Name : Selly Amelia Putri (2141762142)

Class : SIB 4C (16)

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 is an international, community-driven effort aimed at identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. This initiative operates according to specific rules and guidelines to ensure a consistent and comprehensive approach to vulnerability management

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

Show Answer Hide Answer

What is a CVE Numbering Authority (CNA)?

A CVE Numbering Authority (CNA) is an organization authorized to assign CVE IDs to vulnerabilities and to create and publish associated CVE Records. Each CNA operates within a defined scope of responsibility, focusing on specific projects or products for which they can identify and catalog vulnerabilities. The responsibilities of a CNA include ensuring that a proper vetting process is followed for each vulnerability reported, providing accessible information about the vulnerability, and maintaining communication with relevant stakeholders throughout the process.

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.

Show Answer Hide Answer

What is an Authorized Data Publisher (ADP)?

An Authorized Data Publisher (ADP) is an organization that has been authorized within the CVE Program to enhance a CVE Record that has already been published by a CVE Numbering Authority (CNA). This enrichment includes adding additional related information such as risk scores (e.g., Common Vulnerability Scoring System - CVSS), lists of affected products, and specific versions. Each ADP operates within a defined scope, ensuring that the information they provide is relevant and beneficial for understanding the vulnerabilities associated with the CVE Records they enrich .

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.

Show Answer Hide Answer

What is the **CVE List**?

The CVE List is a searchable catalog that contains all CVE Records identified by or reported to the CVE Program. It serves as a comprehensive repository of publicly disclosed cybersecurity vulnerabilities and exposures, providing a standardized method for referencing known security threats. Each entry in the CVE List includes a unique identifier (CVE ID), a brief description of the vulnerability, and references to additional information, facilitating easier communication and coordination among security professionals and organizations .

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

Show Answer Hide Answer

What is a **CVE Record**?

A CVE Record is the detailed descriptive data associated with a specific vulnerability identified by a CVE ID. This record is created by a CVE Numbering Authority (CNA) and can be further enriched by Authorized Data Publishers (ADPs) who add additional relevant information. The CVE Record includes multiple formats that are both human-readable and machine-readable, ensuring accessibility for various users. Each CVE Record is categorized into one of three states: Reserved, Published, or Rejected, indicating its status within the CVE system.

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.

Show Answer Hide Answer

What is a **CVE ID**?

A CVE ID is a unique, alphanumeric identifier assigned by the CVE Program to reference a specific cybersecurity vulnerability. This identifier enables automation and facilitates discussions among multiple parties regarding the same vulnerability, ensuring consistent communication and information sharing. The format of a CVE ID typically follows the structure "CVE-Year-Number," where "Year" indicates the year the CVE was assigned, and "Number" is a sequential identifier for that year. This standardization helps security professionals efficiently track and address vulnerabilities across various platforms and databases.

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.

Show Answer Hide 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.

What is the name of the advisory that you chose?

The advisory I chose is titled "Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature." This advisory addresses critical vulnerabilities associated with the web UI feature in Cisco IOS XE Software, specifically detailing the exploitation of two previously unknown issues leading to privilege escalation and potential system compromise.

The relevant CVEs mentioned in this advisory are CVE-2023-20198 and CVE-2023-20273, with CVE-2023-20198 assigned a CVSS score of 10.0, indicating a critical severity level, while CVE-2023-20273 has a CVSS score of 7.2, categorized as high severity.

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"

Show Answer Hide Answer

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

I chose the advisory entitled "Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature."

The CVE ID associated with this advisory is CVE-2023-20198.

- Description: This advisory identifies multiple critical vulnerabilities in the web user interface (Web UI) feature of Cisco IOS XE Software. This vulnerability can be exploited to escalate privileges and potentially compromise the system.
- CVSS Score: CVE-2023-20198 has a CVSS score of 10.0, indicating critical severity.
- Related Vulnerabilities: In addition to CVE-2023-20198, this advisory also includes CVE-2023-20273, which has a CVSS score of 7.2 and is categorized as high severity.

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.

Show Answer Hide 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.

Is there a **workaround** for the advisory you chose?

Yes, there is a workaround for the advisory regarding CVE-2023-20198. Cisco recommends disabling the HTTP Server feature on any Cisco IOS XE systems that are internet-facing as a mitigation strategy. This can be done using the following commands in global configuration mode:

- no ip http server
- no ip http secure-server

Additionally, it is advised to implement access controls to restrict access to trusted source addresses to further mitigate risks. However, users should evaluate the applicability and potential impact of these workarounds on their specific environments before implementation.

The answer is most likely "No".

Show Answer Hide 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]**.

Briefly describe the vulnerability.

CVE-2023-20198 is a critical vulnerability found in the Web User Interface (Web UI) feature of Cisco IOS XE Software. This vulnerability allows unauthenticated remote attackers to gain full administrator privileges on affected devices, enabling them to take complete control of routers and switches.

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.

Show Answer Hide 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.

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

In the MITRE ATT&CK matrix, Reconnaissance tactics have 10 related techniques. These techniques include various methods used by threat actors to gather information before carrying out further attacks.

These techniques are designed to assist threat actors in identifying targets and gathering the information necessary to plan attacks.

Answers may vary, but at the time of this writing there were 10 techniques under the Reconnaissance tactic.

Show Answer Hide Answer

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 collect reconnaissance information through phishing techniques in the following ways:

1. Sending Phishing Messages: They send emails or messages that appear legitimate to deceive targets.

2. Social Engineering: Messages often create a sense of urgency or trust to encourage targets to take action.

3. Stealing Information: If the target clicks on a link or opens an attachment, the perpetrator can steal sensitive information, such as login credentials.

In this way, perpetrators can obtain important data that is used to plan further attacks.

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.

Show Answer Hide 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?

Sub-techniques used in phishing techniques to obtain information include:

1. Spearphishing Services: Sending highly targeted messages to specific individuals or organizations to steal sensitive information.

2. Spearphishing Attachments: Using emails that include malicious attachments, such as documents or files containing malware.

3. Spearphishing links: Directs targets to links that appear legitimate, but actually lead to malicious websites to steal credentials or personal information.

These three sub-techniques enable threat actors to effectively target and exploit individuals or organizations.

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

Show Answer Hide Answer

What steps could you take to mitigate these techniques?

To reduce the risk of phishing techniques, steps that can be taken include:

1. Software Configuration: Use anti-spoofing and email authentication such as SPF, DKIM, and DMARC to filter suspicious messages. This helps ensure that emails received come from legitimate sources.

2. User Training: Provide training to employees to recognize the signs of social engineering and phishing attacks. This education is important so they can recognize and report suspicious emails.

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

Show Answer Hide 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.

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

In Command and Control tactics in the MITER ATT&CK matrix, there are 16 related techniques. These techniques include a variety of methods used by threat actors to communicate with systems they have controlled within a target network.

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

Show Answer Hide 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?

Threat actors can use data encoding for command and control in the following ways:

1. Hiding Content: By encoding data, actors can make command and control (C2) traffic more difficult for security systems to detect. This helps them avoid detection by security tools that may monitor network communications.

2. Use of Standard Formats: They can use standard data encoding systems such as ASCII, Unicode, Base64, or MIME. For example, Base64 converts binary data into printable text, making it easier to send over channels that only support text.

3. Data Compression: In addition to coding, perpetrators can also use compression techniques such as gzip to further disguise the content sent, thereby increasing the difficulty in detecting malicious activity.

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).

Show Answer Hide Answer

What could you do to mitigate this technique?

To mitigate the technique of Data Encoding used in Command and Control (C2) communications, you can implement the following measures:

1. Network Intrusion Detection and Prevention Systems (IDS/IPS): Utilize IDS/IPS that employ signature-based detection to identify and block malicious traffic. These systems analyze network packets against a database of known attack signatures, allowing them to detect encoded C2 communications effectively.
2. Regular Updates of Signatures: Ensure that the IDS/IPS signature databases are regularly updated with the latest threat intelligence to recognize new encoding techniques or malware variants.
3. Anomaly-Based Detection: Incorporate anomaly-based detection methods that establish a baseline of normal network behavior. This allows the system to flag any deviations, which could indicate the presence of encoded C2 traffic.
4. Reputation-Based Detection: Implement reputation-based detection to block traffic from known malicious IP addresses or domains associated with C2 activities.

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.

Show Answer Hide 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.

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

In the Impact tactics on the MITER ATT&CK matrix, there are 13 related techniques. These techniques include a variety of methods used by threat actors to disrupt, damage, or destroy data and business processes.

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

Show Answer Hide Answer

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 very detrimental, including:

1. Availability Disruption: Deleting data on a disk can disrupt the availability of system and network resources, causing the system to not function properly or even shut down completely.

2. Data Loss: Important and sensitive data can be lost permanently, including information necessary for business operations, which can cause financial and reputational loss.

3. Malware Spread: Malware used for disk wiping may have worm-like features, which allows it to spread over the network and increase the scale of the attack.

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.

Show Answer Hide Answer

What could you do to mitigate this technique?

To reduce disk wiping techniques, you can take the following steps:

1. Implement an IT Disaster Recovery Plan: Create and implement a disaster recovery plan that includes procedures for performing regular data backups. This ensures that the organization's data can be recovered in the event of a disk wipe.

2. Secure Data Backup: Make sure backups are stored in a secure location and separate from the main system. This protects the backup from attacks that might target the primary system.

3. Protect Backups from Unauthorized Access: Implement security measures to protect backups from common methods that attackers can use to gain access and destroy backups, thereby preventing data recovery.

4. Test the Recovery Process: Routinely test the recovery process to ensure that data can be recovered quickly and effectively when needed.

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.

Show Answer Hide Answer

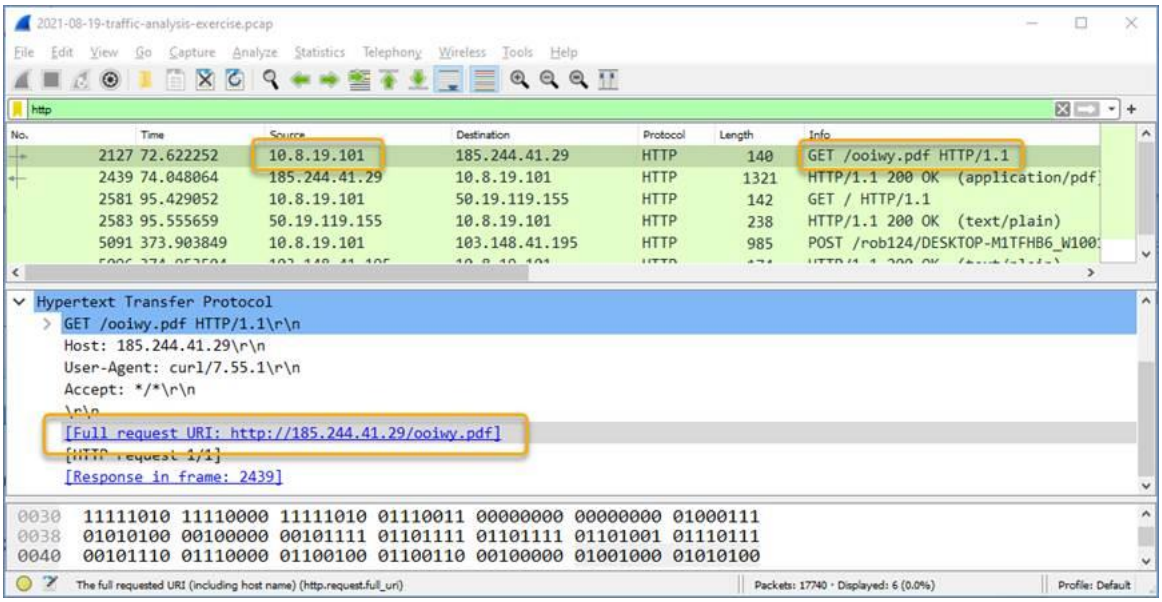
Part 3: Investigate Potential Malware

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.



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?

The reputation score of a Talos file is scaled between 1 to 100, where a score of 100 indicates that the file is highly malicious. If the analyzed file gets a score of 100, this means that the file is considered very risky and is very likely to be dangerous malware. Handling files like this must be done with extreme care to prevent negative impacts on the system.

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.

Show Answer Hide 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.

When was this file created?

Based on the information available on the DETAILS page on VirusTotal, this file was created on 2021-07-06 13:28:40.

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

Show Answer Hide Answer

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

1. RegistryDemo: This name may indicate that the file pretends to be a demo of an application related to the operating system registry, such as a tool for managing or modifying the Windows registry. This name may be used to disguise the malware to make it look like legitimate software.

2. RegistryDemo.EXE: This is a variant of the name RegistryDemo, where the .EXE extension indicates that the file is a Windows executable file. .EXE format files are often used by software, but can also be used by malware to infect systems.

3. cdnupdatherapy.png: This name is misleading because it uses the .png extension, which is usually associated with images. Malware sometimes uses unsuspecting file extensions to avoid detection by users or security systems.

4. ooiwy.pdf.exe: This name appears to imitate the file name ooiwy.pdf, but with the addition of the .exe extension. This is a trick often used by malware to hide a malicious executable file behind a safe-looking extension, such as .pdf, so that users think the file is a regular document.

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

Show Answer Hide Answer

What is the target machine?

The target machine of this file is an Intel Processor 386 or later and compatible processors. This means that this malware is designed to run on systems based on Intel 32-bit and compatible processor architectures, which is a common standard for many computers running the Windows operating system.

Intel 386 or later processors and compatible processors

Show Answer Hide Answer

Show All Answers Hide All Answers Clear My Responses

© 2017 - 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public