

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 catalog vulnerabilities in accordance with the effort's rules and guidelines.



Show Answer

What is a CVE Numbering Authority (CNA)?

Answer Area

A CNA (CVE Numbering Authority) is an entity tasked with assigning CVE IDs to vulnerabilities on a regular basis and providing detailed information about the vulnerabilities in the corresponding CVE Record. Each CNA operates within a defined scope, focusing on identifying and publishing vulnerabilities within its area of responsibility.



Show Answer

What is an Authorized Data Publisher (ADP)?

Answer Area

ADP is an organization authorized within the CVE Program to enrich previously published CVE Records by a CNA with additional related information, including risk scores (e.g., Common Vulnerability Scoring System (CVSS)), a list of affected products, and their versions.



Show Answer

What is the **CVE List**?

Answer Area

The CVE List is a searchable catalog of all CVE Records that have been identified by, or reported to, the CVE Program.



Show Answer

What is a **CVE Record**?

Answer Area

A CVE Record contains detailed information about a vulnerability linked to a specific CVE ID, provided by a CNA and enhanced by ADPs. This information is available in various human- and machine-readable formats. Each CVE Record falls under one of three statuses: Reserved, Published, or Rejected.



Show Answer

What is a **CVE ID**?

Answer Area

A CVE ID is a unique alphanumeric identifier assigned by the CVE Program. Each identifier refers to a specific vulnerability. The CVE ID enables automation and allows multiple parties to discuss, share, and link information about a particular vulnerability, ensuring they are referring to the same issue.



Show Answer

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

"Cisco Smart Software Manager On-Prem Password Change Vulnerability".

Show Answer

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

Answer Area

"Cisco Smart Software Manager On-Prem Password Change Vulnerability" is CVE-2024-20419.

Show Answer

- 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.

Show Answer

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

CVE-2024-20419 describes a vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users.

Show Answer

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

There are 10 techniques under the Reconnaissance tactic.

Show Answer

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

Adversaries may send phishing messages to obtain sensitive information that can be leveraged for targeting purposes. All types of phishing are forms of electronically delivered social engineering. Phishing can also be specifically focused, known as spearphishing, where a particular individual, company, or industry is singled out by the attacker.

Show Answer

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 Service, Spearphishing Attachment, and Spearphishing Link.

Show Answer

What steps could you take to mitigate these techniques?

Answer Area

Configuring software with anti-spoofing measures and email authentication to filter messages,



Show Answer

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 18 techniques under the Comannd and Control tactic.



Show Answer

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

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. 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.



Show Answer

What could you do to mitigate this technique?

Answer Area

Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool C2 signatures over time or construct protocols in such a way as to avoid detection by common defensive tools.



[Show Answer](#)

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 14 techniques under the Impact tactic.

[Show Answer](#)

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

Answer Area

interrupt availability to system and network resources. With direct write access to a disk, adversaries may

[Show Answer](#)

What could you do to mitigate this technique?

Answer Area

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.

[Show Answer](#)

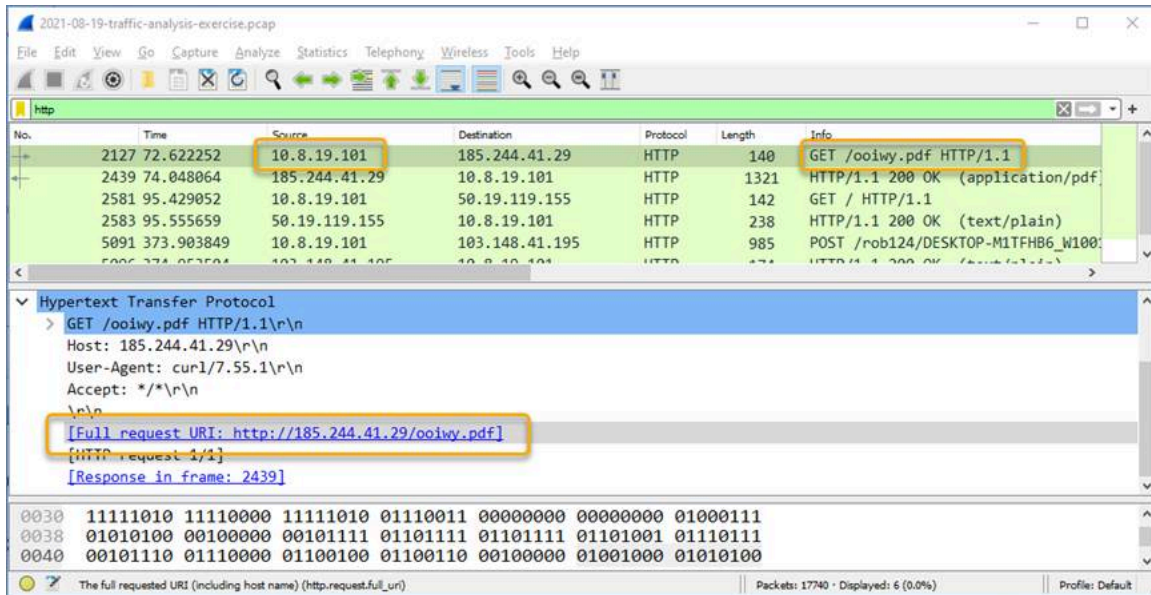
Part 3: Investigate Potential Malware

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.



Blank Line. No additional information

- 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.

- Search for "Cisco Talos" and click the first link to access the Cisco Talos Intelligence Group website.
- 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.
- 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**.
- Review the information for this file.

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

Answer Area

The file score is 100 which identifies this file as extremely malicious.

Show Answer

- 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

Creation Time 2021-07-06 13:28:40.



Show Answer

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

Answer Area

RegistryDemo, RegistryDemo.EXE,
cdnupdaterapi.png, and ooiwy.pdf.exe.



Show Answer

What is the target machine?

Answer Area

Intel 386 or later processors and compatible processors.



Show Answer

End of document

Show All Answers

Clear My Responses