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.

****TASK 1****

Step 1: Research the CVE website.

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

****QUESTION 1****

What is the CVE Program?

****ANSWER****

The CVE (Common Vulnerabilities and Exposures) Program is an international initiative sponsored by the U.S. Department of Homeland Security and managed by MITRE. It identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities. The goal is to make it easier to share data across separate vulnerability databases and security tools using a common identifier.

QUESTION 2

What is a CVE Numbering Authority (CNA)?

ANSWER

A CVE Numbering Authority (CNA) is an organization authorized by the CVE Program to assign CVE IDs to vulnerabilities affecting products within its scope. CNAs are typically software vendors, research organizations, or coordination centers that follow CVE guidelines for assigning and publishing vulnerability information.

QUESTION 3

What is an Authorized Data Publisher (ADP)?

ANSWER

An Authorized Data Publisher (ADP) is an organization authorized by the CVE Program to publish CVE Records to the official CVE List. ADPs are responsible for formatting and uploading detailed CVE information in a standardized and consistent way.

QUESTION 4

What is the CVE List?

ANSWER

The CVE List is a publicly available, comprehensive list of all CVE Records that have been assigned and published. Each entry includes a unique CVE ID and basic information about the vulnerability. It serves as a reference point for cybersecurity professionals and tools worldwide.

QUESTION 5

What is a CVE Record?

ANSWER

A CVE Record is a published entry in the CVE List that provides a unique CVE ID, a brief description of a vulnerability, and references to related advisories, patches, and technical details. It helps standardize how information about vulnerabilities is shared across the industry.

QUESTION 6

What is a CVE ID?

ANSWER

A CVE ID (Identifier) is a unique identifier assigned to a specific publicly known cybersecurity vulnerability. It follows a standardized format, such as CVE-2025-12345, and is used to ensure consistent tracking and discussion of that vulnerability across various platforms and tools.

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.

****QUESTION 7****

What is the name of the advisory that you chose?

****ANSWER****

Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities

****QUESTION 8****

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

****ANSWER****

CVE-2025-20281, CVE-2025-20337

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 9****

Is there a workaround for the advisory you chose?

****ANSWER****

There are no workarounds that address these vulnerabilities.

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 10****

Briefly describe the vulnerability.

****ANSWER****

A vulnerability in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.

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.

****TASK 2****

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.

****QUESTION 1****

How many techniques are attributed to the Reconnaissance tactic?

****ANSWER****

10 techniques are attributed.

****QUESTION 2****

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 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 spear phishing. In spear phishing, a specific individual, company, or industry will be targeted by the adversary. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means

****QUESTION 3****

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****

Spear phishing Service, Spear phishing Attachment, Spear Phishing Link, Spear Phishing Voice

****QUESTION 4****

What steps could you take to mitigate these techniques?

****ANSWER****

Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation.

Users can be trained to identify social engineering techniques and spear 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.

****QUESTION 5****

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

****ANSWER****

18 techniques are attributed.

****QUESTION 6****

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****

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems. Some data encoding systems may also result in data compression, such as gzip.

****QUESTION 7****

What could you do to mitigate this technique?

****ANSWER****

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

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.

****QUESTION 8****

How many techniques are attributed to the Impact tactic?

****ANSWER**** 15 techniques are attributed.

****QUESTION 9****

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

****ANSWER****

Adversaries may wipe or corrupt raw disk data on specific systems or in large numbers in a network to interrupt availability to system and network resources. Malware used for wiping disks may have worm-like features to propagate across a network.

****QUESTION 10****

What could you do to mitigate this technique?

****ANSWER****

Consider implementing IT disaster recovery plans 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.

Part 3: Investigate Potential Malware

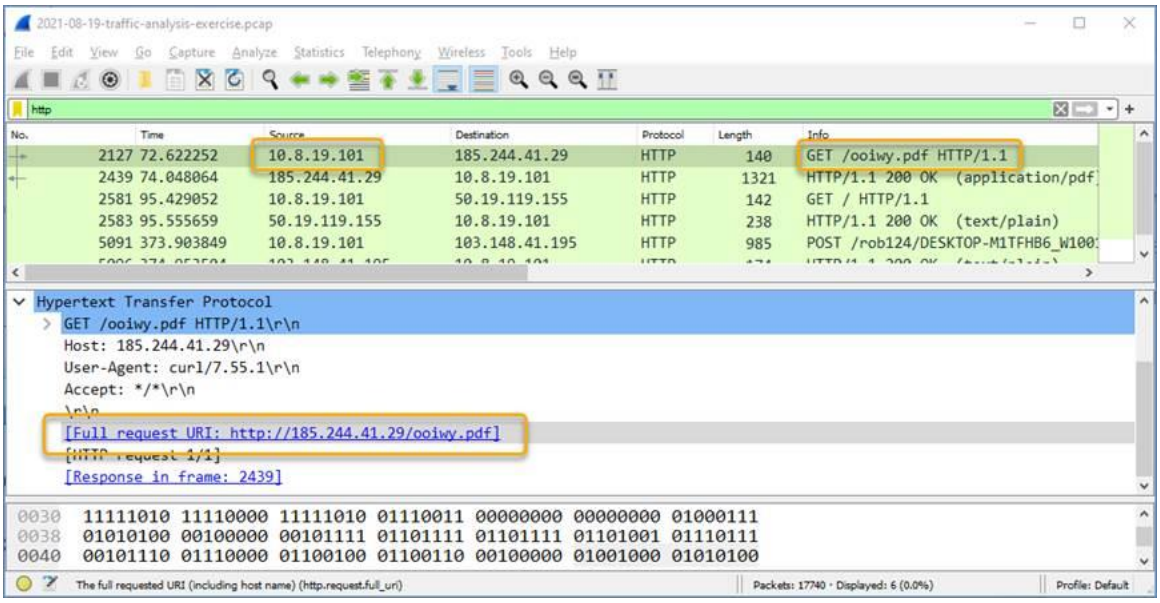
There are a number of tools that a cybersecurity analyst can use to validate malicious software. In this part, you will investigate an IPS alert to see if it is malicious software.

TASK 3

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.

****QUESTION 1****

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

****ANSWER****

The file score is 100 which identifies this file as 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.

****QUESTION 2****

When was this file created?

****ANSWER****

2021-07-06 13:28:40

****QUESTION 3****

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

****ANSWER****

RegistryDemo.EXE, RegistryDemo, ooiwy.NOpdf, ooiwy.pdf.defang

****QUESTION 4****

What is the target machine?

****ANSWER****

Intel 386 or later processors and compatible processors.