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**?

Answer:

The CVE Program is an international, community-driven effort to catalog publicly disclosed cybersecurity vulnerabilities. It aims to identify, define, and catalog vulnerabilities according to established rules and guidelines, making it easier for organizations to communicate about specific security issues.

What is a CVE Numbering Authority (CNA)?

Answer:

A CNA is an organization authorized to assign CVE IDs to newly discovered vulnerabilities and create CVE Records. CNAs are responsible for the regular assignment of CVE IDs within a defined scope, which includes identifying and publishing information about the vulnerability.

What is an Authorized Data Publisher (ADP)?

Answer:

An ADP is an organization authorized to add more detailed information to existing CVE Records, such as risk scores like the Common Vulnerability Scoring System (CVSS), affected product lists, and versions. ADPs enhance the information provided by CNAs.

What is the **CVE List**?

Answer:

The CVE List is a searchable, comprehensive catalog of CVE Records that have been identified by the CVE Program. It serves as a central reference point for vulnerabilities and exposures across different software and systems.

What is a **CVE Record**?

Answer:

A CVE Record contains detailed information about a specific vulnerability, including its description, impact, and affected systems. It is provided by a CNA and can be enriched by ADPs. A CVE Record can be in one of three states: Reserved (CVE ID has been assigned but not yet published), Published (CVE Record is available), or Rejected (CVE ID was assigned but later deemed not a valid vulnerability).

What is a **CVE ID**?

Answer:

A CVE ID is a unique, alphanumeric identifier assigned to a specific vulnerability. It allows security professionals and organizations to reference the same vulnerability and share data consistently. The CVE ID ensures that everyone discussing the vulnerability refers to the same issue.

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:

Use your browser to search for “Cisco Security Advisories” and open the link to the Cisco security page (typically tools.cisco.com).

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

Answer:

- On the advisories page, find the "Impact" column.
- Click the down arrow, uncheck all options except for "Critical," and click "Done."

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?

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:

- What is the name of the advisory that you chose?

  Answer: (Example) "Cisco RV340 Series Routers Command Injection Vulnerability"

- What is the CVE ID?

  Answer: (Example) CVE-2022-20827

- Is there a workaround for the advisory you chose?

  Answer: After reviewing the advisory details, if there is no suggested workaround, you can state:

  Answer: "No workaround is 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.

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

Answer:

At the time of writing, there are 10 techniques under the Reconnaissance tactic.

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

Answer:

Adversaries may use phishing to gather reconnaissance information by sending deceptive messages to trick individuals into providing sensitive information. This information can then be used for further attacks. Phishing includes social engineering techniques, and when it is targeted at specific individuals or organizations, it is called spearphishing.

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: The sub-techniques are:

- Spearphishing Service
- Spearphishing Attachment
- Spearphishing Link

What steps could you take to mitigate these techniques?

Answer: Mitigation techniques include:

- Configuring software with anti-spoofing measures and email authentication methods (e.g., SPF, DKIM, DMARC) to filter out phishing emails.
- Providing user training to help individuals recognize social engineering attacks and avoid interacting with suspicious messages.

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?

Answer:

There are 16 techniques attributed to the Command and Control tactic at the time of this writing.

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:

Threat actors may use data encoding to obscure the content of command and control (C2) traffic, making it more difficult to detect. They can encode data using standard encoding systems (e.g., ASCII, Unicode, Base64, MIME) or compression techniques (e.g., gzip) to evade security detection mechanisms.

What could you do to mitigate this technique?

Answer:

Mitigating this technique can involve using network intrusion detection and prevention systems (IDS/IPS) that employ network signatures or rules to identify suspicious traffic patterns, including those associated with specific adversary malware. These systems can be configured to detect encoded traffic indicative of malicious 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.

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

Answer:

There are 13 techniques attributed to the Impact tactic at the time of this writing.

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

Answer:

A disk wipe can result in the loss or corruption of raw data on a system's disk, rendering the system or its network resources unavailable. The attack may prevent the recovery of important information, disrupt operations, and may propagate across the network, affecting multiple systems.

What could you do to mitigate this technique?

Answer:

Mitigation strategies include implementing an IT disaster recovery plan that involves regular backups of important data. These backups should be stored offline or in a separate, protected environment to prevent adversaries from accessing and destroying the backup data. Furthermore, access controls and monitoring should be in place to safeguard the integrity of the backup system.

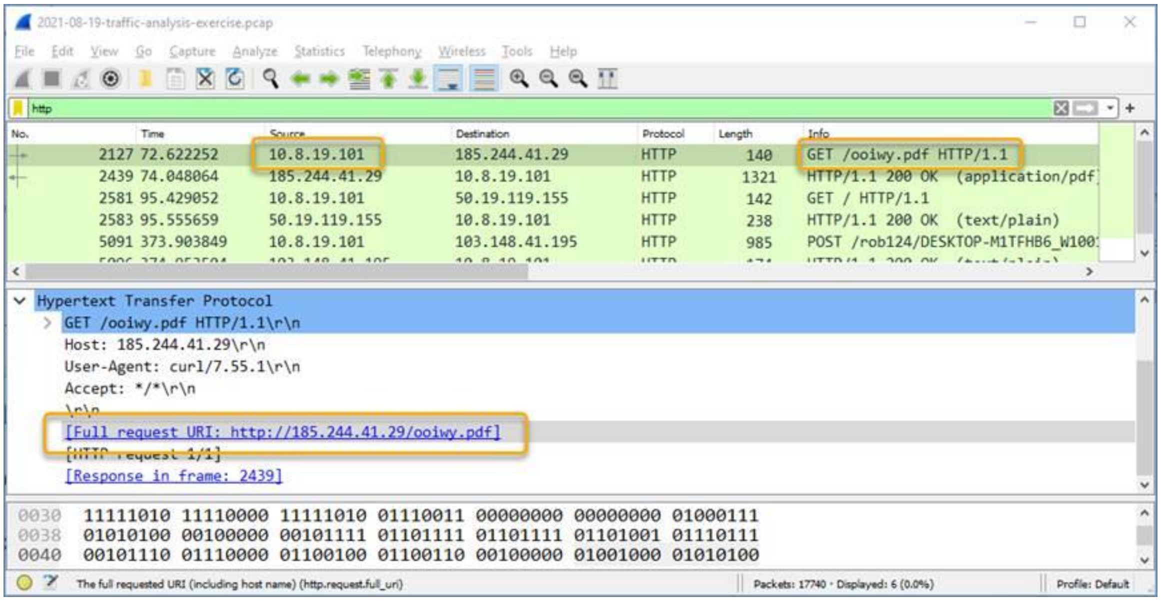
Part 3: Investigate Potential Malware

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.

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

Answer: The Talos File Reputation Score is **100**, which indicates that the file is **extremely malicious**. This score is on a scale from 1 to 100, where 100 represents the highest level of maliciousness.

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.

When was this file created?

Answer:

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

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

Answer: The file is also known by the following names:

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

What is the target machine?

Answer: The target machine is specified as **Intel 386 or later processors and compatible processors**.