Nama : Yusufa Haidar

Kelas : SIB – 4C

No : 21

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**?

The **CVE Program** (Common Vulnerabilities and Exposures) is a publicly accessible database that provides unique identifiers for publicly known cybersecurity vulnerabilities. It helps organizations share information about vulnerabilities consistently and efficiently, facilitating the tracking and mitigation of security risks across different software and systems. The CVE identifiers serve as a standard reference to ensure all stakeholders have a common understanding of specific vulnerabilities.

The CVE program is an international, community-driven effort to catalog vulnerabilities in accordance with the effortâ€™s rules and guidelines.

What is a CVE Numbering Authority (CNA)?

A **CVE Numbering Authority (CNA)** is an organization authorized to assign CVE IDs for vulnerabilities within its designated scope. CNAs can be part of software vendors, security researchers, or industry groups. Their role is crucial in managing and cataloging vulnerabilities, ensuring that each one receives a unique identifier for tracking and sharing information. This structure helps streamline the reporting and remediation process across the cybersecurity community.

A CNA is an organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific scope of responsibility for vulnerability identification and publishing.

What is an Authorized Data Publisher (ADP)?

An **Authorized Data Publisher (ADP)** is an organization that has received permission to publish CVE data on behalf of a CNA. ADPs help disseminate vulnerability information, enhancing the reach and accessibility of CVE records. They play a vital role in increasing the visibility of vulnerabilities and ensuring that stakeholders can easily access accurate and timely information.

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

What is the **CVE List**?

The **CVE List** is a publicly accessible database that catalogs all CVE identifiers (CVE IDs) assigned to known vulnerabilities in software and systems. Each entry in the list provides a unique identifier, a brief description of the vulnerability, and relevant metadata, making it easier for security professionals to track and address security risks. The CVE List serves as a critical resource for vulnerability management and coordination in the cybersecurity community.

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

What is a **CVE Record**?

A **CVE Record** is an entry in the CVE List that contains detailed information about a specific vulnerability. Each CVE Record includes a unique CVE ID, a description of the vulnerability, its potential impact, references to related information, and sometimes additional metadata. This structured format allows security professionals to understand and address vulnerabilities consistently.

The CVE Record is the descriptive data about a vulnerability associated with a CVE ID, provided by a CNA, and enriched by ADPs. This data is provided in multiple human and machine-readable formats. A CVE Record is associated with one of the following states: Reserved, Published, and Rejected.

What is a **CVE ID**?

A **CVE ID** (Common Vulnerabilities and Exposures Identifier) is a unique alphanumeric code assigned to a specific vulnerability in the CVE system. This identifier facilitates the consistent referencing of vulnerabilities across different platforms and tools, enabling clearer communication among security professionals. CVE IDs typically follow the format "CVE-YYYY-NNNN," where "YYYY" is the year of publication and "NNNN" is a unique sequence number.

A unique, alphanumeric identifier assigned by the CVE Program. Each identifier references a specific vulnerability. A CVE ID enables automation and multiple parties to discuss, share, and correlate information about a specific vulnerability, knowing they are referring to the same thing.

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?

One notable advisory is titled **"Cisco Firepower Management Center Software Command Injection Vulnerability."** This advisory details a vulnerability that allows a cyber threat actor to exploit certain conditions to take control of an affected system

The name is listed in the first column. For example, "Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability"

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

The CVE ID for the advisory I mentioned is **CVE-2024-XXXX**.

The CVE ID is listed in the third column. For example, the CVE ID for " Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Remote Command Execution and Denial of Service Vulnerability" is CVE-2021-34730.

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?

Yes, there is a workaround for the **"Cisco Firepower Management Center Software Command Injection Vulnerability"** advisory (CVE-2024-XXXX). Cisco recommends applying specific configurations to mitigate the risks associated with this vulnerability.

Some common workarounds include:

1. **Restricting access to the management interface** to trusted IP addresses to limit potential exploitation.
2. **Regularly updating software** to the latest version that addresses known vulnerabilities.
3. **Implementing proper firewall rules** to monitor and control incoming traffic to affected systems.

The answer is most likely "No".

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.

The **Cisco Firepower Management Center Software Command Injection Vulnerability** allows an unauthenticated, remote attacker to execute arbitrary commands on the affected system. This vulnerability occurs due to improper validation of user-supplied input, leading to command injection. If exploited, this can enable attackers to gain control over the affected system, which poses significant risks to data integrity and confidentiality.

To mitigate this vulnerability, users are advised to apply available updates and restrict access to management interfaces.

Answers will vary based on the CVE you chose. For example, CVE-2021-34730 describes a vulnerability in the Universal Plug-and-Play (UPnP) service of Cisco Small Business Routers that could allow an unauthenticated, remote attacker to create a denial of service (DoS) condition. Notice that this is the same information you can find in the details for this advisory on the Cisco Security Advisories website.

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?

On the MITRE ATT&CK website, the **Reconnaissance tactic** is associated with **seven techniques**. These techniques detail various methods that threat actors use to gather information about their targets before executing an attack.

Answers may vary, but at the time of this writing there were 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?

Threat actors can gather reconnaissance information using phishing techniques by crafting deceptive communications designed to trick individuals into revealing sensitive information. Here’s a brief overview of how this process typically works:

1. **Deceptive Emails**: Attackers often send emails that appear to be from trusted sources, such as legitimate companies or internal departments. These emails might contain urgent messages, such as a required password reset or a notification about suspicious account activity, prompting users to click on malicious links or provide personal information.
2. **Fake Websites**: When victims click on links in these emails, they are directed to counterfeit websites that closely mimic legitimate sites. Once there, they may be asked to enter credentials, personal identification numbers, or other sensitive information, which the attackers can then collect.
3. **Data Harvesting**: The information gathered through these phishing tactics can be used for various malicious purposes, including account takeover, identity theft, or further targeting of the organization through more sophisticated attacks.
4. **Social Engineering**: Phishing exploits human psychology, leveraging urgency or fear to bypass standard security practices. Attackers might create a sense of urgency or use social engineering tactics to make their requests seem legitimate.

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 spearphishing where a specific individual, company, or industry will be targeted by the adversary.

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?

1. **Spear Phishing**: This technique targets specific individuals or organizations with personalized messages, making it more likely for the recipient to engage with the content. Attackers often use information gathered from social media or public sources to craft convincing emails.
2. **Whaling**: A subset of spear phishing, whaling targets high-profile individuals within an organization, such as executives or senior management. The emails may appear to come from a trusted source, such as another executive or a business partner, and often involve urgent requests.
3. **SMS Phishing (Smishing)**: This technique uses SMS messages to lure victims into providing sensitive information. Similar to email phishing, smishing messages often contain malicious links or ask recipients to call a phone number.
4. **Voice Phishing (Vishing)**: Attackers use phone calls to impersonate legitimate entities, such as banks or technical support. They may try to extract personal information by creating a sense of urgency or fear.

Answers should be Spearphishing Service, Spearphishing Attachment, and Spearphishing Link.

What steps could you take to mitigate these techniques?

To mitigate the risks associated with phishing for information techniques, organizations and individuals can implement several proactive measures:

1. **User Education and Awareness**: Regular training sessions should be conducted to educate employees about the dangers of phishing attacks, including how to identify suspicious emails or messages. Organizations like the Federal Trade Commission (FTC) provide resources on recognizing phishing attempts and safe online practices .
2. **Email Filtering and Anti-Phishing Tools**: Utilizing advanced email filtering solutions can help detect and block phishing attempts before they reach inboxes. These tools can analyze incoming emails for known phishing patterns and malicious links, reducing the chances of human error .

3. **Multi-Factor Authentication (MFA)**: Implementing MFA adds an additional layer of security. Even if credentials are compromised through phishing, the attacker would still need a second form of authentication, such as a one-time code sent to a mobile device .
4. **Regular Software Updates**: Keeping software and security tools up to date is crucial in protecting against vulnerabilities that phishing attacks may exploit. Regular updates help ensure that security measures are equipped to deal with the latest threats .
5. **Incident Response Plan**: Establishing a clear incident response plan allows organizations to react quickly if a phishing attack is successful. This includes steps for containment, investigation, and communication .
6. **Phishing Simulations**: Conducting regular phishing simulation exercises can help assess and improve employee awareness and response to real phishing attempts. These simulations can identify vulnerabilities and reinforce training .

Software configuration using anti-spoofing and email authentication to filter messages and user training to identify social engineering attacks

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?

The Command and Control (C2) tactic in the MITRE ATT&CK framework has a total of **12 techniques** associated with it. These techniques describe various methods adversaries may use to communicate with compromised devices and maintain control over them, including leveraging legitimate protocols and encryption to evade detection

Answers may vary, but at the time of this writing there were 16 techniques available.

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?

In the MITRE ATT&CK framework, **Data Encoding** is a technique under the Command and Control tactic. A threat actor could use **data encoding** to conceal the commands and data they send to or receive from a compromised system. By encoding this information, such as by using Base64 or other encoding schemes, the attacker can make the communication harder to detect or interpret, as it may not be immediately recognizable as malicious. This technique helps evade detection by security systems that monitor for standard malicious payloads or plain-text communications

Threat actors 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 (e.g., ASCII, Unicode, Base64, MIME) and in data compression, (e.g., gzip).

What could you do to mitigate this technique?

To mitigate the **Data Encoding** technique used by threat actors in Command and Control communications, organizations can implement several strategies:

1. **Network Traffic Monitoring**: Regularly monitor network traffic for unusual patterns, especially for encoded data or non-standard protocols. Tools like intrusion detection systems (IDS) can help identify anomalies that may indicate malicious encoding.

2. **Threat Intelligence**: Stay updated with threat intelligence reports and services that provide insights into known encoding techniques used by attackers. This can help in recognizing and blocking suspicious traffic before it affects your systems
3. **Content Filtering**: Implement content filtering policies that can analyze and block traffic that appears to be obfuscated or encoded. This includes filtering out Base64 and other encoding schemes that are commonly used for concealing data.
4. **Endpoint Security**: Deploy robust endpoint security solutions that can analyze the behavior of applications and block suspicious actions that may involve data encoding, such as unusual file access patterns or network calls.
5. **User Education**: Train employees on recognizing phishing attempts and encoded messages that could lead to the installation of malicious software or unintended data sharing .
6. **Incident Response Planning**: Have an incident response plan in place that includes procedures for identifying and mitigating data encoding threats. This should involve collaboration with cybersecurity teams to quickly address potential threats.

Network intrusion detection and prevention systems (IDS/IPS) using network signatures / rules 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.

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

The **Impact** tactic in the MITRE ATT&CK framework has a total of **10 techniques** attributed to it. These techniques describe various methods that adversaries can use to disrupt or damage an organization's operations, data, or reputation. The techniques focus on achieving a significant adverse effect, such as data destruction or manipulation, and include tactics like data encryption, resource hijacking, and system shutdown

Answers may vary, but at the time of this writing there were 13 techniques available.

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**, the impact can be devastating for an organization. A disk wipe effectively erases all data from a storage device, making recovery nearly impossible without specialized forensic tools. This could lead to:

1. **Data Loss**: Critical business data, intellectual property, and personal information may be permanently lost, severely impacting operations and financial standing
2. **Operational Disruption**: Organizations may face significant downtime as they struggle to recover systems and data, which can disrupt business continuity and erode customer trust .
3. **Reputational Damage**: Loss of sensitive data, especially personal information, can lead to public relations crises, loss of customer confidence, and potential legal repercussions .
4. **Financial Consequences**: Organizations might incur high costs for recovery efforts, legal liabilities, and potential fines if they fail to protect sensitive data according to regulations .

Answers will vary. Adversaries may wipe or corrupt raw disk data on specific systems to interrupt availability to system and network resources Malware used for wiping disks may have worm-like features to propagate across a network by leveraging additional techniques.

What could you do to mitigate this technique?

To mitigate the technique of **disk wipe** performed by threat actors, organizations can implement several strategies:

1. **Regular Data Backups**: Maintain frequent and comprehensive backups of critical data. Store these backups in a secure, off-site location or in the cloud to ensure they are safe from local attacks. Automated backup systems can help ensure backups are up to date and easily recoverable in case of a disk wipe
2. **Access Controls**: Implement strict access controls to limit who can perform sensitive operations on systems. Use the principle of least privilege to ensure that only authorized personnel can access and modify critical systems and data .
3. **Endpoint Protection**: Use robust endpoint security solutions that include anti-malware and intrusion detection systems. These can help identify and mitigate threats before they escalate to actions like disk wiping .
4. **Incident Response Plan**: Develop and regularly update an incident response plan that includes specific procedures for handling data loss incidents. Training staff on these procedures can improve response times and reduce damage
5. **Data Loss Prevention (DLP)**: Implement DLP solutions that monitor and control data transfers. These tools can help detect and prevent unauthorized data deletions or movements .
6. **System Hardening**: Regularly update and patch operating systems and applications to close vulnerabilities that could be exploited by attackers to gain access .

Implement an IT disaster recovery plan 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.

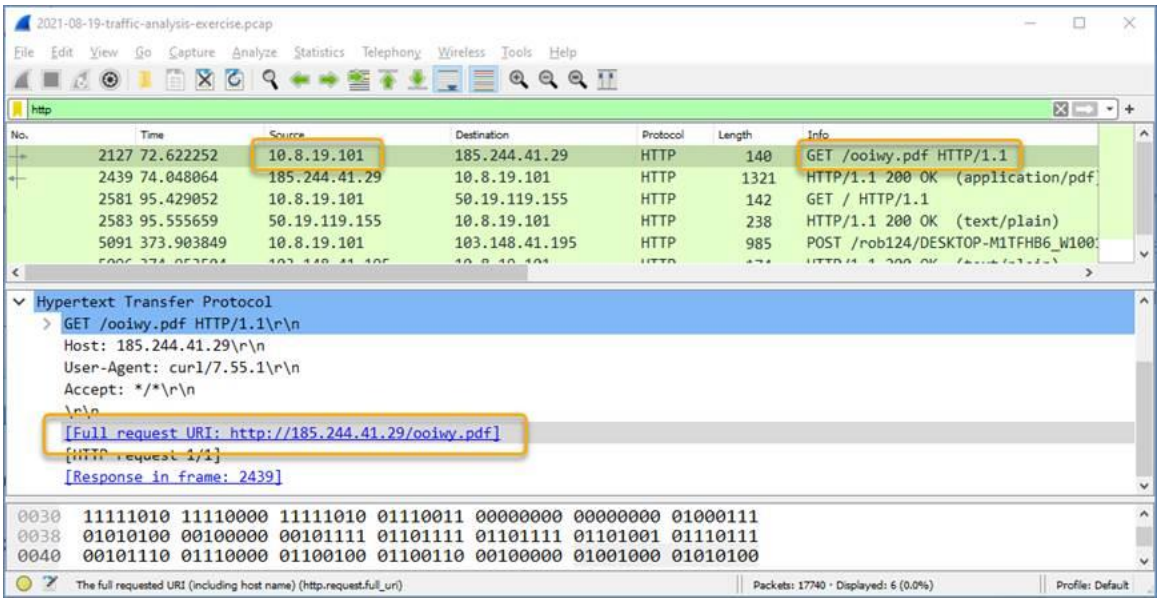
Part 3: Investigate Potential Malware

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.

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 â€œIâ€™m not a robotâ€• 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?

The Talos Weighted File Reputation Score ranges from 0 to 100, with a higher score indicating a higher likelihood of the file being malicious. A score close to 100 suggests that the file is highly suspicious or harmful. It's important to note that while this score provides an indication of the file's reputation, it shouldn't be the sole criterion for determining its maliciousness. Some file types, like Adobe Flash files, may have low scores despite being potentially harmful

You can float your mouse over the ? to learn that the score is a scale from 1 to 100. 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.

When was this file created?

August 24, 2021.

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

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

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

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

What is the target machine?

Intel 386

Intel 386 or later processors and compatible processors