known vulnerabilities that could be exploited by malicious applications, as the application of patches is a crucial aspect of maintaining a secure environment.
MV1630-H3	The lack of user awareness and guidance, which may lead to user unknowingly engaging in risky behavior such as device rooting or granting unnecessary access to the accessibility service, creating opportunities for security risks to be exploited.

3.5.15 Indicator Removal on Host: Uninstall Malicious Application (T1630.001) [711]

MV Code	Vulnerability Description
MV1630.001-S1	Improper implementation of device owner permissions, allowing adversaries to abuse them for silent uninstallation using device owner API calls.
MV1630.001-S2	Insufficient protection of root permissions, enabling adversaries to exploit these permissions to delete files from the filesystem.
MV1630.001-S3	The vulnerability in the accessibility service, which can be manipulated by adversaries to send uninstallation intents and subsequently abuse the service to interact with the screen for confirmation.

MV1630.001-S4	Lack of attestation implementation, allowing adversaries to go undetected on rooted devices; this could be mitigated by implementing attestation mechanisms.
MV1630.001-H1	User allows the malicious application to acquire device owner permissions, providing the adversary with the opportunity to abuse these permissions for silent uninstallation using device owner API calls.
MV1630.001-H2	User grants root permissions to the malicious application, thereby enabling adversaries to exploit these permissions for unauthorized file deletion from the filesystem.
MV1630.001-H3	User permits accessibility service requests without proper scrutiny, allowing the adversary to manipulate the service to initiate uninstallation through screen interactions.
MV1630.001-H4	Delayed or inadequate application of security updates, leaving devices susceptible to known vulnerabilities that could be exploited for rooting; consistent and prompt application of security updates is necessary for mitigation.

3.5.16 Indicator Removal on Host: File Deletion (T1630.002) **[712]**

MV Code	Vulnerability Description
MV1630.002-S1	The potential lack of proper access controls, allowing an application with administrator access to fully wipe the device.
MV1630.002-H1	The risk of inadvertently granting excessive permissions to an application, potentially enabling it to delete files without requiring special permissions depending on their storage location.
MV1630.002-H2	User inadvertently grants device administrator permissions to malicious applications, as users may not be adequately trained to recognize and avoid phishing popups requesting such permissions.

3.5.17 Indicator Removal on Host: Disguise Root/Jailbreak Indicators (T1630.003) [713]

MV Code	Vulnerability Description
MV1630.003-S1	The reliance on specific artifacts, such as the presence of an installed "su" binary, by mobile security products for compromised device detection, which can be exploited by renaming the binary to evade detection.
MV1630.003-H1	The potential oversight in configuring security software, enabling adversaries to exploit polymorphic code techniques and evade signature-based detection.

3.5.18 Input Injection (T1516) [718]

MV Code	Vulnerability Description
MV1516-S1	The inadequacy in the implementation of the Android DevicePolicyManager.setPermittedAccessibilityServices method, leading to misconfigurations that may inadvertently permit unauthorized applications to exploit accessibility features.
MV1516-H1	User inadvertently installs malicious applications that exploit the system's accessibility APIs, enabling input injection and posing a risk of unauthorized transactions or actions initiated by the adversary.
MV1516-H2	User inadvertently approve dangerous permissions for applications, potentially allowing malicious actors to manipulate accessibility features

3.5.19 Masquerading (T1655) [723]

MV Code	Vulnerability Description
MV1655-H1	The susceptibility to being tricked into misidentifying the file type, contributing to the success of masquerading attacks.
MV1655-H2	User installs apps from unauthorized sources, increasing the risk of malicious repackaged apps and undermining the effectiveness of the provided mitigation strategy.

3.5.20 Masquerading: Match Legitimate Name or Location (T1655.001) [724]

MV Code	Vulnerability Description
MV1655.001-H1	The tendency to implicitly trust files or resources solely based on their names or locations, enabling adversaries to exploit human errors in judgment and facilitate the success of masquerading attacks.
MV1655.001-H2	User inadvertently installs malicious repackaged apps from unauthorized sources, as the lack of strict enforcement of app installation policies may allow the execution of masquerading attacks.

3.5.21 Native API (T1575) [725]

MV Code	Vulnerability Description
MV1575-S1	The potential exploitation of weaknesses in Android's Native Development Kit (NDK), allowing them to write native code in C or C++ that bypasses higher-level language safeguards, making it harder to analyze and detect malicious behavior.
MV1575-H1	The potential misuse of the Java Native Interface (JNI) by developers, allowing Java functions in Android apps to call functions in a native library, which could inadvertently execute malicious code if not properly secured.

3.5.22 Obfuscated Files of Information (T1406) [729]

MV Code	Vulnerability Description
MV1406-S1	Inadequate detection mechanisms, as the obfuscation techniques employed by adversaries, such as encryption, encoding, and compression, can evade traditional defenses and hinder the discovery of malicious payloads.

MV1406-H1	The risk of inadvertently facilitating obfuscated file execution, as users may unknowingly open or execute seemingly benign files that, when reassembled, reveal malicious functionality, contributing to successful initial access or evasion of detection.

3.5.23 Obfuscated Files of Information: Steganography (T1406.001) [730]

MV Code	Vulnerability Description
MV1406.001-S1	The susceptibility to data exfiltration or covert communication due to the inability to detect hidden information in digital media, such as images, audio tracks, video clips, or text files.

3.5.24 Obfuscated Files of Information: Software Packing (T1406.002) [731]

MV Code	Vulnerability Description
MV1406.002-S1	The susceptibility of executable files to software packing, which involves compressing or encrypting executables to change file signatures and evade signature-based detection, exploiting the weakness in the system's ability to recognize such alterations.

3.5.25 Process Injection (T1631) [735]

MV Code	Vulnerability Description
MV1631-S1	The lack of inherent mechanisms in both Android and iOS to prevent process injection, allowing adversaries to abuse existing root access or exploit vulnerabilities for unauthorized code execution.

3.5.26 Process Injection: Ptrace System Calls (T1631.001) [736]

MV Code	Vulnerability Description
MV1631.001-S1	The vulnerability in the ptrace system call, which allows adversaries to inject malicious code into processes and execute arbitrary actions in the context of another process, potentially gaining unauthorized access, manipulating memory, and evading detection from security products.
MV1631.001-H1	The improper handling of process memory, such as writing arbitrary code into a running process using malloc, and invoking that memory with PTRACE_SETREGS, which can lead to the execution of unauthorized instructions and compromise the integrity of the targeted system.

3.5.27 Proxy Through Victim (T1604) [742]

MV Code	Vulnerability Description
MV1604-S1	The vulnerability in the standard OS-level APIs and 3rd party libraries, allowing adversaries to hide their C2 server's true IP address and masquerade their traffic as legitimate, thereby evading IP-based restrictions and alerts on services like bank accounts and social media websites.

3.5.28 Subvert Trust Controls (T1632) [753]

MV Code	Vulnerability Description
MV1632-S1	The reliance on code signing certificates for trust, which, if compromised, allows malicious programs to be executed with apparent legitimacy.
MV1632-H1	The susceptibility of older mobile operating systems to adversary-in-the-middle attacks through untrusted certificates, emphasizing the importance of using recent OS versions (iOS 10.3 and higher, Android 7 and higher) to enhance security against such attacks.

MV1632-H2	The possibility of ignoring or bypassing security alerts from the operating system, leading to the execution of applications from untrusted sources and potential security breaches.
MV1632-H3	User installs apps signed using enterprise distribution keys, which can be mitigated by enforcing restrictions using iOS configuration profiles (allowEnterpriseAppTrust and allowEnterpriseAppTrustModification).
MV1632-H4	The risk of installing insecure or malicious configuration settings without explicit consent, highlighting the importance of user guidance to advise against installing unexpected configuration settings (CA certificates, iOS Configuration Profiles, Mobile Device Management server provisioning).

3.5.29 Subvert Trust Controls: Code Signing Policy Modification (T1632.001) [754]

MV Code	Vulnerability Description
MV1632.001-H1	The failure to properly configure or safeguard against code signing policy modifications, potentially enabling the execution of malicious applications on the system.
MV1632.001-H2	User installs apps signed with enterprise distribution keys on iOS, as enterprise policy controls (allowEnterpriseAppTrust and allowEnterpriseAppTrustModification) may not be effectively enforced.
MV1632.001-H3	The susceptibility of mobile devices running outdated operating systems (OS) to adversary-in-the-middle attacks, as using a recent OS version (iOS 10.3 and higher or Android 7 and higher) adds security measures that make it more difficult to trick users into installing untrusted certificates and configurations.
MV1632.001-H4	The risk of installing insecure or malicious configuration settings without explicit consent, highlighting the importance of user guidance to advise against installing unexpected configuration settings (CA certificates, iOS Configuration Profiles, Mobile Device Management server provisioning).

3.5.30 Virtualization/Sandbox Evasion (T1633) [763]

MV Code	Vulnerability Description
MV1633-S1	The presence of artifacts indicative of a virtual machine environment, which can be exploited through changing behaviors to disengage from the victim or concealing the core functions of the payload upon detection.
MV1633-H1	The failure to conceal legitimate user activity in an analysis environment, providing adversaries with information to determine if the system is under analysis, potentially leading to evasion.

3.5.31 Virtualization/Sandbox Evasion: System Checks (T1633.001) [764]

MV Code	Vulnerability Description
MV1633.001-S1	The lack of robust virtualization detection mechanisms, allowing adversaries to evade detection by altering malware behavior in response to identifying artifacts indicative of a virtual environment or sandbox.
MV1633.001-H1	The misconfigurations in generic system properties such as host/domain name, network traffic patterns, network adapter addresses, CPU core count, and available memory/drive size, providing potential clues for adversaries to identify and evade virtual environments.
MV1633.001-H2	User neglects to secure hardware elements like motion sensors, which adversaries could exploit to gather evidence indicative of a virtual environment, contributing to the evasion of detection.

3.6 Credential Access (TA0031) [23]

3.6.1 Access Notification (T1517) [657]

MV Code	Vulnerability Description
MV1517-S1	Unauthorized access to notifications in Android devices with a work profile, as the DevicePolicyManager.setPermittedCrossProfileNotificationListeners method could be misconfigured or mismanaged, allowing unintended applications within the personal profile to access notifications generated within the work profile.
MV1517-H1	The inadvertent dismissal of notifications, enabling adversaries to prevent users from noticing the arrival of notifications and potentially taking action buttons contained within them
MV1517-H2	The risk of granting applications dangerous or privacy-intrusive permissions, specifically access to notifications, due to user oversight or lack of awareness, which could lead to unauthorized access and potential misuse of sensitive information.

3.6.2 Clipboard Data (T1414) [667]

MV Code	Vulnerability Description
MV1414-S1	The vulnerability in the clipboard manager APIs on Android and iOS, which allows unauthorized access to sensitive information copied to the device clipboard, such as passwords, when certain conditions are met.
MV1414-H1	The potential mistake of copying sensitive information, like passwords from a password manager, to the clipboard, enabling malicious applications installed on the device to capture and misuse this data.
MV1414-H2	The potential mistake of using an outdated Android version (prior to Android 10), which lacks the security enhancement preventing unauthorized access to clipboard data by applications not in the foreground or set as the default IME, thereby exposing sensitive information to potential misuse.

3.6.3 Credentials from Password Store (T1634) [672]

MV Code	Vulnerability Description
MV1634-S1	The susceptibility of devices to jailbreaking, potentially allowing adversaries to bypass security measures and compromise password stores.
MV1634-H1	The practice of storing passwords in common and predictable locations on a device, which increases the risk of unauthorized access by adversaries searching for credentials.
MV1634-H2	The failure to promptly apply security updates, leaving the system exposed to known OS vulnerabilities and increasing the risk of unauthorized access to password stores.

3.6.4 Credentials from Password Store: Keychain (T1634.001) [673]

MV Code	Vulnerability Description
MV1634.001-S1	Inadequate protection of the keychain database outside application sandboxes, allowing unauthorized access if an adversary exploits privilege escalation or gains root access.
MV1634.001-H1	Storing sensitive credentials on an iOS device without implementing additional security measures, making it susceptible to compromise if the device is exploited by an adversary with privilege escalation or root access.
MV1634.001-H2	Delayed or neglected implementation of security updates by users or administrators, leaving the system exposed to known vulnerabilities that could be exploited by adversaries.
MV1634.001-H3	Failure to deploy or activate device attestation and compromised device detection methods, allowing adversaries to operate undetected on jailbroken devices and potentially access password stores.

3.6.5 Input Capture (T1417) [715]

MV Code	Vulnerability Description
MV1417-S1	Inadequate control over third-party keyboards in Samsung Knox, as they need to be explicitly added to an allow list, potentially leaving the system open to malicious input capture if not properly managed.
MV1417-S2	Potential overlay window manipulation in Android versions prior to 12, as apps with the SYSTEM_ALERT_WINDOW permission could create overlay windows on top of other applications, potentially facilitating deceptive GUI Input Capture prompts.
MV1417-H1	Falling for deceptive tactics that trick users into providing input, such as responding to a GUI Input Capture prompt they believe to be from a legitimate application.
MV1417-H2	User grants applications dangerous or privacy-intrusive permissions, such as keyboard registration or accessibility service access, which may expose the user to input capture attacks.

3.6.6 Input Capture: Keylogging (T1417.001) [716]

MV Code	Vulnerability Description
MV1417.001-S1	The vulnerability in the accessibility features on Android, where adversaries can register an AccessibilityService class, override the onAccessibilityEvent method, and listen for the AccessibilityEvent.TYPE_VIEW_TEXT_CHANGED event type to record user keystrokes.
MV1417.001-H1	User grants explicit authorization to third-party keyboard apps on Android and iOS without exercising caution, potentially allowing adversaries to masquerade as legitimate keyboards and log user keystrokes.
MV1417.001-H2	The potential for third-party keyboards on Samsung Knox to be available to end-users without explicit approval, as they must be explicitly added to an allow list for mitigation.

MV1417.001-H3	User grants dangerous or privacy-intrusive permissions, such as keyboard registration or accessibility service access, despite user guidance advising caution.

3.6.7 Input Capture: GUI Input Capture (T1417.002) [717]

MV Code	Vulnerability Description
MV1417.002-S1	The vulnerability in the Android's accessibility features, enabling the determination of the foreground application, which can be exploited to display deceptive prompts on top of running legitimate applications.
MV1417.002-S2	The potential lack of proper Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) configuration, as the Android DevicePolicyManager.setPermittedAccessibilityServices method may not be utilized to explicitly define permitted applications, allowing adversaries to exploit accessibility features.
MV1417.002-H1	User fails to implement and configure EMM/MDM solutions effectively, as users may neglect to set explicit lists of permitted applications for accessibility features, leaving the system vulnerable to abuse.
MV1417.002-H2	The susceptibility to input prompts from seemingly legitimate sources, such as fake device notifications or prompts overlaid on running applications, potentially leading to the unintentional disclosure of sensitive information.
MV1417.002-H3	Delay or neglect in updating to recent Android versions, as users who do not promptly adopt Android 12 or later may miss out on the HIDE_OVERLAY_WINDOWS permission, exposing their devices to potential overlay window attacks.

3.6.8 Steal Application Access Token (T1635) [750]

MV Code	Vulnerability Description
MV1635-S1	The potential weakness in the OAuth 2.0 implementation, which may expose application access tokens, allowing unauthorized access to cloud-based services and protected APIs.
MV1635-S2	A weakness in the secure binding between URIs and applications
MV1635-H1	The risk of falling victim to social engineering or URI hijacking, as the adversary relies on user actions, such as interacting with a system "Open With" dialogue, to grant access and steal application access tokens.

3.6.9 Steal Application Access Token: URI Hijacking (T1635.001) [751]

MV Code	Vulnerability Description
MV1635.001-H1	The inadvertent registration of a URI already in use by a genuine application, enabling adversaries to intercept sensitive data meant for the legitimate application, potentially resulting in unauthorized access to protected resources or successful phishing attacks.
MV1635.001-H2	Insecure binding between URIs and applications, as developers may not implement Android App Links and iOS Universal Links, allowing malicious applications to intercept redirections and compromise data.
MV1635.001-H3	The failure to use recent OS versions, as users on outdated operating systems may lack the security features introduced in iOS 11 or Android 6, making them susceptible to URI interception by malicious applications.
MV1635.001-H4	The act of opening links in unrecognized applications, as users may unknowingly expose themselves to phishing attacks or unauthorized data interception by malicious applications.

3.7 Discovery (TA0032) [24]

3.7.1 File and Directory Discovery (T1420) [697]

MV Code	Vulnerability Description
MV1420-S1	Android and Linux systems may be vulnerable due to file permissions and SELinux policies that, if not properly configured, could allow unauthorized access to sensitive data stored in the external storage directory.
MV1420-H1	Human users on Android and Linux systems may inadvertently expose sensitive data by storing it inappropriately in the external storage directory, which is generally visible to apps.
MV1420-H2	Human users may introduce a vulnerability by neglecting to update their operating systems, leaving their devices susceptible to privilege escalation and weakened application sandboxing.

3.7.2 Location Tracking (T1430) [719]

MV Code	Vulnerability Description
MV1430-S1	The Android system's vulnerability allows adversaries to track a device's physical location by exploiting applications with the ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION permissions, and on Android 10 and up, by abusing the ACCESS_BACKGROUND_LOCATION permission.
MV1430-S2	When devices are not enrolled using Apple User Enrollment or a profile owner enrollment mode for Android, it potentially allows enterprises to access the device's physical location, particularly in Bring Your Own Device (BYOD) deployments.
MV1430-H1	User can inadvertently grant excessive location access permissions to malicious Android applications, enabling adversaries to track their device's location.
MV1430-H2	On iOS, user may unknowingly grants location access without explicit consent if an adversary with elevated privileges exploits the com.apple.locationd.preauthorized entitlement key.

MV1430-H3	User on iOS devices may unintentionally grant location access by installing applications that do not provide clear descriptions (NSLocationWhenInUseUsageDescription, NSLocationAlwaysAndWhenInUseUsageDescription, NSLocationAlwaysUsageDescription) regarding the extent of location information access.
MV1430-H4	User may inadvertently expose their device's physical location if they do not use the latest operating system versions on Android or iOS, as these versions include security features that restrict location access and provide users with more control.
MV1430-H5	User may compromise their privacy by not being cautious when selecting location permission options, especially on Android 11 and up, where users must manually navigate to settings to choose the "Allow all the time" option.
MV1430-H6	User may overlook the importance of protecting their account credentials, potentially leading to adversaries gaining unauthorized access to location data. Enabling multi-factor authentication options is a crucial preventive measure.

3.7.3 Location Tracking: Remote Device Management Services (T1430.001) **[720]**

MV Code	Vulnerability Description
MV1430.001-S1	The potential weaknesses in cloud services (e.g., Google's Android Device Manager or Apple iCloud's Find my iPhone) or enterprise mobility management (EMM)/mobile device management (MDM) server consoles that allow unauthorized access for tracking the location of mobile devices managed by the service.
MV1430.001-H1	Insufficient security practices, such as weak passwords or inadequate access controls, leading to unauthorized access to cloud services or enterprise mobility management (EMM)/mobile device management (MDM) server consoles and enabling the tracking of mobile device locations.

3.7.4 Location Tracking: Impersonate SS7 Nodes (T1430.002) [721]

MV Code	Vulnerability Description
MV1430.002-S1	The lack of authentication in signaling system network nodes, allowing for the impersonation of nodes and exploitation of this weakness to track the location of mobile devices.
MV1430.002-S2	The misconfiguration or inadequate implementation of interconnection filtering, which could result in incomplete protection and still leave the system susceptible to location tracking attacks.
MV1430.002-H1	The potential disclosure of sensitive information, such as the victim's MSISDN (phone number)

3.7.5 Network Service Scanning (T1423) [727]

MV Code	Vulnerability Description
MV1423-S1	Inadequate security configurations on network services, potentially allowing unauthorized access and exploitation.
MV1423-H1	Failure to implement proper security measures on the mobile device, such as allowing unauthorized access to internal enterprise networks through local connectivity or Virtual Private Network (VPN) connections.

3.7.6 Process Discovery (T1424) [734]

MV Code	Vulnerability Description
MV1424-S1	The inability of recent Android versions (7 and later) to allow applications to obtain a list of running processes without abusing elevated privileges due to the hidepid mount feature in the Android kernel.
MV1424-S2	The absence of the hidepid mount feature on Android versions prior to 7, allowing applications to easily obtain a list of running processes, potentially aiding in automated discovery.

MV1424-S3	Incomplete or ineffective attestation mechanisms, as attestation may not always accurately detect rooted devices, leading to a false sense of security.
MV1424-H1	The inadvertent failure to update the operating system to Android 7 or later on Android devices, leaving them susceptible to Process Discovery attacks due to the lack of recent security enhancements.

3.7.7 Software Discovery (T1418) [748]

MV Code	Vulnerability Description
MV1418-S1	The lack of proper access controls or security measures that allow an adversary to gather a listing of installed applications.
MV1418-H1	Users not keeping their Android devices up to date with the latest OS version, which could lead to a lack of privacy enhancements and increased vulnerability to Software Discovery attacks.
MV1418-H2	Failure to configure or implement adequate security measures, such as restricting access to software information, allowing adversaries to gather intelligence about the system.
MV1418-H3	User neglects the guidance to avoid downloading applications from unofficial sources on iOS devices, potentially exposing them to exploitation of the private API on older iOS versions, allowing adversaries to list installed applications.

3.7.8 Software Discovery: Security Software Discovery (T1418.001) [749]

MV Code	Vulnerability Description
MV1418.001-H1	The inadvertent installation or misconfiguration of security applications, potentially providing adversaries with information to shape follow-on behaviors.
MV1418.001-H2	The reliance on outdated operating systems that lack recent privacy enhancements, making it easier for adversaries to perform security software discovery.

MV1418.001-H3	User downloads applications from unofficial sources on iOS devices, as this action may expose the user to security risks, allowing adversaries to gather information through security software discovery.

3.7.9 System Information Discovery (T1426) [759]

MV Code	Vulnerability Description
MV1426-S1	The programmatically accessible information on Android devices through the android.os.Build class, providing adversaries potential access to sensitive system details.

3.7.10 System Network Configuration Discovery (T1422) [760]

MV Code	Vulnerability Description
MV1422-S1	The exposure of network configuration details, including IP and/or MAC addresses, through operating systems or remote system information discovery, providing potential entry points for unauthorized access.
MV1422-H1	User mishandles Android device permissions by allowing apps to access telephony-related device identifiers, such as IMSI, IMEI, and phone number, prior to Android 10, potentially exposing sensitive information.
MV1422-H2	User mishandles iOS device permissions by not requiring root access for gathering network configuration information, potentially leading to unauthorized access to sensitive details.
MV1422-H3	The reliance on an outdated iOS version, as mitigation measures specific to Android 10 may not apply, potentially leaving iOS devices vulnerable to unauthorized network configuration information access.

3.7.11 System Network Connections Discovery (T1421) [761]

MV Code	Vulnerability Description
MV1421-S1	Android and other systems may be vulnerable due to the use of device APIs like WifiInfo and BluetoothAdapter. These APIs may expose network connection information without proper authorization checks.
MV1421-S2	Android and Linux systems may be vulnerable due to improperly configured file permissions. If file permissions are not set correctly, unauthorized access to sensitive data stored in the external storage directory may occur.
MV1421-S3	Android and Linux systems may also be at risk if SELinux policies are not properly configured. Misconfigurations could potentially allow unauthorized access to sensitive data in the external storage directory.
MV1421-H1	User grants excessive permissions to applications. For example, accessing network information through APIs often requires permissions such as ACCESS_FINE_LOCATION, and users might grant these permissions without understanding the potential risks.

3.8 Lateral Movement (TA0033) [25]

3.8.1 Exploitation of Remote Services (T1428) [696]

MV Code	Vulnerability Description
MV1428-S1	Software vulnerabilities, including programming errors in programs, services, or the operating system, allowing the execution of adversary-controlled code.
MV1428-S2	Inadequate configuration of VPN policies at the device level, rather than per-app, may allow adversaries to gain unauthorized access to internal enterprise resources via VPN through non-approved applications.
MV1428-H1	Failure to apply necessary patches or updates to address known software vulnerabilities, potentially leading to exploitation by adversaries.

3.8.2 Replication Through Removable Media (T1458) [744]

MV Code	Vulnerability Description
MV1458-S1	Insecure bootloaders in Nexus 6 or 6P devices over USB, allowing actions such as intercepting phone calls, intercepting network traffic, and obtaining the device's physical location.
MV1458-S2	Weakly-enforced security boundaries in Android devices like the Google Pixel 2 over USB, providing an avenue for unauthorized access and potential data compromise.
MV1458-H1	Allowing adversaries to move onto devices by connecting them to compromised or malicious charging stations or PCs, bypassing application store requirements and facilitating the direct installation of malicious applications.
MV1458-H2	Potentially using USB connections as an initial access point, adversaries may exploit the device's connection to compromise security and gain entry to the device.
MV1458-H3	Failure to implement enterprise policies allowing USB debugging on Android devices without specific need, potentially exposing the device to exploitation.
MV1458-H4	Users not promptly applying security updates may overlook critical patches, leaving the device vulnerable to known exploits that could be mitigated by updates.
MV1458-H5	Using an outdated iOS version without USB Restricted Mode (iOS 11.4.1 and higher) may allow adversaries to exploit the device's charging port for data access, bypassing security measures.
MV1458-H6	Users clicking on device prompts to trust attached computers without necessity may compromise device security, underscoring the importance of cautious interaction with external devices.

3.9 Collection (TA0035) [26]

3.9.1 Access Notification (T1517) [657]

MV Code	Vulnerability Description
MV1517-S1	Unauthorized access to notifications in Android devices with a work profile, as the DevicePolicyManager.setPermittedCrossProfileNotificationListeners method could be misconfigured or mismanaged, allowing unintended applications within the personal profile to access notifications generated within the work profile.
MV1517-H1	The inadvertent dismissal of notifications, enabling adversaries to prevent users from noticing the arrival of notifications and potentially taking action buttons contained within them
MV1517-H2	The risk of granting applications dangerous or privacy-intrusive permissions, specifically access to notifications, due to user oversight or lack of awareness, which could lead to unauthorized access and potential misuse of sensitive information.

3.9.2 Adversary-in-the-Middle (T1638) [659]

MV Code	Vulnerability Description
MV1638-H1	User grants consent to a malicious application registering as a VPN client, allowing the adversary to redirect device traffic and capture sensitive data.
MV1638-H2	User fail to update the operating system. The potential weakness in older operating systems, as they may allow applications to more easily register as VPN providers, facilitating Adversary-in-the-Middle (AiTM) attacks.

3.9.3 Archive Collected Data (T1532) **[663]**

MV Code	Vulnerability Description
MV1532-S1	The potential weakness in the data compression and encryption implementation, which may allow for exploitation, unauthorized access, or compromise during the exfiltration process.
MV1532-H1	The improper configuration or misuse of the compression and encryption tools, leading to a suboptimal security posture and potentially facilitating unauthorized access to compressed or encrypted data.

3.9.4 Audio Capture (T1429) **[664]**

MV Code	Vulnerability Description
MV1429-S1	The lack of default restrictions on CAPTURE_AUDIO_OUTPUT permission for third-party applications on Android devices, which could be exploited after privilege escalation.
MV1429-H1	The failure to scrutinize or grant microphone access permissions to applications on Android and iOS devices, potentially allowing malicious apps to capture audio without the user's awareness.
MV1429-H2	The failure to keep the operating system up-to-date, specifically on Android devices, leaving them susceptible to the lack of access restrictions on microphone and sensor usage imposed by recent OS versions.

3.9.5 Call Control (T1616) **[666]**

MV Code	Vulnerability Description
MV1616-S1	The lack of sufficient safeguards or warnings in the Android operating system, allowing users to change their default call handler to unrecognized applications easily, which may expose them to malicious activities.

MV1616-H1	User inadvertently grants sensitive permissions, such as ANSWER_PHONE_CALLS, CALL_PHONE, PROCESS_OUTGOING_CALLS, MANAGE_OWN_CALLS, BIND_TELECOM_CONNECTION_SERVICE, and WRITE_CALL_LOG, which can lead to unauthorized manipulation of phone calls, compromising the device's integrity and user privacy.
MV1616-H2	User might inadvertently change their default call handler to unrecognized applications due to a lack of awareness or understanding of the potential risks, contributing to the vulnerability of unauthorized phone call manipulation.

3.9.6 Clipboard Data (T1414) [667]

MV Code	Vulnerability Description
MV1414-S1	The vulnerability in the clipboard manager APIs on Android and iOS, which allows unauthorized access to sensitive information copied to the device clipboard, such as passwords, when certain conditions are met.
MV1414-H1	The potential mistake of copying sensitive information, like passwords from a password manager, to the clipboard, enabling malicious applications installed on the device to capture and misuse this data.
MV1414-H2	The potential mistake of using an outdated Android version (prior to Android 10), which lacks the security enhancement preventing unauthorized access to clipboard data by applications not in the foreground or set as the default IME, thereby exposing sensitive information to potential misuse.

3.9.7 Data from Local System (T1533) [676]

MV Code	Vulnerability Description
MV1533-H1	User grants excessive permissions, particularly storage-related permissions on Android devices, allowing adversaries to access files from external storage and compromise sensitive data.

3.9.8 Input Capture (T1417) [715]

MV Code	Vulnerability Description
MV1417-S1	Inadequate control over third-party keyboards in Samsung Knox, as they need to be explicitly added to an allow list, potentially leaving the system open to malicious input capture if not properly managed.
MV1417-S1	Potential overlay window manipulation in Android versions prior to 12, as apps with the SYSTEM_ALERT_WINDOW permission could create overlay windows on top of other applications, potentially facilitating deceptive GUI Input Capture prompts.
MV1417-H1	Falling for deceptive tactics that trick users into providing input, such as responding to a GUI Input Capture prompt they believe to be from a legitimate application.
MV1417-H2	User grants applications dangerous or privacy-intrusive permissions, such as keyboard registration or accessibility service access, which may expose the user to input capture attacks.

3.9.9 Input Capture: Keylogging (T1417.001) [716]

MV Code	Vulnerability Description
MV1417.001-S1	The vulnerability in the accessibility features on Android, where adversaries can register an AccessibilityService class, override the onAccessibilityEvent method, and listen for the AccessibilityEvent.TYPE_VIEW_TEXT_CHANGED event type to record user keystrokes.
MV1417.001-H1	User grants explicit authorization to third-party keyboard apps on Android and iOS without exercising caution, potentially allowing adversaries to masquerade as legitimate keyboards and log user keystrokes.
MV1417.001-H2	The potential for third-party keyboards on Samsung Knox to be available to end-users without explicit approval, as they must be explicitly added to an allow list for mitigation.

MV1417.001-H3	User grants dangerous or privacy-intrusive permissions, such as keyboard registration or accessibility service access, despite user guidance advising caution.

3.9.10 Input Capture: GUI Input Capture (T1417.002) [717]

MV Code	Vulnerability Description
MV1417.002-S1	The vulnerability in the Android's accessibility features, enabling the determination of the foreground application, which can be exploited to display deceptive prompts on top of running legitimate applications.
MV1417.002-S2	The potential lack of proper Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) configuration, as the Android DevicePolicyManager.setPermittedAccessibilityServices method may not be utilized to explicitly define permitted applications, allowing adversaries to exploit accessibility features.
MV1417.002-H1	User fails to implement and configure EMM/MDM solutions effectively, as users may neglect to set explicit lists of permitted applications for accessibility features, leaving the system vulnerable to abuse.
MV1417.002-H2	The susceptibility to input prompts from seemingly legitimate sources, such as fake device notifications or prompts overlaid on running applications, potentially leading to the unintentional disclosure of sensitive information.
MV1417.002-H3	Delay or neglect in updating to recent Android versions, as users who do not promptly adopt Android 12 or later may miss out on the HIDE_OVERLAY_WINDOWS permission, exposing their devices to potential overlay window attacks.

3.9.11 Location Tracking (T1430) [719]

MV Code	Vulnerability Description
MV1430-S1	The Android system's vulnerability allows adversaries to track a device's physical location by exploiting applications with the ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION permissions, and on Android 10 and up, by abusing the ACCESS_BACKGROUND_LOCATION permission.
MV1430-S2	When devices are not enrolled using Apple User Enrollment or a profile owner enrollment mode for Android, it potentially allows enterprises to access the device's physical location, particularly in Bring Your Own Device (BYOD) deployments.
MV1430-H1	User can inadvertently grant excessive location access permissions to malicious Android applications, enabling adversaries to track their device's location.
MV1430-H2	On iOS, user may unknowingly grants location access without explicit consent if an adversary with elevated privileges exploits the com.apple.locationd.preauthorized entitlement key.
MV1430-H3	User on iOS devices may unintentionally grant location access by installing applications that do not provide clear descriptions (NSLocationWhenInUseUsageDescription, NSLocationAlwaysAndWhenInUseUsageDescription, NSLocationAlwaysUsageDescription) regarding the extent of location information access.
MV1430-H4	User may inadvertently expose their device's physical location if they do not use the latest operating system versions on Android or iOS, as these versions include security features that restrict location access and provide users with more control.
MV1430-H5	User may compromise their privacy by not being cautious when selecting location permission options, especially on Android 11 and up, where users must manually navigate to settings to choose the "Allow all the time" option.

MV1430-H6	User may overlook the importance of protecting their account credentials, potentially leading to adversaries gaining unauthorized access to location data. Enabling multi-factor authentication options is a crucial preventive measure.

3.9.12 Location Tracking: Remote Device Management Services (T1430.001) [720]

MV Code	Vulnerability Description
MV1430.001-S1	The potential weaknesses in cloud services (e.g., Google's Android Device Manager or Apple iCloud's Find my iPhone) or enterprise mobility management (EMM)/mobile device management (MDM) server consoles that allow unauthorized access for tracking the location of mobile devices managed by the service.
MV1430.001-H1	Insufficient security practices, such as weak passwords or inadequate access controls, leading to unauthorized access to cloud services or enterprise mobility management (EMM)/mobile device management (MDM) server consoles and enabling the tracking of mobile device locations.

3.9.13 Location Tracking: Impersonate SS7 Nodes (T1430.002) [721]

MV Code	Vulnerability Description
MV1430.002-S1	The lack of authentication in signaling system network nodes, allowing for the impersonation of nodes and exploitation of this weakness to track the location of mobile devices.
MV1430.002-S2	The misconfiguration or inadequate implementation of interconnection filtering, which could result in incomplete protection and still leave the system susceptible to location tracking attacks.
MV1430.002-H1	The potential disclosure of sensitive information, such as the victim’s MSISDN (phone number)

3.9.14 Protected User Data (T1636) **[737]**

MV Code	Vulnerability Description
MV1636-H1	The failure to carefully review and manage application permissions, especially on Android where permissions must be declared in the application's manifest or on iOS in the Info.plist file, potentially leading to unauthorized access to sensitive user data.
MV1636-H2	The user is the potential lack of awareness regarding additional privacy controls introduced by vendors, such as the ability to grant permission to an application only while actively used, which could result in unintentional exposure of Protected User Data.
MV1636-H3	User fails to update operating systems, as adversaries may exploit security gaps that have not been addressed by recent updates, leaving devices more susceptible to unauthorized access of Protected User Data.
MV1636-H4	The lack of awareness and adherence to user guidance, where users may not fully comprehend the security implications of granting unnecessary permissions, leading to inadvertent exposure of Protected User Data.

3.9.15 Protected User Data: Calendar Entries (T1636.001) **[738]**

MV Code	Vulnerability Description
MV1636.001-H1	User does not exercise extra scrutiny when granting calendar access permissions, as calendar access is an uncommonly needed permission, and users should be cautious in authorizing such access to their device.
MV1636.001-H2	If the device has been jailbroken or rooted, it allows the adversary to access Calendar Entries without the user's knowledge or approval.

3.9.16 Protected User Data: Call Log (T1636.002) [739]

MV Code	Vulnerability Description
MV1636.002-S1	The vulnerability in the Call Log Content Provider API, allowing adversaries to gather call log data using standard APIs.
MV1636.002-H1	In the case of a jailbroken or rooted device, the system vulnerability arises from the ability of adversaries to access the Call Log without the user's knowledge or approval.
MV1636.002-H2	The overreliance on user discretion in granting access to call logs, as users may inadvertently provide permissions without fully understanding the uncommonly needed nature of this access.

3.9.17 Protected User Data: Contact List (T1636.003) [740]

MV Code	Vulnerability Description
MV1636.003-S1	The vulnerability in the Contacts Content Provider on Android or the Contacts framework on iOS, which enable adversary to gather contact list data.
MV1636.003-S2	Lack of the proper controls or restrictions on permissions, especially for uncommonly needed permissions like access to the contact list, which enables adversaries could exploit this weakness.
MV1636.003-H1	If the device is jailbroken or rooted, the user's mistake is not securing the device, allowing adversaries to potentially access the Contact List without the user’s knowledge or approval.
MV1636.003-H2	User might make the mistake of not exercising extra scrutiny when granting access to user's contact list, potentially allowing malicious actors to misuse this permission.

3.9.18 Protected User Data: SMS Messages (T1636.004) [741]

MV Code	Vulnerability Description
MV1636.004-S1	The Android operating system's vulnerability allows adversaries to access SMS messages using standard APIs, specifically the SMS Content Provider.
MV1636.004-H1	If the user's device is jailbroken or rooted, it introduces a vulnerability where adversaries can access SMS messages without the user's knowledge or approval.
MV1636.004-H2	User may grant unnecessary access to SMS messages, as adversaries may exploit this permission, leading to unauthorized access.

3.9.19 Screen Capture (T1513) [746]

MV Code	Vulnerability Description
MV1513-S1	The susceptibility of the Android operating system to unauthorized screen capture through the use of Android MediaProjectionManager, accessibility services, or commands like screencap and screenrecord, particularly when the device user grants consent or when an adversary has root access or Android Debug Bridge (adb) access.
MV1513-S2	The lack of secure handling of sensitive screens by application developers, as the FLAG_SECURE property is not applied, making it easier for adversaries to capture screen contents.
MV1513-H1	User grants unnecessary or inappropriate consent to Android MediaProjectionManager, allowing adversaries to capture sensitive information through screen captures or videos.
MV1513-H2	User enables USB debugging (Android Debug Bridge) without explicit need, potentially allowing unauthorized access to ADB, which could be exploited by adversaries.
MV1513-H3	User allows unrestricted access to accessibility features, as user may not follow enterprise policies that explicitly specify which applications are permitted to use Android's accessibility features.

3.9.20 Stored Application Data (T1409) [752]

MV Code	Vulnerability Description
MV1409-H1	The insecure storage of application data in external storage, which can be accessed due to the lack of proper safeguards.
MV1409-H2	The insecure storage of application data in the internal storage directory with inadequate permissions (e.g., 777), enabling unauthorized access.
MV1409-H3	User grants root permissions to applications without considering the potential security implications, leading to unauthorized access to sensitive data on the device.
MV1409-H4	The use of an outdated Android OS version, as versions prior to Android 9 lack the security policy preventing applications from reading or writing data to other applications' internal storage directories, regardless of permissions.

3.9.21 Video Capture (T1512) [762]

MV Code	Vulnerability Description
MV1512-S1	The absence of a visual indicator on the status bar (such as the green dot introduced in iOS 14 and Android 12) in older operating system versions, making it more challenging for users to detect when an application is accessing the device's camera.
MV1512-H1	The failure to carefully manage app permissions, such as granting the android.permission.CAMERA permission on Android or providing the NSCameraUsageDescription key in the Info.plist file on iOS without due consideration.
MV1512-H2	The failure to update the operating system to the latest version (Android 9 and above, iOS 14, and Android 12), thereby not benefiting from enhanced security features and indicators that mitigate unauthorized camera access.

3.10 Command and Control (TA0037) [27]

3.10.1 Application Layer Protocol (T1437) [660]

MV Code	Vulnerability Description
MV1437-S1	The potential weaknesses in application layer protocols, such as web browsing, file transfer, electronic mail, or DNS, which could be exploited to facilitate malicious communication and evade detection.

3.10.2 Application Layer Protocol: Web Protocols (T1437.001) [661]

MV Code	Vulnerability Description
MV1437.001-S1	The lack of effective network filtering for application layer protocols associated with web traffic, allowing adversaries to blend in and avoid detection.
MV1437.001-H1	The failure to inspect routine device traffic effectively, especially in the context of mobile messaging services like Google Cloud Messaging (GCM), Firebase Cloud Messaging (FCM), and Apple Push Notification Service (APNS), which use HTTP/S for communication, creating opportunities for abuse by adversaries.

3.10.3 Call Control (T1616) [666]

MV Code	Vulnerability Description
MV1616-S1	The lack of sufficient safeguards or warnings in the Android operating system, allowing users to change their default call handler to unrecognized applications easily, which may expose them to malicious activities.
MV1616-H1	User inadvertently grants sensitive permissions, such as ANSWER_PHONE_CALLS, CALL_PHONE, PROCESS_OUTGOING_CALLS, MANAGE_OWN_CALLS, BIND_TELECOM_CONNECTION_SERVICE, and WRITE_CALL_LOG, which can lead to unauthorized manipulation of phone calls, compromising the device's integrity and user privacy.

MV1616-H2	User might inadvertently change their default call handler to unrecognized applications due to a lack of awareness or understanding of the potential risks, contributing to the vulnerability of unauthorized phone call manipulation.

3.10.4 Dynamic Resolution (T1637) [681]

MV Code	Vulnerability Description
MV1637-H1	The inadvertent sharing of a common algorithm between malware and command and control infrastructure, enabling the adversary to dynamically adjust communication parameters and evade detection.

3.10.5 Dynamic Resolution: Domain Generation Algorithms (T1637.001) [682]

MV Code	Vulnerability Description
MV1637.001-S1	The potential inability to effectively block, track, or take over the command and control channel due to the use of Domain Generation Algorithms (DGAs), which can generate numerous domains for malware communication, increasing the difficulty for defenders.

3.10.6 Encrypted Channel (T1521) [683]

MV Code	Vulnerability Description
MV1521-S1	The potential for reverse engineering of the encryption implementation, particularly if secret keys are encoded and/or generated within malware samples or configuration files.

3.10.7 Encrypted Channel: Symmetric Cryptography (T1521.001) [684]

MV Code	Vulnerability Description
MV1521.001-S1	The potential weakness in the implementation of symmetric encryption algorithms such as AES, Blowfish, and RC4, which could be exploited to compromise the confidentiality of command and control traffic.

3.10.8 Encrypted Channel: Asymmetric Cryptography (T1521.002) [685]

MV Code	Vulnerability Description
MV1521.002-S1	The use of known asymmetric encryption algorithms, such as RSA, ElGamal, and ECDSA, without relying on inherent protections provided by communication protocols.
MV1521.002-H1	The improper management or exposure of the private key, as asymmetric cryptography relies on the user's responsibility to keep the private key confidential.

3.10.9 Ingress Tool Transfer (T1544) [714]

MV Code	Vulnerability Description
MV1544-S1	The lack of proper access controls or network segmentation, allowing files to be copied from an external adversary-controlled system through the command and control channel or alternate protocols.
MV1544-H1	The inadvertent exposure of sensitive credentials or information during the file transfer process, potentially leading to unauthorized access or data compromise.

3.10.10 Non-Standard Port (T1509) **[728]**

MV Code	Vulnerability Description
MV1509-S1	The potential for misconfiguration, allowing the use of non-standard ports for network traffic, which may bypass filtering or complicate network data analysis.
MV1509-H1	The mismanagement of protocol and port configurations, such as setting up HTTPS over unconventional ports (e.g., port 8088 or port 587), introducing the risk of evasion and hindering effective network monitoring.

3.10.11 Out of Band Data (T1644) **[732]**

MV Code	Vulnerability Description
MV1644-S1	The lack of a more robust permission model or notification system on Android, which could mitigate the risk of users unknowingly granting excessive permissions to applications.
MV1644-H1	The granting of notification access to applications on Android, allowing them to read push notifications and capture content from SMS messages or other out-of-band data streams, potentially compromising sensitive information.

3.10.12 Remote Access Software (T1663) **[743]**

MV Code	Vulnerability Description
MV1663-S1	The security weaknesses in legitimate remote access software, such as VNC, TeamViewer, AirDroid, AirMirror, etc., that may be used as an interactive command and control channel for unauthorized access to target mobile devices.
MV1663-H1	The inadvertent installation and use of remote access applications post-compromise, providing adversaries with an alternate communication channel for redundant access or establishing interactive remote sessions on the compromised device.

MV1663-H2	The potential failure of an enterprise policy to adequately enforce restrictions on the installation of specific remote access applications on managed devices, allowing adversaries to exploit legitimate software for unauthorized access.
MV1663-H3	The inadvertent granting of dangerous permissions, such as device administrator or access to device accessibility, due to a lack of user awareness or caution, potentially facilitating malicious actions by adversaries on the compromised device.

3.10.13 Web Service (T1481) [765]

MV Code	Vulnerability Description
MV1481-S1	The reliance on existing, legitimate external Web services as a means for relaying data, which introduces the risk of adversaries exploiting these services to establish command and control channels, leveraging the likelihood of hosts within a network already communicating with them.
MV1481-H1	The potential for inadvertently using popular websites and social media for malicious command and control activities, as adversaries may exploit the user's routine interactions with these services to hide within expected network noise, highlighting the importance of user awareness and vigilance.

3.10.14 Web Service: Dead Drop Resolver (T1481.001) [766]

MV Code	Vulnerability Description
MV1481.001-S1	The reliance on legitimate external web services, such as popular websites and social media, as dead drop resolvers, which provides cover due to pre-existing communication within the network and the use of SSL/TLS encryption, making it easier for adversaries to hide in expected noise.

MV1481.001-H1	The potential oversight or lack of awareness, leading to unwitting interaction with seemingly legitimate content on common services like Google or Twitter, facilitating the use of dead drop resolvers by adversaries.

3.10.15 Web Service: Bidirectional Communication (T1481.002) [767]

MV Code	Vulnerability Description
MV1481.002-S1	The reliance on existing, legitimate external web service channels for bidirectional communication, providing a potential avenue for adversaries to send commands and receive outputs from compromised systems.
MV1481.002-H1	Potential human error in not recognizing or preventing the use of popular websites and social media for command and control (C2) instructions, allowing adversaries to exploit these platforms for covert communication with compromised systems.

3.10.16 Web Service: One-Way Communication (T1481.003) [768]

MV Code	Vulnerability Description
MV1481.003-S1	The reliance on common services, such as those provided by Google or Twitter, for C2 communication, leveraging the expected communication noise with these services to obscure malicious activities, making it challenging for defenders to distinguish between normal and malicious traffic.
MV1481.003-H1	The potential failure to adequately monitor and detect unauthorized commands sent through Web service channels, as compromised systems might not receive return output or exhibit unusual behavior when processing C2 instructions, leading to a lack of timely response to the security threat.

3.11 Exfiltration (TA0036) [28]

3.11.1 Exfiltration Over Alternative Protocol (T1639) [691]

MV Code	Vulnerability Description
MV1639-S1	The potential weakness in the system's network security, allowing adversaries to exploit alternate protocols like FTP, SMTP, HTTP/S, DNS, SMB, or other unused network protocols for exfiltrating data.
MV1639-H1	Human mistakes in configuring and monitoring network security, leading to the inadvertent allowance of data exfiltration over alternative protocols due to misconfigurations in firewalls or security policies.

3.11.2 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (T1639.001) [692]

MV Code	Vulnerability Description
MV1639.001-S1	The lack of encryption in certain network protocols (e.g., HTTP, FTP, DNS), allowing adversaries to exfiltrate data over these unencrypted channels.
MV1639.001-H1	Choosing not to implement encryption for data transfer over network protocols, leaving the data susceptible to interception during exfiltration.

3.11.3 Exfiltration Over C2 Channel (T1646) [693]

MV Code	Vulnerability Description
MV1646-S1	The potential weakness in the command and control channel, allowing for data exfiltration without detection.
MV1646-H1	The failure to implement proper data encryption or obfuscation within the command and control channel, enabling the adversary to easily encode stolen data into normal communications.

3.12 Impact (TA0034) [29]

3.12.1 Account Access Removal (T1640) [658]

MV Code	Vulnerability Description
MV1640-S1	The lack of robust access controls, allowing unauthorized deletion, locking, or manipulation of user accounts.
MV1640-H1	Weak or easily guessable passwords, enabling adversaries to change credentials and gain unauthorized access to accounts.
MV1640-H2	User may inadvertently grants excessive access to applications, leading to increased risks of unauthorized account access or manipulation.

3.12.2 Call Control (T1616) [666]

MV Code	Vulnerability Description
MV1616-S1	The lack of sufficient safeguards or warnings in the Android operating system, allowing users to change their default call handler to unrecognized applications easily, which may expose them to malicious activities.
MV1616-H1	User inadvertently grants sensitive permissions, such as ANSWER_PHONE_CALLS, CALL_PHONE, PROCESS_OUTGOING_CALLS, MANAGE_OWN_CALLS, BIND_TELECOM_CONNECTION_SERVICE, and WRITE_CALL_LOG, which can lead to unauthorized manipulation of phone calls, compromising the device's integrity and user privacy.
MV1616-H2	User might inadvertently change their default call handler to unrecognized applications due to a lack of awareness or understanding of the potential risks, contributing to the vulnerability of unauthorized phone call manipulation.

3.12.3 Data Destruction (T1662) [674]

MV Code	Vulnerability Description
MV1662-S1	The lack of robust access controls and permissions enforcement, allowing the use of commands such as pm uninstall and rm to uninstall packages and delete specific files.
MV1662-H1	The failure to implement adequate data backup mechanisms, resulting in the irrecoverability of destroyed data due to the lack of proper safeguards.
MV1662-H2	User inadvertently grants device administrator permissions to phishing popups, as the user may not be adequately trained to recognize legitimate prompts, leading to unauthorized access and malicious activities.

3.12.4 Data Encrypted for Impact (T1471) [675]

MV Code	Vulnerability Description
MV1471-S1	The lack of robust file encryption mechanisms, allowing the adversary to exploit and encrypt files on the mobile device.
MV1471-H1	The failure to implement secure backup practices, leading to the risk of permanent data loss if the decryption key is not saved or transmitted.

3.12.5 Data Manipulation (T1641) [677]

MV Code	Vulnerability Description
MV1641-S1	Weaknesses in data integrity mechanisms within the target system, allowing them to insert, delete, or alter data to manipulate external outcomes.
MV1641-H1	User uses outdated operating systems, which may lack the security features and access controls present in more recent versions, potentially facilitating Data Manipulation by adversaries.

3.12.6 Data Manipulation: Transmitted Data Manipulation (T1641.001) [678]

MV Code	Vulnerability Description
MV1641.001-S1	The susceptibility to clipboard manipulation, where malicious applications can monitor clipboard activity on Android devices without explicit permissions, enabling adversaries to read and modify clipboard contents, such as replacing copied Bitcoin wallet addresses with those under adversarial control.
MV1641.001-H1	User fails to update to the latest Android OS version, leaving the system exposed to clipboard manipulation by adversaries as the mitigation is specifically implemented in Android 10 and may not be present in earlier versions.

3.12.7 Endpoint Denial of Service (T1642) [686]

MV Code	Vulnerability Description
MV1642-S1	The ability of Android versions prior to 7 to allow apps with Device Administrator access to reset the device lock passcode, thereby preventing the user from unlocking the device.
MV1642-H1	User may jailbreak iOS devices, where malware can be introduced, locking the user out of the device.
MV1642-H2	User uses the outdated OS version on Android devices prior to version 7, which allows abuse of Device Administrator access to reset the device lock passcode.
MV1642-H3	User grants administrative access to applications, as cautioned against in the mitigation strategy, leading to the exploitation of the Android Device Administrator API.

3.12.8 Generate Traffic from Victim (T1643) **[699]**

MV Code	Vulnerability Description
MV1643-S1	The lack of proper permission controls on Android devices, specifically the requirement for Android apps to hold the SEND_SMS permission, potentially enabling unauthorized generation of outbound SMS traffic.
MV1643-H1	User inadvertently grants consent to send SMS messages to premium numbers, as sending an SMS message to such numbers requires user consent, thereby exposing the system to carrier billing fraud.
MV1643-H2	The lack of user awareness, as users may not be adequately informed that applications generally do not require permission to send SMS messages, leading to a potential oversight in granting unnecessary permissions.

3.12.9 Input Injection (T1516) **[718]**

MV Code	Vulnerability Description
MV1516-S1	The inadequacy in the implementation of the Android DevicePolicyManager.setPermittedAccessibilityServices method, leading to misconfigurations that may inadvertently permit unauthorized applications to exploit accessibility features.
MV1516-H1	User inadvertently installs malicious applications that exploit the system's accessibility APIs, enabling input injection and posing a risk of unauthorized transactions or actions initiated by the adversary.
MV1516-H2	User inadvertently approve dangerous permissions for applications, potentially allowing malicious actors to manipulate accessibility features

3.12.10 Network Denial of Service (T1464) **[726]**

MV Code	Vulnerability Description
MV1464-S1	The susceptibility to network bandwidth exhaustion, potentially leading to degraded or blocked availability of targeted resources.

3.12.11 SMS Control (T1582) **[747]**

MV Code	Vulnerability Description
MV1582-S1	The lack of robust controls or restrictions on SMS permissions, allowing applications to potentially misuse SMS access for malicious purposes.
MV1582-H1	User grants excessive permissions to malicious applications, such as setting the app as the default SMS handler, which enables unauthorized access to the messaging database and manipulation of SMS messages on the device.

4 Summary

In this technical report, we outline our methodology for leveraging the capabilities of OpenAI's ChatGPT [781] to identify vulnerabilities associated with each MITRE ATT&CK technique. Subsequently, the report provides a comprehensive catalog of enterprise and mobile vulnerabilities, serving as essential elements for the modeling and simulation of authentic interactions between cybercriminal agents and device agents within targeted organizations. These vulnerabilities manifest within genuine organizational contexts due to a variety of factors, including specific human behaviors, organizational policies, and the diverse operating systems employed in computing devices. By utilizing the vulnerability list presented in this technical report, modelers can replicate similar environments by designing device agents with specific system vulnerabilities that may be exploited by cybercriminal agents. Similarly, human agents can be modeled with the potential to exhibit specific human vulnerabilities based on their behaviors. The presence of vulnerabilities within the target device or human is crucial for a cybercriminal agent to execute a successful attack technique. This criterion enables a more realistic portrayal of the success or failure of each attempted attack, thereby enhancing the authenticity of decision-making processes throughout a cyber attack campaign. Furthermore, modelers can assess various defense strategies by mitigating existing vulnerabilities in the model, providing an accurate evaluation of the effectiveness of each defense strategy.

In summary, the compilation of vulnerabilities in this report is intended to replicate real-world organizational scenarios with greater fidelity. This, in turn, facilitates the development of cyber attack campaign and defense strategy simulations that closely mirror reality, enabling more accurate and insightful analyses of cyber attack and defense strategies.

5 Reference

[1] "MITRE ATT&CK®." MITRE ATT&CK®, attack.mitre.org/. Accessed 23 Dec. 2023.

[2] "Enterprise Tactics." Tactics - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/enterprise/. Accessed 23 Dec. 2023.

[3] "Mobile Tactics." Tactics - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/mobile/. Accessed 23 Dec. 2023.

[4] "Reconnaissance." Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0043/. Accessed 22 Dec. 2023.

[5] "Resource Development." Resource Development, Tactic TA0042 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0042/. Accessed 22 Dec. 2023.

[6] "Initial Access." Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0001/. Accessed 22 Dec. 2023.

[7] "Execution." Execution, Tactic TA0002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0002/. Accessed 22 Dec. 2023.

[8] "Persistence." Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0003/. Accessed 22 Dec. 2023.

[9] "Privilege Escalation." Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0004/. Accessed 22 Dec. 2023.

[10] "Defense Evasion." Defense Evasion, Tactic TA0005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0005/. Accessed 22 Dec. 2023.

[11] "Credential Access." Credential Access, Tactic TA0006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0006/. Accessed 22 Dec. 2023.

[12] "Discovery." Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0007/. Accessed 22 Dec. 2023.

[13] "Lateral Movement." Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0008/. Accessed 22 Dec. 2023.

[14] "Collection." Collection, Tactic TA0009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0009/. Accessed 22 Dec. 2023.

[15] "Command and Control." Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0011/. Accessed 22 Dec. 2023.

[16] "Exfiltration." Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0010/. Accessed 22 Dec. 2023.

[17] "Impact." Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®, attack.mitre.org/tactics/TA0040/. Accessed 22 Dec. 2023.

[18] "Initial Access." Initial Access, Tactic TA0027 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0027/. Accessed 22 Dec. 2023.

[19] "Execution." Execution, Tactic TA0041 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0041/. Accessed 22 Dec. 2023.

[20] “Persistence.” Persistence, Tactic TA0028 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0028/. Accessed 22 Dec. 2023.

[21] “Privilege Escalation.” Privilege Escalation, Tactic TA0029 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0029/. Accessed 22 Dec. 2023.

[22] “Defense Evasion.” Defense Evasion, Tactic TA0030 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0030/. Accessed 22 Dec. 2023.

[23] “Credential Access.” Credential Access, Tactic TA0031 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0031/. Accessed 22 Dec. 2023.

[24] “Discovery.” Discovery, Tactic TA0032 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0032/. Accessed 22 Dec. 2023.

[25] “Lateral Movement.” Lateral Movement, Tactic TA0033 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0033/. Accessed 22 Dec. 2023.

[26] “Collection.” Collection, Tactic TA0035 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0035/. Accessed 22 Dec. 2023.

[27] “Command and Control.” Command and Control, Tactic TA0037 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0037/. Accessed 22 Dec. 2023.

[28] “Exfiltration.” Exfiltration, Tactic TA0036 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0036/. Accessed 22 Dec. 2023.

[29] “Impact.” Impact, Tactic TA0034 - Mobile | MITRE ATT&CK®, attack.mitre.org/tactics/TA0034/. Accessed 22 Dec. 2023.

[30] “Abuse Elevation Control Mechanism.” Abuse Elevation Control Mechanism, Technique T1548 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/. Accessed 22 Dec. 2023.

[31] “Abuse Elevation Control Mechanism: Setuid and Setgid.” Abuse Elevation Control Mechanism: Setuid and Setgid, Sub-Technique T1548.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/001/. Accessed 22 Dec. 2023.

[32] “Abuse Elevation Control Mechanism: Bypass User Account Control.” Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-Technique T1548.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/002/. Accessed 22 Dec. 2023.

[33] “Abuse Elevation Control Mechanism: Sudo and Sudo Caching.” Abuse Elevation Control Mechanism: Sudo and Sudo Caching, Sub-Technique T1548.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/003/. Accessed 22 Dec. 2023.

[34] “Abuse Elevation Control Mechanism: Elevated Execution with Prompt.” Abuse Elevation Control Mechanism: Elevated Execution with Prompt, Sub-Technique T1548.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/004/. Accessed 22 Dec. 2023.

[35] “Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access.” Abuse Elevation Control Mechanism: Temporary Elevated Cloud Access, Sub-Technique T1548.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1548/005/. Accessed 22 Dec. 2023.

[36] “Access Token Manipulation.” Access Token Manipulation, Technique T1134 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/. Accessed 22 Dec. 2023.

[37] “Access Token Manipulation: Token Impersonation/Theft.” Access Token Manipulation: Token Impersonation/Theft, Sub-Technique T1134.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/001/. Accessed 22 Dec. 2023.

[38] “Access Token Manipulation: Create Process with Token.” Access Token Manipulation: Create Process with Token, Sub-Technique T1134.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/002/. Accessed 22 Dec. 2023.

[39] “Access Token Manipulation: Make and Impersonate Token.” Access Token Manipulation: Make and Impersonate Token, Sub-Technique T1134.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/003/. Accessed 22 Dec. 2023.

[40] “Access Token Manipulation: Parent PID Spoofing.” Access Token Manipulation: Parent PID Spoofing, Sub-Technique T1134.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/004/. Accessed 22 Dec. 2023.

[41] “Access Token Manipulation: Sid-History Injection.” Access Token Manipulation: SID-History Injection, Sub-Technique T1134.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1134/005/. Accessed 22 Dec. 2023.

[42] “Account Access Removal.” Account Access Removal, Technique T1531 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1531/. Accessed 22 Dec. 2023.

[43] “Account Discovery.” Account Discovery, Technique T1087 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1087/. Accessed 22 Dec. 2023.

[44] “Account Discovery: Local Account.” Account Discovery: Local Account, Sub-Technique T1087.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1087/001/. Accessed 22 Dec. 2023.

[45] “Account Discovery: Domain Account.” Account Discovery: Domain Account, Sub-Technique T1087.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1087/002/. Accessed 22 Dec. 2023.

[46] “Account Discovery: Email Account.” Account Discovery: Email Account, Sub-Technique T1087.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1087/003/. Accessed 22 Dec. 2023.

[47] “Account Discovery: Cloud Account.” Account Discovery: Cloud Account, Sub-Technique T1087.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1087/004/. Accessed 22 Dec. 2023.

[48] “Account Manipulation.” Account Manipulation, Technique T1098 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/. Accessed 22 Dec. 2023.

[49] “Account Manipulation: Additional Cloud Credentials.” Account Manipulation: Additional Cloud Credentials, Sub-Technique T1098.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/001/. Accessed 22 Dec. 2023.

[50] “Account Manipulation: Additional Email Delegate Permissions.” Account Manipulation: Additional Email Delegate Permissions, Sub-Technique T1098.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/002/. Accessed 22 Dec. 2023.

[51] “Account Manipulation: Additional Cloud Roles.” Account Manipulation: Additional Cloud Roles, Sub-Technique T1098.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/003/. Accessed 22 Dec. 2023.

[52] “Account Manipulation: SSH Authorized Keys.” Account Manipulation: SSH Authorized Keys, Sub-Technique T1098.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/004/. Accessed 22 Dec. 2023.

[53] “Account Manipulation: Device Registration.” Account Manipulation: Device Registration, Sub-Technique T1098.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/005/. Accessed 22 Dec. 2023.

[54] “Account Manipulation: Additional Container Cluster Roles.” Account Manipulation: Additional Container Cluster Roles, Sub-Technique T1098.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1098/006/. Accessed 22 Dec. 2023.

[55] “Acquire Access.” Acquire Access, Technique T1650 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1650/. Accessed 22 Dec. 2023.

[56] “Acquire Infrastructure.” Acquire Infrastructure, Technique T1583 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/. Accessed 22 Dec. 2023.

[57] “Acquire Infrastructure: Domains.” Acquire Infrastructure: Domains, Sub-Technique T1583.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/001/. Accessed 22 Dec. 2023.

[58] “Acquire Infrastructure: DNS Server.” Acquire Infrastructure: DNS Server, Sub-Technique T1583.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/002/. Accessed 22 Dec. 2023.

[59] “Acquire Infrastructure: Virtual Private Server.” Acquire Infrastructure: Virtual Private Server, Sub-Technique T1583.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/003/. Accessed 22 Dec. 2023.

[60] “Acquire Infrastructure: Server.” Acquire Infrastructure: Server, Sub-Technique T1583.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/004/. Accessed 22 Dec. 2023.

[61] “Acquire Infrastructure: Botnet.” Acquire Infrastructure: Botnet, Sub-Technique T1583.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/005/. Accessed 22 Dec. 2023.

[62] “Acquire Infrastructure: Web Services.” Acquire Infrastructure: Web Services, Sub-Technique T1583.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/006/. Accessed 22 Dec. 2023.

[63] “Acquire Infrastructure: Serverless.” Acquire Infrastructure: Serverless, Sub-Technique T1583.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/007/. Accessed 22 Dec. 2023.

[64] “Acquire Infrastructure: Malvertising.” Acquire Infrastructure: Malvertising, Sub-Technique T1583.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1583/008/. Accessed 22 Dec. 2023.

[65] “Active Scanning.” Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1595/. Accessed 22 Dec. 2023.

[66] “Active Scanning: Scanning IP Blocks.” Active Scanning: Scanning IP Blocks, Sub-Technique T1595.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1595/001/. Accessed 22 Dec. 2023.

[67] “Active Scanning: Vulnerability Scanning.” Active Scanning: Vulnerability Scanning, Sub-Technique T1595.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1595/002/. Accessed 22 Dec. 2023.

[68] “Active Scanning: Wordlist Scanning.” Active Scanning: Wordlist Scanning, Sub-Technique T1595.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1595/003/. Accessed 22 Dec. 2023.

[69] “Adversary-in-the-Middle.” Adversary-in-the-Middle, Technique T1557 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1557/. Accessed 22 Dec. 2023.

[70] “Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay.” Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Sub-Technique T1557.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1557/001/. Accessed 22 Dec. 2023.

[71] “Adversary-in-the-Middle: Arp Cache Poisoning.” Adversary-in-the-Middle: ARP Cache Poisoning, Sub-Technique T1557.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1557/002/. Accessed 22 Dec. 2023.

[72] “Adversary-in-the-Middle: DHCP Spoofing.” Adversary-in-the-Middle: DHCP Spoofing, Sub-Technique T1557.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1557/003/. Accessed 22 Dec. 2023.

[73] “Application Layer Protocol.” Application Layer Protocol, Technique T1071 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1071/. Accessed 22 Dec. 2023.

[74] “Application Layer Protocol: Web Protocols.” Application Layer Protocol: Web Protocols, Sub-Technique T1071.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1071/001/. Accessed 22 Dec. 2023.

[75] “Application Layer Protocol: File Transfer Protocols.” Application Layer Protocol: File Transfer Protocols, Sub-Technique T1071.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1071/002/. Accessed 22 Dec. 2023.

[76] “Application Layer Protocol: Mail Protocols.” Application Layer Protocol: Mail Protocols, Sub-Technique T1071.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1071/003/. Accessed 22 Dec. 2023.

[77] “Application Layer Protocol: DNS.” Application Layer Protocol: DNS, Sub-Technique T1071.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1071/004/. Accessed 22 Dec. 2023.

[78] “Application Window Discovery.” Application Window Discovery, Technique T1010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1010/. Accessed 22 Dec. 2023.

[79] “Archive Collected Data.” Archive Collected Data, Technique T1560 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1560/. Accessed 22 Dec. 2023.

[80] “Archive Collected Data: Archive via Utility.” Archive Collected Data: Archive via Utility, Sub-Technique T1560.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1560/001/. Accessed 22 Dec. 2023.

[81] “Archive Collected Data: Archive via Library.” Archive Collected Data: Archive via Library, Sub-Technique T1560.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1560/002/. Accessed 22 Dec. 2023.

[82] “Archive Collected Data: Archive via Custom Method.” Archive Collected Data: Archive via Custom Method, Sub-Technique T1560.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1560/003/. Accessed 22 Dec. 2023.

[83] “Audio Capture.” Audio Capture, Technique T1123 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1123/. Accessed 22 Dec. 2023.

[84] “Automated Collection.” Automated Collection, Technique T1119 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1119/. Accessed 22 Dec. 2023.

[85] “Automated Exfiltration.” Automated Exfiltration, Technique T1020 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1020/. Accessed 22 Dec. 2023.

[86] “Automated Exfiltration: Traffic Duplication.” Automated Exfiltration: Traffic Duplication, Sub-Technique T1020.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1020/001/. Accessed 22 Dec. 2023.

[87] “Bits Jobs.” BITS Jobs, Technique T1197 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1197/. Accessed 22 Dec. 2023.

[88] “Boot or Logon Autostart Execution.” Boot or Logon Autostart Execution, Technique T1547 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/. Accessed 22 Dec. 2023.

[89] “Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder.” Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-Technique T1547.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/001/. Accessed 22 Dec. 2023.

[90] “Boot or Logon Autostart Execution: Authentication Package.” Boot or Logon Autostart Execution: Authentication Package, Sub-Technique T1547.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/002/. Accessed 22 Dec. 2023.

[91] “Boot or Logon Autostart Execution: Time Providers.” Boot or Logon Autostart Execution: Time Providers, Sub-Technique T1547.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/003/. Accessed 22 Dec. 2023.

[92] “Boot or Logon Autostart Execution: Winlogon Helper DLL.” Boot or Logon Autostart Execution: Winlogon Helper DLL, Sub-Technique T1547.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/004/. Accessed 22 Dec. 2023.

[93] “Boot or Logon Autostart Execution: Security Support Provider.” Boot or Logon Autostart Execution: Security Support Provider, Sub-Technique T1547.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/005/. Accessed 22 Dec. 2023.

[94] “Boot or Logon Autostart Execution: Kernel Modules and Extensions.” Boot or Logon Autostart Execution: Kernel Modules and Extensions, Sub-Technique T1547.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/006/. Accessed 22 Dec. 2023.

[95] “Boot or Logon Autostart Execution: Re-Opened Applications.” Re, attack.mitre.org/techniques/T1547/007/. Accessed 22 Dec. 2023.

[96] “Boot or Logon Autostart Execution: LSASS Driver.” Boot or Logon Autostart Execution: LSASS Driver, Sub-Technique T1547.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/008/. Accessed 22 Dec. 2023.

[97] “Boot or Logon Autostart Execution: Shortcut Modification.” Boot or Logon Autostart Execution: Shortcut Modification, Sub-Technique T1547.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/009/. Accessed 22 Dec. 2023.

[98] “Boot or Logon Autostart Execution: Port Monitors.” Boot or Logon Autostart Execution: Port Monitors, Sub-Technique T1547.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/010/. Accessed 22 Dec. 2023.

[99] “Boot or Logon Autostart Execution: Print Processors.” Boot or Logon Autostart Execution: Print Processors, Sub-Technique T1547.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/012/. Accessed 22 Dec. 2023.

[100] “Boot or Logon Autostart Execution: XDG Autostart Entries.” Boot or Logon Autostart Execution: XDG Autostart Entries, Sub-Technique T1547.013 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/013/. Accessed 22 Dec. 2023.

[101] “Boot or Logon Autostart Execution: Active Setup.” Boot or Logon Autostart Execution: Active Setup, Sub-Technique T1547.014 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/014/. Accessed 22 Dec. 2023.

[102] “Boot or Logon Autostart Execution: Login Items.” Boot or Logon Autostart Execution: Login Items, Sub-Technique T1547.015 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1547/015/. Accessed 22 Dec. 2023.

[103] “Boot or Logon Initialization Scripts.” Boot or Logon Initialization Scripts, Technique T1037 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/. Accessed 22 Dec. 2023.

[104] “Boot or Logon Initialization Scripts: Logon Script (Windows).” Boot or Logon Initialization Scripts: Logon Script (Windows), Sub-Technique T1037.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/001/. Accessed 22 Dec. 2023.

[105] “Boot or Logon Initialization Scripts: Login Hook.” Boot or Logon Initialization Scripts: Login Hook, Sub-Technique T1037.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/002/. Accessed 22 Dec. 2023.

[106] “Boot or Logon Initialization Scripts: Network Logon Script.” Boot or Logon Initialization Scripts: Network Logon Script, Sub-Technique T1037.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/003/. Accessed 22 Dec. 2023.

[107] “Boot or Logon Initialization Scripts: RC Scripts.” Boot or Logon Initialization Scripts: RC Scripts, Sub-Technique T1037.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/004/. Accessed 22 Dec. 2023.

[108] “Boot or Logon Initialization Scripts: Startup Items.” Boot or Logon Initialization Scripts: Startup Items, Sub-Technique T1037.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1037/005/. Accessed 22 Dec. 2023.

[109] “Browser Extensions.” Browser Extensions, Technique T1176 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1176/. Accessed 22 Dec. 2023.

[110] “Browser Information Discovery.” Browser Information Discovery, Technique T1217 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1217/. Accessed 22 Dec. 2023.

[111] “Browser Session Hijacking.” Browser Session Hijacking, Technique T1185 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1185/. Accessed 22 Dec. 2023.

[112] “Brute Force.” Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1110/. Accessed 22 Dec. 2023.

[113] “Brute Force: Password Guessing.” Brute Force: Password Guessing, Sub-Technique T1110.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1110/001/. Accessed 22 Dec. 2023.

[114] “Brute Force: Password Cracking.” Brute Force: Password Cracking, Sub-Technique T1110.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1110/002/. Accessed 22 Dec. 2023.

[115] “Brute Force: Password Spraying.” Brute Force: Password Spraying, Sub-Technique T1110.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1110/003/. Accessed 22 Dec. 2023.

[116] “Brute Force: Credential Stuffing.” Brute Force: Credential Stuffing, Sub-Technique T1110.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1110/004/. Accessed 22 Dec. 2023.

[117] “Build Image on Host.” Build Image on Host, Technique T1612 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1612/. Accessed 22 Dec. 2023.

[118] “Clipboard Data.” Clipboard Data, Technique T1115 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1115/. Accessed 22 Dec. 2023.

[119] “Cloud Administration Command.” Cloud Administration Command, Technique T1651 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1651/. Accessed 22 Dec. 2023.

[120] “Cloud Infrastructure Discovery.” Cloud Infrastructure Discovery, Technique T1580 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1580/. Accessed 22 Dec. 2023.

[121] “Cloud Service Dashboard.” Cloud Service Dashboard, Technique T1538 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1538/. Accessed 22 Dec. 2023.

[122] “Cloud Service Discovery.” Cloud Service Discovery, Technique T1526 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1526/. Accessed 22 Dec. 2023.

[123] “Cloud Storage Object Discovery.” Cloud Storage Object Discovery, Technique T1619 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1619/. Accessed 22 Dec. 2023.

[124] “Command and Scripting Interpreter.” Command and Scripting Interpreter, Technique T1059 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/. Accessed 22 Dec. 2023.

[125] “Command and Scripting Interpreter: PowerShell.” Command and Scripting Interpreter: PowerShell, Sub-Technique T1059.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/001/. Accessed 22 Dec. 2023.

[126] "Command and Scripting Interpreter: Applescript." Command and Scripting Interpreter: AppleScript, Sub-Technique T1059.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/002/. Accessed 22 Dec. 2023.

[127] "Command and Scripting Interpreter: Windows Command Shell." Command and Scripting Interpreter: Windows Command Shell, Sub-Technique T1059.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/003/. Accessed 22 Dec. 2023.

[128] "Command and Scripting Interpreter: Unix Shell." Command and Scripting Interpreter: Unix Shell, Sub-Technique T1059.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/004/. Accessed 22 Dec. 2023.

[129] "Command and Scripting Interpreter: Visual Basic." Command and Scripting Interpreter: Visual Basic, Sub-Technique T1059.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/005/. Accessed 22 Dec. 2023.

[130] "Command and Scripting Interpreter: Python." Command and Scripting Interpreter: Python, Sub-Technique T1059.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/006/. Accessed 22 Dec. 2023.

[131] "Command and Scripting Interpreter: JavaScript." Command and Scripting Interpreter: JavaScript, Sub-Technique T1059.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/007/. Accessed 22 Dec. 2023.

[132] "Command and Scripting Interpreter: Network Device CLI." Command and Scripting Interpreter: Network Device CLI, Sub-Technique T1059.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/008/. Accessed 22 Dec. 2023.

[133] "Command and Scripting Interpreter: Cloud API." Command and Scripting Interpreter: Cloud API, Sub-Technique T1059.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1059/009/. Accessed 22 Dec. 2023.

[134] "Communication through Removable Media." Communication Through Removable Media, Technique T1092 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1092/. Accessed 22 Dec. 2023.

[135] "Compromise Accounts." Compromise Accounts, Technique T1586 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1586/. Accessed 22 Dec. 2023.

[136] "Compromise Accounts: Social Media Accounts." Compromise Accounts: Social Media Accounts, Sub-Technique T1586.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1586/001/. Accessed 22 Dec. 2023.

[137] "Compromise Accounts: Email Accounts." Compromise Accounts: Email Accounts, Sub-Technique T1586.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1586/002/. Accessed 22 Dec. 2023.

[138] "Compromise Accounts: Cloud Accounts." Compromise Accounts: Cloud Accounts, Sub-Technique T1586.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1586/003/. Accessed 22 Dec. 2023.

[139] "Compromise Client Software Binary." Compromise Client Software Binary, Technique T1554 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1554/. Accessed 22 Dec. 2023.

[140] “Compromise Infrastructure.” Compromise Infrastructure, Technique T1584 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/. Accessed 22 Dec. 2023.

[141] “Compromise Infrastructure: Domains.” Compromise Infrastructure: Domains, Sub-Technique T1584.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/001/. Accessed 22 Dec. 2023.

[142] “Compromise Infrastructure: DNS Server.” Compromise Infrastructure: DNS Server, Sub-Technique T1584.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/002/. Accessed 22 Dec. 2023.

[143] “Compromise Infrastructure: Virtual Private Server.” Compromise Infrastructure: Virtual Private Server, Sub-Technique T1584.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/003/. Accessed 22 Dec. 2023.

[144] “Compromise Infrastructure: Server.” Compromise Infrastructure: Server, Sub-Technique T1584.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/004/. Accessed 22 Dec. 2023.

[145] “Compromise Infrastructure: Botnet.” Compromise Infrastructure: Botnet, Sub-Technique T1584.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/005/. Accessed 22 Dec. 2023.

[146] “Compromise Infrastructure: Web Services.” Compromise Infrastructure: Web Services, Sub-Technique T1584.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/006/. Accessed 22 Dec. 2023.

[147] “Compromise Infrastructure: Serverless.” Compromise Infrastructure: Serverless, Sub-Technique T1584.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1584/007/. Accessed 22 Dec. 2023.

[148] “Container Administration Command.” Container Administration Command, Technique T1609 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1609/. Accessed 22 Dec. 2023.

[149] “Container and Resource Discovery.” Container and Resource Discovery, Technique T1613 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1613/. Accessed 22 Dec. 2023.

[150] “Content Injection.” Content Injection, Technique T1659 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1659/. Accessed 22 Dec. 2023.

[151] “Create Account.” Create Account, Technique T1136 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1136/. Accessed 22 Dec. 2023.

[152] “Create Account: Local Account.” Create Account: Local Account, Sub-Technique T1136.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1136/001/. Accessed 22 Dec. 2023.

[153] “Create Account: Domain Account.” Create Account: Domain Account, Sub-Technique T1136.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1136/002/. Accessed 22 Dec. 2023.

[154] “Create Account: Cloud Account.” Create Account: Cloud Account, Sub-Technique T1136.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1136/003/. Accessed 22 Dec. 2023.

[155] “Create or Modify System Process.” Create or Modify System Process, Technique T1543 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1543/. Accessed 22 Dec. 2023.

[156] “Create or Modify System Process: Launch Agent.” Create or Modify System Process: Launch Agent, Sub-Technique T1543.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1543/001/. Accessed 22 Dec. 2023.

[157] “Create or Modify System Process: Systemd Service.” Create or Modify System Process: Systemd Service, Sub-Technique T1543.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1543/002/. Accessed 22 Dec. 2023.

[158] “Create or Modify System Process: Windows Service.” Create or Modify System Process: Windows Service, Sub-Technique T1543.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1543/003/. Accessed 22 Dec. 2023.

[159] “Create or Modify System Process: Launch Daemon.” Create or Modify System Process: Launch Daemon, Sub-Technique T1543.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1543/004/. Accessed 22 Dec. 2023.

[160] “Credentials from Password Stores.” Credentials from Password Stores, Technique T1555 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/. Accessed 22 Dec. 2023.

[161] “Credentials from Password Stores: Keychain.” Credentials from Password Stores: Keychain, Sub-Technique T1555.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/001/. Accessed 22 Dec. 2023.

[162] “Credentials from Password Stores: Securityd Memory.” Credentials from Password Stores: Securityd Memory, Sub-Technique T1555.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/002/. Accessed 22 Dec. 2023.

[163] “Credentials from Password Stores: Credentials from Web Browsers.” Credentials from Password Stores: Credentials from Web Browsers, Sub-Technique T1555.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/003/. Accessed 22 Dec. 2023.

[164] “Credentials from Password Stores: Windows Credential Manager.” Credentials from Password Stores: Windows Credential Manager, Sub-Technique T1555.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/004/. Accessed 22 Dec. 2023.

[165] “Credentials from Password Stores: Password Managers.” Credentials from Password Stores: Password Managers, Sub-Technique T1555.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/005/. Accessed 22 Dec. 2023.

[166] “Credentials from Password Stores: Cloud Secrets Management Stores.” Credentials from Password Stores: Cloud Secrets Management Stores, Sub-Technique T1555.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1555/006/. Accessed 22 Dec. 2023.

[167] “Data Destruction.” Data Destruction, Technique T1485 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1485/. Accessed 22 Dec. 2023.

[168] “Data Encoding.” Data Encoding, Technique T1132 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1132/. Accessed 22 Dec. 2023.

[169] “Data Encoding: Standard Encoding.” Data Encoding: Standard Encoding, Sub-Technique T1132.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1132/001/. Accessed 22 Dec. 2023.

[170] “Data Encoding: Non-Standard Encoding.” Data Encoding: Non-Standard Encoding, Sub-Technique T1132.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1132/002/. Accessed 22 Dec. 2023.

[171] “Data Encrypted for Impact.” Data Encrypted for Impact, Technique T1486 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1486/. Accessed 22 Dec. 2023.

[172] “Data from Cloud Storage.” Data from Cloud Storage, Technique T1530 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1530/. Accessed 22 Dec. 2023.

[173] “Data from Configuration Repository.” Data from Configuration Repository, Technique T1602 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1602/. Accessed 22 Dec. 2023.

[174] “Data from Configuration Repository: SNMP (MIB Dump).” Data from Configuration Repository: SNMP (MIB Dump), Sub-Technique T1602.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1602/001/. Accessed 22 Dec. 2023.

[175] “Data from Configuration Repository: Network Device Configuration Dump.” Data from Configuration Repository: Network Device Configuration Dump, Sub-Technique T1602.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1602/002/. Accessed 22 Dec. 2023.

[176] “Data from Information Repositories.” Data from Information Repositories, Technique T1213 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1213/. Accessed 22 Dec. 2023.

[177] “Data from Information Repositories: Confluence.” Data from Information Repositories: Confluence, Sub-Technique T1213.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1213/001/. Accessed 22 Dec. 2023.

[178] “Data from Information Repositories: Sharepoint.” Data from Information Repositories: Sharepoint, Sub-Technique T1213.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1213/002/. Accessed 22 Dec. 2023.

[179] “Data from Information Repositories: Code Repositories.” Data from Information Repositories: Code Repositories, Sub-Technique T1213.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1213/003/. Accessed 22 Dec. 2023.

[180] “Data from Local System.” Data from Local System, Technique T1005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1005/. Accessed 22 Dec. 2023.

[181] “Data from Network Shared Drive.” Data from Network Shared Drive, Technique T1039 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1039/. Accessed 22 Dec. 2023.

[182] “Data from Removable Media.” Data from Removable Media, Technique T1025 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1025/. Accessed 22 Dec. 2023.

[183] “Data Manipulation.” Data Manipulation, Technique T1565 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1565/. Accessed 22 Dec. 2023.

[184] “Data Manipulation: Stored Data Manipulation.” Data Manipulation: Stored Data Manipulation, Sub-Technique T1565.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1565/001/. Accessed 22 Dec. 2023.

[185] “Data Manipulation: Transmitted Data Manipulation.” Data Manipulation: Transmitted Data Manipulation, Sub-Technique T1565.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1565/002/. Accessed 22 Dec. 2023.

[186] “Data Manipulation: Runtime Data Manipulation.” Data Manipulation: Runtime Data Manipulation, Sub-Technique T1565.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1565/003/. Accessed 22 Dec. 2023.

[187] “Data Obfuscation.” Data Obfuscation, Technique T1001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1001/. Accessed 22 Dec. 2023.

[188] “Data Obfuscation: Junk Data.” Data Obfuscation: Junk Data, Sub-Technique T1001.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1001/001/. Accessed 22 Dec. 2023.

[189] “Data Obfuscation: Steganography.” Data Obfuscation: Steganography, Sub-Technique T1001.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1001/002/. Accessed 22 Dec. 2023.

[190] “Data Obfuscation: Protocol Impersonation.” Data Obfuscation: Protocol Impersonation, Sub-Technique T1001.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1001/003/. Accessed 22 Dec. 2023.

[191] “Data Staged.” Data Staged, Technique T1074 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1074/. Accessed 22 Dec. 2023.

[192] “Data Staged: Local Data Staging.” Data Staged: Local Data Staging, Sub-Technique T1074.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1074/001/. Accessed 22 Dec. 2023.

[193] “Data Staged: Remote Data Staging.” Data Staged: Remote Data Staging, Sub-Technique T1074.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1074/002/. Accessed 22 Dec. 2023.

[194] “Data Transfer Size Limits.” Data Transfer Size Limits, Technique T1030 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1030/. Accessed 22 Dec. 2023.

[195] “Debugger Evasion.” Debugger Evasion, Technique T1622 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1622/. Accessed 22 Dec. 2023.

[196] “Defacement.” Defacement, Technique T1491 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1491/. Accessed 22 Dec. 2023.

[197] “Defacement: Internal Defacement.” Defacement: Internal Defacement, Sub-Technique T1491.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1491/001/. Accessed 22 Dec. 2023.

[198] “Defacement: External Defacement.” Defacement: External Defacement, Sub-Technique T1491.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1491/002/. Accessed 22 Dec. 2023.

[199] “Deobfuscate/Decode Files or Information.” Deobfuscate/Decode Files or Information, Technique T1140 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1140/. Accessed 22 Dec. 2023.

[200] “Deploy Container.” Deploy Container, Technique T1610 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1610/. Accessed 22 Dec. 2023.

[201] “Develop Capabilities.” Develop Capabilities, Technique T1587 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1587/. Accessed 22 Dec. 2023.

[202] “Develop Capabilities: Malware.” Develop Capabilities: Malware, Sub-Technique T1587.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1587/001/. Accessed 22 Dec. 2023.

[203] “Develop Capabilities: Code Signing Certificates.” Develop Capabilities: Code Signing Certificates, Sub-Technique T1587.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1587/002/. Accessed 22 Dec. 2023.

[204] “Develop Capabilities: Digital Certificates.” Develop Capabilities: Digital Certificates, Sub-Technique T1587.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1587/003/. Accessed 22 Dec. 2023.

[205] “Develop Capabilities: Exploits.” Develop Capabilities: Exploits, Sub-Technique T1587.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1587/004/. Accessed 22 Dec. 2023.

[206] “Device Driver Discovery.” Device Driver Discovery, Technique T1652 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1652/. Accessed 22 Dec. 2023.

[207] “Direct Volume Access.” Direct Volume Access, Technique T1006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1006/. Accessed 22 Dec. 2023.

[208] “Disk Wipe.” Disk Wipe, Technique T1561 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1561/. Accessed 22 Dec. 2023.

[209] “Disk Wipe: Disk Content Wipe.” Disk Wipe: Disk Content Wipe, Sub-Technique T1561.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1561/001/. Accessed 22 Dec. 2023.

[210] “Disk Wipe: Disk Structure Wipe.” Disk Wipe: Disk Structure Wipe, Sub-Technique T1561.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1561/002/. Accessed 22 Dec. 2023.

[211] “Domain Policy Modification.” Domain Policy Modification, Technique T1484 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1484/. Accessed 22 Dec. 2023.

[212] “Domain Policy Modification: Group Policy Modification.” Domain Policy Modification: Group Policy Modification, Sub-Technique T1484.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1484/001/. Accessed 22 Dec. 2023.

[213] “Domain Policy Modification: Domain Trust Modification.” Domain Policy Modification: Domain Trust Modification, Sub-Technique T1484.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1484/002/. Accessed 22 Dec. 2023.

[214] “Domain Trust Discovery.” Domain Trust Discovery, Technique T1482 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1482/. Accessed 22 Dec. 2023.

[215] “Drive-by Compromise.” Drive-by Compromise, Technique T1189 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1189/. Accessed 22 Dec. 2023.

[216] “Dynamic Resolution.” Dynamic Resolution, Technique T1568 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1568/. Accessed 22 Dec. 2023.

[217] "Dynamic Resolution: Fast Flux DNS." Dynamic Resolution: Fast Flux DNS, Sub-Technique T1568.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1568/001/. Accessed 22 Dec. 2023.

[218] "Dynamic Resolution: Domain Generation Algorithms." Dynamic Resolution: Domain Generation Algorithms, Sub-Technique T1568.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1568/002/. Accessed 22 Dec. 2023.

[219] "Dynamic Resolution: DNS Calculation." Dynamic Resolution: DNS Calculation, Sub-Technique T1568.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1568/003/. Accessed 22 Dec. 2023.

[220] "Email Collection." Email Collection, Technique T1114 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1114/. Accessed 22 Dec. 2023.

[221] "Email Collection: Local Email Collection." Email Collection: Local Email Collection, Sub-Technique T1114.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1114/001/. Accessed 22 Dec. 2023.

[222] "Email Collection: Remote Email Collection." Email Collection: Remote Email Collection, Sub-Technique T1114.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1114/002/. Accessed 22 Dec. 2023.

[223] "Email Collection: Email Forwarding Rule." Email Collection: Email Forwarding Rule, Sub-Technique T1114.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1114/003/. Accessed 22 Dec. 2023.

[224] "Encrypted Channel." Encrypted Channel, Technique T1573 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1573/. Accessed 22 Dec. 2023.

[225] "Encrypted Channel: Symmetric Cryptography." Encrypted Channel: Symmetric Cryptography, Sub-Technique T1573.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1573/001/. Accessed 22 Dec. 2023.

[226] "Encrypted Channel: Asymmetric Cryptography." Encrypted Channel: Asymmetric Cryptography, Sub-Technique T1573.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1573/002/. Accessed 22 Dec. 2023.

[227] "Endpoint Denial of Service." Endpoint Denial of Service, Technique T1499 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1499/. Accessed 22 Dec. 2023.

[228] "Endpoint Denial of Service: Os Exhaustion Flood." Endpoint Denial of Service: OS Exhaustion Flood, Sub-Technique T1499.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1499/001/. Accessed 22 Dec. 2023.

[229] "Endpoint Denial of Service: Service Exhaustion Flood." Endpoint Denial of Service: Service Exhaustion Flood, Sub-Technique T1499.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1499/002/. Accessed 22 Dec. 2023.

[230] "Endpoint Denial of Service: Application Exhaustion Flood." Endpoint Denial of Service: Application Exhaustion Flood, Sub-Technique T1499.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1499/003/. Accessed 22 Dec. 2023.

[231] "Endpoint Denial of Service: Application or System Exploitation." Endpoint Denial of Service: Application or System Exploitation, Sub-Technique T1499.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1499/004/. Accessed 22 Dec. 2023.

[232] “Escape to Host.” Escape to Host, Technique T1611 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1611/. Accessed 22 Dec. 2023.

[233] “Establish Accounts.” Establish Accounts, Technique T1585 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1585/. Accessed 22 Dec. 2023.

[234] “Establish Accounts: Social Media Accounts.” Establish Accounts: Social Media Accounts, Sub-Technique T1585.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1585/001/. Accessed 22 Dec. 2023.

[235] “Establish Accounts: Email Accounts.” Establish Accounts: Email Accounts, Sub-Technique T1585.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1585/002/. Accessed 22 Dec. 2023.

[236] “Establish Accounts: Cloud Accounts.” Establish Accounts: Cloud Accounts, Sub-Technique T1585.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1585/003/. Accessed 22 Dec. 2023.

[237] “Event Triggered Execution.” Event Triggered Execution, Technique T1546 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/. Accessed 22 Dec. 2023.

[238] “Event Triggered Execution: Change Default File Association.” Event Triggered Execution: Change Default File Association, Sub-Technique T1546.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/001/. Accessed 22 Dec. 2023.

[239] “Event Triggered Execution: Screensaver.” Event Triggered Execution: Screensaver, Sub-Technique T1546.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/002/. Accessed 22 Dec. 2023.

[240] “Event Triggered Execution: Windows Management Instrumentation Event Subscription.” Event Triggered Execution: Windows Management Instrumentation Event Subscription, Sub-Technique T1546.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/003/. Accessed 22 Dec. 2023.

[241] “Event Triggered Execution: Unix Shell Configuration Modification.” Event Triggered Execution: Unix Shell Configuration Modification, Sub-Technique T1546.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/004/. Accessed 22 Dec. 2023.

[242] “Event Triggered Execution: Trap.” Event Triggered Execution: Trap, Sub-Technique T1546.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/005/. Accessed 22 Dec. 2023.

[243] “Event Triggered Execution: LC_LOAD_DYLIB Addition.” Event Triggered Execution: LC_LOAD_DYLIB Addition, Sub-Technique T1546.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/006/. Accessed 22 Dec. 2023.

[244] “Event Triggered Execution: NETSH HELPER DLL.” Event Triggered Execution: Netsh Helper DLL, Sub-Technique T1546.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/007/. Accessed 22 Dec. 2023.

[245] “Event Triggered Execution: Accessibility Features.” Event Triggered Execution: Accessibility Features, Sub-Technique T1546.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/008/. Accessed 22 Dec. 2023.

[246] “Event Triggered Execution: Appcert Dlls.” Event Triggered Execution: AppCert DLLs, Sub-Technique T1546.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/009/. Accessed 22 Dec. 2023.

[247] “Event Triggered Execution: Appinit Dlls.” Event Triggered Execution: AppInit DLLs, Sub-Technique T1546.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/010/. Accessed 22 Dec. 2023.

[248] “Event Triggered Execution: Application Shimming.” Event Triggered Execution: Application Shimming, Sub-Technique T1546.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/011/. Accessed 22 Dec. 2023.

[249] “Event Triggered Execution: Image File Execution Options Injection.” Event Triggered Execution: Image File Execution Options Injection, Sub-Technique T1546.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/012/. Accessed 22 Dec. 2023.

[250] “Event Triggered Execution: Powershell Profile.” Event Triggered Execution: PowerShell Profile, Sub-Technique T1546.013 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/013/. Accessed 22 Dec. 2023.

[251] “Event Triggered Execution: Emond.” Event Triggered Execution: Emond, Sub-Technique T1546.014 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/014/. Accessed 22 Dec. 2023.

[252] “Event Triggered Execution: Component Object Model Hijacking.” Event Triggered Execution: Component Object Model Hijacking, Sub-Technique T1546.015 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/015/. Accessed 22 Dec. 2023.

[253] “Event Triggered Execution: Installer Packages.” Event Triggered Execution: Installer Packages, Sub-Technique T1546.016 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1546/016/. Accessed 22 Dec. 2023.

[254] “Execution Guardrails.” Execution Guardrails, Technique T1480 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1480/. Accessed 22 Dec. 2023.

[255] “Execution Guardrails: Environmental Keying.” Execution Guardrails: Environmental Keying, Sub-Technique T1480.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1480/001/. Accessed 22 Dec. 2023.

[256] “Exfiltration over Alternative Protocol.” Exfiltration Over Alternative Protocol, Technique T1048 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1048/. Accessed 22 Dec. 2023.

[257] “Exfiltration over Alternative Protocol: Exfiltration over Symmetric Encrypted Non-C2 Protocol.” Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol, Sub-Technique T1048.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1048/001/. Accessed 22 Dec. 2023.

[258] “Exfiltration over Alternative Protocol: Exfiltration over Asymmetric Encrypted Non-C2 Protocol.” Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol, Sub-Technique T1048.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1048/002/. Accessed 22 Dec. 2023.

[259] “Exfiltration over Alternative Protocol: Exfiltration over Unencrypted Non-C2 Protocol.” Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Sub-Technique T1048.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1048/003/. Accessed 22 Dec. 2023.

[260] “Exfiltration over C2 Channel.” Exfiltration Over C2 Channel, Technique T1041 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1041/. Accessed 22 Dec. 2023.

[261] “Exfiltration over Other Network Medium.” Exfiltration Over Other Network Medium, Technique T1011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1011/. Accessed 22 Dec. 2023.

[262] “Exfiltration over Other Network Medium: Exfiltration over Bluetooth.” Exfiltration Over Other Network Medium: Exfiltration Over Bluetooth, Sub-Technique T1011.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1011/001/. Accessed 22 Dec. 2023.

[263] “Exfiltration over Physical Medium.” Exfiltration Over Physical Medium, Technique T1052 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1052/. Accessed 22 Dec. 2023.

[264] “Exfiltration over Physical Medium: Exfiltration over USB.” Exfiltration Over Physical Medium: Exfiltration over USB, Sub-Technique T1052.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1052/001/. Accessed 22 Dec. 2023.

[265] “Exfiltration over Web Service.” Exfiltration Over Web Service, Technique T1567 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1567/. Accessed 22 Dec. 2023.

[266] “Exfiltration over Web Service: Exfiltration to Code Repository.” Exfiltration Over Web Service: Exfiltration to Code Repository, Sub-Technique T1567.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1567/001/. Accessed 22 Dec. 2023.

[267] “Exfiltration over Web Service: Exfiltration to Cloud Storage.” Exfiltration Over Web Service: Exfiltration to Cloud Storage, Sub-Technique T1567.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1567/002/. Accessed 22 Dec. 2023.

[268] “Exfiltration over Web Service: Exfiltration to Text Storage Sites.” Exfiltration Over Web Service: Exfiltration to Text Storage Sites, Sub-Technique T1567.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1567/003/. Accessed 22 Dec. 2023.

[269] “Exfiltration over Web Service: Exfiltration over Webhook.” Exfiltration Over Web Service: Exfiltration Over Webhook, Sub-Technique T1567.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1567/004/. Accessed 22 Dec. 2023.

[270] “Exploit Public-Facing Application.” Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1190/. Accessed 22 Dec. 2023.

[271] “Exploitation for Client Execution.” Exploitation for Client Execution, Technique T1203 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1203/. Accessed 22 Dec. 2023.

[272] “Exploitation for Credential Access.” Exploitation for Credential Access, Technique T1212 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1212/. Accessed 22 Dec. 2023.

[273] “Exploitation for Defense Evasion.” Exploitation for Defense Evasion, Technique T1211 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1211/. Accessed 22 Dec. 2023.

[274] “Exploitation for Privilege Escalation.” Exploitation for Privilege Escalation, Technique T1068 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1068/. Accessed 22 Dec. 2023.

[275] “Exploitation of Remote Services.” Exploitation of Remote Services, Technique T1210 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1210/. Accessed 22 Dec. 2023.

[276] “External Remote Services.” External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1133/. Accessed 22 Dec. 2023.

[277] “Fallback Channels.” Fallback Channels, Technique T1008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1008/. Accessed 22 Dec. 2023.

[278] “File and Directory Discovery.” File and Directory Discovery, Technique T1083 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1083/. Accessed 22 Dec. 2023.

[279] “File and Directory Permissions Modification.” File and Directory Permissions Modification, Technique T1222 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1222/. Accessed 22 Dec. 2023.

[280] “File and Directory Permissions Modification: Windows File and Directory Permissions Modification.” File and Directory Permissions Modification: Windows File and Directory Permissions Modification, Sub-Technique T1222.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1222/001/. Accessed 22 Dec. 2023.

[281] “File and Directory Permissions Modification: Linux and MAC File and Directory Permissions Modification.” File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification, Sub-Technique T1222.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1222/002/. Accessed 22 Dec. 2023.

[282] “Financial Theft.” Financial Theft, Technique T1657 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1657. Accessed 22 Dec. 2023.

[283] “Firmware Corruption.” Firmware Corruption, Technique T1495 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1495/. Accessed 22 Dec. 2023.

[284] “Forced Authentication.” Forced Authentication, Technique T1187 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1187/. Accessed 22 Dec. 2023.

[285] “Forge Web Credentials.” Forge Web Credentials, Technique T1606 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1606/. Accessed 22 Dec. 2023.

[286] “Forge Web Credentials: Web Cookies.” Forge Web Credentials: Web Cookies, Sub-Technique T1606.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1606/001/. Accessed 22 Dec. 2023.

[287] “Forge Web Credentials: SAML TOKENS.” Forge Web Credentials: SAML Tokens, Sub-Technique T1606.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1606/002/. Accessed 22 Dec. 2023.

[288] “Gather Victim Host Information.” Gather Victim Host Information, Technique T1592 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1592/. Accessed 22 Dec. 2023.

[289] “Gather Victim Host Information: Hardware.” Gather Victim Host Information: Hardware, Sub-Technique T1592.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1592/001/. Accessed 22 Dec. 2023.

[290] “Gather Victim Host Information: Software.” Gather Victim Host Information: Software, Sub-Technique T1592.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1592/002/. Accessed 22 Dec. 2023.

[291] “Gather Victim Host Information: Firmware.” Gather Victim Host Information: Firmware, Sub-Technique T1592.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1592/003/. Accessed 22 Dec. 2023.

[292] “Gather Victim Host Information: Client Configurations.” Gather Victim Host Information: Client Configurations, Sub-Technique T1592.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1592/004/. Accessed 22 Dec. 2023.

[293] “Gather Victim Identity Information.” Gather Victim Identity Information, Technique T1589 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1589/. Accessed 22 Dec. 2023.

[294] “Gather Victim Identity Information: Credentials.” Gather Victim Identity Information: Credentials, Sub-Technique T1589.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1589/001/. Accessed 22 Dec. 2023.

[295] “Gather Victim Identity Information: Email Addresses.” Gather Victim Identity Information: Email Addresses, Sub-Technique T1589.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1589/002/. Accessed 22 Dec. 2023.

[296] “Gather Victim Identity Information: Employee Names.” Gather Victim Identity Information: Employee Names, Sub-Technique T1589.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1589/003/. Accessed 22 Dec. 2023.

[297] “Gather Victim Network Information.” Gather Victim Network Information, Technique T1590 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/. Accessed 22 Dec. 2023.

[298] “Gather Victim Network Information: Domain Properties.” Gather Victim Network Information: Domain Properties, Sub-Technique T1590.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/001/. Accessed 22 Dec. 2023.

[299] “Gather Victim Network Information: DNS.” Gather Victim Network Information: DNS, Sub-Technique T1590.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/002/. Accessed 22 Dec. 2023.

[300] “Gather Victim Network Information: Network Trust Dependencies.” Gather Victim Network Information: Network Trust Dependencies, Sub-Technique T1590.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/003/. Accessed 22 Dec. 2023.

[301] “Gather Victim Network Information: Network Topology.” Gather Victim Network Information: Network Topology, Sub-Technique T1590.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/004/. Accessed 22 Dec. 2023.

[302] “Gather Victim Network Information: IP Addresses.” Gather Victim Network Information: IP Addresses, Sub-Technique T1590.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/005/. Accessed 22 Dec. 2023.

[303] “Gather Victim Network Information: Network Security Appliances.” Gather Victim Network Information: Network Security Appliances, Sub-Technique T1590.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1590/006/. Accessed 22 Dec. 2023.

[304] “Gather Victim Org Information.” Gather Victim Org Information, Technique T1591 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1591/. Accessed 22 Dec. 2023.

[305] “Gather Victim Org Information: Determine Physical Locations.” Gather Victim Org Information: Determine Physical Locations, Sub-Technique T1591.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1591/001/. Accessed 22 Dec. 2023.

[306] “Gather Victim Org Information: Business Relationships.” Gather Victim Org Information: Business Relationships, Sub-Technique T1591.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1591/002/. Accessed 22 Dec. 2023.

[307] “Gather Victim Org Information: Identify Business Tempo.” Gather Victim Org Information: Identify Business Tempo, Sub-Technique T1591.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1591/003/. Accessed 22 Dec. 2023.

[308] “Gather Victim Org Information: Identify Roles.” Gather Victim Org Information: Identify Roles, Sub-Technique T1591.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1591/004/. Accessed 22 Dec. 2023.

[309] “Group Policy Discovery.” Group Policy Discovery, Technique T1615 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1615/. Accessed 22 Dec. 2023.

[310] “Hardware Additions.” Hardware Additions, Technique T1200 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1200/. Accessed 22 Dec. 2023.

[311] “Hide Artifacts.” Hide Artifacts, Technique T1564 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/. Accessed 22 Dec. 2023.

[312] “Hide Artifacts: Hidden Files and Directories.” Hide Artifacts: Hidden Files and Directories, Sub-Technique T1564.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/001/. Accessed 22 Dec. 2023.

[313] “Hide Artifacts: Hidden Users.” Hide Artifacts: Hidden Users, Sub-Technique T1564.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/002/. Accessed 22 Dec. 2023.

[314] “Hide Artifacts: Hidden Window.” Hide Artifacts: Hidden Window, Sub-Technique T1564.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/003/. Accessed 22 Dec. 2023.

[315] “Hide Artifacts: NTFS File Attributes.” Hide Artifacts: NTFS File Attributes, Sub-Technique T1564.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/004/. Accessed 22 Dec. 2023.

[316] "Hide Artifacts: Hidden File System." Hide Artifacts: Hidden File System, Sub-Technique T1564.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/005/. Accessed 22 Dec. 2023.

[317] "Hide Artifacts: Run Virtual Instance." Hide Artifacts: Run Virtual Instance, Sub-Technique T1564.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/006/. Accessed 22 Dec. 2023.

[318] "Hide Artifacts: VBA Stomping." Hide Artifacts: VBA Stomping, Sub-Technique T1564.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/007/. Accessed 22 Dec. 2023.

[319] "Hide Artifacts: Email Hiding Rules." Hide Artifacts: Email Hiding Rules, Sub-Technique T1564.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/008/. Accessed 22 Dec. 2023.

[320] "Hide Artifacts: Resource Forking." Hide Artifacts: Resource Forking, Sub-Technique T1564.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/009/. Accessed 22 Dec. 2023.

[321] "Hide Artifacts: Process Argument Spoofing." Hide Artifacts: Process Argument Spoofing, Sub-Technique T1564.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/010/. Accessed 22 Dec. 2023.

[322] "Hide Artifacts: Ignore Process Interrupts." Hide Artifacts: Ignore Process Interrupts, Sub-Technique T1564.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1564/011/. Accessed 22 Dec. 2023.

[323] "Hijack Execution Flow." Hijack Execution Flow, Technique T1574 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/. Accessed 22 Dec. 2023.

[324] "Hijack Execution Flow: DLL Search Order Hijacking." Hijack Execution Flow: DLL Search Order Hijacking, Sub-Technique T1574.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/001/. Accessed 22 Dec. 2023.

[325] "Hijack Execution Flow: DLL Side-Loading." Hijack Execution Flow: DLL Side-Loading, Sub-Technique T1574.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/002/. Accessed 22 Dec. 2023.

[326] "Hijack Execution Flow: Dylib Hijacking." Hijack Execution Flow: Dylib Hijacking, Sub-Technique T1574.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/004/. Accessed 22 Dec. 2023.

[327] "Hijack Execution Flow: Executable Installer File Permissions Weakness." Hijack Execution Flow: Executable Installer File Permissions Weakness, Sub-Technique T1574.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/005/. Accessed 22 Dec. 2023.

[328] "Hijack Execution Flow: Dynamic Linker Hijacking." Hijack Execution Flow: Dynamic Linker Hijacking, Sub-Technique T1574.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/006/. Accessed 22 Dec. 2023.

[329] "Hijack Execution Flow: Path Interception by Path Environment Variable." Hijack Execution Flow: Path Interception by PATH Environment Variable, Sub-Technique T1574.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/007/. Accessed 22 Dec. 2023.

[330] "Hijack Execution Flow: Path Interception by Search Order Hijacking." Hijack Execution Flow: Path Interception by Search Order Hijacking, Sub-Technique T1574.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/008/. Accessed 22 Dec. 2023.

[331] "Hijack Execution Flow: Path Interception by Unquoted Path." Hijack Execution Flow: Path Interception by Unquoted Path, Sub-Technique T1574.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/009/. Accessed 22 Dec. 2023.

[332] "Hijack Execution Flow: Services File Permissions Weakness." Hijack Execution Flow: Services File Permissions Weakness, Sub-Technique T1574.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/010/. Accessed 22 Dec. 2023.

[333] "Hijack Execution Flow: Services Registry Permissions Weakness." Hijack Execution Flow: Services Registry Permissions Weakness, Sub-Technique T1574.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/011/. Accessed 22 Dec. 2023.

[334] "Hijack Execution Flow: Cor_profiler." Hijack Execution Flow: COR_PROFILER, Sub-Technique T1574.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/012/. Accessed 22 Dec. 2023.

[335] "Hijack Execution Flow: Kernelcallbacktable." Hijack Execution Flow: KernelCallbackTable, Sub-Technique T1574.013 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1574/013/. Accessed 22 Dec. 2023.

[336] "Impair Defenses." Impair Defenses, Technique T1562 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/. Accessed 22 Dec. 2023.

[337] "Impair Defenses: Disable or Modify Tools." Impair Defenses: Disable or Modify Tools, Sub-Technique T1562.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/001/. Accessed 22 Dec. 2023.

[338] "Impair Defenses: Disable Windows Event Logging." Impair Defenses: Disable Windows Event Logging, Sub-Technique T1562.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/002/. Accessed 22 Dec. 2023.

[339] "Impair Defenses: Impair Command History Logging." Impair Defenses: Impair Command History Logging, Sub-Technique T1562.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/003/. Accessed 22 Dec. 2023.

[340] "Impair Defenses: Disable or Modify System Firewall." Impair Defenses: Disable or Modify System Firewall, Sub-Technique T1562.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/004/. Accessed 22 Dec. 2023.

[341] "Impair Defenses: Indicator Blocking." Impair Defenses: Indicator Blocking, Sub-Technique T1562.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/006/. Accessed 22 Dec. 2023.

[342] "Impair Defenses: Disable or Modify Cloud Firewall." Impair Defenses: Disable or Modify Cloud Firewall, Sub-Technique T1562.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/007/. Accessed 22 Dec. 2023.

[343] "Impair Defenses: Disable or Modify Cloud Logs." Impair Defenses: Disable or Modify Cloud Logs, Sub-Technique T1562.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/008/. Accessed 22 Dec. 2023.

[344] "Impair Defenses: Safe Mode Boot." Impair Defenses: Safe Mode Boot, Sub-Technique T1562.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/009/. Accessed 22 Dec. 2023.

[345] "Impair Defenses: Downgrade Attack." Impair Defenses: Downgrade Attack, Sub-Technique T1562.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/010/. Accessed 22 Dec. 2023.

[346] "Impair Defenses: Spoof Security Alerting." Impair Defenses: Spoof Security Alerting, Sub-Technique T1562.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/011/. Accessed 22 Dec. 2023.

[347] "Impair Defenses: Disable or Modify Linux Audit System." Impair Defenses: Disable or Modify Linux Audit System, Sub-Technique T1562.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1562/012/. Accessed 22 Dec. 2023.

[348] "Impersonation." Impersonation, Technique T1656 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1656/. Accessed 22 Dec. 2023.

[349] "Implant Internal Image." Implant Internal Image, Technique T1525 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1525/. Accessed 22 Dec. 2023.

[350] "Indicator Removal." Indicator Removal, Technique T1070 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/. Accessed 22 Dec. 2023.

[351] "Indicator Removal: Clear Windows Event Logs." Indicator Removal: Clear Windows Event Logs, Sub-Technique T1070.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/001/. Accessed 22 Dec. 2023.

[352] "Indicator Removal: Clear Linux or Mac System Logs." Indicator Removal: Clear Linux or Mac System Logs, Sub-Technique T1070.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/002/. Accessed 22 Dec. 2023.

[353] "Indicator Removal: Clear Command History." Indicator Removal: Clear Command History, Sub-Technique T1070.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/003/. Accessed 22 Dec. 2023.

[354] "Indicator Removal: File Deletion." Indicator Removal: File Deletion, Sub-Technique T1070.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/004/. Accessed 22 Dec. 2023.

[355] "Indicator Removal: Network Share Connection Removal." Indicator Removal: Network Share Connection Removal, Sub-Technique T1070.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/005/. Accessed 22 Dec. 2023.

[356] "Indicator Removal: Timestomp." Indicator Removal: Timestomp, Sub-Technique T1070.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/006/. Accessed 22 Dec. 2023.

[357] "Indicator Removal: Clear Network Connection History and Configurations." Indicator Removal: Clear Network Connection History and Configurations, Sub-Technique T1070.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/007/. Accessed 22 Dec. 2023.

[358] "Indicator Removal: Clear Mailbox Data." Indicator Removal: Clear Mailbox Data, Sub-Technique T1070.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/008/. Accessed 22 Dec. 2023.

[359] “Indicator Removal: Clear Persistence.” Indicator Removal: Clear Persistence, Sub-Technique T1070.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1070/009/. Accessed 22 Dec. 2023.

[360] “Indirect Command Execution.” Indirect Command Execution, Technique T1202 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1202/. Accessed 22 Dec. 2023.

[361] “Ingress Tool Transfer.” Ingress Tool Transfer, Technique T1105 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1105/. Accessed 22 Dec. 2023.

[362] “Inhibit System Recovery.” Inhibit System Recovery, Technique T1490 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1490/. Accessed 22 Dec. 2023.

[363] “Input Capture.” Input Capture, Technique T1056 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1056/. Accessed 22 Dec. 2023.

[364] “Input Capture: Keylogging.” Input Capture: Keylogging, Sub-Technique T1056.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1056/001/. Accessed 22 Dec. 2023.

[365] “Input Capture: Gui Input Capture.” Input Capture: GUI Input Capture, Sub-Technique T1056.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1056/002/. Accessed 22 Dec. 2023.

[366] “Input Capture: Web Portal Capture.” Input Capture: Web Portal Capture, Sub-Technique T1056.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1056/003/. Accessed 22 Dec. 2023.

[367] “Input Capture: Credential API Hooking.” Input Capture: Credential API Hooking, Sub-Technique T1056.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1056/004/. Accessed 22 Dec. 2023.

[368] “Inter-Process Communication.” Inter-Process Communication, Technique T1559 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1559/. Accessed 22 Dec. 2023.

[369] “Inter-Process Communication: Component Object Model.” Inter-Process Communication: Component Object Model, Sub-Technique T1559.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1559/001/. Accessed 22 Dec. 2023.

[370] “Inter-Process Communication: Dynamic Data Exchange.” Inter-Process Communication: Dynamic Data Exchange, Sub-Technique T1559.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1559/002/. Accessed 22 Dec. 2023.

[371] “Inter-Process Communication: XPC Services.” Inter-Process Communication: XPC Services, Sub-Technique T1559.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1559/003/. Accessed 22 Dec. 2023.

[372] “Internal Spearphishing.” Internal Spearphishing, Technique T1534 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1534/. Accessed 22 Dec. 2023.

[373] “Lateral Tool Transfer.” Lateral Tool Transfer, Technique T1570 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1570/. Accessed 22 Dec. 2023.

[374] “Log Enumeration.” Log Enumeration, Technique T1654 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1654/. Accessed 22 Dec. 2023.

[375] “Masquerading.” Masquerading, Technique T1036 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/. Accessed 22 Dec. 2023.

[376] “Masquerading: Invalid Code Signature.” Masquerading: Invalid Code Signature, Sub-Technique T1036.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/001/. Accessed 22 Dec. 2023.

[377] “Masquerading: Right-to-Left Override.” Masquerading: Right-to-Left Override, Sub-Technique T1036.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/002/. Accessed 22 Dec. 2023.

[378] “Masquerading: Rename System Utilities.” Masquerading: Rename System Utilities, Sub-Technique T1036.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/003/. Accessed 22 Dec. 2023.

[379] “Masquerading: Masquerade Task or Service.” Masquerading: Masquerade Task or Service, Sub-Technique T1036.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/004/. Accessed 22 Dec. 2023.

[380] “Masquerading: Match Legitimate Name or Location.” Masquerading: Match Legitimate Name or Location, Sub-Technique T1036.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/005/. Accessed 22 Dec. 2023.

[381] “Masquerading: Space after Filename.” Masquerading: Space after Filename, Sub-Technique T1036.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/006/. Accessed 22 Dec. 2023.

[382] “Masquerading: Double File Extension.” Masquerading: Double File Extension, Sub-Technique T1036.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/007/. Accessed 22 Dec. 2023.

[383] “Masquerading: Masquerade File Type.” Masquerading: Masquerade File Type, Sub-Technique T1036.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/008/. Accessed 22 Dec. 2023.

[384] “Masquerading: Break Process Trees.” Masquerading: Break Process Trees, Sub-Technique T1036.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1036/009/. Accessed 22 Dec. 2023.

[385] “Modify Authentication Process.” Modify Authentication Process, Technique T1556 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/. Accessed 22 Dec. 2023.

[386] “Modify Authentication Process: Domain Controller Authentication.” Modify Authentication Process: Domain Controller Authentication, Sub-Technique T1556.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/001/. Accessed 22 Dec. 2023.

[387] “Modify Authentication Process: Password Filter DLL.” Modify Authentication Process: Password Filter DLL, Sub-Technique T1556.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/002/. Accessed 22 Dec. 2023.

[388] “Modify Authentication Process: Pluggable Authentication Modules.” Modify Authentication Process: Pluggable Authentication Modules, Sub-Technique T1556.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/003/. Accessed 22 Dec. 2023.

[389] "Modify Authentication Process: Network Device Authentication." Modify Authentication Process: Network Device Authentication, Sub-Technique T1556.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/004/. Accessed 22 Dec. 2023.

[390] "Modify Authentication Process: Reversible Encryption." Modify Authentication Process: Reversible Encryption, Sub-Technique T1556.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/005/. Accessed 22 Dec. 2023.

[391] "Modify Authentication Process: Multi-Factor Authentication." Modify Authentication Process: Multi-Factor Authentication, Sub-Technique T1556.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/006/. Accessed 22 Dec. 2023.

[392] "Modify Authentication Process: Hybrid Identity." Modify Authentication Process: Hybrid Identity, Sub-Technique T1556.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/007/. Accessed 22 Dec. 2023.

[393] "Modify Authentication Process: Network Provider DLL." Modify Authentication Process: Network Provider DLL, Sub-Technique T1556.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1556/008/. Accessed 22 Dec. 2023.

[394] "Modify Cloud Compute Infrastructure." Modify Cloud Compute Infrastructure, Technique T1578 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/. Accessed 22 Dec. 2023.

[395] "Modify Cloud Compute Infrastructure: Create Snapshot." Modify Cloud Compute Infrastructure: Create Snapshot, Sub-Technique T1578.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/001/. Accessed 22 Dec. 2023.

[396] "Modify Cloud Compute Infrastructure: Create Cloud Instance." Modify Cloud Compute Infrastructure: Create Cloud Instance, Sub-Technique T1578.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/002/. Accessed 22 Dec. 2023.

[397] "Modify Cloud Compute Infrastructure: Delete Cloud Instance." Modify Cloud Compute Infrastructure: Delete Cloud Instance, Sub-Technique T1578.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/003/. Accessed 22 Dec. 2023.

[398] "Modify Cloud Compute Infrastructure: Revert Cloud Instance." Modify Cloud Compute Infrastructure: Revert Cloud Instance, Sub-Technique T1578.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/004/. Accessed 22 Dec. 2023.

[399] "Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations." Modify Cloud Compute Infrastructure: Modify Cloud Compute Configurations, Sub-Technique T1578.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1578/005/. Accessed 22 Dec. 2023.

[400] "Modify Registry." Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1112/. Accessed 22 Dec. 2023.

[401] "Modify System Image." Modify System Image, Technique T1601 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1601/. Accessed 22 Dec. 2023.

[402] “Modify System Image: Patch System Image.” Modify System Image: Patch System Image, Sub-Technique T1601.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1601/001/. Accessed 22 Dec. 2023.

[403] “Modify System Image: Downgrade System Image.” Modify System Image: Downgrade System Image, Sub-Technique T1601.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1601/002/. Accessed 22 Dec. 2023.

[404] “Multi-Factor Authentication Interception.” Multi-Factor Authentication Interception, Technique T1111 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1111/. Accessed 22 Dec. 2023.

[405] “Multi-Factor Authentication Request Generation.” Multi-Factor Authentication Request Generation, Technique T1621 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1621/. Accessed 22 Dec. 2023.

[406] “Multi-Stage Channels.” Multi-Stage Channels, Technique T1104 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1104/. Accessed 22 Dec. 2023.

[407] “Native Api.” Native API, Technique T1106 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1106/. Accessed 22 Dec. 2023.

[408] “Network Boundary Bridging.” Network Boundary Bridging, Technique T1599 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1599/. Accessed 22 Dec. 2023.

[409] “Network Boundary Bridging: Network Address Translation Traversal.” Network Boundary Bridging: Network Address Translation Traversal, Sub-Technique T1599.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1599/001/. Accessed 22 Dec. 2023.

[410] “Network Denial of Service.” Network Denial of Service, Technique T1498 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1498/. Accessed 22 Dec. 2023.

[411] “Network Denial of Service: Direct Network Flood.” Network Denial of Service: Direct Network Flood, Sub-Technique T1498.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1498/001/. Accessed 22 Dec. 2023.

[412] “Network Denial of Service: Reflection Amplification.” Network Denial of Service: Reflection Amplification, Sub-Technique T1498.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1498/002/. Accessed 22 Dec. 2023.

[413] “Network Service Discovery.” Network Service Discovery, Technique T1046 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1046/. Accessed 22 Dec. 2023.

[414] “Network Share Discovery.” Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1135/. Accessed 22 Dec. 2023.

[415] “Network Sniffing.” Network Sniffing, Technique T1040 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1040/. Accessed 22 Dec. 2023.

[416] “Non-Application Layer Protocol.” Non-Application Layer Protocol, Technique T1095 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1095/. Accessed 22 Dec. 2023.

[417] “Non-Standard Port.” Non-Standard Port, Technique T1571 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1571/. Accessed 22 Dec. 2023.

[418] "Obfuscated Files or Information." Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/. Accessed 22 Dec. 2023.

[419] "Obfuscated Files or Information: Binary Padding." Obfuscated Files or Information: Binary Padding, Sub-Technique T1027.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/001/. Accessed 22 Dec. 2023.

[420] "Obfuscated Files or Information: Software Packing." Obfuscated Files or Information: Software Packing, Sub-Technique T1027.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/002/. Accessed 22 Dec. 2023.

[421] "Obfuscated Files or Information: Steganography." Obfuscated Files or Information: Steganography, Sub-Technique T1027.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/003/. Accessed 22 Dec. 2023.

[422] "Obfuscated Files or Information: Compile after Delivery." Obfuscated Files or Information: Compile After Delivery, Sub-Technique T1027.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/004/. Accessed 22 Dec. 2023.

[423] "Obfuscated Files or Information: Indicator Removal from Tools." Obfuscated Files or Information: Indicator Removal from Tools, Sub-Technique T1027.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/005/. Accessed 22 Dec. 2023.

[424] "Obfuscated Files or Information: HTML Smuggling." Obfuscated Files or Information: HTML Smuggling, Sub-Technique T1027.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/006/. Accessed 22 Dec. 2023.

[425] "Obfuscated Files or Information: Dynamic API Resolution." Obfuscated Files or Information: Dynamic API Resolution, Sub-Technique T1027.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/007/. Accessed 22 Dec. 2023.

[426] "Obfuscated Files or Information: Stripped Payloads." Obfuscated Files or Information: Stripped Payloads, Sub-Technique T1027.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/008/. Accessed 22 Dec. 2023.

[427] "Obfuscated Files or Information: Embedded Payloads." Obfuscated Files or Information: Embedded Payloads, Sub-Technique T1027.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/009/. Accessed 22 Dec. 2023.

[428] "Obfuscated Files or Information: Command Obfuscation." Obfuscated Files or Information: Command Obfuscation, Sub-Technique T1027.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/010/. Accessed 22 Dec. 2023.

[429] "Obfuscated Files or Information: Fileless Storage." Obfuscated Files or Information: Fileless Storage, Sub-Technique T1027.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/011/. Accessed 22 Dec. 2023.

[430] "Obfuscated Files or Information: LNK Icon Smuggling." Obfuscated Files or Information: LNK Icon Smuggling, Sub-Technique T1027.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1027/012/. Accessed 22 Dec. 2023.

[431] "Obtain Capabilities." Obtain Capabilities, Technique T1588 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/. Accessed 22 Dec. 2023.

[432] “Obtain Capabilities: Malware.” Obtain Capabilities: Malware, Sub-Technique T1588.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/001/. Accessed 22 Dec. 2023.

[433] “Obtain Capabilities: Tool.” Obtain Capabilities: Tool, Sub-Technique T1588.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/002/. Accessed 22 Dec. 2023.

[434] “Obtain Capabilities: Code Signing Certificates.” Obtain Capabilities: Code Signing Certificates, Sub-Technique T1588.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/003/. Accessed 22 Dec. 2023.

[435] “Obtain Capabilities: Digital Certificates.” Obtain Capabilities: Digital Certificates, Sub-Technique T1588.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/004/. Accessed 22 Dec. 2023.

[436] “Obtain Capabilities: Exploits.” Obtain Capabilities: Exploits, Sub-Technique T1588.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/005/. Accessed 22 Dec. 2023.

[437] “Obtain Capabilities: Vulnerabilities.” Obtain Capabilities: Vulnerabilities, Sub-Technique T1588.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1588/006/. Accessed 22 Dec. 2023.

[438] “Office Application Startup.” Office Application Startup, Technique T1137 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/. Accessed 22 Dec. 2023.

[439] “Office Application Startup: Office Template Macros.” Office Application Startup: Office Template Macros, Sub-Technique T1137.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/001/. Accessed 22 Dec. 2023.

[440] “Office Application Startup: Office Test.” Office Application Startup: Office Test, Sub-Technique T1137.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/002/. Accessed 22 Dec. 2023.

[441] “Office Application Startup: Outlook Forms.” Office Application Startup: Outlook Forms, Sub-Technique T1137.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/003/. Accessed 22 Dec. 2023.

[442] “Office Application Startup: Outlook Home Page.” Office Application Startup: Outlook Home Page, Sub-Technique T1137.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/004/. Accessed 22 Dec. 2023.

[443] “Office Application Startup: Outlook Rules.” Office Application Startup: Outlook Rules, Sub-Technique T1137.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/005/. Accessed 22 Dec. 2023.

[444] “Office Application Startup: Add-Ins.” Office Application Startup: Add-Ins, Sub-Technique T1137.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1137/006/. Accessed 22 Dec. 2023.

[445] “Os Credential Dumping.” OS Credential Dumping, Technique T1003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/. Accessed 22 Dec. 2023.

[446] “Os Credential Dumping: LSASS MEMORY.” OS Credential Dumping: LSASS Memory, Sub-Technique T1003.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/001/. Accessed 22 Dec. 2023.

[447] “Os Credential Dumping: Security Account Manager.” OS Credential Dumping: Security Account Manager, Sub-Technique T1003.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/002/. Accessed 22 Dec. 2023.

[448] “Os Credential Dumping: NTDS.” OS Credential Dumping: NTDS, Sub-Technique T1003.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/003/. Accessed 22 Dec. 2023.

[449] “Os Credential Dumping: LSA Secrets.” OS Credential Dumping: LSA Secrets, Sub-Technique T1003.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/004/. Accessed 22 Dec. 2023.

[450] “Os Credential Dumping: Cached Domain Credentials.” OS Credential Dumping: Cached Domain Credentials, Sub-Technique T1003.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/005/. Accessed 22 Dec. 2023.

[451] “Os Credential Dumping: DCSync.” OS Credential Dumping: DCSync, Sub-Technique T1003.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/006/. Accessed 22 Dec. 2023.

[452] “Os Credential Dumping: Proc Filesystem.” OS Credential Dumping: Proc Filesystem, Sub-Technique T1003.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/007/. Accessed 22 Dec. 2023.

[453] “Os Credential Dumping: /Etc/Passwd and /Etc/Shadow.” OS Credential Dumping: /Etc/Passwd and /Etc/Shadow, Sub-Technique T1003.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1003/008/. Accessed 22 Dec. 2023.

[454] “Password Policy Discovery.” Password Policy Discovery, Technique T1201 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1201/. Accessed 22 Dec. 2023.

[455] “Peripheral Device Discovery.” Peripheral Device Discovery, Technique T1120 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1120/. Accessed 22 Dec. 2023.

[456] “Permission Groups Discovery.” Permission Groups Discovery, Technique T1069 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1069/. Accessed 22 Dec. 2023.

[457] “Permission Groups Discovery: Local Groups.” Permission Groups Discovery: Local Groups, Sub-Technique T1069.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1069/001/. Accessed 22 Dec. 2023.

[458] “Permission Groups Discovery: Domain Groups.” Permission Groups Discovery: Domain Groups, Sub-Technique T1069.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1069/002/. Accessed 22 Dec. 2023.

[459] “Permission Groups Discovery: Cloud Groups.” Permission Groups Discovery: Cloud Groups, Sub-Technique T1069.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1069/003/. Accessed 22 Dec. 2023.

[460] “Phishing.” Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1566/. Accessed 22 Dec. 2023.

[461] “Phishing: Spearphishing Attachment.” Phishing: Spearphishing Attachment, Sub-Technique T1566.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1566/001/. Accessed 22 Dec. 2023.

[462] “Phishing: Spearphishing Link.” Phishing: Spearphishing Link, Sub-Technique T1566.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1566/002/. Accessed 22 Dec. 2023.

[463] “Phishing: Spearphishing via Service.” Phishing: Spearphishing via Service, Sub-Technique T1566.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1566/003/. Accessed 22 Dec. 2023.

[464] “Phishing: Spearphishing Voice.” Phishing: Spearphishing Voice, Sub-Technique T1566.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1566/004/. Accessed 22 Dec. 2023.

[465] “Phishing for Information.” Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1598/. Accessed 22 Dec. 2023.

[466] “Phishing for Information: Spearphishing Service.” Phishing for Information: Spearphishing Service, Sub-Technique T1598.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1598/001/. Accessed 22 Dec. 2023.

[467] “Phishing for Information: Spearphishing Attachment.” Phishing for Information: Spearphishing Attachment, Sub-Technique T1598.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1598/002/. Accessed 22 Dec. 2023.

[468] “Phishing for Information: Spearphishing Link.” Phishing for Information: Spearphishing Link, Sub-Technique T1598.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1598/003/. Accessed 22 Dec. 2023.

[469] “Phishing for Information: Spearphishing Voice.” Phishing for Information: Spearphishing Voice, Sub-Technique T1598.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1598/004/. Accessed 22 Dec. 2023.

[470] “Plist File Modification.” Plist File Modification, Technique T1647 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1647/. Accessed 22 Dec. 2023.

[471] “Power Settings.” Power Settings, Technique T1653 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1653/. Accessed 22 Dec. 2023.

[472] “Pre-OS Boot.” Pre-OS Boot, Technique T1542 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/. Accessed 22 Dec. 2023.

[473] “Pre-OS Boot: System Firmware.” Pre-OS Boot: System Firmware, Sub-Technique T1542.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/001/. Accessed 22 Dec. 2023.

[474] “Pre-OS Boot: Component Firmware.” Pre-OS Boot: Component Firmware, Sub-Technique T1542.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/002/. Accessed 22 Dec. 2023.

[475] “Pre-OS Boot: Bootkit.” Pre-OS Boot: Bootkit, Sub-Technique T1542.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/003/. Accessed 22 Dec. 2023.

[476] “Pre-OS Boot: Rommonkit.” Pre-OS Boot: ROMMONkit, Sub-Technique T1542.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/004/. Accessed 22 Dec. 2023.

[477] “Pre-OS Boot: TFTP Boot.” Pre-OS Boot: TFTP Boot, Sub-Technique T1542.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1542/005/. Accessed 22 Dec. 2023.

[478] “Process Discovery.” Process Discovery, Technique T1057 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1057/. Accessed 22 Dec. 2023.

[479] “Process Injection.” Process Injection, Technique T1055 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/. Accessed 22 Dec. 2023.

[480] “Process Injection: Dynamic-Link Library Injection.” Process Injection: Dynamic-Link Library Injection, Sub-Technique T1055.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/001/. Accessed 22 Dec. 2023.

[481] “Process Injection: Portable Executable Injection.” Process Injection: Portable Executable Injection, Sub-Technique T1055.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/002/. Accessed 22 Dec. 2023.

[482] “Process Injection: Thread Execution Hijacking.” Process Injection: Thread Execution Hijacking, Sub-Technique T1055.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/003/. Accessed 22 Dec. 2023.

[483] “Process Injection: Asynchronous Procedure Call.” Process Injection: Asynchronous Procedure Call, Sub-Technique T1055.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/004/. Accessed 22 Dec. 2023.

[484] “Process Injection: Thread Local Storage.” Process Injection: Thread Local Storage, Sub-Technique T1055.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/005/. Accessed 22 Dec. 2023.

[485] “Process Injection: Ptrace System Calls.” Process Injection: Ptrace System Calls, Sub-Technique T1055.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/008/. Accessed 22 Dec. 2023.

[486] “Process Injection: Proc Memory.” Process Injection: Proc Memory, Sub-Technique T1055.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/009/. Accessed 22 Dec. 2023.

[487] “Process Injection: Extra Window Memory Injection.” Process Injection: Extra Window Memory Injection, Sub-Technique T1055.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/011/. Accessed 22 Dec. 2023.

[488] “Process Injection: Process Hollowing.” Process Injection: Process Hollowing, Sub-Technique T1055.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/012/. Accessed 22 Dec. 2023.

[489] “Process Injection: Process Doppelgänging.” Process Injection: Process Doppelgänging, Sub-Technique T1055.013 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/013/. Accessed 22 Dec. 2023.

[490] “Process Injection: VDSO Hijacking.” Process Injection: VDSO Hijacking, Sub-Technique T1055.014 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/014/. Accessed 22 Dec. 2023.

[491] “Process Injection: Listplanting.” Process Injection: ListPlanting, Sub-Technique T1055.015 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1055/015/. Accessed 22 Dec. 2023.

[492] “Protocol Tunneling.” Protocol Tunneling, Technique T1572 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1572/. Accessed 22 Dec. 2023.

[493] “Proxy.” Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1090/. Accessed 22 Dec. 2023.

[494] “Proxy: Internal Proxy.” Proxy: Internal Proxy, Sub-Technique T1090.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1090/001/. Accessed 22 Dec. 2023.

[495] “Proxy: External Proxy.” Proxy: External Proxy, Sub-Technique T1090.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1090/002/. Accessed 22 Dec. 2023.

[496] “Proxy: Multi-Hop Proxy.” Proxy: Multi-Hop Proxy, Sub-Technique T1090.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1090/003/. Accessed 22 Dec. 2023.

[497] “Proxy: Domain Fronting.” Proxy: Domain Fronting, Sub-Technique T1090.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1090/004/. Accessed 22 Dec. 2023.

[498] “Query Registry.” Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1012/. Accessed 22 Dec. 2023.

[499] “Reflective Code Loading.” Reflective Code Loading, Technique T1620 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1620/. Accessed 22 Dec. 2023.

[500] “Remote Access Software.” Remote Access Software, Technique T1219 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1219/. Accessed 22 Dec. 2023.

[501] “Remote Service Session Hijacking.” Remote Service Session Hijacking, Technique T1563 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1563/. Accessed 22 Dec. 2023.

[502] “Remote Service Session Hijacking: SSH Hijacking.” Remote Service Session Hijacking: SSH Hijacking, Sub-Technique T1563.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1563/001/. Accessed 22 Dec. 2023.

[503] “Remote Service Session Hijacking: RDP Hijacking.” Remote Service Session Hijacking: RDP Hijacking, Sub-Technique T1563.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1563/002/. Accessed 22 Dec. 2023.

[504] “Remote Services.” Remote Services, Technique T1021 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/. Accessed 22 Dec. 2023.

[505] “Remote Services: Remote Desktop Protocol.” Remote Services: Remote Desktop Protocol, Sub-Technique T1021.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/001/. Accessed 22 Dec. 2023.

[506] “Remote Services: SMB/Windows Admin Shares.” Remote Services: SMB/Windows Admin Shares, Sub-Technique T1021.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/002/. Accessed 22 Dec. 2023.

[507] “Remote Services: Distributed Component Object Model.” Remote Services: Distributed Component Object Model, Sub-Technique T1021.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/003/. Accessed 22 Dec. 2023.

[508] “Remote Services: SSH.” Remote Services: SSH, Sub-Technique T1021.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/004/. Accessed 22 Dec. 2023.

[509] “Remote Services: VNC.” Remote Services: VNC, Sub-Technique T1021.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/005/. Accessed 22 Dec. 2023.

[510] “Remote Services: Windows Remote Management.” Remote Services: Windows Remote Management, Sub-Technique T1021.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/006/. Accessed 22 Dec. 2023.

[511] “Remote Services: Cloud Services.” Remote Services: Cloud Services, Sub-Technique T1021.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/007/. Accessed 22 Dec. 2023.

[512] “Remote Services: Direct Cloud VM Connections.” Remote Services: Direct Cloud VM Connections, Sub-Technique T1021.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1021/008/. Accessed 22 Dec. 2023.

[513] “Remote System Discovery.” Remote System Discovery, Technique T1018 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1018/. Accessed 22 Dec. 2023.

[514] “Replication through Removable Media.” Replication Through Removable Media, Technique T1091 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1091/. Accessed 22 Dec. 2023.

[515] “Resource Hijacking.” Resource Hijacking, Technique T1496 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1496/. Accessed 22 Dec. 2023.

[516] “Rogue Domain Controller.” Rogue Domain Controller, Technique T1207 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1207/. Accessed 22 Dec. 2023.

[517] “Rootkit.” Rootkit, Technique T1014 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1014/. Accessed 22 Dec. 2023.

[518] “Scheduled Task/Job.” Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/. Accessed 22 Dec. 2023.

[519] “Scheduled Task/Job: At.” Scheduled Task/Job: At, Sub-Technique T1053.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/002/. Accessed 22 Dec. 2023.

[520] “Scheduled Task/Job: Cron.” Scheduled Task/Job: Cron, Sub-Technique T1053.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/003/. Accessed 22 Dec. 2023.

[521] “Scheduled Task/Job: Scheduled Task.” Scheduled Task/Job: Scheduled Task, Sub-Technique T1053.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/005/. Accessed 22 Dec. 2023.

[522] “Scheduled Task/Job: Systemd Timers.” Scheduled Task/Job: Systemd Timers, Sub-Technique T1053.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/006/. Accessed 22 Dec. 2023.

[523] “Scheduled Task/Job: Container Orchestration Job.” Scheduled Task/Job: Container Orchestration Job, Sub-Technique T1053.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1053/007/. Accessed 22 Dec. 2023.

[524] “Scheduled Transfer.” Scheduled Transfer, Technique T1029 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1029/. Accessed 22 Dec. 2023.

[525] “Screen Capture.” Screen Capture, Technique T1113 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1113/. Accessed 22 Dec. 2023.

[526] “Search Closed Sources.” Search Closed Sources, Technique T1597 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1597/. Accessed 22 Dec. 2023.

[527] “Search Closed Sources: Threat Intel Vendors.” Search Closed Sources: Threat Intel Vendors, Sub-Technique T1597.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1597/001/. Accessed 22 Dec. 2023.

[528] “Search Closed Sources: Purchase Technical Data.” Search Closed Sources: Purchase Technical Data, Sub-Technique T1597.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1597/002/. Accessed 22 Dec. 2023.

[529] “Search Open Technical Databases.” Search Open Technical Databases, Technique T1596 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/. Accessed 22 Dec. 2023.

[530] “Search Open Technical Databases: DNS/Passive DNS.” Search Open Technical Databases: DNS/Passive DNS, Sub-Technique T1596.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/001/. Accessed 22 Dec. 2023.

[531] “Search Open Technical Databases: WHOIS.” Search Open Technical Databases: WHOIS, Sub-Technique T1596.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/002/. Accessed 22 Dec. 2023.

[532] “Search Open Technical Databases: Digital Certificates.” Search Open Technical Databases: Digital Certificates, Sub-Technique T1596.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/003/. Accessed 22 Dec. 2023.

[533] “Search Open Technical Databases: Cdns.” Search Open Technical Databases: CDNs, Sub-Technique T1596.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/004/. Accessed 22 Dec. 2023.

[534] “Search Open Technical Databases: Scan Databases.” Search Open Technical Databases: Scan Databases, Sub-Technique T1596.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1596/005/. Accessed 22 Dec. 2023.

[535] “Search Open Websites/Domains.” Search Open Websites/Domains, Technique T1593 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1593/. Accessed 22 Dec. 2023.

[536] “Search Open Websites/Domains: Social Media.” Search Open Websites/Domains: Social Media, Sub-Technique T1593.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1593/001/. Accessed 22 Dec. 2023.

[537] “Search Open Websites/Domains: Search Engines.” Search Open Websites/Domains: Search Engines, Sub-Technique T1593.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1593/002/. Accessed 22 Dec. 2023.

[538] “Search Open Websites/Domains: Code Repositories.” Search Open Websites/Domains: Code Repositories, Sub-Technique T1593.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1593/003/. Accessed 22 Dec. 2023.

[539] “Search Victim-Owned Websites.” Search Victim-Owned Websites, Technique T1594 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1594/. Accessed 22 Dec. 2023.

[540] “Server Software Component.” Server Software Component, Technique T1505 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/. Accessed 22 Dec. 2023.

[541] “Server Software Component: SQL Stored Procedures.” Server Software Component: SQL Stored Procedures, Sub-Technique T1505.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/001/. Accessed 22 Dec. 2023.

[542] “Server Software Component: Transport Agent.” Server Software Component: Transport Agent, Sub-Technique T1505.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/002/. Accessed 22 Dec. 2023.

[543] “Server Software Component: Web Shell.” Server Software Component: Web Shell, Sub-Technique T1505.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/003/. Accessed 22 Dec. 2023.

[544] “Server Software Component: IIS Components.” Server Software Component: IIS Components, Sub-Technique T1505.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/004/. Accessed 22 Dec. 2023.

[545] “Server Software Component: Terminal Services DLL.” Server Software Component: Terminal Services DLL, Sub-Technique T1505.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1505/005/. Accessed 22 Dec. 2023.

[546] “Serverless Execution.” Serverless Execution, Technique T1648 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1648/. Accessed 22 Dec. 2023.

[547] “Service Stop.” Service Stop, Technique T1489 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1489/. Accessed 22 Dec. 2023.

[548] “Shared Modules.” Shared Modules, Technique T1129 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1129/. Accessed 22 Dec. 2023.

[549] “Software Deployment Tools.” Software Deployment Tools, Technique T1072 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1072/. Accessed 22 Dec. 2023.

[550] “Software Discovery.” Software Discovery, Technique T1518 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1518/. Accessed 22 Dec. 2023.

[551] “Software Discovery: Security Software Discovery.” Software Discovery: Security Software Discovery, Sub-Technique T1518.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1518/001/. Accessed 22 Dec. 2023.

[552] “Stage Capabilities.” Stage Capabilities, Technique T1608 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/. Accessed 22 Dec. 2023.

[553] “Stage Capabilities: Upload Malware.” Stage Capabilities: Upload Malware, Sub-Technique T1608.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/001/. Accessed 22 Dec. 2023.

[554] “Stage Capabilities: Upload Tool.” Stage Capabilities: Upload Tool, Sub-Technique T1608.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/002/. Accessed 22 Dec. 2023.

[555] “Stage Capabilities: Install Digital Certificate.” Stage Capabilities: Install Digital Certificate, Sub-Technique T1608.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/003/. Accessed 22 Dec. 2023.

[556] “Stage Capabilities: Drive-by Target.” Stage Capabilities: Drive-by Target, Sub-Technique T1608.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/004/. Accessed 22 Dec. 2023.

[557] “Stage Capabilities: Link Target.” Stage Capabilities: Link Target, Sub-Technique T1608.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/005/. Accessed 22 Dec. 2023.

[558] “Stage Capabilities: Seo Poisoning.” Stage Capabilities: SEO Poisoning, Sub-Technique T1608.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1608/006/. Accessed 22 Dec. 2023.

[559] “Steal Application Access Token.” Steal Application Access Token, Technique T1528 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1528/. Accessed 22 Dec. 2023.

[560] “Steal or Forge Authentication Certificates.” Steal or Forge Authentication Certificates, Technique T1649 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1649/. Accessed 22 Dec. 2023.

[561] “Steal or Forge Kerberos Tickets.” Steal or Forge Kerberos Tickets, Technique T1558 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1558/. Accessed 22 Dec. 2023.

[562] “Steal or Forge Kerberos Tickets: Golden Ticket.” Steal or Forge Kerberos Tickets: Golden Ticket, Sub-Technique T1558.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1558/001/. Accessed 22 Dec. 2023.

[563] “Steal or Forge Kerberos Tickets: Silver Ticket.” Steal or Forge Kerberos Tickets: Silver Ticket, Sub-Technique T1558.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1558/002/. Accessed 22 Dec. 2023.

[564] “Steal or Forge Kerberos Tickets: Kerberoasting.” Steal or Forge Kerberos Tickets: Kerberoasting, Sub-Technique T1558.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1558/003/. Accessed 22 Dec. 2023.

[565] “Steal or Forge Kerberos Tickets: As-Rep Roasting.” Steal or Forge Kerberos Tickets: AS-REP Roasting, Sub-Technique T1558.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1558/004/. Accessed 22 Dec. 2023.

[566] “Steal Web Session Cookie.” Steal Web Session Cookie, Technique T1539 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1539/. Accessed 22 Dec. 2023.

[567] “Subvert Trust Controls.” Subvert Trust Controls, Technique T1553 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/. Accessed 22 Dec. 2023.

[568] “Subvert Trust Controls: Gatekeeper Bypass.” Subvert Trust Controls: Gatekeeper Bypass, Sub-Technique T1553.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/001/. Accessed 22 Dec. 2023.

[569] “Subvert Trust Controls: Code Signing.” Subvert Trust Controls: Code Signing, Sub-Technique T1553.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/002/. Accessed 22 Dec. 2023.

[570] “Subvert Trust Controls: SIP and Trust Provider Hijacking.” Subvert Trust Controls: SIP and Trust Provider Hijacking, Sub-Technique T1553.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/003/. Accessed 22 Dec. 2023.

[571] “Subvert Trust Controls: Install Root Certificate.” Subvert Trust Controls: Install Root Certificate, Sub-Technique T1553.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/004/. Accessed 22 Dec. 2023.

[572] “Subvert Trust Controls: Mark-of-the-Web Bypass.” Subvert Trust Controls: Mark-of-the-Web Bypass, Sub-Technique T1553.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/005/. Accessed 22 Dec. 2023.

[573] “Subvert Trust Controls: Code Signing Policy Modification.” Subvert Trust Controls: Code Signing Policy Modification, Sub-Technique T1553.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1553/006/. Accessed 22 Dec. 2023.

[574] “Supply Chain Compromise.” Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1195/. Accessed 22 Dec. 2023.

[575] “Supply Chain Compromise: Compromise Software Dependencies and Development Tools.” Supply Chain Compromise: Compromise Software Dependencies and Development Tools, Sub-Technique T1195.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1195/001/. Accessed 22 Dec. 2023.

[576] “Supply Chain Compromise: Compromise Software Supply Chain.” Supply Chain Compromise: Compromise Software Supply Chain, Sub-Technique T1195.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1195/002/. Accessed 22 Dec. 2023.

[577] “Supply Chain Compromise: Compromise Hardware Supply Chain.” Supply Chain Compromise: Compromise Hardware Supply Chain, Sub-Technique T1195.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1195/003/. Accessed 22 Dec. 2023.

[578] “System Binary Proxy Execution.” System Binary Proxy Execution, Technique T1218 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/. Accessed 22 Dec. 2023.

[579] “System Binary Proxy Execution: Compiled HTML File.” System Binary Proxy Execution: Compiled HTML File, Sub-Technique T1218.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/001/. Accessed 22 Dec. 2023.

[580] “System Binary Proxy Execution: Control Panel.” System Binary Proxy Execution: Control Panel, Sub-Technique T1218.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/002/. Accessed 22 Dec. 2023.

[581] “System Binary Proxy Execution: CMSTP.” System Binary Proxy Execution: CMSTP, Sub-Technique T1218.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/003/. Accessed 22 Dec. 2023.

[582] “System Binary Proxy Execution: Installutil.” System Binary Proxy Execution: InstallUtil, Sub-Technique T1218.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/004/. Accessed 22 Dec. 2023.

[583] “System Binary Proxy Execution: Mshta.” System Binary Proxy Execution: Mshta, Sub-Technique T1218.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/005/. Accessed 22 Dec. 2023.

[584] “System Binary Proxy Execution: MSIEXEC.” System Binary Proxy Execution: Msiexec, Sub-Technique T1218.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/007/. Accessed 22 Dec. 2023.

[585] “System Binary Proxy Execution: ODBCCONF.” System Binary Proxy Execution: Odbcconf, Sub-Technique T1218.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/008/. Accessed 22 Dec. 2023.

[586] “System Binary Proxy Execution: Regsvcs/REGASM.” System Binary Proxy Execution: Regsvcs/Regasm, Sub-Technique T1218.009 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/009/. Accessed 22 Dec. 2023.

[587] “System Binary Proxy Execution: REGSVR32.” System Binary Proxy Execution: Regsvr32, Sub-Technique T1218.010 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/010/. Accessed 22 Dec. 2023.

[588] “System Binary Proxy Execution: Rundll32.” System Binary Proxy Execution: Rundll32, Sub-Technique T1218.011 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/011/. Accessed 22 Dec. 2023.

[589] “System Binary Proxy Execution: Verclsid.” System Binary Proxy Execution: Verclsid, Sub-Technique T1218.012 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/012/. Accessed 22 Dec. 2023.

[590] “System Binary Proxy Execution: MAVINJECT.” System Binary Proxy Execution: Mavinject, Sub-Technique T1218.013 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/013/. Accessed 22 Dec. 2023.

[591] “System Binary Proxy Execution: MMC.” System Binary Proxy Execution: MMC, Sub-Technique T1218.014 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1218/014/. Accessed 22 Dec. 2023.

[592] “System Information Discovery.” System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1082/. Accessed 22 Dec. 2023.

[593] “System Location Discovery.” System Location Discovery, Technique T1614 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1614/. Accessed 22 Dec. 2023.

[594] “System Location Discovery: System Language Discovery.” System Location Discovery: System Language Discovery, Sub-Technique T1614.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1614/001/. Accessed 22 Dec. 2023.

[595] “System Network Configuration Discovery.” System Network Configuration Discovery, Technique T1016 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1016/. Accessed 22 Dec. 2023.

[596] “System Network Configuration Discovery: Internet Connection Discovery.” System Network Configuration Discovery: Internet Connection Discovery, Sub-Technique T1016.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1016/001/. Accessed 22 Dec. 2023.

[597] “System Network Configuration Discovery: Wi-Fi Discovery.” System Network Configuration Discovery: Wi-Fi Discovery, Sub-Technique T1016.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1016/002/. Accessed 22 Dec. 2023.

[598] “System Network Connections Discovery.” System Network Connections Discovery, Technique T1049 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1049/. Accessed 22 Dec. 2023.

[599] “System Owner/User Discovery.” System Owner/User Discovery, Technique T1033 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1033/. Accessed 22 Dec. 2023.

[600] "System Script Proxy Execution." System Script Proxy Execution, Technique T1216 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1216/. Accessed 22 Dec. 2023.

[601] "System Script Proxy Execution: PubPrn." System Script Proxy Execution: PubPrn, Sub-Technique T1216.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1216/001/. Accessed 22 Dec. 2023.

[602] "System Service Discovery." System Service Discovery, Technique T1007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1007/. Accessed 22 Dec. 2023.

[603] "System Services." System Services, Technique T1569 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1569/. Accessed 22 Dec. 2023.

[604] "System Services: Launchctl." System Services: Launchctl, Sub-Technique T1569.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1569/001/. Accessed 22 Dec. 2023.

[605] "System Services: Service Execution." System Services: Service Execution, Sub-Technique T1569.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1569/002/. Accessed 22 Dec. 2023.

[606] "System Shutdown/Reboot." System Shutdown/Reboot, Technique T1529 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1529/. Accessed 22 Dec. 2023.

[607] "System Time Discovery." System Time Discovery, Technique T1124 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1124/. Accessed 22 Dec. 2023.

[608] "Taint Shared Content." Taint Shared Content, Technique T1080 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1080/. Accessed 22 Dec. 2023.

[609] "Template Injection." Template Injection, Technique T1221 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1221/. Accessed 22 Dec. 2023.

[610] "Traffic Signaling." Traffic Signaling, Technique T1205 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1205/. Accessed 22 Dec. 2023.

[611] "Traffic Signaling: Port Knocking." Traffic Signaling: Port Knocking, Sub-Technique T1205.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1205/001/. Accessed 22 Dec. 2023.

[612] "Traffic Signaling: Socket Filters." Traffic Signaling: Socket Filters, Sub-Technique T1205.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1205/002/. Accessed 22 Dec. 2023.

[613] "Transfer Data to Cloud Account." Transfer Data to Cloud Account, Technique T1537 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1537/. Accessed 22 Dec. 2023.

[614] "Trusted Developer Utilities Proxy Execution." Trusted Developer Utilities Proxy Execution, Technique T1127 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1127/. Accessed 22 Dec. 2023.

[615] "Trusted Developer Utilities Proxy Execution: MSBuild." Trusted Developer Utilities Proxy Execution: MSBuild, Sub-Technique T1127.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1127/001/. Accessed 22 Dec. 2023.

[616] "Trusted Relationship." Trusted Relationship, Technique T1199 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1199/. Accessed 22 Dec. 2023.

[617] "Unsecured Credentials." Unsecured Credentials, Technique T1552 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/. Accessed 22 Dec. 2023.

[618] "Unsecured Credentials: Credentials in Files." Unsecured Credentials: Credentials In Files, Sub-Technique T1552.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/001/. Accessed 22 Dec. 2023.

[619] "Unsecured Credentials: Credentials in Registry." Unsecured Credentials: Credentials in Registry, Sub-Technique T1552.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/002/. Accessed 22 Dec. 2023.

[620] "Unsecured Credentials: Bash History." Unsecured Credentials: Bash History, Sub-Technique T1552.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/003/. Accessed 22 Dec. 2023.

[621] "Unsecured Credentials: Private Keys." Unsecured Credentials: Private Keys, Sub-Technique T1552.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/004/. Accessed 22 Dec. 2023.

[622] "Unsecured Credentials: Cloud Instance Metadata API." Unsecured Credentials: Cloud Instance Metadata API, Sub-Technique T1552.005 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/005/. Accessed 22 Dec. 2023.

[623] "Unsecured Credentials: Group Policy Preferences." Unsecured Credentials: Group Policy Preferences, Sub-Technique T1552.006 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/006/. Accessed 22 Dec. 2023.

[624] "Unsecured Credentials: Container API." Unsecured Credentials: Container API, Sub-Technique T1552.007 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/007/. Accessed 22 Dec. 2023.

[625] "Unsecured Credentials: Chat Messages." Unsecured Credentials: Chat Messages, Sub-Technique T1552.008 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1552/008/. Accessed 22 Dec. 2023.

[626] "Unused/Unsupported Cloud Regions." Unused/Unsupported Cloud Regions, Technique T1535 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1535/. Accessed 22 Dec. 2023.

[627] "Use Alternate Authentication Material." Use Alternate Authentication Material, Technique T1550 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1550/. Accessed 22 Dec. 2023.

[628] "Use Alternate Authentication Material: Application Access Token." Use Alternate Authentication Material: Application Access Token, Sub-Technique T1550.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1550/001/. Accessed 22 Dec. 2023.

[629] "Use Alternate Authentication Material: Pass the Hash." Use Alternate Authentication Material: Pass the Hash, Sub-Technique T1550.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1550/002/. Accessed 22 Dec. 2023.

[630] "Use Alternate Authentication Material: Pass the Ticket." Use Alternate Authentication Material: Pass the Ticket, Sub-Technique T1550.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1550/003/. Accessed 22 Dec. 2023.

[631] "Use Alternate Authentication Material: Web Session Cookie." Use Alternate Authentication Material: Web Session Cookie, Sub-Technique T1550.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1550/004/. Accessed 22 Dec. 2023.

[632] "User Execution." User Execution, Technique T1204 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1204/. Accessed 22 Dec. 2023.

[633] "User Execution: Malicious Link." User Execution: Malicious Link, Sub-Technique T1204.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1204/001/. Accessed 22 Dec. 2023.

[634] "User Execution: Malicious File." User Execution: Malicious File, Sub-Technique T1204.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1204/002/. Accessed 22 Dec. 2023.

[635] "User Execution: Malicious Image." User Execution: Malicious Image, Sub-Technique T1204.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1204/003/. Accessed 22 Dec. 2023.

[636] "Valid Accounts." Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1078/. Accessed 22 Dec. 2023.

[637] "Valid Accounts: Default Accounts." Valid Accounts: Default Accounts, Sub-Technique T1078.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1078/001/. Accessed 22 Dec. 2023.

[638] "Valid Accounts: Domain Accounts." Valid Accounts: Domain Accounts, Sub-Technique T1078.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1078/002/. Accessed 22 Dec. 2023.

[639] "Valid Accounts: Local Accounts." Valid Accounts: Local Accounts, Sub-Technique T1078.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1078/003/. Accessed 22 Dec. 2023.

[640] "Valid Accounts: Cloud Accounts." Valid Accounts: Cloud Accounts, Sub-Technique T1078.004 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1078/004/. Accessed 22 Dec. 2023.

[641] "Video Capture." Video Capture, Technique T1125 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1125/. Accessed 22 Dec. 2023.

[642] "Virtualization/Sandbox Evasion." Virtualization/Sandbox Evasion, Technique T1497 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1497/. Accessed 22 Dec. 2023.

[643] "Virtualization/Sandbox Evasion: System Checks." Virtualization/Sandbox Evasion: System Checks, Sub-Technique T1497.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1497/001/. Accessed 22 Dec. 2023.

[644] "Virtualization/Sandbox Evasion: User Activity Based Checks." Virtualization/Sandbox Evasion: User Activity Based Checks, Sub-Technique T1497.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1497/002/. Accessed 22 Dec. 2023.

[645] "Virtualization/Sandbox Evasion: Time Based Evasion." Virtualization/Sandbox Evasion: Time Based Evasion, Sub-Technique T1497.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1497/003/. Accessed 22 Dec. 2023.

[646] “Weaken Encryption.” Weaken Encryption, Technique T1600 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1600/. Accessed 22 Dec. 2023.

[647] “Weaken Encryption: Reduce Key Space.” Weaken Encryption: Reduce Key Space, Sub-Technique T1600.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1600/001/. Accessed 22 Dec. 2023.

[648] “Weaken Encryption: Disable Crypto Hardware.” Weaken Encryption: Disable Crypto Hardware, Sub-Technique T1600.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1600/002/. Accessed 22 Dec. 2023.

[649] “Web Service.” Web Service, Technique T1102 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1102/. Accessed 22 Dec. 2023.

[650] “Web Service: Dead Drop Resolver.” Web Service: Dead Drop Resolver, Sub-Technique T1102.001 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1102/001/. Accessed 22 Dec. 2023.

[651] “Web Service: Bidirectional Communication.” Web Service: Bidirectional Communication, Sub-Technique T1102.002 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1102/002/. Accessed 22 Dec. 2023.

[652] “Web Service: One-Way Communication.” Web Service: One-Way Communication, Sub-Technique T1102.003 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1102/003/. Accessed 22 Dec. 2023.

[653] “Windows Management Instrumentation.” Windows Management Instrumentation, Technique T1047 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1047/. Accessed 22 Dec. 2023.

[654] “XSL Script Processing.” XSL Script Processing, Technique T1220 - Enterprise | MITRE ATT&CK®, attack.mitre.org/techniques/T1220/. Accessed 22 Dec. 2023.

[655] “Abuse Elevation Control Mechanism.” Abuse Elevation Control Mechanism, Technique T1626 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1626/. Accessed 22 Dec. 2023.

[656] “Abuse Elevation Control Mechanism: Device Administrator Permissions.” Abuse Elevation Control Mechanism: Device Administrator Permissions, Sub-Technique T1626.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1626/001/. Accessed 22 Dec. 2023.

[657] “Access Notifications.” Access Notifications, Technique T1517 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1517/. Accessed 22 Dec. 2023.

[658] “Account Access Removal.” Account Access Removal, Technique T1640 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1640/. Accessed 22 Dec. 2023.

[659] “Adversary-in-the-Middle.” Adversary-in-the-Middle, Technique T1638 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1638/. Accessed 22 Dec. 2023.

[660] “Application Layer Protocol.” Application Layer Protocol, Technique T1437 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1437/. Accessed 22 Dec. 2023.

[661] “Application Layer Protocol: Web Protocols.” Application Layer Protocol: Web Protocols, Sub-Technique T1437.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1437/001/. Accessed 22 Dec. 2023.

[662] “Application Versioning.” Application Versioning, Technique T1661 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1661/. Accessed 22 Dec. 2023.

[663] “Archive Collected Data.” Archive Collected Data, Technique T1532 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1532/. Accessed 22 Dec. 2023.

[664] “Audio Capture.” Audio Capture, Technique T1429 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1429/. Accessed 22 Dec. 2023.

[665] “Boot or Logon Initialization Scripts.” Boot or Logon Initialization Scripts, Technique T1398 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1398/. Accessed 22 Dec. 2023.

[666] “Call Control.” Call Control, Technique T1616 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1616/. Accessed 22 Dec. 2023.

[667] “Clipboard Data.” Clipboard Data, Technique T1414 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1414/. Accessed 22 Dec. 2023.

[668] “Command and Scripting Interpreter.” Command and Scripting Interpreter, Technique T1623 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1623/. Accessed 22 Dec. 2023.

[669] “Command and Scripting Interpreter: Unix Shell.” Command and Scripting Interpreter: Unix Shell, Sub-Technique T1623.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1623/001/. Accessed 22 Dec. 2023.

[670] “Compromise Application Executable.” Compromise Application Executable, Technique T1577 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1577/. Accessed 22 Dec. 2023.

[671] “Compromise Client Software Binary.” Compromise Client Software Binary, Technique T1645 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1645/. Accessed 22 Dec. 2023.

[672] “Credentials from Password Store.” Credentials from Password Store, Technique T1634 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1634/. Accessed 22 Dec. 2023.

[673] “Credentials from Password Store: Keychain.” Credentials from Password Store: Keychain, Sub-Technique T1634.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1634/001/. Accessed 22 Dec. 2023.

[674] “Data Destruction.” Data Destruction, Technique T1662 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1662/. Accessed 22 Dec. 2023.

[675] “Data Encrypted for Impact.” Data Encrypted for Impact, Technique T1471 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1471/. Accessed 22 Dec. 2023.

[676] “Data from Local System.” Data from Local System, Technique T1533 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1533/. Accessed 22 Dec. 2023.

[677] “Data Manipulation.” Data Manipulation, Technique T1641 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1641/. Accessed 22 Dec. 2023.

[678] “Data Manipulation: Transmitted Data Manipulation.” Data Manipulation: Transmitted Data Manipulation, Sub-Technique T1641.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1641/001/. Accessed 22 Dec. 2023.

[679] “Download New Code at Runtime.” Download New Code at Runtime, Technique T1407 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1407/. Accessed 22 Dec. 2023.

[680] “Drive-by Compromise.” Drive-By Compromise, Technique T1456 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1456/. Accessed 22 Dec. 2023.

[681] “Dynamic Resolution.” Dynamic Resolution, Technique T1637 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1637/. Accessed 22 Dec. 2023.

[682] “Dynamic Resolution: Domain Generation Algorithms.” Dynamic Resolution: Domain Generation Algorithms, Sub-Technique T1637.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1637/001/. Accessed 22 Dec. 2023.

[683] “Encrypted Channel.” Encrypted Channel, Technique T1521 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1521/. Accessed 22 Dec. 2023.

[684] “Encrypted Channel: Symmetric Cryptography.” Encrypted Channel: Symmetric Cryptography, Sub-Technique T1521.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1521/001/. Accessed 22 Dec. 2023.

[685] “Encrypted Channel: Asymmetric Cryptography.” Encrypted Channel: Asymmetric Cryptography, Sub-Technique T1521.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1521/002/. Accessed 22 Dec. 2023.

[686] “Endpoint Denial of Service.” Endpoint Denial of Service, Technique T1642 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1642/. Accessed 22 Dec. 2023.

[687] “Event Triggered Execution.” Event Triggered Execution, Technique T1624 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1624/. Accessed 22 Dec. 2023.

[688] “Event Triggered Execution: Broadcast Receivers.” Event Triggered Execution: Broadcast Receivers, Sub-Technique T1624.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1624/001/. Accessed 22 Dec. 2023.

[689] “Execution Guardrails.” Execution Guardrails, Technique T1627 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1627/. Accessed 22 Dec. 2023.

[690] “Execution Guardrails: Geofencing.” Execution Guardrails: Geofencing, Sub-Technique T1627.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1627/001/. Accessed 22 Dec. 2023.

[691] “Exfiltration over Alternative Protocol.” Exfiltration Over Alternative Protocol, Technique T1639 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1639/. Accessed 22 Dec. 2023.

[692] “Exfiltration over Alternative Protocol: Exfiltration over Unencrypted Non-C2 Protocol.” Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Sub-Technique T1639.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1639/001/. Accessed 22 Dec. 2023.

[693] “Exfiltration over C2 Channel.” Exfiltration Over C2 Channel, Technique T1646 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1646/. Accessed 22 Dec. 2023.

[694] “Exploitation for Client Execution.” Exploitation for Client Execution, Technique T1658 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1658/. Accessed 22 Dec. 2023.

[695] “Exploitation for Privilege Escalation.” Exploitation for Privilege Escalation, Technique T1404 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1404/. Accessed 22 Dec. 2023.

[696] “Exploitation of Remote Services.” Exploitation of Remote Services, Technique T1428 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1428/. Accessed 22 Dec. 2023.

[697] “File and Directory Discovery.” File and Directory Discovery, Technique T1420 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1420/. Accessed 22 Dec. 2023.

[698] “Foreground Persistence.” Foreground Persistence, Technique T1541 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1541/. Accessed 22 Dec. 2023.

[699] “Generate Traffic from Victim.” Generate Traffic from Victim, Technique T1643 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1643/. Accessed 22 Dec. 2023.

[700] “Hide Artifacts.” Hide Artifacts, Technique T1628 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1628/. Accessed 22 Dec. 2023.

[701] “Hide Artifacts: Suppress Application Icon.” Hide Artifacts: Suppress Application Icon, Sub-Technique T1628.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1628/001/. Accessed 22 Dec. 2023.

[702] “Hide Artifacts: User Evasion.” Hide Artifacts: User Evasion, Sub-Technique T1628.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1628/002/. Accessed 22 Dec. 2023.

[703] “Hijack Execution Flow.” Hijack Execution Flow, Technique T1625 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1625/. Accessed 22 Dec. 2023.

[704] “Hijack Execution Flow: System Runtime API Hijacking.” Hijack Execution Flow: System Runtime API Hijacking, Sub-Technique T1625.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1625/001/. Accessed 22 Dec. 2023.

[705] “Hooking.” Hooking, Technique T1617 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1617/. Accessed 22 Dec. 2023.

[706] “Impair Defenses.” Impair Defenses, Technique T1629 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1629/. Accessed 22 Dec. 2023.

[707] “Impair Defenses: Prevent Application Removal.” Impair Defenses: Prevent Application Removal, Sub-Technique T1629.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1629/001/. Accessed 22 Dec. 2023.

[708] “Impair Defenses: Device Lockout.” Impair Defenses: Device Lockout, Sub-Technique T1629.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1629/002/. Accessed 22 Dec. 2023.

[709] “Impair Defenses: Disable or Modify Tools.” Impair Defenses: Disable or Modify Tools, Sub-Technique T1629.003 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1629/003/. Accessed 22 Dec. 2023.

[710] “Indicator Removal on Host.” Indicator Removal on Host, Technique T1630 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1630/. Accessed 22 Dec. 2023.

[711] “Indicator Removal on Host: Uninstall Malicious Application.” Indicator Removal on Host: Uninstall Malicious Application, Sub-Technique T1630.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1630/001/. Accessed 22 Dec. 2023.

[712] “Indicator Removal on Host: File Deletion.” Indicator Removal on Host: File Deletion, Sub-Technique T1630.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1630/002/. Accessed 22 Dec. 2023.

[713] “Indicator Removal on Host: Disguise Root/Jailbreak Indicators.” Indicator Removal on Host: Disguise Root/Jailbreak Indicators, Sub-Technique T1630.003 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1630/003/. Accessed 22 Dec. 2023.

[714] “Ingress Tool Transfer.” Ingress Tool Transfer, Technique T1544 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1544/. Accessed 22 Dec. 2023.

[715] “Input Capture.” Input Capture, Technique T1417 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1417/. Accessed 22 Dec. 2023.

[716] “Input Capture: Keylogging.” Input Capture: Keylogging, Sub-Technique T1417.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1417/001/. Accessed 22 Dec. 2023.

[717] “Input Capture: Gui Input Capture.” Input Capture: GUI Input Capture, Sub-Technique T1417.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1417/002/. Accessed 22 Dec. 2023.

[718] “Input Injection.” Input Injection, Technique T1516 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1516/. Accessed 22 Dec. 2023.

[719] “Location Tracking.” Location Tracking, Technique T1430 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1430/. Accessed 22 Dec. 2023.

[720] “Location Tracking: Remote Device Management Services.” Location Tracking: Remote Device Management Services, Sub-Technique T1430.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1430/001/. Accessed 22 Dec. 2023.

[721] “Location Tracking: Impersonate SS7 Nodes.” Location Tracking: Impersonate SS7 Nodes, Sub-Technique T1430.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1430/002/. Accessed 22 Dec. 2023.

[722] “Lockscreen Bypass.” Lockscreen Bypass, Technique T1461 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1461/. Accessed 22 Dec. 2023.

[723] “Masquerading.” Masquerading, Technique T1655 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1655/. Accessed 22 Dec. 2023.

[724] “Masquerading: Match Legitimate Name or Location.” Masquerading: Match Legitimate Name or Location, Sub-Technique T1655.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1655/001/. Accessed 22 Dec. 2023.

[725] “Native Api.” Native API, Technique T1575 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1575/. Accessed 22 Dec. 2023.

[726] “Network Denial of Service.” Network Denial of Service, Technique T1464 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1464/. Accessed 22 Dec. 2023.

[727] “Network Service Scanning.” Network Service Scanning, Technique T1423 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1423/. Accessed 22 Dec. 2023.

[728] “Non-Standard Port.” Non-Standard Port, Technique T1509 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1509/. Accessed 22 Dec. 2023.

[729] “Obfuscated Files or Information.” Obfuscated Files or Information, Technique T1406 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1406/. Accessed 22 Dec. 2023.

[730] “Obfuscated Files or Information: Steganography.” Obfuscated Files or Information: Steganography, Sub-Technique T1406.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1406/001/. Accessed 22 Dec. 2023.

[731] “Obfuscated Files or Information: Software Packing.” Obfuscated Files or Information: Software Packing, Sub-Technique T1406.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1406/002/. Accessed 22 Dec. 2023.

[732] “Out of Band Data.” Out of Band Data, Technique T1644 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1644/. Accessed 22 Dec. 2023.

[733] “Phishing.” Phishing, Technique T1660 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1660/. Accessed 22 Dec. 2023.

[734] “Process Discovery.” Process Discovery, Technique T1424 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1424/. Accessed 22 Dec. 2023.

[735] “Process Injection.” Process Injection, Technique T1631 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1631/. Accessed 22 Dec. 2023.

[736] “Process Injection: Ptrace System Calls.” Process Injection: Ptrace System Calls, Sub-Technique T1631.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1631/001/. Accessed 22 Dec. 2023.

[737] “Protected User Data.” Protected User Data, Technique T1636 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1636/. Accessed 22 Dec. 2023.

[738] “Protected User Data: Calendar Entries.” Protected User Data: Calendar Entries, Sub-Technique T1636.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1636/001/. Accessed 22 Dec. 2023.

[739] “Protected User Data: Call Log.” Protected User Data: Call Log, Sub-Technique T1636.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1636/002/. Accessed 22 Dec. 2023.

[740] “Protected User Data: Contact List.” Protected User Data: Contact List, Sub-Technique T1636.003 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1636/003/. Accessed 22 Dec. 2023.

[741] “Protected User Data: SMS Messages.” Protected User Data: SMS Messages, Sub-Technique T1636.004 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1636/004/. Accessed 22 Dec. 2023.

[742] “Proxy through Victim.” Proxy Through Victim, Technique T1604 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1604/. Accessed 22 Dec. 2023.

[743] “Remote Access Software.” Remote Access Software, Technique T1663 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1663/. Accessed 22 Dec. 2023.

[744] “Replication through Removable Media.” Replication Through Removable Media, Technique T1458 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1458/. Accessed 22 Dec. 2023.

[745] “Scheduled Task/Job.” Scheduled Task/Job, Technique T1603 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1603/. Accessed 22 Dec. 2023.

[746] “Screen Capture.” Screen Capture, Technique T1513 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1513/. Accessed 22 Dec. 2023.

[747] “SMS Control.” SMS Control, Technique T1582 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1582/. Accessed 22 Dec. 2023.

[748] “Software Discovery.” Software Discovery, Technique T1418 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1418/. Accessed 22 Dec. 2023.

[749] “Software Discovery: Security Software Discovery.” Software Discovery: Security Software Discovery, Sub-Technique T1418.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1418/001/. Accessed 22 Dec. 2023.

[750] “Steal Application Access Token.” Steal Application Access Token, Technique T1635 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1635/. Accessed 22 Dec. 2023.

[751] “Steal Application Access Token: Uri Hijacking.” Steal Application Access Token: URI Hijacking, Sub-Technique T1635.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1635/001/. Accessed 22 Dec. 2023.

[752] “Stored Application Data.” Stored Application Data, Technique T1409 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1409/. Accessed 22 Dec. 2023.

[753] “Subvert Trust Controls.” Subvert Trust Controls, Technique T1632 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1632/. Accessed 22 Dec. 2023.

[754] “Subvert Trust Controls: Code Signing Policy Modification.” Subvert Trust Controls: Code Signing Policy Modification, Sub-Technique T1632.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1632/001/. Accessed 22 Dec. 2023.

[755] “Supply Chain Compromise.” Supply Chain Compromise, Technique T1474 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1474/. Accessed 22 Dec. 2023.

[756] “Supply Chain Compromise: Compromise Software Dependencies and Development Tools.” Supply Chain Compromise: Compromise Software Dependencies and Development Tools, Sub-Technique T1474.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1474/001/. Accessed 22 Dec. 2023.

[757] “Supply Chain Compromise: Compromise Hardware Supply Chain.” Supply Chain Compromise: Compromise Hardware Supply Chain, Sub-Technique T1474.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1474/002/. Accessed 22 Dec. 2023.

[758] “Supply Chain Compromise: Compromise Software Supply Chain.” Supply Chain Compromise: Compromise Software Supply Chain, Sub-Technique T1474.003 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1474/003/. Accessed 22 Dec. 2023.

[759] “System Information Discovery.” System Information Discovery, Technique T1426 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1426/. Accessed 22 Dec. 2023.

[760] “System Network Configuration Discovery.” System Network Configuration Discovery, Technique T1422 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1422/. Accessed 22 Dec. 2023.

[761] “System Network Connections Discovery.” System Network Connections Discovery, Technique T1421 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1421/. Accessed 22 Dec. 2023.

[762] “Video Capture.” Video Capture, Technique T1512 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1512/. Accessed 22 Dec. 2023.

[763] “Virtualization/Sandbox Evasion.” Virtualization/Sandbox Evasion, Technique T1633 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1633/. Accessed 22 Dec. 2023.

[764] “Virtualization/Sandbox Evasion: System Checks.” Virtualization/Sandbox Evasion: System Checks, Sub-Technique T1633.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1633/001/. Accessed 22 Dec. 2023.

[765] “Web Service.” Web Service, Technique T1481 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1481/. Accessed 22 Dec. 2023.

[766] “Web Service: Dead Drop Resolver.” Web Service: Dead Drop Resolver, Sub-Technique T1481.001 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1481/001/. Accessed 22 Dec. 2023.

[767] “Web Service: Bidirectional Communication.” Web Service: Bidirectional Communication, Sub-Technique T1481.002 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1481/002/. Accessed 22 Dec. 2023.

[768] “Web Service: One-Way Communication.” Web Service: One-Way Communication, Sub-Technique T1481.003 - Mobile | MITRE ATT&CK®, attack.mitre.org/techniques/T1481/003/. Accessed 22 Dec. 2023.

[769] Strom, Blake E., et al. "MITRE ATT&CK: Design and philosophy." Technical report. The MITRE Corporation, 2018.

[770] Dobson, Geoffrey B., and Kathleen M. Carley. "Cyber-FIT: an agent-based modelling approach to simulating cyber warfare." Social, Cultural, and Behavioral Modeling: 10th International Conference, SBP-BRiMS 2017, Washington, DC, USA, July 5-8, 2017, Proceedings 10. Springer International Publishing, 2017.

[771] Dobson, G. B., A. Rege, and K. M. Carley. "Informing active cyber defence with realistic adversarial behaviour." Journal of Information Warfare 17.2 (2018): 16-31.

[772] Dobson, Geoffrey B., and Kathleen M. Carley. "A computational model of cyber situational awareness." Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, July 10-13, 2018, Proceedings 11. Springer International Publishing, 2018.

[773] Dobson, Geoffrey B., and Kathleen M. Carley. "Cyber-FIT Agent-Based Simulation Framework Version 4." Center for the Computational Analysis of Social and Organizational Systems (2021).

[774] Dobson, Geoffrey. Cyber-Forces, Interactions, Terrain: An agent-based framework for simulating cyber team performance. Diss. Carnegie Mellon University, 2022.

[775] Shin, Jeongkeun, et al. "OSIRIS: Organization Simulation in Response to Intrusion Strategies." International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Cham: Springer International Publishing, 2022.

[776] Shin, Jeongkeun, et al. "Modeling and Simulation of the Human Firewall Against Phishing Attacks in Small and Medium-Sized Businesses." 2023 Annual Modeling and Simulation Conference (ANNSIM). IEEE, 2023.

[777] Shin, Jeongkeun, et al. “Leveraging OSIRIS to Simulate Real-world Ransomware Attacks on Organization”. 2022 Winter Simulation Conference (WSC) Poster Session, 2022.

[778] Shin, Jeongkeun, Kathleen M. Carley, and L. Richard Carley. "Integrating Human Factors into Agent-Based Simulation for Dynamic Phishing Susceptibility." International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Cham: Springer Nature Switzerland, 2023.

[779] Shin, Jeongkeun, et al. "Beyond Accuracy: Cybersecurity Resilience Evaluation of Intrusion Detection System against DoS Attacks using Agent-based Simulation." 2023 Winter Simulation Conference (WSC). Forthcoming, 2023.

[780] MITRE CVE. “CVE List.” CVE, cve.mitre.org/cve/. Accessed 22 Dec. 2023.

[781] OpenAI, “GPT-4 Technical Report,” 2023, https://cdn.openai.com/papers/gpt-4.pdf.

[782] “Enterprise Mitigations.” Mitigations - Enterprise | MITRE ATT&CK®, attack.mitre.org/mitigations/enterprise/. Accessed 22 Dec. 2023.

[783] “Mobile Mitigations.” Mitigations - Mobile | MITRE ATT&CK®, attack.mitre.org/mitigations/mobile/. Accessed 22 Dec. 2023.

[784] Carley, Kathleen M. "Social cybersecurity: an emerging science." Computational and mathematical organization theory 26.4 (2020): 365-381.