## Senior Upgrade Cheats v1.0 HOST

[Senior Upgrade Cheats v1.0 HOST 1](#_Toc153445528)

[1.1.1 (U) (U) Given intelligence reporting describe how to integrate it into tactical planning. 2](#_Toc1044548427)

[Training Resources & Technical References: 2](#_Toc1710311672)

[1.1.2 (U) Describe the process of developing analytics to support mission requirements and reporting. 5](#_Toc1336477003)

[Training Resources & Technical References: 5](#_Toc1532846545)

[1.1.4 (U) Describe under what circumstances you would need to engage with the local Counter Intelligence or law enforcement agencies. 7](#_Toc185775710)

[1.1.5 (U) Given a critical asset list/key terrain cyber prioritize vulnerabilities for the mission owner. 7](#_Toc1465302816)

[1.1.6 (U) Describe the chain of custody and your role in maintaining it and relationship with CI/LE. 8](#_Toc941817065)

[1.1.7 (U) Demonstrate understanding of the following policies and documents: 9](#_Toc1241327149)

[1.1.8 (U) Explain the difference between Cyberspace authorities and SIGINT authorities. 10](#_Toc1366529568)

[1.1.9 (U) (U) Describe the ME Lead’s responsibilities toward mission owner interaction. 10](#_Toc131433397)

[1.1.10 (U) Describe how the ME Lead will synchronize efforts with local defenders, customer and key stakeholders. 11](#_Toc2072857491)

[1.1.11 (U) Describe how, by working with the mission owner, the ME Lead can determine where to concentrate data collection. 11](#_Toc1516222172)

[1.1.12 (U) Explain the importance of an out-brief and what should be included. 12](#_Toc1873640108)

[1.1.13 (U) Explain the importance of the final report and what it should include. 15](#_Toc85340296)

[1.1.14 (U) Explain how to prioritize Host Analyst findings and mitigation recommendations in the final report. 15](#_Toc2092868894)

[1.1.15 (U) Describe the ME Leads responsibilities for reporting. 15](#_Toc1267521917)

[1.1.16 (U) Describe how to utilize “phase line” when executing the mission and the importance of it. 16](#_Toc613063006)

[1.2.1 (U) Discuss what a collection plan is and how pertinent it is to accomplish a successful mission. 18](#_Toc92409513)

[1.2.2 (U) Given a list of resources define what is relevant in building a collection plan. 18](#_Toc2099385324)

[1.2.3 (U) Identify the steps on building a collection plan. 19](#_Toc659086098)

[1.2.4 (U) (U) Explain why it is important to understand the customer’s organizational policies for users and computers. 21](#_Toc455614977)

[1.2.5 (U) Identify the importance of a Pre-Deployment Site Survey. 21](#_Toc1318210218)

[1.2.6 (U) Define the term “Rules of Engagement” and how it applies to a mission. 21](#_Toc2112220299)

[1.3.1 (U) (U) Given organization system policy identify invalid active directory objects. 21](#_Toc1620024420)

[1.3.2 (U) Given an Active Directory domain audit policy and threat actor tactics, techniques and procedures identify auditing gaps that would prevent logging. 22](#_Toc1668182820)

[1.3.3 (U) Demonstrate using PowerShell to manage Active Directory applicable to cyber operations. 23](#_Toc1321645361)

[1.3.4 (U) Interpret and configure host-based firewalls and Host Intrusion Prevention Systems through group policy. 23](#_Toc1639221930)

[1.3.5 (U) Explain how to ensure patches are up to date for all domain workstations and determine effectiveness of current process for updating. 25](#_Toc1621253166)

[1.3.6 (U) Given a list of IOCs identify key log entries/Event IDs ,use a Security information and event management (SIEM) platform to correlate indicators of compromise, and develop dashboards to better visualize data. 25](#_Toc76706626)

[1.3.7 (U) Using a SIEM create alerts to detect the creation of unauthorized accounts. 25](#_Toc1785220479)

[1.3.8 (U) (U) Configure, forward, and statically analyze logs from all workstations in an enterprise environment. 26](#_Toc1902203248)

[1.3.9 (U) Explain how to oversee the development of host-based IDS/IPS signatures, settings, and applicable agents. 26](#_Toc1885141033)

[1.3.10 (U) Explain how to oversee the tuning of host-based IDS/IPS alerts in order to evaluate their severity while eliminating false positives. 27](#_Toc152623334)

[1.3.11 (U) Given a list of active processes identify libraries, modules, executables, and binaries against databases of known advanced malware. 29](#_Toc559703602)

[1.3.12 (U) Given an IOC, explain how to utilize tools and analysis techniques to identify processes, libraries, modules, and other activity that have been obfuscated and might indicate the presence of a more advanced rootkit on endpoint. 31](#_Toc1995070280)

[1.3.13 (U) Given a Prioritized Defended Asset list, identify which dependent systems are key terrain. 31](#_Toc1422726813)

[1.3.14 (U) Evaluate patch levels on host machines across a complex Windows domain to determine the current patch level consistency. 31](#_Toc1406433180)

[1.3.15 (U) Given a host baseline of configuration/state, for host machines on a network conduct a scan for anomalous configurations. 32](#_Toc1191479539)

[1.3.16 (U) Given a Windows Domain Controller, evaluate information (e.g. users, groups, trust relationships, and security policies) from a complex Domain to identify vulnerabilities/misconfiguration, and how to export this information. 32](#_Toc1616481627)

[1.3.17 (U) Given a script determine what is occurring. 32](#_Toc39966448)

[1.3.18 (U) Perform device discovery in order to conduct enumeration of a complex network while limiting the amount of network traffic generated. 34](#_Toc1987728693)

[1.3.19 (U) Analyze host discovery tool output to generate accurate maps of endpoint systems. 34](#_Toc896747870)

[1.4.1 (U) Given an enterprise domain, explain how to identify potentially malicious processes, connections, libraries, and other malicious code/activity from a memory image and perform trend and outlier analysis. 34](#_Toc2020828412)

[1.4.2 (U) Automate advanced and repetitive tasks on remote workstations within a domain. 35](#_Toc1049980586)

[1.4.3 (U) Assess customer security posture across a complex enterprise network to Identify security posture shortcomings. 36](#_Toc1513207692)

[1.5.1 (U) (U) Given a vulnerability scan and mission owner network information prioritize vulnerabilities for action. 36](#_Toc1713037138)

[1.5.2 (U) Describe and display knowledge of the “After Action Report” and all areas needed to complete one. 36](#_Toc288739427)

[1.5.3 (U) Utilizing MITRE ATT&CK framework, perform complex root-cause analysis to determine the sequence of events related to a compromise and recommend mitigations. 37](#_Toc206311927)

[1.5.4 (U) Utilizing MITRE ATT&CK framework, perform complex root-cause analysis to determine the sequence of events related to a compromise and recommend mitigations 37](#_Toc2142953032)

[1.5.5 (U) Demonstrate familiarity with STIGs on host machines by using any software platform to generate a report for a complex network and follow-up with recommendations. 37](#_Toc168540240)

[1.5.6 (U) Discuss the term “Lessons Learned” and how it applies to the CPT life cycle. 38](#_Toc1043573797)

[1.5.7 (U) Given a scenario, identify steps to recover from a full- network compromise. 38](#_Toc532546468)

[2.1.1 (U) Identify PS modules that are helpful for local analysis. 38](#_Toc1858664099)

[2.1.2 (U) Identify PS module that are helpful for remote analysis. 40](#_Toc1328786485)

[2.1.3 (U) Define what an Agent Based Security System is and how it could be advantageous during a mission. 40](#_Toc1266873201)

[2.1.4 (U) Deploy an agent based security system to an enterprise network. 41](#_Toc532946432)

[2.1.5 (U) Configure and develop rules for CPT host-based agents. 41](#_Toc1479191018)

[2.1.6 (U) Given the Sysinternals suite identify what the specific capabilities the tools can provide. 42](#_Toc1082797723)

[2.1.7 (U) Given a set of sysmon logs identify malicious process creation. 43](#_Toc508098508)

[3.1.1 (U) Detect adversary modification of the following: 44](#_Toc2046430939)

[3.1.2 (U) Detect adversary addition of user to local administrator group: 44](#_Toc823294486)

[3.1.3 (U) Detect adversary addition of root user and sudoer. 45](#_Toc1055584126)

[3.1.4 (U) Detect adversary presence in windows logon and startup scripts. 45](#_Toc1836570708)

[3.1.5 (U) Detect adversary presence in linux logon and startup scripts. 45](#_Toc1387628267)

[3.1.6 (U) Detect adversary addition to BITS jobs. 46](#_Toc587718272)

[3.1.7 (U) Detect DLL Search Order Hijacking. 47](#_Toc1722930165)

[3.1.8 (U) Detect malicious hidden files and/or directories. 48](#_Toc1859219535)

[3.1.l9 (U) Detect the presence of a rootkit. 48](#_Toc90253597)

[3.1.10 (U) Detect the presence of a malicious cronjob. 48](#_Toc133183375)

[3.1.11 (U) Detect the presence of a malware maintaining persistence through scheduled tasks. 49](#_Toc32782982)

[3.1.12 (U) Detect the presence of malware maintaining persistence through modified services. 49](#_Toc582975673)

[3.1.13 (U) Detect the adversary changes to PATH variables. 50](#_Toc733920023)

[3.1.14 (U) Detect the presence of malicious activity using elevated execution permissions from the following methods: 50](#_Toc1027385673)

[3.1.15 (U) Detect the use of shortcut modification. 50](#_Toc1901173059)

[3.1.16 (U) Detect malicious use of WMI event subscription. 51](#_Toc381715858)

[3.1.17 (U) Detect the use of data staging and encoding used prior to exfiltration. 52](#_Toc1833934533)

[3.1.18 (U) Detect the exfiltration of data over removable devices. 53](#_Toc233411999)

[Event ID 6416 - A new external device was recognized by the system. 53](#_Toc30184117)

[3.1.19 (U) Demonstrate the ability to search for Indicators of Compromise on a dead disk. 55](#_Toc434308994)

[3.1.20 (U) Triage malware from dead disk and identify the process to get assistance with reverse engineering. 56](#_Toc1307142486)

[3.1.21 (U) Detect malware in Memory. 56](#_Toc425032090)

[3.1.22 (U) Discover Files using Alternate Data streams. 58](#_Toc2073959843)

[3.1.23 (U) Submit tool and capability requirements to resolve mission gaps in accordance with established policies, regulations, and procedures. 59](#_Toc1421528061)

[3.1.24 (U) Evaluate a comprehensive assessment strategy that leverages available information sources, personnel, and systems to address potential vulnerabilities and risk-related practices. 60](#_Toc1758139951)

[3.1.25 (U) Incorporate open source vulnerability assessment tools into a virtual machine for use in a test environment. 62](#_Toc1396176675)

[3.21 (U) Given current intelligence and a network map, create a host collection plan. 62](#_Toc658918207)

[3.22 (U) Given a scenario and required data, draft or provide input to the host section of a risk mitigation plan. 62](#_Toc681300351)

## 1.1.1 (U) (U) Given intelligence reporting describe how to integrate it into tactical planning.

### Training Resources & Technical References:

 JP 2-01.3

 JP 3-0

 JP 5-0

<https://irp.fas.org/doddir/dod/jp2-01-3.pdf>

<https://irp.fas.org/doddir/dod/jp3_0.pdf>

<https://irp.fas.org/doddir/dod/jp5_0.pdf>

[What is OSINT Open Source Intelligence? - CrowdStrike](https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/)

https://mitre-attack.github.io/attack-navigator/

**Your tactical plan will be a copy and paste from previous missions or you’ll have to create one from scratch. To create a tactical plan, you need to understand that adversary. Sometimes, Intel provides good information and sometimes they don’t. What you should do on every mission is use the tool from Mitre. The tool is** [**https://mitre-attack.github.io/attack-navigator/**](https://mitre-attack.github.io/attack-navigator/)**. You can use existing APTs to see what TTPs they use or upload your own. Each tactical task will cover an area that Mitre or Intel has seen the APT use in the past. You will also have to create MOPs for each tactical task as a way to measure that the task is complete. An example would be: “100% of computers investigated for possibly malicious scheduled tasks.” You will also need to make contingencies if stuff goes wrong. An example is: “switch to Arkime to detect outbound connections if logging isn’t correct to detect EXFIL.**

Intelligence reporting can be integrated into tactical planning by providing information that can help MC/MELs/Leads make informed decisions. Tactical intelligence supports MC in the planning and execution (Researching known APTs TTPs)

Analyze the intelligence report: Start by carefully reviewing and analyzing the intelligence report. Understand the nature of the threats, the attack vectors used, the tools and techniques employed, and any indicators of compromise (IOCs) mentioned. Identify the potential impact on your organization's systems and networks.

Assess the relevance and credibility: Evaluate the relevance and credibility of the intelligence report. Consider the source of the report, its reputation, and the methodology used to gather the information. Verify the accuracy and reliability of the information provided, cross-referencing with other trusted sources if possible.

Conduct a risk assessment: Assess the potential risks and vulnerabilities within the mission partners systems and networks based on the information provided in the intelligence report. Identify any gaps in your current security measures that might be exploited by the threat actors mentioned in the report.

Determine actionable intelligence: Identify actionable intelligence from the report that can be used to improve your organization's defenses or response capabilities. This may include specific IOCs, tactics, techniques, and procedures (TTPs) used by threat actors, or patterns of behavior that can be used to detect and mitigate attacks.

Update Tactical Planning and Hunt Plan: Incorporate the intelligence findings into your hunt platform. This may involve updating intrusion detection systems (IDS), firewall rules, endpoint protection tools, or network monitoring solutions to detect and block the identified IOCs or TTPs.

[Open Source Intelligence (OSINT) is the act of gathering and analyzing publicly available data for intelligence purposes](https://www.bing.com/aclk?ld=e8uKqTrgimIxomzSoLCmW6NDVUCUzChAtAeKOP5ZWT6W4DnGEvX7wCg1XzvOo6QtW_Bh91R8o_YHd3ZPajVS_JmsqlJfETOjxVC3kRgiFWXWpyo5hOgpmKReSci0p-_odC1anLrvgEEuEDhUtxxH_Zz7Oyr_0gxgGaxjcxiMMZ2njwg1rm&u=&rlid=c91fcc5bb1c11a937a50a89c624990d3)[1](https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/). [OSINT provides enterprise cybersecurity teams with publicly available information that can be used to enhance security procedures, validate security controls, and improve their understanding of the threat landscape2](https://flare.io/learn/resources/blog/osint-in-cybersecurity/).

[In the context of cybersecurity, intelligence researchers and analysts leverage open source data to better understand the threat landscape and help defend organizations and individuals from known risks within their IT environment](https://www.bing.com/aclk?ld=e8uKqTrgimIxomzSoLCmW6NDVUCUzChAtAeKOP5ZWT6W4DnGEvX7wCg1XzvOo6QtW_Bh91R8o_YHd3ZPajVS_JmsqlJfETOjxVC3kRgiFWXWpyo5hOgpmKReSci0p-_odC1anLrvgEEuEDhUtxxH_Zz7Oyr_0gxgGaxjcxiMMZ2njwg1rm&u=&rlid=c91fcc5bb1c11a937a50a89c624990d3)[1](https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/). [Some common use cases for OSINT in cybersecurity include measuring the risk to your own organization and understanding the actor, tactics, and targets](https://www.bing.com/aclk?ld=e8uKqTrgimIxomzSoLCmW6NDVUCUzChAtAeKOP5ZWT6W4DnGEvX7wCg1XzvOo6QtW_Bh91R8o_YHd3ZPajVS_JmsqlJfETOjxVC3kRgiFWXWpyo5hOgpmKReSci0p-_odC1anLrvgEEuEDhUtxxH_Zz7Oyr_0gxgGaxjcxiMMZ2njwg1rm&u=&rlid=c91fcc5bb1c11a937a50a89c624990d3)[1](https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/).

A cyber protection team can add open source intelligence to their possible courses of action by using OSINT techniques to gather and analyze publicly available data. [This can include sources such as newspaper and magazine articles, academic papers, social media activity, census data, court filings, public trading data, breach or compromise disclosure information, publicly shared cyberattack indicators like IP addresses or domain/file hashes, certificate or domain registration data, and application or system vulnerability data](https://www.bing.com/aclk?ld=e8uKqTrgimIxomzSoLCmW6NDVUCUzChAtAeKOP5ZWT6W4DnGEvX7wCg1XzvOo6QtW_Bh91R8o_YHd3ZPajVS_JmsqlJfETOjxVC3kRgiFWXWpyo5hOgpmKReSci0p-_odC1anLrvgEEuEDhUtxxH_Zz7Oyr_0gxgGaxjcxiMMZ2njwg1rm&u=&rlid=c91fcc5bb1c11a937a50a89c624990d3)[1](https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/). By leveraging this information, a cyber protection team can gain valuable insights into potential threats and vulnerabilities, allowing them to make more informed decisions about how to protect their organization. [Additionally, there are many free cybersecurity tools and services available that can help organizations further advance their security capabilities3](https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools).

## 1.1.2 (U) Describe the process of developing analytics to support mission requirements and reporting.

### Training Resources & Technical References:

 Local SOP

Developing analytics to support mission requirements and reporting involves building big data collection (KIT) and analytics capabilities. It also involves analyzing data sources and proposing solutions to strategic planning problems.

The 833d and 836th now collaborate on the same playbooks to store our analytics. The location of the playbooks is: [836 COS / Playbooks · GitLab (af.mil)](https://code.levelup.cce.af.mil/836-cos/playbooks)

* Define mission requirements: Start by clearly defining the mission requirements for your DFIR team or organization. Understand the specific objectives and goals you aim to achieve through your analytics efforts. This may include detecting and analyzing security incidents, identifying patterns of malicious activity, or assessing the impact of cyber threats.
* Identify data sources: Determine the relevant data sources that need to be collected and analyzed to support your mission requirements. This could include log files, network traffic data, system artifacts, memory dumps, or any other sources that can provide valuable insights into security incidents or potential threats.
* Data collection and preprocessing: Develop a strategy for collecting and preprocessing the required data. This may involve deploying monitoring tools, configuring logging mechanisms, or establishing data feeds from various sources. Ensure that the collected data is stored securely and is easily accessible for analysis.
* Define metrics and indicators: Identify the metrics and indicators that will be used to assess the security posture, detect anomalies, or measure the effectiveness of your DFIR efforts. These metrics could be related to network traffic patterns, system behavior, user activities, or any other relevant aspects of your organization's IT infrastructure.
* Analytical techniques selection: Determine the appropriate analytical techniques that can be applied to the collected data to extract meaningful insights. This may include statistical analysis, data mining, machine learning, or behavioral analysis. Consider the specific requirements of your mission and select techniques that align with your goals.
* Develop analytical models: Based on the selected techniques, develop analytical models or algorithms that can process the collected data and generate actionable results. This may involve creating custom scripts, leveraging existing software tools, or developing machine learning models for anomaly detection, classification, or correlation analysis.
* Validate and refine models: Test and validate the developed analytical models using representative datasets or simulated scenarios. Assess their accuracy, performance, and reliability in detecting security incidents or providing relevant insights. Refine the models based on the feedback and make necessary adjustments.
* Continuous improvement: Monitor the performance of your analytics capabilities and continuously refine and enhance them based on the evolving threat landscape and mission requirements. Stay updated with the latest tools, techniques, and industry best practices to ensure the effectiveness and relevance of your analytics capabilities.
* From the information above, you can create Kibana dashboards or use Python3 to find adversary behaviors.

1.1.3 (U) Describe the process for surveilling Named Areas of Interest (NAIs).

Training Resources & Technical References:

 JP 5-0

<https://irp.fas.org/doddir/dod/jp5_0.pdf>

Is a process that involves analyzing the adversary and other relevant aspects of the operational environment to identify possible courses of action and to support joint operation planning, execution. Named areas of interest facilitate intelligence collection, reconnaissance, and surveillance asset employment and intelligence analysis because they focus attention on areas where the threat force must appear if it has selected particular mobility corridor

## 1.1.4 (U) Describe under what circumstances you would need to engage with the local Counter Intelligence or law enforcement agencies.

Training Resources & Technical References:

 EO12333, “Raw SIGINT availability procedures”, <https://fas.org/sgp/othergov/intel/sigint-raw.pdf>

Counter Intelligence or law enforcement agencies are engaged when there is a need to identify challenges, issues, and concerns that emerge at the neighborhood level by gathering real-time data. Law enforcement agencies also need to identify the movement and synergies between terrorists and like-minded individuals and criminal enterprises operating within the continental U.S.

## 1.1.5 (U) Given a critical asset list/key terrain cyber prioritize vulnerabilities for the mission owner.

Training Resources & Technical References:

 CIS Critical Security Controls

<https://www.cisecurity.org/cybersecurity-tools/mapping-compliance>

We prioritize vulnerabilities for the mission owner by discovering, prioritizing, and remediating vulnerabilities and misconfigurations to what the mission owner deems as critical.

First we would take the following list of prioritized terrain (Example from MDS1)

**Prioritized CAPON A1: Key Terrain – Cyber (KT-C)**

1. Mystery-file 131.14.2.3 & muggle-file 131.9.2.4 - These servers are where the mission partner's critical data is stored, and where the adversary is likely to conduct actions on objectives based on the COAs provided

2. Mystery-dc 131.14.2.5 & muggle-dc 131.9.2.3 - If this device is compromised, all other devices can be accessed enabling covert adversary operations and both of the intelligence COAs

3. muggle-mail 131.9.2.5 & Mystery-mail 131.14.2.2 - If these servers are compromised, there are alternate means for the mission partner to communicate (phone for necessary social interactions and the file servers to share files)

4. muggle-clients 131.9.3.0/24 & Mystery-clients 131.14.3.0/24 - The workstations can be exchanged if compromised. The network infrastructure and other assets can help mitigate the risk posed from having vulnerable workstations.

Next, we can use Nessus scan results and the following methodology to perform final prioritization.

**From a Nessus scan on the Key Terrain the following level of vulnerabilities need prioritised by category**

1. Critical: This category includes vulnerabilities that pose a significant risk to the security of the scanned system. These vulnerabilities often have a high severity level and can potentially lead to unauthorized access, data breaches, or system compromise.
2. High: High-risk vulnerabilities that may not be as severe as critical ones but still present a significant security concern. They can potentially lead to unauthorized access or system compromise if left unaddressed.
3. Medium: Medium-risk vulnerabilities that have a moderate impact on the system's security. These vulnerabilities might not pose an immediate threat but should still be addressed to reduce the overall risk level.
4. Low: Low-risk vulnerabilities that have minimal impact on the system's security. These vulnerabilities are typically less critical and may not require immediate attention. However, it's recommended to address them over time to maintain a secure environment.
5. Informational: This category includes non-security-related findings that provide additional information about the scanned system, such as system configurations, software versions, or other details that can help with system management or compliance.
6. Compliance: Nessus can also include a category specific to compliance-related vulnerabilities. These vulnerabilities are often tied to regulatory standards and industry best practices. The compliance category helps identify issues that may impact the system's adherence to specific standards, such as PCI DSS, HIPAA, or ISO 27001.

## 1.1.6 (U) Describe the chain of custody and your role in maintaining it and relationship with CI/LE.

Training Resources & Technical References:

 NIST SP 800-86

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>

Before the analyst begins to collect any data, a decision should be made by the analyst or management (in accordance with the organization’s policies and legal advisors) on the need to collect and preserve evidence in a way that supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. This involves keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence. If it is unclear whether evidence needs to be preserved, by default it generally should be preserved.

## 1.1.7 (U) Demonstrate understanding of the following policies and documents:

[**https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf**](https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf)

[**https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/524001p.pdf**](https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/524001p.pdf)

[**https://dodsioo.defense.gov/Portals/46/DoDD%205148.13%20Intel%20Oversight.pdf?ver=2017-04-27-170536-607**](https://dodsioo.defense.gov/Portals/46/DoDD%205148.13%20Intel%20Oversight.pdf?ver=2017-04-27-170536-607)

**a. Executive Order 12333 (as amended)**

Executive Order 12333 is a United States presidential executive order signed on December 4, 1981 by U.S. President Ronald Reagan. The order defines the responsibilities of the United States Intelligence Community and directs the collection of foreign intelligence information. It also authorizes the use of human intelligence (HUMINT) to collect information not available through other means.

**b. DOD Directive 5240.1 (change 2)**

DoD Directive 5240.1 is a document that reissues and updates policy and direction for DoD intelligence activities, including the collection, retention, and dissemination of information concerning U.S. persons. It implements and is governed by various laws, Executive orders, and Presidential directives. It authorizes the publication of DoD 5240.1-R, a regulation that provides procedures for DoD intelligence activities. It also assigns the Under Secretary of Defense for Intelligence (USD(I)) as the focal point for the Secretary of Defense and other U.S. Government entities and agencies on DoD intelligence matters

**c. DODM 5240.01**

DoD Manual 5240.01 implements the requirement in Executive Order 12333 that Intelligence Community elements establish procedures, approved by the Attorney General, after consultation with the Director of National Intelligence, governing the collection, retention, and dissemination of information concerning U.S. persons. It establishes procedures to enable DoD to conduct authorized intelligence activities in a manner that protects the constitutional and legal rights and the privacy and civil liberties of U.S. persons.

**d. DOD Directive 5148.13**

DoD Directive 5148.13 is a document that establishes policies, responsibilities, and procedures for intelligence oversight in the Department of Defense. It was issued on April 26, 2017 by the Office of the Deputy Chief Management Officer of the Department of Defense. It also prescribes the role and authority of the DoD Senior Intelligence Oversight Official (SIOO), who is responsible for the independent oversight of all intelligence, counterintelligence, and intelligence-related activities in the Department of Defense

Training Resources & Technical References:

 USCC Intelligence Oversight Plan

## 1.1.8 (U) Explain the difference between Cyberspace authorities and SIGINT authorities.

Training Resources & Technical References:

 EO12333, “Raw SIGINT vailability procedures” <https://fas.org/sgp/othergov/intel/sigint-raw.pdf>

 USSID1231

 USSID1610

 ISS-268-11

 ISS-166-11

Cyberspace authorities are responsible for conducting operations in cyberspace to defend the nation’s interests. Signals Intelligence (SIGINT) is intelligence-gathering by interception of signals, whether communications between people or from electronic signals not directly used in communication.

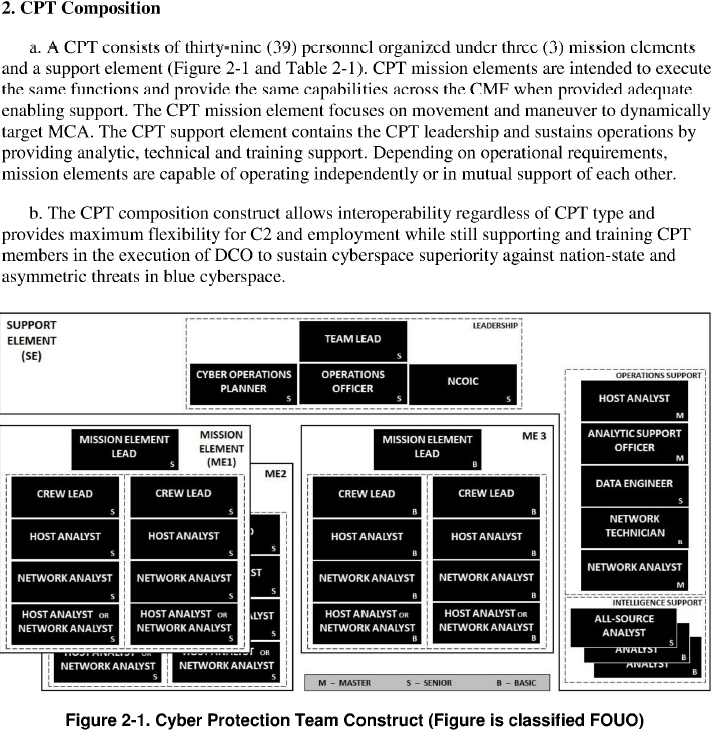
## 1.1.9 (U) (U) Describe the ME Lead’s responsibilities toward mission owner interaction.

Training Resources & Technical References:

 EO12333, “Raw SIGINT availability procedures”,

<https://fas.org/sgp/othergov/intel/sigint-raw.pdf>

The MEL is responsible for the coordination of mission owner interaction and the development of mission requirements. The MEL is also responsible for ensuring that the CPT is properly aligned with the mission owner’s objectives and that the CPT is providing the necessary support to achieve those objectives. The mission element lead also ensures communication happens between the two sub-elements and back home support.



## 1.1.10 (U) Describe how the ME Lead will synchronize efforts with local defenders, customer and key stakeholders.

Training Resources & Technical References:

 Joint Chiefs of Staff, “CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL”,

<https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-0205-175710-897>

Based on the training resources, the Mission Element Lead shall be deeply involved in the successful synchronization coordination and deconfliction of local defenders, customer and key stakeholders who could be affected in order to prevent any unnecessary interference or overlap between ongoing activities during an operation.

## 1.1.11 (U) Describe how, by working with the mission owner, the ME Lead can determine where to concentrate data collection.

Training Resources & Technical References:

 Local SOP

The MEL works with the mission owner to determine where to concentrate data collection by identifying the critical assets that need protection and then prioritizing those assets based on their importance to the mission. The mission owner determines the control status of application data and must ensure that the protection status of the CSP accommodates the data and network access

A good start for this is the scoping document. The scoping document received from the system administrators of the network lists what is connected to their network. Once the ME Lead understands what is on the actual network, he or she can start to infuse other information to determine where the highest probability of adversary presence. The infusion of Intel can show active connections to public facing devices. Open source intelligence can point to the TTPs of the suspected adversaries. Finally, the cyber key terrain is what the adversary probably wants to access.

* + Logging on public facing webservers to detect backdoors and web shell that could allow the adversary to by-pass the firewall
  + Logging on the domain controller to hunt for compromised accounts
  + Logging on any production servers and computers that the adversary wants access to
  + Logging on the Email servers if the adversary tend to exfil email for intelligence

## 1.1.12 (U) Explain the importance of an out-brief and what should be included.

Training Resources & Technical References:

 National Institute of Standards and Technology . (2013, September 13). 4th Cybersecurity Framework Workshop Outbrief and Discussion of Next Steps. Dallas Texas

<https://www.nist.gov/system/files/documents/itl/csd/closing_plenary_4th-cybersecurity-framework-workshop.pdf>

An out-brief, also known as a debriefing or exit briefing, is a crucial component of the incident response process. It involves sharing information, insights, and lessons learned with relevant stakeholders after the completion of an incident response activity. The National Institute of Standards and Technology (NIST) recognizes the importance of an out-brief and provides guidance on what should be included. Here's an explanation of the importance of an out-brief and its key components according to NIST:

* Knowledge transfer: An out-brief ensures the transfer of knowledge gained during the incident response process to relevant stakeholders. It enables the dissemination of information about the incident, the actions taken, and the outcomes achieved. This knowledge sharing is crucial for organizational learning and future incident response improvements.
* Lessons learned: Out-briefs facilitate the identification and documentation of lessons learned from the incident response effort. They provide an opportunity to reflect on the strengths and weaknesses of the response, highlight areas for improvement, and capture best practices. Lessons learned can help enhance incident response capabilities and prevent similar incidents in the future.
* Accountability and transparency: An out-brief promotes accountability by providing a transparent account of the incident response activities. It helps stakeholders understand the decision-making processes, actions taken, and the rationale behind them. This transparency builds trust and confidence among stakeholders and ensures that the incident response effort aligns with organizational goals and policies.
* Continuous improvement: Out-briefs support the concept of continuous improvement in incident response. By analyzing the effectiveness of response actions, identifying gaps or deficiencies, and proposing recommendations, organizations can refine their incident response plans, procedures, and technical controls. This iterative approach fosters a proactive and evolving incident response capability.

Key Components of an Out-Brief according to NIST:

* Incident Overview: Provide a summary of the incident, including the nature of the incident, its impact on the organization, and the timeline of events. Describe the initial detection, response actions taken, and the resolution or containment measures implemented.
* Response Activities: Detail the specific actions perfformed during the incident response process. This includes the deployment of technical tools, incident triage and analysis, containment measures, evidence preservation, communication and coordination efforts, and any involvement of external parties such as law enforcement or incident response teams.
* Observations and Findings: Share key observations, findings, and insights gained during the incident response. Highlight any unique characteristics of the incident, novel attack techniques, vulnerabilities exploited, or indicators of compromise (IOCs) discovered. Provide an analysis of the impact of the incident on the organization's systems, networks, or data.
* Lessons Learned: Document the lessons learned from the incident response effort. Identify strengths and weaknesses in the response process, procedures, and technical controls. Recommend improvements, additional training needs, or adjustments to incident response plans. Focus on preventive measures to avoid similar incidents in the future.
* Recommendations: Offer specific recommendations for remediation, further investigation, or mitigation measures based on the incident's findings. Provide guidance on enhancing incident response capabilities, including improvements to detection mechanisms, response procedures, communication protocols, or incident documentation practices.
* Documentation and Reporting: Emphasize the importance of proper documentation and reporting throughout the incident response process. Discuss the documentation requirements, such as incident reports, evidence logs, chain of custody records, and any legal or regulatory obligations. Highlight the significance of accurate and comprehensive reporting for future reference and analysis.
* By conducting thorough out-briefings and incorporating the key components mentioned above, organizations can foster a culture of learning, continuous improvement, and enhanced incident response effectiveness.

## 1.1.13 (U) Explain the importance of the final report and what it should include.

Training Resources & Technical References:

 SANS, “Tips for Creating a Strong Cybersecurity Assessment Report”,

<https://www.sans.org/blog/tips-for-creating-a-strong-cybersecurity-assessment-report/>

 Local SOP

Final report documents the "history" of the mission. It should include all IOCs and TTPs associated with the attack, as well as internal issues that may have been manipulated by the threat actor to gain entry. It should also include recommendations to mitigate MCA activity.

## 1.1.14 (U) Explain how to prioritize Host Analyst findings and mitigation recommendations in the final report.

Training Resources & Technical References:

 National Infrastructure Advisory Council, Vulnerability Disclosure Framework "Final Report and Recommendations by the Council", Chamber J.T., Thompson J.W. 13 January 2004.

<https://www.cisa.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf>

* + Any vulnerability, malware or attack that the adversary uses will be detailed in the report.
  + Vulnerabilities that are found but not exploited by the adversary, but pose a real and significant risk will be included in the final report.
  + The recommendations should include patching, blocking, or otherwise fixing vulnerabilities at scale.
  + Determining the risk factor posed by the various identified threats, it is possible to create a prioritized list of threats to support a risk mitigation strategy, such as prioritizing the threats to be mitigated first

## 1.1.15 (U) Describe the ME Leads responsibilities for reporting.

Training Resources & Technical References:

 National Infrastructure Advisory Council, Vulnerability Disclosure Framework "Final Report and Recommendations by the Council", Chamber J.T., Thompson J.W. 13 January 2004.

<https://www.cisa.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf>

MELs are responsible for providing situational awareness and reporting on the status of their respective mission elements. They also ensure that all security incidents are reported. Documents and incidents also include Task Force Commander CCIRs.

SPOT Repots are for when the adversary is found on the network and should be filled out promptly.

The leads should be accomplishing quality control of all reports.

* **Reports** should be written in a active first person voice.
* **Clarity:** The report should be written in a clear and concise manner, avoiding unnecessary jargon or overly complex language. It should be easily understandable to the target audience, which may include both technical and non-technical readers.
* **Accuracy:** A high-quality technical report should be based on accurate and reliable data. It should be well-researched and supported by relevant sources and evidence.
* **Structure:** The report should follow a well-organized structure with a clear introduction, main body, and conclusion. Each section should flow logically, leading the reader through the information presented.
* **Objectivity:** Technical reports should maintain objectivity and impartiality. Personal opinions and biases should be avoided, and the focus should be on presenting facts and analysis.

## 1.1.16 (U) Describe how to utilize “phase line” when executing the mission and the importance of it.

Training Resources & Technical References:

 Local SOP

The phase line is used to separate different phases of the mission. During the planning phase, leads identify key phases in the operation and assign phase lines to mark the boundaries between these phases. These phase lines are typically given descriptive names (e.g., Phase Line Alpha, Phase Line Bravo, etc.) to make them easily recognizable and distinguishable.

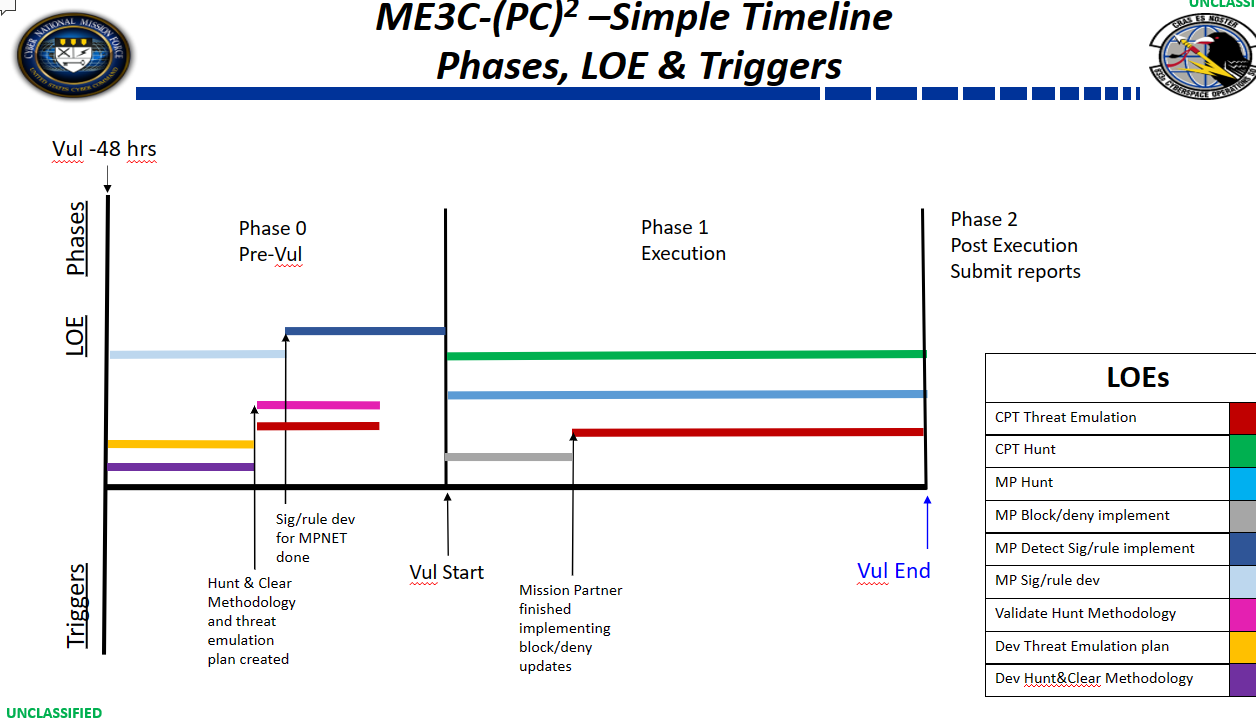
The planning phase is where the team develops a plan for how they will execute their mission. The concept of phase lines is common in military planning and is often associated with the military decision-making process (MDMP). The MDMP is a structured approach that military commanders and staff use to analyze, plan, and execute operations. Possible phases for a mission are pre-deployment, deployment, baselineing, hunting, clear, and etc. The execution phase is where the team carries out that plan.

The importance of the phase line is that it helps ensure that the team is properly prepared for their mission. By separating the planning and execution phases, the team can focus on developing a solid plan without being distracted by the details of executing that plan.

**The phase lines serve several purposes which could include the following.**

* **Coordination and Control:** Phase lines help synchronize the actions of different units and elements within the force. They provide common reference points for coordination, ensuring that units are on the same page and working toward shared objectives.
* **Timing and Progression:** Phase lines help in controlling the tempo of the operation by designating points where certain actions or events are supposed to occur. They serve as time-sensitive markers that indicate when to move from one phase of the operation to the next.

Example



## 1.2.1 (U) Discuss what a collection plan is and how pertinent it is to accomplish a successful mission.

Training Resources & Technical References:

 TarLogic, “Data Collection Plan: A key Component of the Intelligence Cycle”, <https://www.tarlogic.com/en/blog/data-collection-plan-a-key-component-of-the-intelligence-cycle/>

A collection plan is used to guide the team in collecting the data that is needed for successful hunt. What is the mission partner auditing on the domain? Where is the network traffic flowing? Are spans located in the correct spots for lateral movement?

Some of the sources of the collection plan are logs and network traffic. Don’t forget about Intel which could have some insight to the adversaries. Also, many open-source security companies make reports on what these adversaries are doing.

An example of some stuff you want to collect:

* + Security logs from the Windows Boxes and ensure audit policy is correct.
  + Sysmon logs if available (superior log source)
  + Network traffic that can be used to detect lateral movement
  + Webserver logs from public facing webservers that could be used for bypassing the firewall
  + Firewall logs to detect anomalous connections
  + DNS logs to accomplish LFA to find beacons
  + Microsoft Defender Anti-Virus logs
  + Exchange logs to detect mailbox exfil

## 1.2.2 (U) Given a list of resources define what is relevant in building a collection plan.

Training Resources & Technical References:

 TarLogic, “Data Collection Plan: A key Component of the Intelligence Cycle”, <https://www.tarlogic.com/en/blog/data-collection-plan-a-key-component-of-the-intelligence-cycle/>

When building a collection plan, it is important to consider a variety of resources. These resources can include internal sources such as logs and network traffic data, as well as external sources such as threat intelligence feeds and open-source intelligence.

An example of some stuff you want to collect:

* + Security logs from the Windows Boxes and ensure audit policy is correct.
  + Sysmon logs if available (superior log source)
  + Network traffic that can be used to detect lateral movement
  + Webserver logs from public facing webservers that could be used for bypassing the firewall
  + Firewall logs to detect anomalous connections
  + DNS logs to accomplish LFA to find beacons
  + Microsoft Defender Anti-Virus logs
  + Exchange logs to detect mailbox exfil

## 1.2.3 (U) Identify the steps on building a collection plan.

Training Resources & Technical References: TarLogic, “Data Collection Plan: A key Component of the Intelligence Cycle”, <https://www.tarlogic.com/en/blog/data-collection-plan-a-key-component-of-the-intelligence-cycle/>

Creating a data collection plan for cyber intelligence involves careful planning and consideration of various factors to ensure effective and efficient data gathering. Here are the steps to create a data collection plan for cyber intelligence:

A better source is the following:

Title: "Intelligence-Driven Incident Response: Outwitting the Adversary" Author: Scott J. Roberts, Rebekah Brown, et al. Publisher: Addison-Wesley Professional Year: 2017 Chapter 2.

* **Define Objectives and Requirements:**
* Clearly outline the objectives of your cyber intelligence efforts. Determine what specific information you need to collect to support those objectives. This may include indicators of compromise (IOCs), threat actor profiles, vulnerabilities, attack techniques, etc.
* **Identify Data Sources:**
* Identify potential sources of relevant data. These could include network logs, endpoint data, threat intelligence feeds, open-source intelligence (OSINT), social media, dark web sources, and other external resources.
* **Prioritize Data Sources:**
* Prioritize the data sources based on their relevance, reliability, and potential impact on your cyber intelligence objectives. Some sources may be more critical than others for specific use cases.
* **Set Data Collection Methods:**
* Determine the methods and tools you will use to collect data from the identified sources. This could involve leveraging cybersecurity tools, SIEM (Security Information and Event Management) systems, web scraping tools for OSINT, or engaging with threat intelligence vendors.
* **Establish Data Collection Schedule:**
* Define a regular data collection schedule that aligns with your cyber intelligence objectives. Some data sources may require real-time or near-real-time monitoring, while others may only need periodic checks.
* **Ensure Data Privacy and Legal Compliance:**
* Consider data privacy regulations and legal requirements when collecting and storing data. Ensure that your data collection plan complies with relevant laws and policies.
* **Design Data Validation and Verification Methods:**
* Develop processes to validate and verify the accuracy and integrity of collected data. This step is crucial to ensure the data is reliable and free from errors.
* **Data Handling and Storage:**
* Plan how you will handle, store, and secure the collected data. Follow best practices for data encryption, access control, and data retention.
* **Document the Data Collection Plan:**
* Create a formal document that outlines the data collection plan, including objectives, sources, methods, schedules, validation processes, and storage procedures. Share this document with relevant stakeholders for transparency and alignment.
* **Test and Refine the Plan:**
* Before implementing the plan at scale, conduct a pilot test to identify any issues or improvements needed. Refine the data collection plan based on the results of the pilot test.
* **Execute the Plan:**
* Implement the data collection plan and begin collecting cyber intelligence data based on the established schedule and methodologies.
* **Monitor and Evaluate:**
* Continuously monitor the data collection process to ensure it remains effective and aligned with the objectives. Regularly evaluate the quality and relevance of the collected data.

By following these steps, you can develop a robust data collection plan for cyber intelligence that supports your organization's cybersecurity efforts and helps in identifying and mitigating cyber threats effectively.

## 1.2.4 (U) (U) Explain why it is important to understand the customer’s organizational policies for users and computers.

Training Resources & Technical References:

 PowerDMS, “Following Policies and procedures, and why it’s important”, <https://www.powerdms.com/blog/following-policies-and-procedures-why-its-important/>

Policies and procedures are an essential part of any organization. Together, policies and procedures provide a roadmap for day-to-day operations. They ensure compliance or non-compliance with laws and regulations, give guidance for decision-making, and streamline internal processes. By following policies and procedures, employees can help their organization maintain compliance with laws and regulations, reduce risk, and improve overall efficiency. Understanding the policy can unlock holes in their organization such as: password policy, remote-access policy, MFA and etc.

## 1.2.5 (U) Identify the importance of a Pre-Deployment Site Survey.

Training Resources & Technical References:

 Cisco, “Take your network as seriously as your business”, <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/CMX/CMX_PreDeployRFSite.html>

Pre-deployment surveys are used for on-site validation of the scoping document, network plan and host plan. It helps identify potential issues that may arise during deployment and provides an opportunity to address them before deployment. This is most likely the first time the team will meet with the system administrators of the network and start forming the plans for connected the kit to the network.

## 1.2.6 (U) Define the term “Rules of Engagement” and how it applies to a mission.

Training Resources & Technical References:

 Military.com, “Cyber Attacks and Warfare – Rules of Engagement”, <https://www.military.com/defensetech/2008/11/28/cyber-attacks-warfare-rules-of-engagement>

It is a set of detailed guidelines and constraints regarding the execution. Used to ensure that all members of the team are aware of their roles and responsibilities during a mission.

## 1.3.1 (U) (U) Given organization system policy identify invalid active directory objects.

Training Resources & Technical References:

 Microsoft, “MCSA Windows server 2016 complete study guide 2nd edition by William Panek”, March 2016.

 Dishan Francis, “Mastering Active Directory: understanding the core functionalities of active director services using Microsoft server 2016 and PowerShell”, June 2016.

Invalid Active Directory objects can be identified using the organization system policy. Microsoft provides a PowerShell command that can be used to view the objects that have an error associated with them. You can run the following Windows PowerShell commands in the Azure Active Directory Module for Windows PowerShell:

Get-MsolUser | Where {$\_.Errors –ne $null} | Select ObjectID, DisplayName

Get-MsolContact | Where {$\_.Errors –ne $null} | Select ObjectID, DisplayName

## 1.3.2 (U) Given an Active Directory domain audit policy and threat actor tactics, techniques and procedures identify auditing gaps that would prevent logging.

Training Resources & Technical References:

 Microsoft, “MCSA Windows server 2016 complete study guide 2nd edition by William Panek”, March 2016.

|  |  |  |  |
| --- | --- | --- | --- |
| Wicked Panda(APT41) | | | |
| [T1110](https://attack.mitre.org/techniques/T1110) | [0.002](https://attack.mitre.org/techniques/T1110/002) | Brute Force: Password Cracking | APT41 performed password brute-force attacks on the local admin account.[1] |
| Requires auditing of logon failures to detect failed logons. Auditing for the failed logons would generate events documenting failed logon attempts. These events could reveal the use of the Brute Force: Password Cracking technique. If the audit policy is not applied across the defended asset list, then it would prevent logging these events. | | | |

## 1.3.3 (U) Demonstrate using PowerShell to manage Active Directory applicable to cyber operations.

Training Resources & Technical References:

 Dishan Francis, “Mastering Active Directory: understanding the core functionalities of active director services using Microsoft server 2016 and PowerShell”, June 2016.

You can use PowerShell to manage Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) configuration sets, and Active Directory Database Mounting Tool instances in a single, self-contained package

Managing AD user accounts with PowerShell requires a freely available PowerShell module aptly named ActiveDirectory. This module comes with the Remote Server Administration Toolkit (RSAT)

Example from MDS1

**IF RSAT IS MISSING**

enter-pssession-computer 131.7.14.2.2 -credentials mystery\Administrators

Install-windowsfeature RSAT-AD-Tools

Install-windowsfeature RSAT-AD-Powershell

Restart-computer

The following command will interrogate all the users of the muggle domain and allow you to look oddities with excel.

Invoke-Command -ComputerName 131.9.2.3 -Credential $creds -ScriptBlock {get-aduser -filter \* -property \*} | ConvertTo-Csv | out-file muggle\_users.csv

While examining the output you can see many users that have non-stig policy and the jake.potts account that was created with oddities

## 1.3.4 (U) Interpret and configure host-based firewalls and Host Intrusion Prevention Systems through group policy.

Training Resources & Technical References:

 Microsoft, “MCSA Windows server 2016 complete study guide 2nd edition by William Panek”, March 2016.

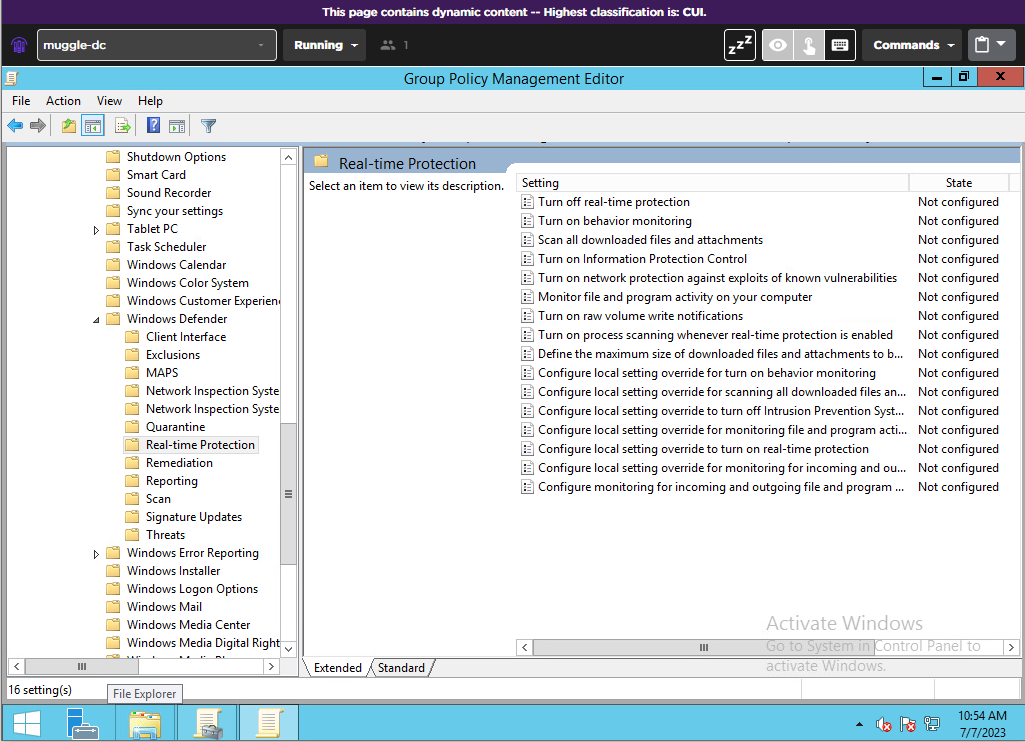
Host-based firewalls and Host Intrusion Prevention Systems (HIPS) can be configured through group policy. HIPS adds a third level of protection to your firewall and anti-virus programs by continuously monitoring the software that’s running in your machine.

To configure host-based firewall policy, you can use Group Policy Management console and decide whether to use an existing GPO or creating a new one. Then, click on the Windows Firewall with Advanced Security on the left pane, then configure the firewall rules

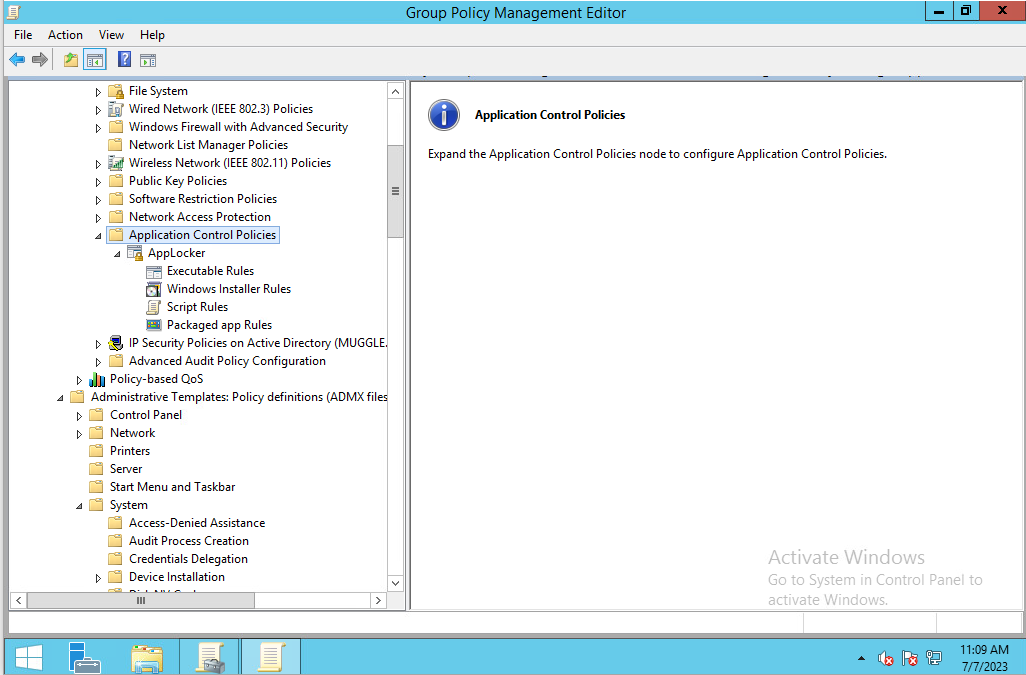
To configure Windows Defender Firewall, you can optimize protection for devices in your network by configuring your Windows Firewall based on the following best practices

To configure Host Intrusion Prevention Systems through group policy, you can use Microsoft Defender Antivirus. You can use the following procedure to configure or change some settings for Microsoft Defender Antivirus. On your Group Policy management machine, open the Group Policy Management Console, right-click the Group Policy Object (GPO) you want to configure and click Edit. Then, go to Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > MAPS. In the right pane, double-click Configure protection for potentially unwanted applications and select Enabled

Many additional options are available through group policy as shown in the screen shot.



Additionally, Windows AppLocker should be considered for HIDS/HIPS. Windows Applocker protectings against unknown threats: By restricting the execution of applications to authorized and trusted ones, App Locker helps protect systems against unknown or zero-day threats. Since only approved applications can run, the risk of unknown malware or unauthorized software causing harm is significantly reduced.



## 1.3.5 (U) Explain how to ensure patches are up to date for all domain workstations and determine effectiveness of current process for updating.

Training Resources & Technical References:

 Microsoft, “MCSA Windows server 2016 complete study guide 2nd edition by William Panek”, March 2016.

1. Run Nessus
2. Establish a baseline inventory of all production systems.
3. Prioritize patches based on their criticality either for security or functional reasons.
4. Automate the patch management process to decrease the time between the release and application of patches.
5. Validate that patches work as expected and don’t break any of your systems or applications.

## 1.3.6 (U) Given a list of IOCs identify key log entries/Event IDs ,use a Security information and event management (SIEM) platform to correlate indicators of compromise, and develop dashboards to better visualize data.

Training Resources & Technical References:

 Jason T. Luttgens, Matthew Pepe and Kevin Mandia, “Incident Response & Computer Forensics, Third Edition”

 Betsy Sigman & Erickson Delgado, “Splunk essentials 2nd Edition Sep. 2016.”

To use Security Information and Event Management (SIEM) to identify key log entries/Event IDs, you can collect log and event data from an organization’s applications, servers, security devices and systems into a centralized platform.

A SIEM will sort this data into categories and analyze it for deviations against behavioral rules defined by the organization

## 1.3.7 (U) Using a SIEM create alerts to detect the creation of unauthorized accounts.

Training Resources & Technical References:

 Microsoft, “MCSA Windows server 2016 complete study guide 2nd edition by William Panek”, March 2016.

 Dishan Francis, “Mastering Active Directory: understanding the core functionalities of active director services using Microsoft server 2016 and PowerShell”, June 2016.

searches for the creation of accounts that are not authorized:

{

"query": {

"bool": {

"must\_not": [

{

"term": {

"authorized": true

}

}

]

}

}

}

This query will return all documents where the field authorized is not set to true. You can then set up an alert based on this query and configure the exact trigger conditions.

In Elastic:

1. Click on hamburger on the top left corner

2. navigate to the “Security” section and click on “detections”

3.

## 1.3.8 (U) (U) Configure, forward, and statically analyze logs from all workstations in an enterprise environment.

Training Resources & Technical References:

 Andrei Miroshnikov, “Windows Security Monitoring, 2018.”

To configure, forward, and statically analyze logs from all workstations in an enterprise environment, you can use a log management tool such as Datadog Log Management.

## 1.3.9 (U) Explain how to oversee the development of host-based IDS/IPS signatures, settings, and applicable agents.

Training Resources & Technical References:

 William Panek, M”CSA Windows 10 Study guide 2016.”

 Andrei Miroshnikov, “Windows Security Monitoring 2018.

To oversee the development of host-based IDS/IPS signatures, settings, and applicable agents, you can follow these steps:

Install an IDS/IPS on your client computers or network itself.

Look for deviations from normal activity and known attack signatures.

Anomalous patterns are sent up the stack and examined at protocol and application layers.

Apply signatures to your hosts and update intrusion detection signatures by checking cloud-based service

## 1.3.10 (U) Explain how to oversee the tuning of host-based IDS/IPS alerts in order to evaluate their severity while eliminating false positives.

Training Resources & Technical References:

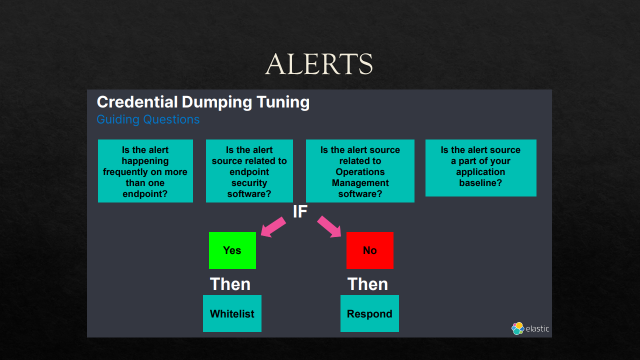
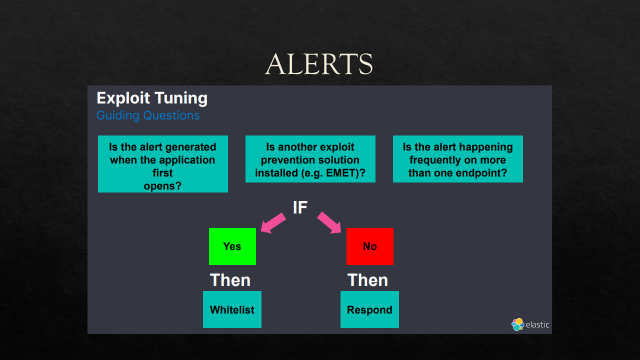
 MCSA Windows 10 Study guide by William Panek 2016

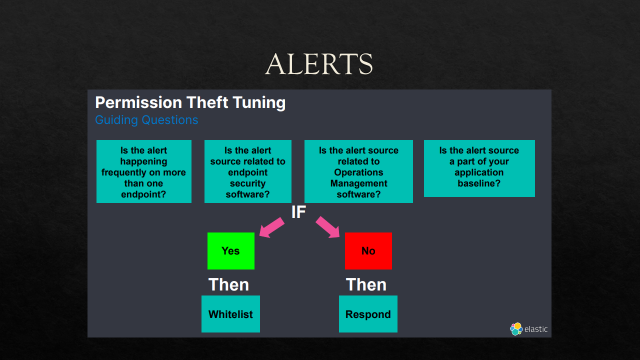
 Windows Security Monitoring by Andrei Miroshnikov 2018.

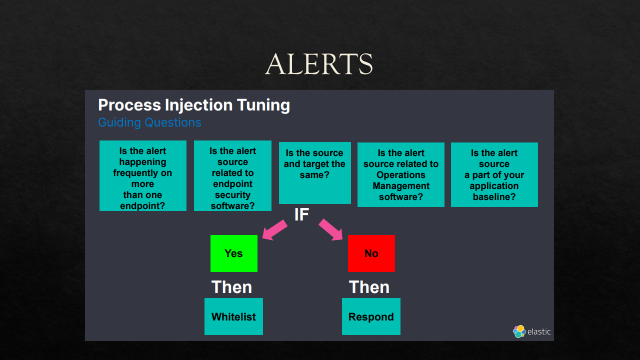
* + Investigate the signatures that trigger most.
  + Focus on the High and Critical severity ones first.
  + Determine what the source and destination IP addresses should be doing in the environment.
  + Use tools such as dashboards, reports, or logs to visualize and analyze the alerts and identify any trends, patterns, or anomalies.

For Endgame, check the Alerts section of this PowerPoint for Endgame Core accelerated

(pages 57 - 61).







## 1.3.11 (U) Given a list of active processes identify libraries, modules, executables, and binaries against databases of known advanced malware.

Training Resources & Technical References:

 Dmitry Vostokov, “Windows memory dump analysis advanced V2.0 2017.”

Use the SANs Windows Hunt Evil poster to identify parent and process relationship that are anomalous. Please ensure you are using the correct profile. You can find the profile by running the

**Digital Forensics and Incident Response - Third Edition**

**You can also use the GUI version** [**Volatility Workbench - A GUI for Volatility memory forensics (osforensics.com)**](https://www.osforensics.com/tools/volatility-workbench.html)

[(969) Volatility WorkBench tool - YouTube](https://www.youtube.com/watch?v=oZk0OD8CWBw)

[](https://www.youtube.com/watch?v=oZk0OD8CWBw)

* **vol.py -f “/path/to/file” windows.info**
* **vol.py -f “/path/to/file” windows.pstree**
* **vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles ‑‑pid <PID>**
* **vol.py -f “/path/to/file” -o “/path/to/dir” windows.memmap ‑‑dump ‑‑pid <PID>**
* **vol.py -f “/path/to/file” windows.handles ‑‑pid <PID>**
* **vol.py -f “/path/to/file” windows.dlllist ‑‑pid <PID>**
* **vol.py -f “/path/to/file” windows.cmdline**
* **vol.py -f “/path/to/file” windows.netstat**
* **vol.py -f “/path/to/file” windows.malfind**
* **vol.py -f “/path/to/file” yarascan -y “/path/to/file.yar”**

## 1.3.12 (U) Given an IOC, explain how to utilize tools and analysis techniques to identify processes, libraries, modules, and other activity that have been obfuscated and might indicate the presence of a more advanced rootkit on endpoint.

Training Resources & Technical References:

 Christopher c. Elisan, Michael A. Davis; Sean M. Bodmer and Aaron LeMasters, “Hacking exposed Malware & Rootkits: security secrets and solutions 2nd Edition June 2016.”

You need to use logs and memory forensics to detect and find a rootkit. A training module has been created at the following location.

[836 COS / rootkit\_training · GitLab (af.mil)](https://code.levelup.cce.af.mil/836-cos/rootkit_training)

## 1.3.13 (U) Given a Prioritized Defended Asset list, identify which dependent systems are key terrain.

Training Resources & Technical References:

 Conrad, Misenar, and Feldman, “CISSP Study Guide Third Edition 2016.

To identify which dependent systems are key terrain, you can develop a methodology for prioritizing HVAs (High Value Assets) based on criticality and mission importance

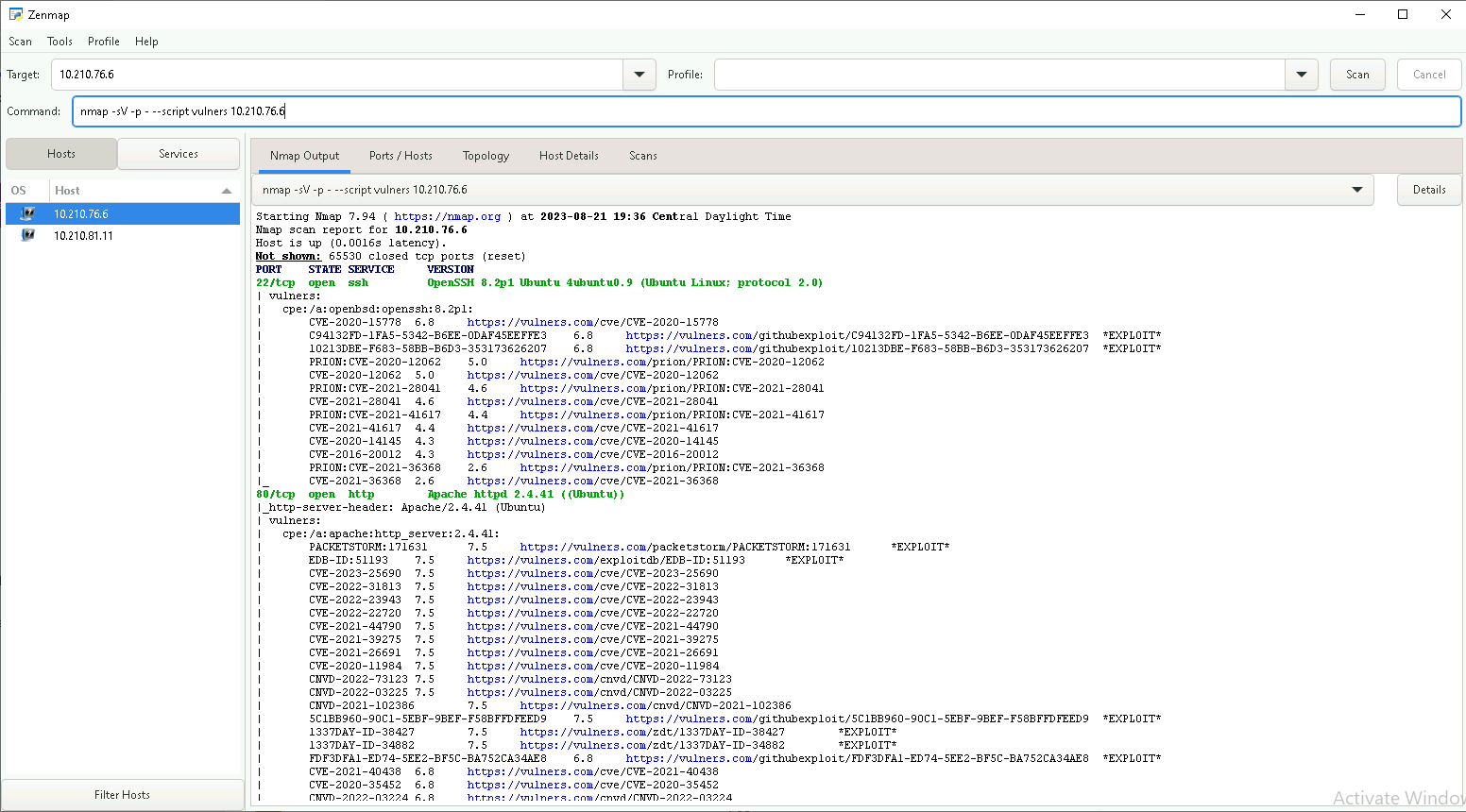
These systems are rank ordered and dependent due to the DAL.

## 1.3.14 (U) Evaluate patch levels on host machines across a complex Windows domain to determine the current patch level consistency.

**Training Resources & Technical References:**

**https://nmap.org/nsedoc/scripts/vulners.html**

**To quickly evaluate patch levels use the nmap script vulners. The vulners script requires a internet connection.**



## 1.3.15 (U) Given a host baseline of configuration/state, for host machines on a network conduct a scan for anomalous configurations.

* **Endgame Hunt**

## 1.3.16 (U) Given a Windows Domain Controller, evaluate information (e.g. users, groups, trust relationships, and security policies) from a complex Domain to identify vulnerabilities/misconfiguration, and how to export this information.

Training Resources & Technical References:

 Dishan Francis, “Mastering Active Directory: understanding the core functionalities of active director services using Microsoft server 2016 and Powershell, June 2016.”

To evaluate information from a complex domain to identify vulnerabilities/misconfiguration, you can use Microsoft’s Microsoft Baseline Security Analyzer (MBSA) tool.

To export information from a Windows Domain Controller, you can use the Active Directory Users and Computers tool.

(Akins note: We used some kind of STIG last time I went out. Need to find what we used)

<https://public.cyber.mil/stigs/>

## 1.3.17 (U) Given a script determine what is occurring.

Training Resources & Technical References:

 Christopher c. Elisan, Michael A. Davis; Sean M. Bodmer and Aaron LeMasters, “Hacking exposed Malware & Rootkits: security secrets and solutions 2nd Edition, June 2016.”

**The following script uses a function to pull ip address from a cidr range. The ips are then looped through to collect and display operating system, patch level and service pack.**

# Establish a variable with the desired CIDR range

$cidrRange = "192.168.0.0/24"

# Get IP addresses from the CIDR range and adds it to an array

$ipAddresses = Get-IPAddressFromCIDR $cidrRange

# For each IP in the array

foreach ($ipAddress in $ipAddresses) {

# Write to the screen for the current IP “Checking patch level for $ipAddress..."

Write-Host "Checking patch level for $ipAddress..."

#Ping the current IP address to check if it's reachable; if it is, try below.

$pingReply = Test-Connection -ComputerName $ipAddress -Count 1 -Quiet

if ($pingReply) {

try {

#Retrieve patch information using WMI

$os = Get-WmiObject -Class Win32\_OperatingSystem -ComputerName $ipAddress -ErrorAction Stop

$patchLevel = $os.CSDVersion

$servicePack = $os.ServicePackMajorVersion

Write-Host "Patch level for $ipAddress: $patchLevel"

Write-Host "Service Pack for $ipAddress: $servicePack"

}

catch {

Write-Host "Error retrieving patch information for $ipAddress: $\_"

}

}

else {

Write-Host "$ipAddress is not reachable."

}

Write-Host

}

# Function to get IP addresses from CIDR range

function Get-IPAddressFromCIDR {

param (

[Parameter(Mandatory = $true)]

[string]$cidrRange

)

$cidr = $cidrRange -split '/'

$ipAddress = $cidr[0]

$subnetMask = 0xFFFFFFFF -shl (32 - $cidr[1])

$ip = [System.Net.IPAddress]::Parse($ipAddress).GetAddressBytes() -bor $subnetMask

$ipAddresses = @()

for ($i = $ip[0]; $i -le $ip[0] + $subnetMask - 1; $i++) {

$ipAddresses += [System.Net.IPAddress]::Parse("$([BitConverter]::ToString([BitConverter]::GetBytes($i)) -join '.')")

}

return $ipAddresses

}

## 1.3.18 (U) Perform device discovery in order to conduct enumeration of a complex network while limiting the amount of network traffic generated.

Training Resources & Technical References:

 Mohammad Junaid, “Analyzing Network traffic with wireshark 2.6, Sept. 2018.”

The following query will accomplish device discovery for the muggle and mystery ranges

query:

winlog.event\_data.IpAddress:131.9.3\* or winlog.event\_data.IpAddress:131.14.3\*

## 1.3.19 (U) Analyze host discovery tool output to generate accurate maps of endpoint systems.

Training Resources & Technical References:

 Mohammad Junaid, “Analyzing Network traffic with wireshark 2.6, Sept. 2018.”

To generate accurate maps of endpoint systems from host discovery tool output, you can launch a host discovery scan to see what hosts are on your network, and associated information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan

## 1.4.1 (U) Given an enterprise domain, explain how to identify potentially malicious processes, connections, libraries, and other malicious code/activity from a memory image and perform trend and outlier analysis.

Training Resources & Technical References:

 EC-Council, “Computer Forensics: Investigation Procedures and Response (CHFI) Second Edition.”

You can identify a malicious process which will lead you to other artifacts. In a memory dump, the name of a process and its PID (Process Identifier) number will map to other things such as loaded DLLs which may include libraries supplied by the attacker that you did not previously locate, and their storage location.

You can also detect suspicious or malicious activity by looking for out-of-the-ordinary activity. Through continuous analysis of network patterns, NBAD aims to identify any unusual or abnormal activities, events, or trends that may indicate potential security threats

## 1.4.2 (U) Automate advanced and repetitive tasks on remote workstations within a domain.

Training Resources & Technical References:

 A. Sweigart, “Automate the Boring Stuff with Python, 2015.”

To automate advanced and repetitive tasks on remote workstations within a domain, you can use Robotic Process Automation (RPA) which can perform such analyses as much as 15 times faster

**SCENERIO: Create a Python program that calls PowerShell to get all Local Users from the Workstation.**

**Here is an example below:**

#################################################################

import subprocess

import json

def get\_local\_users():

# Define the PowerShell command to get local users from the workstation

ps\_script = r'''

$users = Get-LocalUser | Select-Object Name, Enabled, LastLogon

$users | ConvertTo-Json

'''

try:

# Call PowerShell and execute the script

output = subprocess.check\_output(['powershell', '-Command', ps\_script], text=True)

# Parse the JSON output to extract local users

local\_users = json.loads(output)

return local\_users

except subprocess.CalledProcessError as e:

print("Error executing PowerShell script:", e)

return None

if \_\_name\_\_ == "\_\_main\_\_":

local\_users = get\_local\_users()

if local\_users:

print("Local Users:")

for user in local\_users:

print(f"Name: {user['Name']}, Enabled: {user['Enabled']}, Last Logon: {user['LastLogon']}")

else:

print("Failed to retrieve local users.")

#####################################################################

## 1.4.3 (U) Assess customer security posture across a complex enterprise network to Identify security posture shortcomings.

Training Resources & Technical References:

 Conrad, Misenar, and Feldman, “CISSP Study Guide Third Edition, 2016.

**Identify the assets**: Identify all the assets in the enterprise network.

**Identify the vulnerabilities**: Identify all the vulnerabilities in the assets.

**Assess the risks**: Assess the risks associated with each vulnerability.

**Prioritize the risks**: Prioritize the risks based on their severity.

**Develop a plan**: Develop a plan to mitigate the risks.

**Implement the plan**: Implement the plan to mitigate the risks.

## 1.5.1 (U) (U) Given a vulnerability scan and mission owner network information prioritize vulnerabilities for action.

Training Resources & Technical References:

 J.M. Couretas, “An Introduction to Cyber Mondeling and Simulation, 2019.”

To prioritize vulnerabilities from a vulnerability scan, you can use the following steps:

**Validate the scan results**: Validate the scan results to ensure that they are accurate.

**Categorize and prioritize the incidents**: Categorize and prioritize the incidents based on your risk criteria and the type of vulnerability.

**Group the incidents**: Group the incidents by asset, system, application, or network segment to facilitate the analysis and response.

**Use a scoring system**: Use a scoring system and a remediation timeline.

**Monitor and update your vulnerability information**: Monitor and update your vulnerability information regularly.

**Communicate and collaborate with your stakeholders**: Communicate and collaborate with your stakeholders to ensure that they are aware of the vulnerabilities and their impact.

**Assign priority automatically**: Assign priority automatically through automated scans or manually during the discovery phase.

**Use the Common Vulnerability Scoring System (CVSS)**: Use the Common Vulnerability Scoring System (CVSS) to communicate the vulnerability’s severity and characteristics

## 1.5.2 (U) Describe and display knowledge of the “After Action Report” and all areas needed to complete one.

Training Resources & Technical References:

 PHF, “After Action Report Tool”, <http://www.phf.org/resourcestools/Pages/After_Action_Report_Tool.aspx>

An After-Action Report (AAR) is a detailed analysis performed following a cyber security incident that provides insights into how the event was handled. After-action reports can also follow a cybersecurity exercise, either to test an Incident Response Plans (IRP) or to provide a baseline on which to create one. The format of the final two sections in an after-action report should follow an ABAB configuration. Initially, the General Findings should be shared.

## 1.5.3 (U) Utilizing MITRE ATT&CK framework, perform complex root-cause analysis to determine the sequence of events related to a compromise and recommend mitigations.

Training Resources & Technical References:

 MITRE, “Risk Mitigation Planning, Implementation, and Progress Monitoring”

## 1.5.4 (U) Utilizing MITRE ATT&CK framework, perform complex root-cause analysis to determine the sequence of events related to a compromise and recommend mitigations

Training Resources & Technical References:

 Dmitry Vostokov, “Windows memory dump analysis advanced V2.0, 2017.”

https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

## 1.5.5 (U) Demonstrate familiarity with STIGs on host machines by using any software platform to generate a report for a complex network and follow-up with recommendations.

Training Resources & Technical References:

DISA, “Security Readiness Review (SRR).”

<https://public.cyber.mil/announcement/disa-releases-the-following-updated-security-guidance-security-readiness-review-scripts-supplemental-automation-content-and-benchmarks/>

(STIG Download Link)

Confluence: Nessus Compliance Scan: <https://confluence.90cos.cdl.af.mil/display/OJCCTM/Nessus>

1. Download the appropriate DISA STIG checklists for the systems that you are going to scan (OS Type/version dependent)

1.1: For Manual Checks download STIG Viewer

1.1.1: Load appropriate checklist / go line by line on each item

1.1.2: Repeat process on each box

1.2: For Semi Manual (Per Machine) Checks download SCAP (Win Only)

1.2.1: Open SCAP on Local PC, load STIG checklist into SCAP

1.2.2: Run SCAP and go line by line on any failed checks

1.2.3: Repeat process on each box

2. Using the Nessus, build a few compliance scans for each OS Type/Ver

2.1: Add IP Range

2.2: Add System Credentials

2.3: Load STIG Checklist

2.4: Run Scan(s) / receive reports for all machines hit in each scan

## 1.5.6 (U) Discuss the term “Lessons Learned” and how it applies to the CPT life cycle.

Training Resources & Technical References:

 Joint Publication 3\_12,

[~~https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\_12.pdf~~](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)

<https://irp.fas.org/doddir/dod/jp3_12.pdf>

Lessons Learned” is a term used to describe the process of learning from past experiences and applying that knowledge to future situations. In the context of CPT life cycle, it refers to the process of analyzing past cyber incidents and using that information to improve future responses. This process involves identifying what went wrong during an incident, what went well, and how the team can improve its response in the future.

## 1.5.7 (U) Given a scenario, identify steps to recover from a full- network compromise.

Training Resources & Technical References:

 “Certified Information Systems Security Professional (CISSP).”

<https://usaf.percipio.com/channels/dcabd57f-d6fb-40f5-b132-5c7fcb61a0f4?tab=WATCH>

-Respond to the attack: This should include establishing secure communications, identifying indications of compromise, investigating your environment, establishing continuous monitoring and improving security posture.

-Re-establish trustworthy communications: This will enable effective triage and coordination of business operations recovery.

-Perform system/network validation and testing to certify all systems as operational. Recertify any component that was compromised as both operational and secure.

-Disconnect affected devices from the Internet if possible. Have short-term and long-term containment strategies ready. It’s also good to have a redundant system back-up to help restore business operations.

## 2.1.1 (U) Identify PS modules that are helpful for local analysis.

Training Resources & Technical References:

 ATA Learniing, “Understanding and Building Powershell Modules”, <https://adamtheautomator.com/powershell-modules/>

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_modules?view=powershell-7.3>

Two PS Modules with their cmdlets

* Microsoft.PowerShell.Management
  + Add-Content
  + Clear-Content
  + Clear-Item
  + Clear-ItemProperty
  + Clear-RecycleBin
  + Convert-Path
  + Copy-Item
  + Copy-ItemProperty
  + Debug-Process
  + Get-ChildItem
  + Get-Clipboard
  + Get-ComputerInfo
  + Get-Content
  + Get-HotFix
  + Get-Item
  + Get-ItemProperty
  + Get-ItemPropertyValue
  + Get-Location
  + Get-Process
  + Get-PSDrive
  + Get-PSProvider
  + Get-Service
  + Get-TimeZone
  + Invoke-Item
  + Join-Path
  + Move-Item
  + Move-ItemProperty
  + New-Item
  + New-ItemProperty
  + New-PSDrive
  + New-Service
  + Pop-Location
  + Push-Location
  + Remove-Item
  + Remove-ItemProperty
  + Remove-PSDrive
  + Remove-Service
  + Rename-Computer
  + Rename-Item
  + Rename-ItemProperty
  + Resolve-Path
  + Restart-Computer
  + Restart-Service
  + Resume-Service
  + Set-Clipboard
  + Set-Content
  + Set-Item
  + Set-ItemProperty
  + Set-Location
  + Set-Service
  + Set-TimeZone
  + Split-Path
  + Start-Process
  + Start-Service
  + Stop-Computer
  + Stop-Process
  + Stop-Service
  + Suspend-Service
  + Test-Connection
  + Test-Path
  + Wait-Process
* Microsoft.PowerShell.Host
  + Start-Transcript
  + Stop-Transcript

## 2.1.2 (U) Identify PS module that are helpful for remote analysis.

Training Resources & Technical References:

 ATA Learniing, “Understanding and Building Powershell Modules”, <https://adamtheautomator.com/powershell-modules/>

<https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_modules?view=powershell-7.3>

Two PS Modules with their cmdlets

* Microsoft.WSMan.Management

Connect-WSMan

Invoke-WSManAction

New-WSManInstance

* CimCmdlets

New-CimInstance

* Microsoft.PowerShell.Core

Invoke-Command

New-PSSession

## 2.1.3 (U) Define what an Agent Based Security System is and how it could be advantageous during a mission.

Training Resources & Technical References:

 EasyTechJunkie, “What is a Host-Based Security System?”, <https://www.wisegeek.com/what-is-a-host-based-security-system.htm>

An agent-based security system is a security system that uses software agents to monitor and/or protect computer systems and networks. These agents are installed on each machine and can perform more specialized scanning of components and services. They can also be used as a firewall, since they can block network connections based on filtering rules. Agent-based systems offer runtime protection per host or per application and provide security controls like the ability to block attacks and patch live systems.

The advantages of using an agent-based security system during a mission include real-time, granular security information, making it ideal for monitoring, prevention, and threat blocking. It provides excellent real-time protection but requires every workload to have an agent for big-picture visibility

## 2.1.4 (U) Deploy an agent based security system to an enterprise network.

Training Resources & Technical References:

ENDGAME Administrator’s Guide:

<https://confluence.90cos.cdl.af.mil/display/OJCCTM/Endgame> (pdf attachment on confluence @ end of page)

 EasyTechJunkie, “What is a Host-Based Security System?”, <https://www.wisegeek.com/what-is-a-host-based-security-system.htm>

Deploy Endgame

Can deploy inband through the GUI or out of band with a script

ENDGAME: Deploy a Sensor to Win(In-Band Mgmt): Endgame Admin Guide(Page 90-93)

1. Endpoints / Action Toolbar: Discover Endpoints

1.1: enter ip range / custom port / start scan / finish

2. After “Scan Completed” /action toolbar: Windows Tab

3. Select endpoints

4. Actions: Deploy

5. Deploy Sensor

5.1: Select Sensor / Domain Name / Username / Password

6. Deploy Sensors / Close

7. Action Toolbar: select Windows tab / Active tab

8. Verify Endpoints (with sensor installed) in list as hostname of endpoint

## 2.1.5 (U) Configure and develop rules for CPT host-based agents.

Training Resources & Technical References:

ENDGAME Administrator’s Guide:

<https://confluence.90cos.cdl.af.mil/display/OJCCTM/Endgame> (pdf attachment on confluence @ end of page)

 Tech Target, “Intrusion Detection System (IDS)”, <https://searchsecurity.techtarget.com/definition/intrusion-detection-system>

Tune Endgame to alert on customized conditions and have Endgame ignore certain customized conditions

Can also tune rules within Kibana to alert on certain conditions met within the logs that are ingested

ENDGAME: Create Custom Rule: Endgame Admin Guide (Page 68-75) bottom of page

1. Administration / Rules tab / Create Rule Wizard

1.1: Compose EQL Query

1.2: Classify Alert

1.3: Name Rule

2. Enable Custom Rule: In Endpoint Policy list select policy to enable

3. On Enpoint Policy config page, select Adversary Behaviors

4. Select appropriate rule (toggle on)

## 2.1.6 (U) Given the Sysinternals suite identify what the specific capabilities the tools can provide.

Training Resources & Technical References:

 Microsoft, “Sysinternals Suite”, <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

**AccessChk**: know what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows servicesf

**AccessEnum**: gives you a full view of your file system and Registry security settings in seconds

**AdExplorer**: is an advanced Active Directory (AD) viewer and editor

**Autoruns**: comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players

**Disk Usage (DU)**: By default it recurses directories to show the total size of a directory and its subdirectories.

**Handle**: utility that displays information about open handles for any process in the system. You can use it to see the programs that have a file open, or to see the object types and names of all the handles of a program.

**ListDLLs**: utility that reports the DLLs loaded into processes. You can use it to list all DLLs loaded into all processes, into a specific process, or to list the processes that have a particular DLL loaded.

**LogonSessions**: lists the currently active logon sessions and, if you specify the -p option, the processes running in each session

**ProcessExplorer**: The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded.

**ProcessMonitor**: advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity

**PsExec**: light-weight telnet-replacement that lets you execute processes on other systems

**PsGetsid**: allows you to translate SIDs to their display name and vice versa

**PsInfo**: shows information for the local system. Specify a remote computer name to obtain information from the remote system

**PsList**: display a list of current processes

**PsService**: displays the status, configuration, and dependencies of a service, and allows you to start, stop, pause, resume and restart them

**ShareEnum**: uses NetBIOS enumeration to scan all the computers within the domains accessible to it, showing file and print shares and their security settings (use domain admin for best results)

**Sigcheck**: command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains. It also includes an option to check a file’s status on VirusTotal

**Streams**: will examine the files and directories (note that directories can also have alternate data streams) you specify and inform you of the name and sizes of any named streams it encounters within those files

**Strings**: scans the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters.

**Sysmon**: remains resident across system reboots to monitor and log system activity to the Windows event log

**TCPView**: show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections

# 2.1.7 (U) Given a set of sysmon logs identify malicious process creation.

Training Resources & Technical References:

 JPCERT, “Sysmon search”, <https://blogs.jpcert.or.jp/en/2019/02/sysmonsearch2.html>

To identify malicious process creation in Sysmon logs, you can look for the following events:

Event ID 1: Process creation: This event is generated when a new process is created. You can look for processes that are created from suspicious locations or that have suspicious command line arguments.

Event ID 3: Network connection: This event is generated when a process makes a network connection. You can look for processes that are making connections to known malicious IP addresses or domains.

Event ID 7: Image loaded: This event is generated when a DLL is loaded into a process. You can look for DLLs that are loaded from suspicious locations or that have suspicious names.

Event ID 8: CreateRemoteThread: This event is generated when a process creates a thread in another process. You can look for processes that are creating threads in other processes that they shouldn’t be.

Event ID 11: FileCreate: This event is generated when a file is created. You can look for files that are created in suspicious locations or that have suspicious names.

Event ID 12: RegistryEvent (Object create and delete): This event is generated when a registry key is created or deleted. You can look for registry keys that are created in suspicious locations or that have suspicious names.

By analyzing these events and looking for patterns of behavior, you can identify malicious process creation in Sysmon logs.

## 3.1.1 (U) Detect adversary modification of the following:

Training Resources & Technical References:

 MITRE, “Event Triggered Execution: Unix Shell Configuration Modification”, <https://attack.mitre.org/techniques/T1546/004/>

a. bash\_profile

In the search bar, type event.action: "bash\_profile".

You can also filter by time range or other parameters.

b. bashrc

To detect adversary modification of the bashrc file in Kibana, you can use the following methods

Use the filebeat module: The filebeat module for Linux system logs includes a pre-built dashboard that can be used to monitor for changes to the bashrc file. This dashboard includes visualizations that show the number of events over time and the top users who have modified the file.

Create a custom dashboard: You can also create a custom dashboard in Kibana that is tailored to your specific needs. This dashboard can include visualizations that show the number of events over time, the top users who have modified the file, and any other relevant information.

Use machine learning: You can also use machine learning in Kibana to detect anomalies in the data. This can help you identify when the bashrc file has been modified in an unusual way.

## 3.1.2 (U) Detect adversary addition of user to local administrator group:

Training Resources & Technical References:

 MITRE, “Account Manipulation”, <https://attack.mitre.org/techniques/T1098/>

a. Account manipulation

Windows Event ID: 4728 (added to AD security group)

Windows Event ID: 4732 (added to local security group)

Windows Event ID: 4738 (user object changed)

Windows Event ID: 5136 (AD Object Modification)

b. Account creation

Windows Event ID: 4720 (Acct Creation)

Powershell:

Get-localgroup

for list of local group names

Get-localgroupmember –Group administrators

-can substitute “administrators” for any item in local group list

## 3.1.3 (U) Detect adversary addition of root user and sudoer.

 MITRE, “Privilege Escalation”, <https://attack.mitre.org/tactics/TA0004>

 MITRE, “Account Manipulation”, <https://attack.mitre.org/techniques/T1098>

Linux SuperUses:

<https://www.baeldung.com/linux/list-all-superusers>

a. Root

$ cat /etc/passwd

to get a list of users

$ sudo -l -U <username>

to see the permissions the user has to run commands (ALL:ALL) ALL

b. sudoer

$ grep '^sudo:' /etc/group

this will display a list of users in the sudo group

OR

$ getent group sudo   
 searches the /etc/group folder for anyone in the sudo group

Training Resources & Technical References:

$ getent passwd | wc -l

this will do a line count on /etc/passwd to determine the number of users

## 3.1.4 (U) Detect adversary presence in windows logon and startup scripts.

Training Resources & Technical References:

 MITRE, “Boot or Login Initialization Scripts”, <https://attack.mitre.org/techniques/T1037/>

Check the Registry Run Keys and the Startup Folder for any malicious code appended to them.

Check the initialization scripts for any malicious code appended to them.

Check the group policies that are being applied to see which logon script is being run.

Check for any rootkits, compromised software, or other malicious code that may have been installed on the system

Training Resources & Technical References:

 Microsoft, “Sysinternals Suite”, <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

**Autoruns**: comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players

## 3.1.5 (U) Detect adversary presence in linux logon and startup scripts.

Training Resources & Technical References:

 MITRE, “Boot or Login Initialization Scripts”, <https://attack.mitre.org/techniques/T1037/>

1. Check the following files for any malicious code appended to them:

* ~/.bashrc
* ~/.bash\_profile
* /etc/profile
* ~/.bash\_login
* ~/.profile
* ~/.bash\_logout

1. Check the initialization scripts and shell configuration files for any malicious code appended to them.
2. Check the systemd generators for any malicious code appended to them.
3. Check for any rootkits, compromised software, or other malicious code that may have been installed on the system

## 3.1.6 (U) Detect adversary addition to BITS jobs.

Training Resources & Technical References:

 MITRE, “BITS Jobs”, <https://attack.mitre.org/techniques/T1197/>

Resource:

<https://www.mandiant.com/resources/blog/attacker-use-of-windows-background-intelligent-transfer-service>

Check the BITS jobs for any malicious code appended to them.

Check the PowerShell and the BITSAdmin tool for any malicious code appended to them1.

**EventID 59**

BITS started the BITS Transfer transfer job associated with the URL

UNC path of the target file (\\[Destination Host]\BITS\[File Name])

LOG location (Microsoft-Windows-Bits-Client/Operational)

**EventID 60**

BITS has stopped transferring the BITS Transfer transfer job associated with the URL

UNC path of the target file (\\[Destination Host]\BITS\[File Name]) The status code is [Status Code].

LOG location (Microsoft-Windows-Bits-Client/Operational)

or

Open Kibana and navigate to the Discover tab.

Search for any suspicious activity related to BITS jobs.

Check the Windows Registry for any suspicious entries.

Check the system for any rootkits, compromised software, or other malicious code that may have been installed on the system.

## 3.1.7 (U) Detect DLL Search Order Hijacking.

Training Resources & Technical References:

 MITRE, “Hijack Execution Flow: DLL Search Order Hijacking”, <https://attack.mitre.org/techniques/T1574/001/>

Check the Windows Event Viewer for any suspicious activity.

Check the Windows Registry for any suspicious entries.

Check the system for any rootkits, compromised software, or other malicious code that may have been installed on the system.

Training Resources & Technical References:

 Microsoft, “Sysinternals Suite”, <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

**Procmon**

[File Creation](https://attack.mitre.org/datasources/DS0022/#File%20Creation)

Monitor newly constructed .manifest and .local redirection files that do not correlate with software updates.

[File Modification](https://attack.mitre.org/datasources/DS0022/#File%20Modification)

Monitor for changed made to .manifest/.local redirection files, or file systems for moving, renaming, replacing, or modifying DLLs. Changes in the set of DLLs that are loaded by a process (compared with past behavior) that do not correlate with known software, patches, etc., are suspicious.

[Module Load](https://attack.mitre.org/datasources/DS0011/#Module%20Load)

Monitor DLLs loaded into a process and detect DLLs that have the same file name but abnormal paths.

**Kibana**

Here's a general approach to constructing your Kibana query:

* 1. **Identify suspicious Event IDs:**
     1. **event.code : "11"** (A user attempted to load a DLL from a potentially unsafe path)
     2. **event.code : "7"** (A suspicious DLL load was detected)
     3. **event.code : 1 AND process.name: (powershell.exe OR cmd.exe) AND process.command\_line : \*dll\***
  2. **Search for unusual paths:** 
     1. When a DLL is loaded from a directory other than its usual place (like ***C:\Windows\System32)***, it can be a sign of DLL hijacking.
  3. **Look for known critical DLL names**:
     1. If you know the names of critical DLLs that are often targeted in DLL hijacking attacks, you can add them to the query.

## 3.1.8 (U) Detect malicious hidden files and/or directories.

Training Resources & Technical References:

MITRE, “Hide Artifacts: Files and Directories”,

<https://attack.mitre.org/techniques/T1564/001/>

Use either the attrib or dir commands.

Viewing hidden files with dir and attrib command:

dir /ah

attrib -s -h -r /s /d \*. \*

## 3.1.l9 (U) Detect the presence of a rootkit.

Training Resources & Technical References:

 MITRE, “Rootkit”, <https://attack.mitre.org/techniques/T1014/>

example query to detect the presence of a rootkit:

Rootkits subvert the operating system and hide IOCs like process names, folders, files and network connections. Eventlogs can catch these for kernel and usermode rootkits. You’ll need to perform memory forensics, once you Identify a box with a userland or kernel rootkit. A training VM with the r77 rootkit has been uploaded to the Purple Forge git lab. [**836 COS / rootkit\_training · GitLab (af.mil)**](https://code.levelup.cce.af.mil/836-cos/rootkit_training)

**Sysmon Event logs can catch the process injection of the r77 rootkit. After that you’ll need to accomplish memory forensics to find the processes and the persistence.**

**windows.psscan.PsScan**

## 3.1.10 (U) Detect the presence of a malicious cronjob.

Training Resources & Technical References:

 MITRE, “Scheduled Task/Job: Cron”, <https://attack.mitre.org/techniques/T1053/003/>

query example:

**Datasource: filebeat collecting syslog**

**Kibana Query: event.dataset : system.syslog and host.hostname : "hostname" and message : (\*crontab\* and \*replace\*)**

**This syslog message indicates that the root user’s crontab file has been replaced. The crontab command, running on the websvr server, has performed a REPLACE operation on the root user’s crontab file. This means that the previous contents of the root user’s crontab file have been replaced with new contents.**

**This will give you the time that the crontab got changed. You'll need to gain access to the system to figure out what changed.**

event.action: "cron\_job" AND event.module: "system" AND event.dataset: "system.cron" AND (process.name: "sh" OR process.name: "bash") AND (process.args: "\*wget\*" OR process.args: "\*curl\*")

## 3.1.11 (U) Detect the presence of a malware maintaining persistence through scheduled tasks.

Training Resources & Technical References:

 MITRE, “Scheduled Task/Job: Scheduled Task”, <https://attack.mitre.org/techniques/T1053/005/>

* Review the creation and modification timestamps of scheduled tasks. If you know roughly when the malware was introduced to the host system, this may reveal malicious entries.

schtasks.exe /query /V /FO CSV | ConvertFrom-Csv |select Taskname,'Next run time','last run time','start Time',schedule,'Run as user','start date'

* Use a query like this one to detect malware that creates scheduled tasks:

schtasks /create /tn \"mysc\" /tr C:UsersPublictest.exe /sc ONLOGON /ru \"System\"

A great tool for finding persistence through scheduled tasks is the Sysinternals tool autoruns.

Logs will also work in Kibana: Event ID

Windows Event IDs for Scheduled Task: 4698(created), 4699 (deleted), 4700 (enabled), 4701 (disabled), and 4702 (updated).

## 3.1.12 (U) Detect the presence of malware maintaining persistence through modified services.

Training Resources & Technical References:

 MITRE, “Create or Modify System Processes”, <https://attack.mitre.org/techniques/T1543>

Windows Service:

<https://redcanary.com/threat-detection-report/techniques/windows-service/#:~:text=You%20may%20be%20able%20to,via%20the%20PUBLIC%20or%20APPDATA%20>)

* Use tools like Autoruns or Sysinternals Suite to identify modified services.

Windows Event Logs such as 4697, 7045 and/or 4688 will respectively alert on new services and processes being created

## 3.1.13 (U) Detect the adversary changes to PATH variables.

Training Resources & Technical References:

MITRE, “Hijack Execution Flow: Path Interception by PATH Environment Variable”, <https://attack.mitre.org/techniques/T1574/007/>

Explained Environmental Variables:

<https://www.malwarebytes.com/blog/news/2017/01/explained-environmental-variables>

dir env:

You can get a quick view of the variables that are preset on your system by using the above command

## 3.1.14 (U) Detect the presence of malicious activity using elevated execution permissions from the following methods:

Training Resources & Technical References:

MITRE, “Abuse Elevation Control Mechanism: Setuid and Setgid”, <https://attack.mitre.org/techniques/T1548/001/>

Finding Files with SUID and SGID Permissions in Linux:

<https://www.geeksforgeeks.org/finding-files-with-suid-and-sgid-permissions-in-linux/>

A. Setuid:

To detect the presence of malicious activity using elevated execution permissions from Setuid, you can use the following command in Linux command prompt:

find / -perm -4000 -type f -exec ls -ld {} \

This command will search for all files with the setuid bit set and list them with their permissions.

B. Setgid

SGID: This is also special file permission for executable files that enables other users to inherit the effective GID(Group Identifier) of a group owner. Here rather than x which represents executable permissions, we will see s(which indicates SGID) special permission for group users

find / -user root -2000 -exec ls -ldb {} \;

C. Setuid and Setgid

To find files that have both SUID and SGID set, run the command below.

find / -user root -perm -6000 -exec ls -ldb {} \;

## 3.1.15 (U) Detect the use of shortcut modification.

Training Resources & Technical References:

MITRE, “Boot or Login Autostart Execution: Registry Run Keys / Startup Folder”, <https://attack.mitre.org/techniques/T1547/009/>

ELK: Shortcut File Written or Modified for Persistence:

<https://www.elastic.co/guide/en/security/7.17/shortcut-file-written-or-modified-for-persistence.html#shortcut-file-written-or-modified-for-persistence>

Shortcuts, also known as symbolic links, are an aspect of operating systems that allow for the referencing of other files, applications or programs. When it is clicked or executing during system startup, what is referenced becomes opened (if a file) or executed (if an application or program). Attackers use this inherent aspect of systems during persistence by executing attack tools with it. The motivation for this attack technique is not so much due to laziness as it is for aiding in the persistence phase of an attack.

There is only one way to detect this attack technique. This involves relating shortcut file change (and other creation events) to potentially malicious events or other known adversary behavioral events. The most telling behavioral event is unknown executable process launches that establish network connections.

**Elastic Rule Query:**

**file where event.type != "deletion" and user.domain != "NT**  
**AUTHORITY" and file.path :**  
**("C:\\Users\\\*\\AppData\\Roaming\\Microsoft\\Windows\\Start**  
**Menu\\Programs\\Startup\\\*",**  
**"C:\\ProgramData\\Microsoft\\Windows\\Start**  
**Menu\\Programs\\StartUp\\\*") and process.name : ("cmd.exe",**  
**"powershell.exe", "wmic.exe",**  
**"mshta.exe", "pwsh.exe",**  
**"cscript.exe", "wscript.exe",**  
**"regsvr32.exe", "RegAsm.exe",**  
**"rundll32.exe", "EQNEDT32.EXE",**  
**"WINWORD.EXE", "EXCEL.EXE",**  
**"POWERPNT.EXE", "MSPUB.EXE",**  
**"MSACCESS.EXE", "iexplore.exe",**  
**"InstallUtil.exe")**

Identifies files written to or modified in the startup folder by commonly abused processes. Adversaries may use this technique to maintain persistence.

## 3.1.16 (U) Detect malicious use of WMI event subscription.

Training Resources & Technical References:

MITRE, “Event Triggered Execution: Windows Management Instrumentation Event Subscription”, <https://attack.mitre.org/techniques/T1546/003/>

Into into abusing/ID’ing WMI Event Subscriptions for Persistence:

<https://in.security/2019/04/03/an-intro-into-abusing-and-identifying-wmi-event-subscriptions-for-persistence/>

Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.[2][3] Adversaries may also compile WMI scripts into Windows Management Object (MOF) files (.mof extension) that can be used to create a malicious subscription.[4][5]

WMI subscription execution is proxied by the WMI Provider Host process (WmiPrvSe.exe) and thus may result in elevated SYSTEM privileges.

To detect malicious use of WMI event subscription, you can use the following command in Windows command prompt:

Get-WmiObject -Namespace root\subscription -Class \_\_FilterToConsumerBinding

This command will list all the filter-to-consumer bindings in the root\subscription namespace.

* + EventID 19 User created Wmi filter
  + EventID 20 User created Wmi consumer
  + EventID 21 User created Wmi subscription
  + \_\_EventFilter is a WQL query that outlines the trigger event of interest.
  + \_\_EventConsumer is an action to perform upon triggering an event.
  + \_\_FilterToConsumerBinding is the registration mechanism that binds a filter to a consumer.

## 3.1.17 (U) Detect the use of data staging and encoding used prior to exfiltration.

Training Resources & Technical References:

 MITRE, “Data Staged: Local Data Staging”, <https://attack.mitre.org/techniques/T1074/001/>

Linux Find Command:

<https://www.geeksforgeeks.org/find-command-in-linux-with-examples/>

o detect the use of data staging and encoding used prior to exfiltration, you can use the following command in Linux command prompt:

find ./ -type f -name "\*.jpg" -o -name "\*.png" -o -name "\*.gif"

This command will search for all image files in the file system. Attackers often use image files to hide data and exfiltrate it from the network

## 3.1.18 (U) Detect the exfiltration of data over removable devices.

Training Resources & Technical References:

 MITRE, “Exfiltration Over Physical Medium”, <https://attack.mitre.org/techniques/T1052/>

**USB EXFIL TRAINING : https://code.levelup.cce.af.mil/836-cos/training-usb-exfil**

* + **A person should be able to understand this document to understand how USB exfil works.**

To detect possible malicious USB connections the following Security Event ID needs to be turned on and monitored.

## Event ID 6416 - A new external device was recognized by the system.

|  |  |
| --- | --- |
| **Event ID** | 6416 |
| **Category** | Process tracking |
| **Sub category** | Plug and play |
| **Description** | A new external device was recognized by the system. |

When the system recognizes a new external device (for example a USB), event ID 6416 is logged.

This log data gives the following information:

|  |  |
| --- | --- |
| **Subject: User who performed the action** | * Security ID * Account Name * Account Domain * Logon ID * Device ID * Device Name * Class ID * Class Name |
| **Vendor IDs** | * Device types specified by vendor. |
| **Compatible IDs** | * Remote IP Address * Remote Port |
| **Port Information** | * Which port it was connected on the computer. |

After you have suspicion of a USB exfil a forensic image of the machine needs to be taken and Windows Artifacts need to be collected.

Please review and practice on the following forensic image:

## 3.1.19 (U) Demonstrate the ability to search for Indicators of Compromise on a dead disk.

Training Resources & Technical References:

 CISCO, “Indicators of Compromise and Where to Find Them”, <https://blogs.cisco.com/security/indicators-of-compromise-and-where-to-find-them>

Autopsy User Documentation (Disk Mounting)

<https://sleuthkit.org/autopsy/docs/user-docs/3.1/ds_page.html>

FTK Imager (Disk Mounting)

<http://www.computersecuritystudent.com/FORENSICS/FTK/IMAGER/FTK_IMG_313/lesson4/index.html>

Autopsy: Practical Cyber Forensics

<https://usaf.percipio.com/books/ae6862cc-94de-4cf8-b8ac-655b93046119#epubcfi(/6/62!/4/2%5Bepubmain%5D/2%5Bch002_s1_5%5D/2/2/1:0>)

Autopsy: Autopsy is a digital forensics platform that allows you to analyze hard drives and smartphones. It has a built-in file viewer and keyword search functionality that can help you find Indicators of Compromise (IOCs) on a dead disk.

1. Open Autopsy: Create New Case
2. Enter Case # and directory to save case at (Base Directory)
3. Toolbar: “Add Data Source”
4. Select Image File, browse to file location
   1. Image Types
      1. Raw Single: \*.img, \*.dd, \*.raw, etc
      2. Raw Split: \*.001, \*.002, \*.aa, \*.ab, etc
      3. EnCase: \*.e01, \*e02, etc
5. Select all ingest modules (ex: Hash Lookup, File Type ID, Extension Mismatch)

Sleuth Kit: Sleuth Kit is a collection of command-line tools that allow you to analyze disk images and recover deleted files. It includes tools such as mactime, which can help you create timelines of file activity on a disk.

Volatility: Volatility is a memory forensics framework that allows you to analyze the memory of a running system or a memory dump. It includes plugins that can help you find IOCs such as malware processes, network connections, and registry keys.

FTK Imager:

1. Launch FTK Imager
2. File – Add Evidence Item – Source (Image File)
3. Browse to File Location / Select File

## 3.1.20 (U) Triage malware from dead disk and identify the process to get assistance with reverse engineering.

Training Resources & Technical References:

 MDPI, “Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions”, <https://www.mdpi.com/2073-8994/9/4/49/pdf>

FTK Forensic Disk Image

<https://usaf.percipio.com/courses/d90a72cd-7f94-4fb6-82a1-d248bb74e316/videos/2910dca8-d127-4561-b9c7-126a2a8f9c15>

“dd” command in Linux

<https://www.geeksforgeeks.org/dd-command-linux/>#

1. To extract the malware from the disk use the Extracting Files and Malware.docx which can be found at [836 COS / training-extracting-files · GitLab (af.mil)](https://code.levelup.cce.af.mil/836-cos/training-extracting-files)
2. If allowed to triage a piece of malware accomplish the following
3. Transfer the sample to a sandboxed environment
4. Ensure that the sandbox is not connected to other machines, the internet, or through file share to the host machine
5. Create a snapshot of the sandbox
6. Perform static analysis and research as required
   1. Check hash against authorized database
   2. Run a offline AV such as clamscan to see if it is a known virus
   3. Base64 encoded data
   4. Strings:
      1. Commands
      2. Function names
      3. Scripts
      4. Usernames
      5. File names
      6. IP addresses
      7. Domain names
      8. Hostnames
      9. URLs
      10. Packed?
7. Document your hypothesis and findings
8. Perform dynamic analysis if allowed
9. Document your conclusion, update your findings, and if required, perform static analysis or dynamic analysis
10. Follow the communication plan to request assistance from a malware triage analyst

## 3.1.21 (U) Detect malware in Memory.

Training Resources & Technical References:

Oreilly, “Hunting Malware in Process Memory”, <https://www.oreilly.com/library/view/the-art-of/9781118824993/c08.xhtml>

Using Volatility Framework

<https://usaf.percipio.com/courses/4621e75e-aa3e-4352-87e5-570d502206d5/videos/57e39702-a084-48d2-b170-3942d8af14bc>

Blue Team Toolkit: Sysinernals

[https://usaf.percipio.com/books/dfe6c708-5fe1-49cc-b148-b1b8e9f895e9#epubcfi(/6/34!/4/2%5Bepubmain%5D/2%5Bch02lev1sec5%5D/14/1:0](https://usaf.percipio.com/books/dfe6c708-5fe1-49cc-b148-b1b8e9f895e9#epubcfi(/6/34!/4/2%5Bepubmain%5D/2%5Bch02lev1sec5%5D/14/1:0)))

Redline User Guide:

<https://fireeye.market/assets/apps/211364/documents/877936_en.pdf>

Volatility: Volatility is a memory forensics framework that allows you to analyze the memory of a running system or a memory dump. It includes plugins that can help you find malware processes, network connections, and registry keys.

Mandiant Redline: Mandiant Redline is a free tool that allows you to analyze running processes and memory dumps for signs of malware. It includes a set of built-in indicators of compromise (IOCs) that can help you detect known malware.

Microsoft Sysinternals Process Explorer: Microsoft Sysinternals Process Explorer is a free tool that allows you to view information about running processes on a system. It includes features such as process highlighting and virus total integration that can help you detect malware.

Examples of Volatility 3 commands

* vol.py -f “/path/to/file” windows.info
* vol.py -f “/path/to/file” windows.pstree
* vol.py -f “/path/to/file” -o “/path/to/dir” windows.dumpfiles ‑‑pid <PID>
* vol.py -f “/path/to/file” -o “/path/to/dir” windows.memmap ‑‑dump ‑‑pid <PID>
* vol.py -f “/path/to/file” windows.handles ‑‑pid <PID>
* vol.py -f “/path/to/file” windows.dlllist ‑‑pid <PID>
* vol.py -f “/path/to/file” windows.cmdline
* vol.py -f “/path/to/file” windows.netstat
* vol.py -f “/path/to/file” windows.malfind
* vol.py -f “/path/to/file” yarascan -y “/path/to/file.yar”

## 3.1.22 (U) Discover Files using Alternate Data streams.

Training Resources & Technical References:

 Malwarebytes, “Introduction to Alternate Data Streams”, <https://blog.malwarebytes.com/101/2015/07/introduction-to-alternate-data-streams/>

To discover files using Alternate Data Streams (ADS), you can use the following command in Windows command prompt: dir /r. This command will display all files and their associated ADS on the file system.

> dir /r /s | findstr “:$DATA”

You can also use the following tools:

Streams: Streams is a free tool that allows you to view and delete ADS on a file system. It includes a graphical user interface (GUI) that makes it easy to use.

NTFS-ADS: NTFS-ADS is a free tool that allows you to view and extract ADS on a file system. It includes a command-line interface (CLI) that can be used to automate the discovery of ADS.

If you know the name of a file you would like to check for an ADS via powershell, you can use the following syntax:

PS> Get-Item -Path .\Testing.txt -Stream \*

## 3.1.23 (U) Submit tool and capability requirements to resolve mission gaps in accordance with established policies, regulations, and procedures.

Training Resources & Technical References:

 Microsoft, “Windows Event Log”, <https://docs.microsoft.com/en-us/windows/win32/wes/windows-event-log>

 Microsoft, “Task Scheduler for Developers”, <https://docs.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page>

 Microsoft, “Registry”, <https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry>

**Adversary Tactic (**[**source**](https://attack.mitre.org/techniques/T1110/002/)**)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Technique ID** | **Sub-Technique ID** | **Technique** | **Procedure** |
| [T1110](https://attack.mitre.org/techniques/T1110) | [0.002](https://attack.mitre.org/techniques/T1110/002) | Brute Force: Password Cracking | APT41 performed password brute-force attacks on the local admin account. |

**Tool/Capability Requirements**

|  |  |  |
| --- | --- | --- |
| **Tool** | **Capability** | **Expectation** |
| Winlogbeat | Forward Windows events to our SIEM | An analyst can use the following query to enumerate adversary brute force attempts.    event.code:4625 AND event\_data.TargetUserName:"Administrator" |

**Detection (**[**source**](https://attack.mitre.org/techniques/T1110/002/)**)**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Data Source** | **Data Component** | **Detects** |
| [DS0015](https://attack.mitre.org/datasources/DS0015) | [Application Log](https://attack.mitre.org/datasources/DS0015) | [Application Log Content](https://attack.mitre.org/datasources/DS0015/#Application%20Log%20Content) | Monitor authentication logs for system and application login failures of [Valid Accounts](https://attack.mitre.org/techniques/T1078). It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network. Consider focusing efforts on detecting other adversary behavior used to acquire credential materials, such as [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) or [Kerberoasting](https://attack.mitre.org/techniques/T1558/003). |
| [DS0002](https://attack.mitre.org/datasources/DS0002) | [User Account](https://attack.mitre.org/datasources/DS0002) | [User Account Authentication](https://attack.mitre.org/datasources/DS0002/#User%20Account%20Authentication) | Monitor for many failed authentication attempts across various accounts that may result from password spraying attempts. It is difficult to detect when hashes are cracked, since this is generally done outside the scope of the target network. (ex: Windows EID 4625 or 5379) |

## 3.1.24 (U) Evaluate a comprehensive assessment strategy that leverages available information sources, personnel, and systems to address potential vulnerabilities and risk-related practices.

Training Resources & Technical References:

Crowdstrike. “WHAT IS CYBER ESPIONAGE?” Kurt Baker - February 28, 2023, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Zdnet. “Eight ways to improve your corporate network security posture.” Tim Nichols on April 5, 2012. https://www.zdnet.com/home-and-office/networking/eight-ways-to-improve-your-corporate-network-security-posture/

The network owner’s top priorities should be to protect the drone testing data, the drone development or research data and the network perimeter. This shift in strategy will help the local defensive cyberspace operators posture against cyber threat groups that target similar organizations and use cyber espionage such as data theft or intellectual property theft.

**Segmentation** - Segmenting the network can help to reduce the risk of a breach. By segmenting the network, you can limit the number of systems that are exposed to an attacker if one system is compromised.

**Access Control** - Access control is a critical component of any security strategy. It involves limiting access to sensitive data and systems to only those who need it. On this network, it was difficult to determine who was responsible for what and who, in fact, needed access for business purposes. A person with knowledge of the location of the drone data could simply transfer it to another device through an external device or using a personal account accessible from the internet.

**Encryption** - Encryption is a powerful tool that can help protect data from unauthorized access. By encrypting data in transit and at rest, you can ensure that even if an attacker gains access to your network, they won't be able to read your data. This includes all drone data that is considered sensitive like testing results of a drone prototype, development data used to plot new design features, or even documents proposing the future testing location.

**Monitoring** - Monitoring your network is essential for detecting and responding to security incidents. By monitoring your network, you can detect unusual activity and respond quickly before it becomes a major issue. Although we uncovered an insider threat and exfiltration of confidential information by a known cyber threat actor during one investigation, the local defensive cyberspace operators need to refine the network map that was created and continue to monitor network traffic and security events on endpoints. Eventually, the operators will be able to develop a baseline for user activities and system communications to detect anomalies.

**Patching** - Keeping your systems up-to-date with the latest patches is essential for maintaining a secure network. Patches often include security updates that address known vulnerabilities. We found that the adversary compromised the poorly patched development environment prior to brute forcing the local administrator account on a user workstation on the business network.

## 3.1.25 (U) Incorporate open source vulnerability assessment tools into a virtual machine for use in a test environment.

Training Resources & Technical References:

Microsoft, “Task Scheduler for Developers”, <https://docs.microsoft.com/en-us/windows/win32/taskschd/task-scheduler-start-page>

Install a virtual machine: Install a virtual machine software such as VirtualBox or VMware on your host machine.

Download an open source vulnerability assessment tool: Download an open source vulnerability assessment tool such as OpenVAS or Nikto.

<https://greenbone.github.io/docs/latest/background.html#architecture>

https://github.com/greenbone/openvas-scanner

Install the tool on the virtual machine: Install the vulnerability assessment tool on the virtual machine.

Configure the virtual machine: Configure the virtual machine to allow network access and assign it an IP address.

Scan the network: Use the vulnerability assessment tool to scan the network for vulnerabilities.

## 3.21 (U) Given current intelligence and a network map, create a host collection plan.

Training Resources & Technical References:

Dragos, “Collection Management Frameworks – Looking Beyond Asset Inventories in Preparation for and Response to Cyber Threats”, <https://www.dragos.com/wp-content/uploads/CMF_For_ICS.pdf?hsCtaTracking=1b2b0c292196-4ebd-a68c-5099dea41ff6%7C27c19e1c-0374-490d-92f9-b9dcf071f9b5>

https://usaf.dps.mil/:x:/r/teams/AFN-CPTCollaboration/Shared%20Documents/1.%20%20Operational%20Training/3.%20JQR%20Qualification/00a%20-%20Host%20Analyst/Supporting%20documentation/Host%20Collection%20Plan.xlsx?d=wb30a70ad6fc54665b70ca2285189f8c2&csf=1&web=1&e=O4A1yi

## 3.22 (U) Given a scenario and required data, draft or provide input to the host section of a risk mitigation plan.

Training Resources & Technical References:

[~~https://www.mitre.org/publications/systems-engineering-guide/acquisition-system-sengineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring~~](https://www.mitre.org/publications/systems-engineering-guide/acquisition-system-sengineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring)

<https://www.mitre.org/our-impact/mitre-labs/systems-engineering-innovation-center/risk-mitigation>

https://www.mitre.org/our-impact/mitre-labs/systems-engineering-innovation-center/risk-management-approach-and-plan

One risk on the CA-1 Enclave was that the adversary may gain access to the production network via the development which could enable access to the drone reconnaissance data that the network owner sought to protect. Since there was no system dependency that requires the connection, the connection should be removed. The development network needs to be isolated since it greatly increases the risk to the attack surface for the organization by having unpatched machines connected to the internet.

This can be performed at the firewall or router through configuration changes or by adding additional hardware and/or policies. The configuration changes would take less than a day to implement and test. The hardware and/or policies has a longer timeline that is difficult to estimate since your organization will be waiting on the physical devices to arrive, testing would need to be accomplished, and the policies take a while to create, formalize, implement, and monitor after implementation. Then, you would need to setup systems and accounts for employees to work or access the isolated environment.

An alternative would be to setup VLANS and separate connections at each employee's desk or through a VPN concentrator.