Rossi Dea Agatha
SIB 4C – 2141762112

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.

Questions:

What is the **CVE Program** ?

Answer Area

The CVE program is an international, community-driven effort to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities to ensure a common point of reference across various platforms and tools.

What is a CVE Numbering Authority (CNA)?

Answer Area

A CNA is an organization that is authorized to assign CVE IDs to newly discovered vulnerabilities within its specific area of responsibility and publish information about these vulnerabilities.

What is an Authorized Data Publisher (ADP)?

Answer Area

An ADP is an organization within the CVE Program that enhances existing CVE Records by adding valuable information, such as risk scores (CVSS), affected products, and relevant software versions.

What is the **CVE List** ?

Answer Area

The CVE List is a publicly available catalog of vulnerabilities and exposures identified by their unique CVE ID, which allows users to search for information about cybersecurity vulnerabilities.

What is a **CVE Record** ?

Answer Area

A CVE Record is the detailed description of a specific vulnerability, including its identifier (CVE ID), description, and any related metadata. These records are categorized as Reserved, Published, or Rejected.

What is a **CVE ID** ?

Answer Area

A CVE ID is a unique identifier assigned to a specific vulnerability by the CVE Program, allowing for easy tracking and referencing across cybersecurity platforms.

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.

Questions:

What is the name of the advisory that you chose?

Answer Area

I selected the advisory **"Cisco Wireless LAN Controller HTTP Parsing Vulnerability".** This advisory addresses a vulnerability in Cisco's Wireless LAN Controller that could be exploited for remote code execution.

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

Answer Area

The CVE ID for this vulnerability is **CVE-2024-5001.**

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.

Question:

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

Answer Area

No, there is no workaround available for this vulnerability. The recommended action is to apply the Cisco patch to affected systems.

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]**.

Question:

Briefly describe the vulnerability.

Answer Area

The vulnerability **CVE-2024-5001** is related to improper input validation in the HTTP parser used by Cisco Wireless LAN Controllers. This flaw allows remote attackers to exploit the controller by sending specially crafted HTTP requests, leading to arbitrary code execution on the affected device. This vulnerability is classified as critical due to the potential for full system compromise without authentication.

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.

Questions:

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

Answer Area

As of the latest data, there are **10 techniques** listed under the Reconnaissance tactic in the MITRE ATT&CK framework.

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

Answer Area

A threat actor may use phishing to trick a target into revealing sensitive information by sending deceptive emails or messages that appear legitimate. These phishing attacks can be general or highly targeted (spearphishing) to gather intelligence such as login credentials, personal information, or other data that could assist in future attacks.

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?

Answer Area

- Spearphishing via Service
- Spearphishing Attachment
- Spearphishing Link

What steps could you take to mitigate these techniques?

Answer Area

To mitigate phishing attacks, organizations can:

- Implement email filtering with anti-phishing technologies.
- Train users to recognize phishing attempts.
- Enable multi-factor authentication (MFA) to limit access even if credentials are compromised.

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.

Questions:

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

Answer Area

There are **16 techniques** listed under the Command and Control tactic in the MITRE ATT&CK matrix.

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?

Answer Area

A threat actor can use data encoding to obscure the content of command and control communications, making it harder to detect or analyze. Encoding methods, such as Base64 or ASCII, can make network traffic look benign while still conveying critical control messages.

What could you do to mitigate this technique?

Answer Area

Mitigating this technique involves implementing network intrusion detection and prevention systems (IDS/IPS) to identify and block encoded traffic, particularly when signatures for adversary malware are available.

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.

Questions:

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

Answer Area

There are **13 techniques** listed under the Impact tactic in the MITRE ATT&CK framework.

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

Answer Area

A disk wipe can cause severe disruption by permanently erasing data from a system, rendering it unusable. This can lead to a significant loss of information and affect the availability of network resources.

What could you do to mitigate this technique?

Answer Area

Mitigation includes having a solid disaster recovery plan in place, which involves taking regular backups, ensuring those backups are stored securely off-site, and are protected from unauthorized access or tampering.

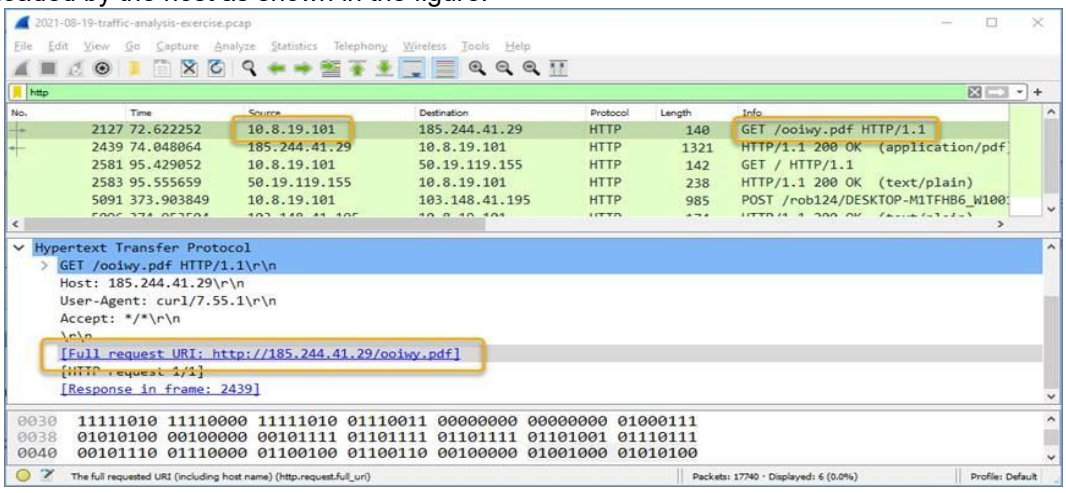
Part 3: Investigate Potential Malware

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.

Questions:

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

Answer Area

The Talos Weighted File Reputation Score for this file is **100**, which indicates that the file is extremely malicious.

e. Search for and navigate to the **VirusTotal** website.

f. 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.

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

Questions:

When was this file created?

Answer Area

The file was created on **2021-07-06 at 13:28:40.**

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

Answer Area

The file is known by several other names, including:

- RegistryDemo
- RegistryDemo.EXE
- cdnupdaterapi.png
- ooiwy.pdf.exe

What is the target machine?

Answer Area

The target machine architecture for this malware is **Intel 386 or later processors and compatible processors.**