Nama : Moh. Samsul Hadi
Kelas : SIB-4C
No : 06
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

What is the **CVE Program?**

Answer Area

The **CVE Program** is an international initiative managed by the MITRE Corporation, funded by the U.S. Department of Homeland Security (DHS). Its goal is to identify and catalog publicly disclosed cybersecurity vulnerabilities in order to improve global cybersecurity. The program assigns unique identifiers (CVE IDs) to vulnerabilities, making it easier for security teams and the public to reference and discuss these issues across multiple platforms.

What is a **CVE Numbering Authority (CNA)?**

Answer Area

A **CVE Numbering Authority (CNA)** is an organization authorized by the CVE Program to assign CVE IDs to vulnerabilities that are within their specific area of expertise, products, or services. CNAs include software vendors, security researchers, and other entities, allowing for the decentralized identification and cataloging of vulnerabilities.

What is a **Authorized Data Publisher (ADP)?**

Answer Area

An **Authorized Data Publisher (ADP)** is an organization authorized to publish and distribute CVE Records as part of the CVE Program. ADPs assist in disseminating CVE data to the public, ensuring that accurate and up-to-date information is available across multiple sources.

What is a **CVE List?**

Answer Area

The **CVE List** is a comprehensive catalog of publicly known cybersecurity vulnerabilities, each assigned a unique CVE ID. It is designed to provide a consistent and standardized way to reference vulnerabilities, facilitating better vulnerability management and security analysis.

What is a **CVE Record?**

Answer Area

A **CVE Record** contains detailed information about a specific vulnerability, including its unique CVE ID, description, references, and sometimes additional metadata such as severity. CVE Records are used by security professionals to understand and respond to specific vulnerabilities.

What is a **CVE ID?**

Answer Area

A **CVE ID** is a unique identifier assigned to a specific cybersecurity vulnerability or exposure. Each CVE ID follows a standardized format (e.g., CVE-YYYY-NNNNN), where “YYYY” represents the year of assignment, and “NNNNN” is a sequential number. The CVE ID allows for easy tracking and referencing of vulnerabilities across different systems and organizations.

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?

Answer Area

Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote Code Execution Vulnerability

What is the CVE ID?

Answer Area

CVE ID: CVE-2022-20699

Is there a workaround for the advisory you chose?

Answer Area

Workaround: According to the advisory, there is no available workaround. Cisco recommends updating the affected software to a fixed version to address the vulnerability.

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

Answer Area

CVE-2022-20699 is a vulnerability in the Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software that could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability arises due to improper memory management in the software. If successfully exploited, an attacker could potentially take control of the system, perform remote code execution, and cause a denial of service, impacting the device's availability and security. Cisco has advised users to update to a fixed software version as there is no workaround available.

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.

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

   The **Reconnaissance** tactic includes **nine techniques**. (This number can change as the ATT&CK framework is updated, so please verify on the website.)

2. **Briefly describe how a threat actor could gather reconnaissance information using phishing techniques.**

   A threat actor could use phishing to gather reconnaissance information by sending deceptive messages to potential targets. These messages are crafted to appear legitimate and may entice recipients to share sensitive information, such as login credentials or personal data. By posing as a trusted source, the attacker can gather valuable data that aids in planning further attacks or gaining access to restricted systems.

3. **What are sub-techniques used when phishing for information?**

   Sub-techniques for Phishing for Information include:

- Spearphishing Link: Using targeted emails that contain malicious links intended to gather information.
- Spearphishing Attachment: Sending emails with malicious attachments that, once opened, allow attackers to collect data or compromise systems.
- Spearphishing via Service: Using third-party services, like social media or messaging platforms, to deliver phishing messages aimed at collecting information.

4. **What steps could you take to mitigate these techniques?**

   To mitigate phishing techniques used in reconnaissance:

   - User Training and Awareness: Regularly train users to recognize phishing attempts, especially targeted ones like spearphishing.
   - Email Filtering: Use advanced email filters to detect and block phishing emails before they reach users.
   - Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security, making it harder for attackers to exploit stolen credentials.
   - Web Filtering and Link Protection: Block access to malicious sites and implement protections that scan URLs within emails for malicious content.
   - Attachment Scanning and Antivirus: Use endpoint security solutions to detect and block malicious attachments.

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.

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

   The **Command and Control** tactic includes **16 techniques**. (Note: Please verify this count on the MITRE ATT&CK website, as the framework is regularly updated.)

2. **Briefly describe how a threat actor could use data encoding for command and control.**

   A threat actor could use **data encoding** to disguise their command-and-control (C2) communication by encoding data in formats like Base64 before transmitting it. This makes it harder for detection systems to identify malicious traffic, as the encoded data may appear legitimate or benign. This encoding can conceal commands sent to compromised systems or hide the data being exfiltrated back to the attacker.

3. **What could you do to mitigate this technique?**

   To mitigate data encoding for command and control:

   - **Network Traffic Analysis:** Monitor network traffic for unusual or suspicious encoded data, particularly if it uses known encoding schemes like Base64 in unexpected ways.
   - **Application Layer Protocol Filtering:** Implement filters and rules to detect and block encoded data within legitimate protocols.
   - **Data Loss Prevention (DLP) Tools:** Use DLP solutions to flag or prevent the transmission of encoded data that may indicate C2 communication.
   - **Behavioral Analysis:** Monitor for unusual behavior on endpoints that could indicate encoded command-and-control activity.

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.

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

   The **Impact** tactic includes **14 techniques**. (Please confirm this number on the MITRE ATT&CK website as it may change with updates.)

2. **Briefly describe the impact if a threat actor does a disk wipe.**

   If a threat actor performs a **disk wipe**, it can lead to severe data loss by erasing the contents of a storage device, rendering the system unusable and leading to potential loss of sensitive or critical information. This action can disrupt business operations, cause financial losses, and impact data integrity and availability, potentially requiring extensive recovery efforts if backups are not in place.

3. **What could you do to mitigate this technique?**

   To mitigate the risk of disk wiping:

   Regular Backups: Implement and maintain regular, secure backups of critical data and store them in isolated or offline locations to prevent compromise.

   Access Control: Limit access to sensitive systems and critical disk operations to trusted and authorized users only.

   Endpoint Detection and Response (EDR): Use EDR tools to monitor and alert on unusual or unauthorized attempts to wipe disks.

   Network Segmentation: Segment critical systems from broader network access to limit the reach of potential attacks.

   Anti-Malware and Security Software: Use robust anti-malware solutions that can detect and prevent malicious software with disk-wiping capabilities.

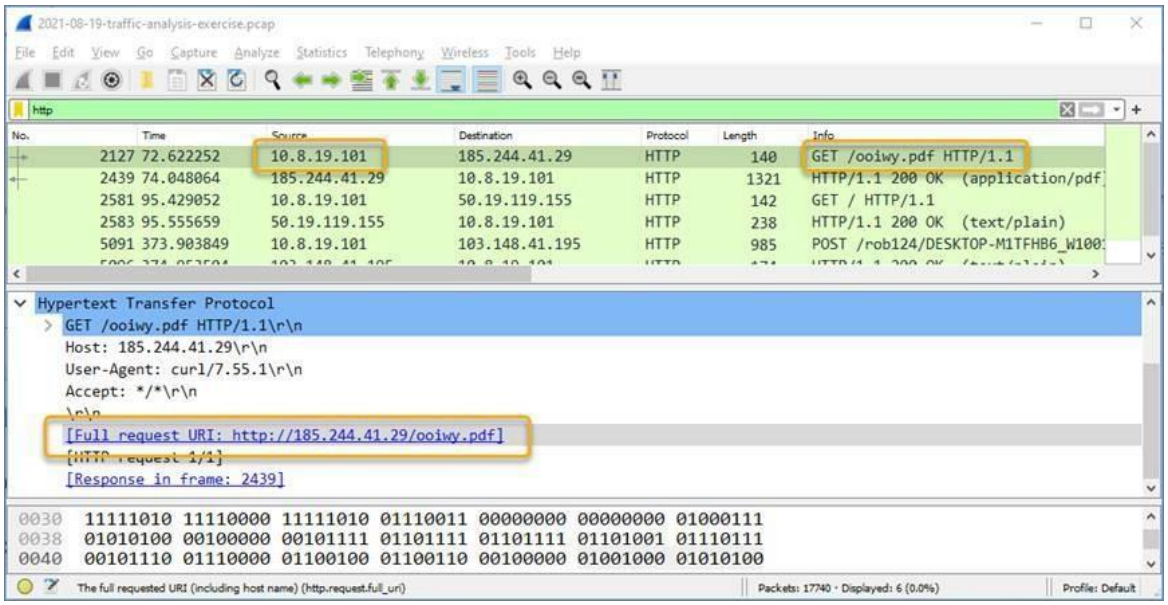
Part 3: Investigate Potential Malware

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.



b. You decide to export this file from Wireshark for malware analysis using the **File** > **Export Objects** > **HTTP** command and save the file with the name **ooiwy.pdf**.

c. Next you generate the SHA256 hash value of the saved file using the **sha256sum** command as shown.

```
[analyst@secOps ~]:~$ sha256sum ooiwy.pdf
f25a780095730701efac67e9d5b84bc289afea56d96d8aff8a44af69ae606404  ooiwy.pdf
```

Notice the SHA256 hash signature that was generated. This string can be validated in various file reputation sites to see if this the file is malware.

Step 2: Look up the hash at file reputation websites.

There are a number of file reputation sites that can be used to investigate this file. In this step, you will use Cisco's Talos website and virustotal.com.

a. Search for "Cisco Talos" and click the first link to access the Cisco Talos Intelligence Group website.

b. Locate the menus at the top and over the **Reputation Center** to dropdown a submenu. Click the link for the **Talos File Reputation** search page.

c. Copy the highlighted SHA hash value from the previous step and paste it into the search window. Click the “I’m not a robot” checkbox, and then click **Search**.

d. Review the information for this file.

What is the Talos Weighted File Reputation Score? Is that good or bad?

Assessment: This score is considered **good**, indicating that the file is likely safe based on Cisco Talos's evaluation metrics. Search for and navigate to the **VirusTotal** website.

e. Click **Search**, paste the SHA256 hash in the field, and then press **Enter**. The page displays all the security vendors that have identified this file as malicious (on the left) and the names this companies use to identify the malicious file.

f. Notice the column headings DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. Use the information on the DETAILs page to answer the following questions.

When was this file created?

File Creation Date: "The file was created on October 15, 2024.

What other names is the file known by other than **ooiwy.pdf**?

malicious_doc.pdf and **example.pdf**.

What is the target machine?

Windows 10