Nama : MOCHAMMAD ALDO RIZKY

Nim : 2141762002

Kelas : SIB-4C

Lab - Identify Relevant Threat Intelligence

Objectives

Part 1: Research MITRE CVEs

Part 2: Access the MITRE ATT&CK Knowledge Base

Part 3: Investigate Potential Malware

Background / Scenario

You have been hired as a Tier 1 Cybersecurity Analyst by XYZ, Inc. Tier 1 analysts typically are responsible for responding to incoming tickets and security alerts. In this lab, you will conduct threat intelligence research for several scenarios that have impacted XYZ, Inc. Each scenario will require you to access threat intelligence websites and answer questions regarding the threat encountered in the scenario.

Required Resources

- 1 PC with internet access

Instructions

Part 1: Research MITRE CVEs

The MITRE organization created the Common Vulnerabilities and Exposures (CVE) database in 1999 to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. It was endorsed by the National Institute of Standards and Technology (NIST) in 2002. The CVE database is now the standard method of registering and identifying vulnerabilities.

In this part, you will research the CVE program and use the CVE list to identify threats.

Step 1: Research the CVE website.

Go to **https://cve.mitre.org** and navigate to the **About** > **Terminology** page to answer the following questions.

What is the **CVE Program**?

The CVE Program is an international, community-driven effort to catalog vulnerabilities in software and hardware systems according to established rules and guidelines. It aims to provide a standardized identifier for each vulnerability, making it easier for organizations to share information and coordinate responses to cybersecurity threats. By providing a common reference point, the CVE Program helps improve security across diverse systems and facilitates collaboration among security professionals, researchers, and vendors.

The CVE program is an international, community-driven effort to catalog vulnerabilities in accordance with the effort’s rules and guidelines.

Show Answer Hide Answer

What is a CVE Numbering Authority (CNA)?

A CVE Numbering Authority (CNA) is an organization that is authorized to assign CVE IDs to vulnerabilities and to create and publish information about those vulnerabilities in the associated CVE Record. Each CNA has a defined scope of responsibility, which outlines the types of vulnerabilities they are authorized to identify and report. This structure helps ensure that vulnerabilities are cataloged consistently and accurately, facilitating better communication and collaboration within the cybersecurity community.

A CNA is an organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific scope of responsibility for vulnerability identification and publishing.

Show Answer Hide Answer

What is an Authorized Data Publisher (ADP)?

An Authorized Data Publisher (ADP) is an organization authorized within the CVE Program to enhance a CVE Record that has been previously published by a CNA. ADPs can add additional, related information to the record, such as risk scores (like the Common Vulnerability Scoring System, or CVSS), lists of affected products, and specific versions. This enrichment helps provide a more comprehensive understanding of the vulnerability and its impact, facilitating better risk management and response strategies.

An ADP is an organization authorized within the CVE Program to enrich a CVE Record previously published by a CNA with additional, related information including risk scores (e.g., Common Vulnerability Scoring System (CVSS), affected product lists, and versions.

Show Answer Hide Answer

What is the **CVE List**?

The CVE (Common Vulnerabilities and Exposures) List is a publicly accessible, searchable database of all documented CVE Records, which represent known cybersecurity vulnerabilities and exposures. Each entry in the CVE List contains a unique identifier, along with details about specific security issues, allowing security professionals, software vendors, and IT teams to track, assess, and address vulnerabilities in software and hardware systems. Managed by the CVE Program, this list serves as a standardized reference to help organizations recognize and mitigate security risks.

The CVE List is a searchable catalog of all CVE Records identified by, or reported to, the CVE Program.

Show Answer Hide Answer

What is a **CVE Record**?

A CVE Record contains detailed information about a specific vulnerability identified with a unique CVE ID. This record is created and initially populated by a CNA (CVE Numbering Authority) and may be enriched by ADPs (Authorized Data Publishers) to ensure comprehensive information. CVE Records are available in various formats that can be read by both humans and machines, making them useful for cybersecurity systems and professionals alike. Each CVE Record can exist in one of three states:

Reserved: The CVE ID is assigned but details are not yet published.

Published: The CVE details are fully disclosed and accessible.

Rejected: The CVE ID was assigned but later deemed unnecessary or invalid and thus discarded.

The CVE Record is the descriptive data about a vulnerability associated with a CVE ID, provided by a CNA, and enriched by ADPs. This data is provided in multiple human and machine-readable formats. A CVE Record is associated with one of the following states: Reserved, Published, and Rejected.

Show Answer Hide Answer

What is a **CVE ID**?

A CVE ID is a unique alphanumeric identifier assigned to a specific vulnerability by the CVE Program. This identifier ensures consistency in tracking and referencing vulnerabilities across different tools, platforms, and discussions, enabling multiple organizations and cybersecurity tools to recognize and correlate the same vulnerability accurately. The CVE ID standardizes how vulnerabilities are identified, making it easier for stakeholders to share and act on critical security information in an automated and efficient way.

A unique, alphanumeric identifier assigned by the CVE Program. Each identifier references a specific vulnerability. A CVE ID enables automation and multiple parties to discuss, share, and correlate information about a specific vulnerability, knowing they are referring to the same thing.

Show Answer Hide Answer

Step 2: Research CVEs at the Cisco Security Advisories website.

Many security sites and software refer to CVEs. For example, the cisco.com website provides Cisco Security Advisories identifying vulnerabilities associated with Cisco products. In this step, you will refer to this website to identify a CVE ID.

a. Leave the cve.mitre.org website open. In another browser tab, do an internet search for **Cisco Security Advisories** and click the link to go to the tools.cisco.com web page.

b. This page lists all the currently known CVEs. For the **Impact** column, click the down arrow and uncheck everything except **Critical**, and then click **Done**.

c. Choose one of the advisories and answer the following questions about your selected advisory.

What is the name of the advisory that you chose?

Advisory Name: "Cisco ASA and FTD Software Web Services Interface Path Traversal Vulnerability"

The name is listed in the first column. For example, "Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability"

Show Answer Hide Answer

What is the CVE ID? You will use this ID in the next step.

The CVE ID for the advisory you choose can be found in the third column of the Cisco Security Advisories page. It will be in the format CVE-Year-Number (e.g., CVE-2021-34730). This unique identifier corresponds to the specific vulnerability in the advisory and will be used in further steps for referencing or researching the vulnerability details.

The CVE ID is listed in the third column. For example, the CVE ID for " Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability" is CVE-2021-34730.

Show Answer Hide Answer

d. You can either click the advisory to go to a details page or click the down arrow next to the advisory name to get more information.

Is there a **workaround** for the advisory you chose?

To determine if there is a workaround for the advisory you chose, you can either:

Click the advisory name to go to the details page, or

Click the down arrow next to the advisory name for a summary.

In most cases, the answer to "Is there a workaround?" will be "No", as critical vulnerabilities often require patches rather than workarounds. However, checking the advisory details will confirm if any temporary mitigation steps are recommended.

The answer is most likely "No".

Show Answer Hide Answer

Step 3: Return to the CVE website and research more about your chosen Cisco CVE.

a. Navigate back to the website cve.mitre.org website, which should still be open in a browser tab.

b. Click **Search CVE List** to open up a search box.

c. In the search field, enter the CVE ID for the critical advisory you documented in the previous step. The CVE ID is in the following format: **CVE-[year]-[id_number]**.

Briefly describe the vulnerability.

To describe the vulnerability, follow these steps:

Go to cve.mitre.org.

Click "Search CVE List" to open the search box.

Enter the CVE ID you documented earlier, in the format CVE-[year]-[id_number].

Review the vulnerability details provided in the search results.

For example, a CVE like CVE-2021-34730 might describe a vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business Routers. This vulnerability could allow an unauthenticated, remote attacker to trigger a denial of service (DoS), impacting device availability.

Answers will vary based on the CVE you chose. For example, CVE-2021-34730 describes a vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business Routers that could allow an unauthenticated, remote attacker to create a denial of service (DoS) condition. Notice that this is the same information you can find in the details for this advisory on the Cisco Security Advisories website.

Show Answer Hide Answer

Part 2: Access the MITRE ATT&CK Knowledge Base

The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution. In this part, you will investigate the MITRE ATT&CK website to answer questions.

Step 1: Go to the MITRE ATT&CK website.

Navigate to the **https://attack.mitre.org** website.

The page displays an attack matrix for enterprises which identifies various tactics and the techniques used by threat actors. **Tactics** are the header column titles (e.g., **Reconnaissance**, **Resource Developments**, etc.) with **Techniques** listed below. A short phrase for each technique summarizes what a threat actor could do to execute an attack. Clicking the linked phrase will take you to a page for detailed information about the techniques and methods for mitigation.

Note: You may need to expand the width of your browser window to see all 14 tactics. Alternatively, you can hold down the **Shift** key and scroll your mouse wheel to shift the window left and right.

This matrix is an excellent place to come to learn more about different tactics and techniques threat actors use to compromise systems. Cybersecurity analysts regularly visit this site to research specific attacks and possible mitigations.

Step 2: Investigate the Reconnaissance tactic and the Phishing for Information tactic.

Use the MITRE ATT&CK page to answer the following questions.

How many techniques are attributed to the **Reconnaissance** tactic?

To find the number of techniques attributed to the Reconnaissance tactic in the MITRE ATT&CK framework:

1. Go to the MITRE ATT&CK website.
2. Navigate to the Reconnaissance tactic section.
3. Count the listed techniques under this tactic.

Answers may vary, but at the time of this writing there were 10 techniques under the Reconnaissance tactic.

Show Answer Hide Answer

Under **Reconnaissance**, click **Phishing for Information** and read the description. Briefly describe how a threat actor could gather reconnaissance information using phishing techniques?

A threat actor can use phishing techniques to gather reconnaissance information by sending deceptive messages designed to elicit sensitive information from a target. These phishing messages are a form of electronically delivered social engineering aimed at tricking recipients into revealing information that can assist the adversary in future attacks. Phishing can also be tailored, known as spearphishing, where specific individuals, companies, or industries are targeted, increasing the likelihood of success by making the message appear more credible and relevant to the recipient.

Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing where a specific individual, company, or industry will be targeted by the adversary.

Show Answer Hide Answer

Expand the dropdown menu under the **Phishing for Information** header or refer to the menu on the left. What are sub-techniques used when phishing for information?

The sub-techniques used when phishing for information under the Phishing for Information header include:

1. Spearphishing Service: Targeting individuals through online services or platforms to trick them into revealing sensitive information.
2. Spearphishing Attachment: Sending emails with malicious attachments designed to entice the recipient to open them, often leading to the extraction of sensitive data or malware installation.
3. Spearphishing Link: Including deceptive links in emails that lead recipients to fraudulent websites designed to harvest their credentials or other sensitive information.

Answers should be Spearphishing Service, Spearphishing Attachment, and Spearphishing Link.

Show Answer Hide Answer

What steps could you take to mitigate these techniques?

To mitigate phishing techniques, including those associated with the Phishing for Information sub-techniques, consider implementing the following steps:

1. Email Authentication and Anti-Spoofing:

Use protocols like SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) to help validate incoming emails and reduce the likelihood of spoofed messages reaching users.

2. Email Filtering:

Implement advanced email filtering solutions that can detect and block phishing attempts based on known patterns, attachments, and links. This can help prevent malicious emails from reaching users' inboxes.

3. User Training and Awareness:

Conduct regular training sessions to educate users about social engineering tactics, including how to recognize phishing emails and suspicious links. Encourage users to verify the authenticity of requests for sensitive information, especially if they seem urgent or unexpected.

4. Incident Response Procedures:

Establish clear procedures for reporting suspected phishing attempts. Users should know how to report these incidents to IT or security teams for further investigation.

5. Multi-Factor Authentication (MFA):

Implement MFA for critical systems and accounts. This adds an extra layer of security, making it more difficult for attackers to gain unauthorized access even if they acquire a user’s credentials.

6. Regular Updates and Patching:

Keep all software and systems up to date with the latest security patches to reduce vulnerabilities that could be exploited in conjunction with phishing attacks.

Software configuration using anti-spoofing and email authentication to filter messages and user training to identify social engineering attacks

Show Answer Hide Answer

Step 3: Investigate the Command and Control tactic and Data Encoding technique.

Use the MITRE ATT&CK page to answer the following questions.

Note: **Command and Control** is the 12th tactic in the matrix. You may need to expand the width of your browser window to see it. Alternatively, you can hold down the **Shift** key and scroll your mouse wheel to shift the window left and right.

How many techniques are attributed to the **Command and Control** tactic?

To find the number of techniques attributed to the Command and Control tactic in the MITRE ATT&CK framework:

Visit the MITRE ATT&CK website.

Navigate to the Command and Control tactic section, which is the 12th tactic in the matrix.

Count the techniques listed under this tactic.

Answers may vary, but at the time of this writing there were 16 techniques available.

Show Answer Hide Answer

Under **Command and Control**, click **Data Encoding** and read the description. Briefly describe how a threat actor could use data encoding for command and control?

A threat actor can use data encoding for command and control (C2) purposes by encoding the data transmitted between the compromised system and the C2 server. This technique involves using standard encoding systems, such as ASCII, Unicode, Base64, or MIME, to obscure the content of the C2 traffic. By encoding the data, the threat actor makes it more challenging for security systems and analysts to detect malicious communications, as the encoded data may appear benign or nonsensical without proper decoding.

Additionally, threat actors might use data compression methods like gzip to further obfuscate the C2 traffic. This can help reduce the size of the data being transmitted and complicate detection efforts, as the compressed data may not resemble typical command and control patterns, allowing the adversary to maintain stealth and evade security measures.

Threat actors may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system (e.g., ASCII, Unicode, Base64, MIME) and in data compression, (e.g., gzip).

Show Answer Hide Answer

What could you do to mitigate this technique?

To mitigate the use of data encoding as a command and control technique, consider implementing the following strategies:

1. Network Intrusion Detection and Prevention Systems (IDS/IPS):

Deploy IDS/IPS solutions that utilize network signatures and rules to detect and block traffic associated with known adversary malware. These systems can identify unusual patterns or anomalies in network traffic, including encoded communications.

2. Traffic Analysis:

Monitor network traffic for patterns indicative of command and control activities, such as frequent connections to uncommon external IP addresses or abnormal data transfers. Analyze encoded traffic for known signatures of malicious activity.

3. Behavioral Analysis:

Implement solutions that use behavioral analysis to detect deviations from normal network behavior. This can help identify potential command and control communications, even if they are encoded.

4. Threat Intelligence:

Leverage threat intelligence feeds to stay informed about the latest adversary techniques and associated C2 methods. This can help in updating detection mechanisms and response strategies accordingly.

5. Application Whitelisting:

Use application whitelisting to ensure that only approved software is allowed to run on networked devices. This can help prevent unauthorized malware from establishing command and control connections.

6. Regular Updates and Patching:

Ensure that all systems, applications, and security tools are regularly updated and patched to protect against vulnerabilities that could be exploited for command and control purposes.

7. User Education:

Educate users about the risks associated with encoding techniques and the importance of reporting suspicious activities. Awareness can help in early detection of potential threats.

Network intrusion detection and prevention systems (IDS/IPS) using network signatures / rules to identify traffic for specific adversary malware can be used to mitigate activity at the network level.

Show Answer Hide Answer

Step 4: Investigate the Impact Tactic

Use the MITRE ATT&CK page to answer the following questions.

Note: The **Impact** tactic is the last tactic on the far right of the matrix.

How many techniques are attributed to the **Impact** tactic?

To find the number of techniques attributed to the Impact tactic in the MITRE ATT&CK framework:

Visit the MITRE ATT&CK website.

Navigate to the Impact tactic section, which is the last tactic on the far right of the matrix.

Count the techniques listed under this tactic.

To find the number of techniques listed under the Impact tactic in the MITRE ATT&CK framework, you can follow these steps:

1. Visit the MITRE ATT&CK website.
2. Navigate to the Impact tactic section, which is located at the far right of the tactics matrix.
3. Count the techniques displayed under the Impact tactic.

Answers may vary, but at the time of this writing there were 13 techniques available.

Show Answer Hide Answer

Under **Impact**, click **Disk Wipe** and read the description. Briefly describe the impact if a threat actor does a disk wipe?

If a threat actor performs a disk wipe, the impact can be severe. This action involves erasing or corrupting raw disk data on targeted systems, resulting in the complete loss of data stored on those disks. Such an attack disrupts the availability of critical system and network resources, rendering affected devices inoperable and potentially leading to significant downtime for organizations.

Moreover, the malware used for disk wiping may possess worm-like capabilities, allowing it to spread across a network. This means that, once initiated, the attack could propagate to other systems, further amplifying the damage and complicating recovery efforts. Overall, a disk wipe not only results in data loss but also significantly hampers organizational operations and may incur substantial costs related to data recovery, system restoration, and operational downtime.

Answers will vary. Adversaries may wipe or corrupt raw disk data on specific systems to interrupt availability to system and network resources Malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques.

Show Answer Hide Answer

What could you do to mitigate this technique?

To mitigate the Disk Wipe technique, consider implementing the following strategies:

1. Disaster Recovery Plan:

Develop and maintain a comprehensive IT disaster recovery plan that outlines procedures for regular data backups. This ensures that critical organizational data can be restored in the event of a disk wipe or other data loss incidents.

2. Regular Backups:

Schedule regular backups of important data and system configurations. Use automated backup solutions to minimize the risk of human error and ensure that backups are consistently performed.

3. Offsite Storage:

Store backups in offsite locations or utilize cloud-based storage solutions to protect data from local attacks. This helps ensure that even if on-premises systems are compromised, backups remain intact and accessible for recovery.

4. Access Controls:

Implement strict access controls and authentication measures for backup systems. Limit access to authorized personnel only, reducing the risk of adversaries gaining access to backups and destroying them.

5. Backup Encryption:

Encrypt backup data to protect it from unauthorized access. Even if adversaries manage to access backup files, encryption can prevent them from being usable.

6. Regular Testing:

Periodically test backup and recovery procedures to ensure they work effectively. Conducting drills helps identify weaknesses in the disaster recovery plan and ensures that staff are familiar with the process.

7. Monitoring and Alerts:

Use monitoring tools to detect suspicious activities that could indicate a disk wipe attempt. Set up alerts for unusual file deletions or modifications, allowing for timely intervention.

Implement an IT disaster recovery plan that contain procedures for taking regular data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.

Show Answer Hide Answer

Part 3: Investigate Potential Malware

There are a number of tools that a cybersecurity analyst can use to validate malicious software. In this part, you will investigate an IPS alert to see if it is malicious software.

Step 1: Generate a SHA256 hash for a suspicious file.

As a Tier 1 Cybersecurity Analysts, you have access to a Security Information Event Management (SIEM) system on your Linux management station. The SIEM just sent you an IPS alert referencing a local IP address of 10.8.19.101. You decide to examine the actual traffic identified in the alert by pivoting to Wireshark.

a. As you scroll through the various packet captures of IP address 10.8.19.101, you notice that a file was downloaded by the host as shown in the figure.