Nama : Sasmita Rachmawati

Absen : 15

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**?

- **The CVE (Common Vulnerabilities and Exposures) program aims to provide a consistent and standardized reference for vulnerabilities found in software. It helps security professionals share information and understand the risks associated with these vulnerabilities.**

What is a CVE Numbering Authority (CNA)?

- **A CVE Numbering Authority (CNA) is an organization that plays a key role in the CVE program. It is responsible for assigning unique identifiers, known as CVE IDs, to vulnerabilities in software and systems. Each CNA focuses on specific areas or types of vulnerabilities, which helps them manage and publish detailed information about these vulnerabilities effectively.**

What is an Authorized Data Publisher (ADP)?

- **An Authorized Data Publisher (ADP) is a group or organization that works within the CVE Program. Their main job is to enhance the information provided in a CVE Record that a CNA has already published. This includes adding more detailed information, such as risk scores (like those from the Common Vulnerability Scoring System, or CVSS), and lists of affected products and their versions.**

What is the **CVE List**?

- **The CVE List is essentially a searchable database that contains all the CVE Records. This list includes vulnerabilities that have been identified or reported to the CVE Program. Security professionals can use the CVE List to find specific vulnerabilities, making it easier to track and address potential security issues across different software and systems.**

What is a **CVE Record**?

- **A CVE Record contains detailed descriptive information about a specific vulnerability linked to a CVE ID. This data is provided by a CNA and can be further enriched by ADPs. The CVE Record includes essential details about the vulnerability, such as its nature, the systems it affects, and potential risks. The information in a CVE Record is available in formats that can be easily understood by humans and also processed by machines. Each CVE Record can have one of three statuses:**
  - **Reserved (set aside for future publication)**
  - **Published (made public and available)**
  - **Rejected (not included in the CVE List for various reasons)**

What is a **CVE ID**?

- **A CVE ID is a unique alphanumeric code assigned by the CVE Program to identify a specific vulnerability. This identifier is crucial because it allows security experts and organizations to discuss, share, and connect information about that vulnerability efficiently.**

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?

- **The name of the advisory is: "Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability." This title indicates that it addresses significant vulnerabilities found in specific models of Cisco routers.**

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

- **The CVE ID for this advisory is:** CVE-2021-34730. **This unique identifier helps categorize the vulnerability, making it easier to track and reference.**

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?

- **There is no official workaround available for this 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]**.

Question:

Briefly describe the vulnerability.

- **The vulnerability described by CVE-2021-34730 involves a flaw in the Universal Plug-and-Play (UPnP) service of the affected Cisco Small Business Routers. This flaw could potentially allow an unauthenticated remote attacker to create a denial of service (DoS) condition, meaning they could disrupt the normal functioning of the routers, making them unavailable to legitimate users.**

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?

- **At the time of this writing, there were 10 techniques attributed to the Reconnaissance tactic. These techniques represent various methods attackers might use to gather information about their targets before launching an attack.**

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

- **Threat actors may employ phishing techniques by sending deceptive messages designed to extract sensitive information from individuals. These phishing messages are a form of social engineering delivered electronically, where attackers might specifically target individuals or organizations—this targeted approach is known as spear phishing.**

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 include:

- **Spearphishing Service: Targeting specific services or platforms to extract information.**
- **Spearphishing Attachment: Sending malicious attachments that, when opened, can compromise systems.**

- **Spearphishing Link: Directing victims to fraudulent websites that capture sensitive data.**

What steps could you take to mitigate these techniques?

To mitigate these phishing techniques, organizations can implement:

- **Software Configuration: Utilizing anti-spoofing measures and email authentication to filter out harmful messages.**
- **User Training: Educating employees about social engineering tactics and how to recognize phishing attempts.**

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?

- **At the time of this writing, there were 16 techniques associated with the Command and Control tactic. These techniques describe how attackers maintain communication with compromised systems.**

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?

- **Threat actors may use data encoding to obscure the content of their command and control (C2) communications, making it harder for security systems to detect malicious activity. They can employ standard encoding methods like ASCII, Unicode, or Base64, along with data compression techniques, to mask their traffic.**

What could you do to mitigate this technique?

To mitigate this data encoding technique, organizations should use:

- **Network Intrusion Detection and Prevention Systems (IDS/IPS): These systems can apply network signatures or rules to identify and block traffic that matches known patterns of adversary malware.**

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?

- **At the time of this writing, there were 13 techniques related to the Impact tactic. These techniques outline how attackers can affect the availability, integrity, or confidentiality of systems.**

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, it could lead to significant data loss. They may corrupt or erase essential disk data on targeted systems, causing interruptions in access to critical resources. Malware designed to wipe disks may propagate across networks, leveraging various techniques to maximize its impact.**

What could you do to mitigate this technique?

To mitigate the threat of disk wiping, organizations should:

- **Implement an IT Disaster Recovery Plan: This plan should include regular data backups that can be used for recovery.**
- **Protect Backups: Ensure that backups are stored securely and are shielded from methods that attackers might use to access and destroy them.**

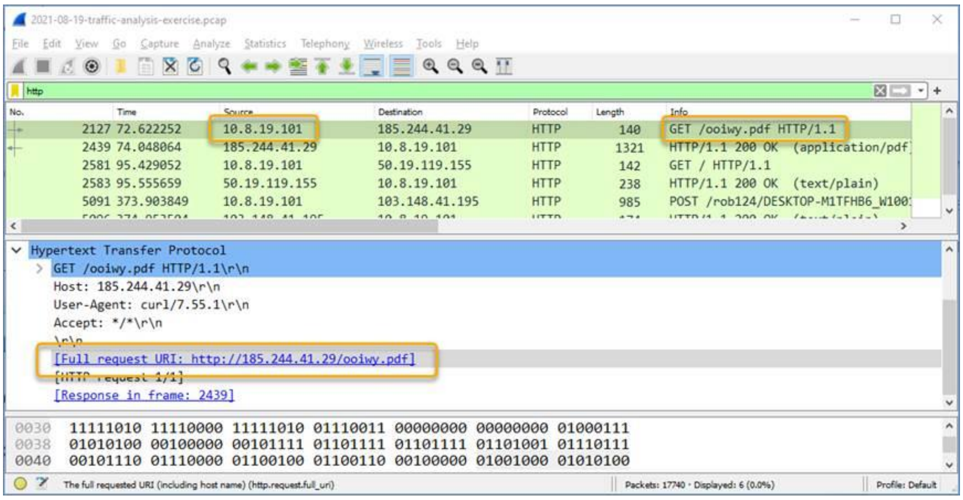
Part 3: Investigate Potential Malware

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.


2021-08-19-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
2127	72.622252	10.8.19.101	185.244.41.29	HTTP	140	GET /ooiwy.pdf HTTP/1.1
2439	74.048064	185.244.41.29	10.8.19.101	HTTP	1321	HTTP/1.1 200 OK (application/pdf
2581	95.429052	10.8.19.101	50.19.119.155	HTTP	142	GET / HTTP/1.1
2583	95.555659	50.19.119.155	10.8.19.101	HTTP	238	HTTP/1.1 200 OK (text/plain)
5091	373.903849	10.8.19.101	103.148.41.195	HTTP	985	POST /rob124/DESKTOP-M1TFHB6_W100

```
Hypertext Transfer Protocol
  > GET /ooiwy.pdf HTTP/1.1\r\n
    Host: 185.244.41.29\r\n
    User-Agent: curl/7.55.1\r\n
    Accept: */*\r\n
    \r\n
    [Full request URI: http://185.244.41.29/ooiwy.pdf]
    [HTTP request 1/1]
    [Response in frame: 2439]
```

```
0030  11111010 11110000 11111010 01110011 00000000 00000000 01000111
0038  01010100 00100000 00101111 01101111 01101111 01101001 01110111
0040  00101110 01110000 01100100 01100110 00100000 01001000 01010100
```

The full requested URI (including host name) (http.request.full_uri) | Packets: 17740 · Displayed: 6 (0.0%) | Profile: Default

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?

- **Look for the Talos Weighted File Reputation Score. This score ranges from 1 to 100, where a higher score indicates a more dangerous file. For instance, if the score is 100, it signifies that the file is deemed 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?

- **The file was created on 2021-07-06 at 13:28:40. This timestamp can help determine how recent the threat might be.**

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

- **The file has several aliases, including RegistryDemo, RegistryDemo.EXE, cdnupdaterapi.png, and ooiwy.pdf.exe. This information can be crucial as it may reveal more about the file's behavior or origins.**

What is the target machine?

- **The file is targeted towards Intel 386 or later processors and compatible processors. Understanding the target architecture can help in assessing the potential impact of the malware.**