NAMA : Wiraswanti Rismanda Putri

NO : 34

KELAS : SIB-4C

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 Area

Program CVE adalah inisiatif global yang dipimpin oleh komunitas untuk mengidentifikasi dan mencatat kerentanan berdasarkan aturan serta pedoman yang telah ditetapkan.

What is a CVE Numbering Authority (CNA)?

Answer Area

CNA merupakan organisasi yang bertugas secara rutin menetapkan ID CVE untuk kerentanan dan menyusun serta menerbitkan informasi terkait kerentanan dalam Catatan CVE. Setiap CNA memiliki area tanggung jawab tertentu dalam hal identifikasi dan publikasi kerentanan.

What is an Authorized Data Publisher (ADP)?

Answer Area

ADP adalah organisasi yang memiliki otoritas dalam Program CVE untuk melengkapi Catatan CVE yang sebelumnya dirilis oleh CNA dengan informasi tambahan, seperti skor risiko (contohnya, Common Vulnerability Scoring System/ CVSS), daftar produk terdampak, serta versi produknya.

What is the **CVE List**?

Answer Area

CVE List adalah katalog yang dapat dicari berisi semua catatan CVE yang telah diidentifikasi atau dilaporkan ke Program CVE.

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

What is a **CVE Record**?

Answer Area

CVE Record adalah informasi deskriptif tentang kerentanan yang dihubungkan dengan ID CVE, yang disediakan oleh CNA dan diperluas oleh ADP. Data ini tersedia dalam berbagai format yang dapat diakses baik oleh manusia maupun mesin. Setiap Catatan CVE memiliki salah satu status berikut: Dicadangkan, Diterbitkan, atau Ditolak.

What is a **CVE ID**?

Answer Area

CVE ID adalah pengenal alfanumerik unik yang diberikan oleh Program CVE. Setiap pengenal mengacu pada kerentanan tertentu. ID CVE memungkinkan berbagai pihak untuk secara otomatis mendiskusikan, berbagi, dan mengaitkan informasi terkait kerentanan tertentu, dengan keyakinan bahwa mereka merujuk pada hal yang sama.

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 Area

Cisco Smart Licensing Utility Vulnerabilities

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

Answer Area

CVE-2024-20439

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?

Answer Area

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.

Answer Area

Kerentanan dalam Cisco Smart Licensing Utility dapat memungkinkan penyerang jarak jauh yang tidak terautentikasi untuk masuk ke sistem yang terpengaruh dengan menggunakan kredensial administratif statis. Kerentanan ini disebabkan oleh kredensial pengguna statis yang tidak terdokumentasi untuk akun administratif. Penyerang dapat mengeksploitasi kerentanan ini dengan menggunakan kredensial statis untuk masuk ke sistem yang terpengaruh. Eksploitasi yang berhasil dapat memungkinkan penyerang masuk ke sistem yang terpengaruh dengan hak administratif atas API aplikasi Cisco Smart Licensing Utility.

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 Area

10

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

Penyerang dapat mengirim pesan phishing untuk memperoleh informasi sensitif yang dapat dimanfaatkan dalam serangan mereka. Semua jenis phishing adalah bentuk rekayasa sosial yang disampaikan secara elektronik. Phishing juga bisa bersifat

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, Spearphishing Link, and Spearphising Link

What steps could you take to mitigate these techniques?

Answer Area

Pengaturan perangkat lunak menggunakan anti-spoofing dan autentikasi email untuk menyaring pesan serta memberikan pelatihan kepada pengguna agar dapat mengenali serangan rekayasa sosial.

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 Area

18

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

Penyerang dapat mengenkripsi data untuk menyamarkan konten lalu lintas perintah dan kontrol sehingga lebih sulit dideteksi. Informasi perintah dan kontrol (C2) bisa dikodekan dengan sistem pengodean data standar seperti ASCII, Unicode, Base64, atau MIME, serta melalui kompresi data seperti gzip.

What could you do to mitigate this technique?

Answer Area

Sistem deteksi dan pencegahan intrusi jaringan (IDS/IPS) yang memanfaatkan tanda tangan atau aturan jaringan untuk mendeteksi lalu lintas terkait malware tertentu dapat diterapkan guna mengurangi aktivitas berbahaya di level jaringan.

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 Area

14

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

Answer Area

Penyerang bisa menghapus atau merusak data pada disk mentah di sistem tertentu guna mengganggu ketersediaan sumber daya sistem dan jaringan. Malware yang digunakan untuk menghapus disk sering kali dilengkapi dengan fitur seperti worm yang memungkinkan penyebaran melalui jaringan dengan menggunakan teknik tambahan.

What could you do to mitigate this technique?

Answer Area

Laksanakan rencana pemulihan bencana TI yang mencakup prosedur pencadangan data secara rutin, sehingga data organisasi dapat dipulihkan jika diperlukan. Pastikan cadangan disimpan di lokasi terpisah dari sistem utama dan dilindungi dari metode umum yang bisa digunakan oleh penyerang untuk mengakses atau merusak cadangan, guna mencegah terhambatnya proses pemulihan.

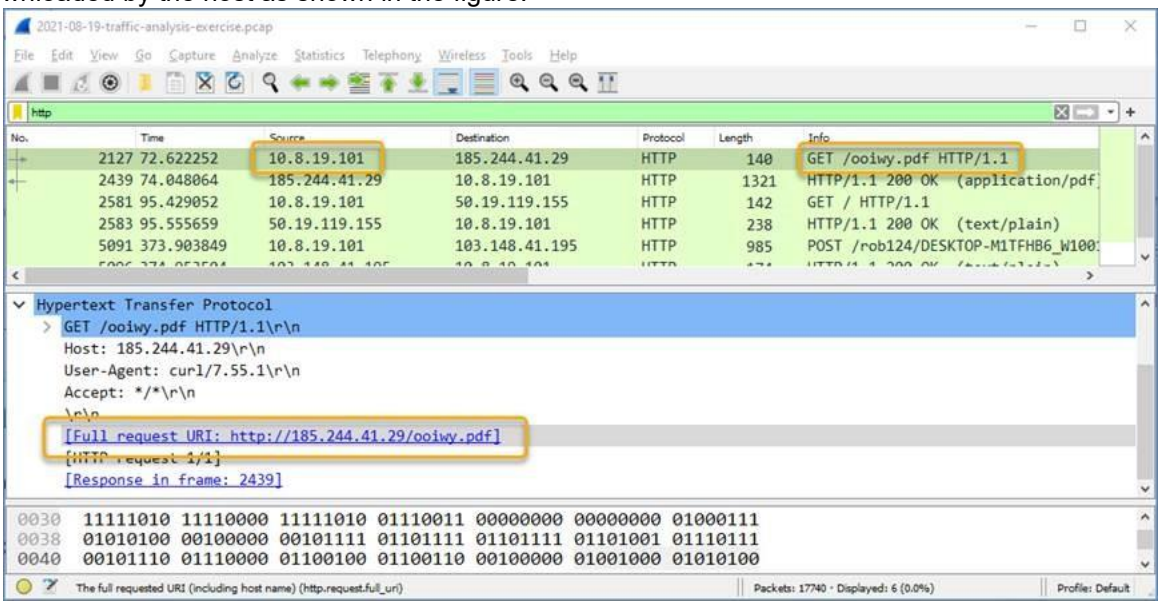
Part 3: Investigate Potential Malware

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?

Answer Area

Score not available

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

When was this file created?

Answer Area

Waktu Pembuatan 2021-07-06

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

Answer Area

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

What is the target machine?

Answer Area

Prosesor Intel 386 atau yang lebih baru serta prosesor yang kompatibel.