**Assignment 6**

**Lab 6.1 - Encrypting and Decrypting Data Using OpenSSL**

**Objectives**

**Part 1: Encrypting Messages with OpenSSL**

**Part 2: Decrypting Messages with OpenSSL**

**Background / Scenario**

OpenSSL is an open source project that provides a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library. In this lab, you will use OpenSSL to encrypt and decrypt text messages.

**Note**: While OpenSSL is the de facto cryptography library today, the use presented in this lab is NOT recommended for robust protection. Below are two security problems with this lab:

1)    The method described in this lab uses a weak key derivation function. The ONLY security is introduced by a very strong password.

2)    The method described in this lab does not guarantee the integrity of the text file.

This lab should be used for instructional purposes only. The methods presented here should NOT be used to secure truly sensitive data.

**Required Resources**

   Security Workstation virtual machine

**Instructions**

**Part 1: Encrypting Messages with OpenSSL**

OpenSSL can be used as a standalone tool for encryption. While many encryption algorithms can be used, this lab focuses on AES. To use AES to encrypt a text file directly from the command line using OpenSSL, follow the steps below:

**Step 1: Encrypting a Text File**

a.     Log into Security Workstation VM.

b.     Open a terminal window.

c.     Because the text file to be encrypted is in the /home/analyst/lab.support.files/ directory, change to that directory:

[analyst@secOps ~]$ **cd ./lab.support.files/**

[analyst@secOps lab.support.files]$

d.     Type the command below to list the contents of the encrypted **letter\_to\_grandma.txt** text file on the screen:

[analyst@secOps lab.support.files]$ **cat letter\_to\_grandma.txt**

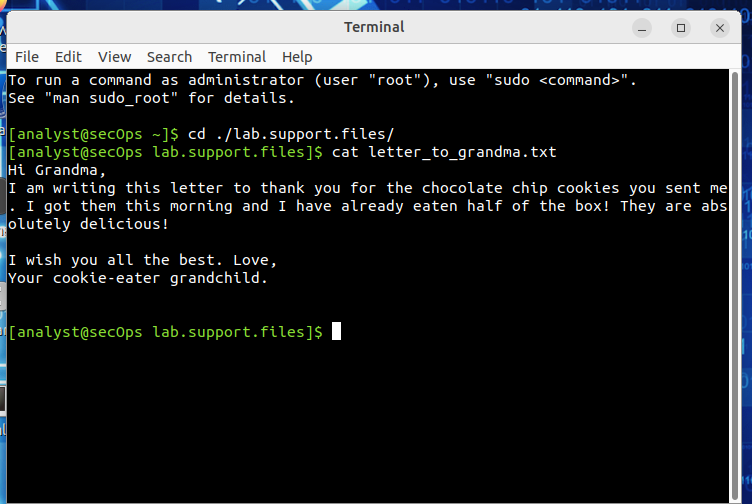
Hi Grandma,

I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,

Your cookie-eater grandchild.

[analyst@secOps lab.support.files]$



e.     From the same terminal window, issue the command below to encrypt the text file. The command will use AES-256 to encrypt the text file and save the encrypted version as **message.enc**. OpenSSL will ask for a password and for password confirmation. Provide the password as requested and be sure to remember the password.

[analyst@secOps lab.support.files]$ **openssl aes-256-cbc -in letter\_to\_grandma.txt -out message.enc**

enter aes-256-cbc encryption password:

Verifying - enter aes-256-cbc encryption password:

[analyst@secOps lab.support.files]$

Question:

Document the password.

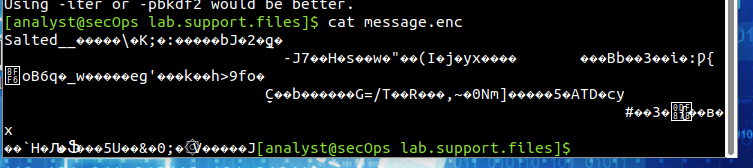
***Type your answers here.***

f.      When the process is finished, use the **cat** command again to display the contents of the **message.enc** file.

[analyst@secOps lab.support.files]$ **cat message.enc**

Question:

Did the contents of the **message.enc** file display correctly? What does it look like? Explain.

***Type your answers here.*** ******

g.     To make the file readable, run the OpenSSL command again, but this time add the **-a** option. The **-a** option tells OpenSSL to encode the encrypted message using a different encoding method of Base64 before storing the results in a file.

**Note**: Base64 is a group of similar binary-to-text encoding schemes used to represent binary data in an ASCII string format.

[analyst@secOps lab.support.files]$ **openssl aes-256-cbc -a -in letter\_to\_grandma.txt -out message.enc**

enter aes-256-cbc encryption password:

Verifying - enter aes-256-cbc encryption password:

h.     Once again, use the **cat** command to display the contents of the, now re-generated, **message.enc** file:

**Note**: The contents of **message.enc** will vary.

[analyst@secOps lab.support.files]$ **cat message.enc**

U2FsdGVkX19ApWyrn8RD5zNp0RPCuMGZ98wDc26u/vmj1zyDXobGQhm/dDRZasG7

rfnth5Q8NHValEw8vipKGM66dNFyyr9/hJUzCoqhFpRHgNn+Xs5+TOtz/QCPN1bi

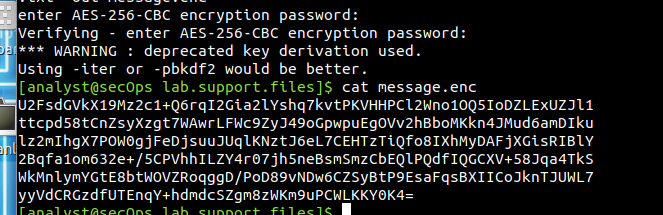
08LGTSzOpfkg76XDCk8uPy1hl/+Ng92sM5rgMzLXfEXtaYe5UgwOD42U/U6q73pj

a1ksQrTWsv5mtN7y6mh02Wobo3A1ooHrM7niOwK1a3YKrSp+ZhYzVTrtksWDl6Ci

XMufkv+FOGn+SoEEuh7l4fk0LIPEfGsExVFB4TGdTiZQApRw74rTAZaE/dopaJn0

sJmR3+3C+dmgzZIKEHWsJ2pgLvj2Sme79J/XxwQVNpw=

[analyst@secOps lab.support.files]$



Questions:

Can you think of a benefit of having **message.enc** Base64-encoded?:

Base64 encoding ensures message.enc can be safely transmitted over text-based protocols, avoiding issues with special characters and binary data corruption. It enhances cross-platform compatibility, prevents misinterpretation in JSON or URLs, and ensures encrypted messages remain intact. However, it increases data size by about 33%.

***Type your answers here.***

**Part 2: Decrypting Messages with OpenSSL**

With a similar OpenSSL command, it is possible to decrypt **message.enc**.

a.     Use the command below to decrypt message.enc:

[analyst@secOps lab.support.files]$ **openssl aes-256-cbc –a -d -in message.enc -out decrypted\_letter.txt**

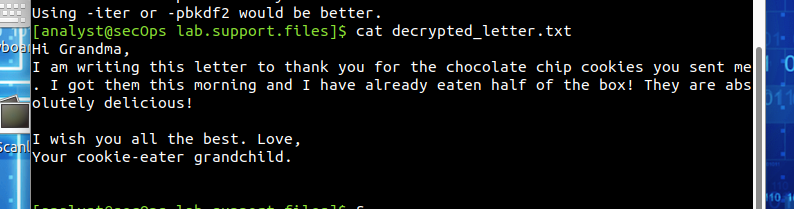
b.     OpenSSL will ask for the password used to encrypt the file. Enter the same password again.

c.     When OpenSSL finishes decrypting the **message.enc** file, it saves the decrypted message in a text file called **decrypted\_letter.txt**. Use the **cat** display the contents of **decrypted\_letter.txt**:

[analyst@secOps lab.support.files]$ **cat decrypted\_letter.txt**

Questions:

Was the letter decrypted correctly?

cd .The command used to decrypt also contains -a option. Can you explain?

***Type your answers here.***

**Lab 6.2 - Encrypting and Decrypting Data using a Hacker Tool**

**Objectives**

**Part 1: Create and Encrypt Files**

**Part 2: Recover Encrypted Zip File Passwords**

**Background / Scenario**

What if you work for a large corporation that had a corporate policy regarding removable media? Specifically, it states that only encrypted zipped documents can be copied to portable USB flash drives.

In this scenario, the Chief Financial Officer (CFO) is out-of-town on business and has contacted you in a panic with an emergency request for help. While out-of-town on business, he attempted to unzip important documents from an encrypted zip file on a USB drive. However, the password provided to open the zip file is invalid. The CFO contacted you to see if there was anything you could to do.

**Note**: The provided scenario is simple and only serves as an example.

There may some tools available to recover lost passwords. This is especially true in situations such as this where the cybersecurity analyst could acquire pertinent information from the CFO. The pertinent information could be the length of the password and an idea of what it could be. Knowing pertinent information dramatically helps when attempting to recover passwords.

Examples of password recovery utilities and programs include hashcat, John the Ripper, Lophtcrack, and others. In our scenario, we will use **fcrackzip** which is a simple Linux utility to recover the passwords of encrypted zip files.

Consider that these same tools can be used by cybercriminals to discover unknown passwords. Although they would not have access to some pertinent information, with time, it is possible to discover passwords to open encrypted zip files. The amount of time required depends on the password strength and the password length. Longer and more complex passwords (mix of different types of characters) are more secure.

In this lab, you will:

         Create and encrypt sample text files.

         Decrypt the encrypted zip file.

**Note:** This lab should be used for instructional purposes only. The methods presented here should NOT be used to secure truly sensitive data.

**Required Resources**

   Security Workstation virtual machine

**Instructions**

**Part 1: Create and Encrypt Files**

In this part, you will create a few text files that will be used to created encrypted zip files in the next step.

**Step 1: Create text files.**

a.     Start the Security Workstation VM.

b.     Open a terminal window. Verify that you are in the analyst home directory. Otherwise, enter **cd ~** at the terminal prompt.

c.     Create a new folder called Zip-Files using the **mkdir Zip-Files** command.

d.     Move into that directory using the **cd Zip-Files** command.

e.     Enter the following to create three text files.

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-1.txt**

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-2.txt**

[analyst@secOps Zip-Files]$ **echo This is a sample text file > sample-3.txt**

f.      Verify that the files have been created, using the **ls** command.

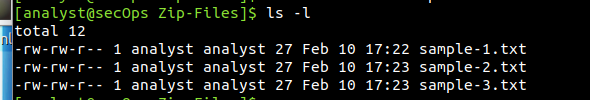
[analyst@secOps Zip-Files]$ **ls -l**

total 12

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-1.txt

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-2.txt

-rw-r--r-- 1 analyst analyst 27 May 13 10:58 sample-3.txt



**Step 2: Zip and encrypt the text files.**

Next, we will create several encrypted zipped files using varying password lengths. To do so, all three text files will be encrypted using the **zip** utility.

a.     Create an encrypted zip file called **file-1.zip** containing the three text files using the following command:

[analyst@secOps Zip-Files]$ **zip –e file-1.zip sample\***

b.     When prompted for a password, enter a one-character password of your choice. In the example, the letter **B** was entered. Enter the same letter when prompted to verify.

[analyst@secOps Zip-Files]$ **zip -e file-1.zip sample-\***

Enter password:

Verify password:

adding: sample-1.txt (stored 0%)

adding: sample-2.txt (stored 0%)

adding: sample-3.txt (stored 0%)

c.     Repeat the procedure to create the following 4 other files

o      **file-2.zip** using a 2-character password of your choice. In our example, we used **R2**.

o      **file-3.zip** using a 3-character password of your choice. In our example, we used **0B1**.

o      **file-4.zip** using a 4-character password of your choice. In our example, we used **Y0Da**.

o      **file-5.zip** using a 5-character password of your choice. In our example, we used **C-3P0**.

d.     Verify that all zipped files have been created using the **ls -l f\*** command.

[analyst@secOps Zip-Files]$ **ls -l f\***

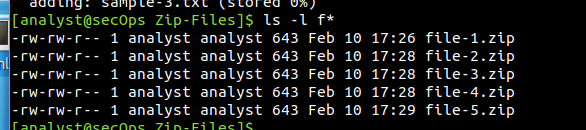
-rw-r--r-- 1 analyst analyst 643 May 13 11:01 file-1.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:02 file-2.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-3.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-4.zip

-rw-r--r-- 1 analyst analyst 643 May 13 11:03 file-5.zip



e.     Attempt to open a zip using an incorrect password as shown.

[analyst@secOps Zip-Files]$ **unzip file-1.zip**

Archive: file-1.zip

[file-1.zip] sample-1.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-1.txt incorrect password

[file-1.zip] sample-2.txt password:

password incorrect--reenter:

password incorrect--reenter:

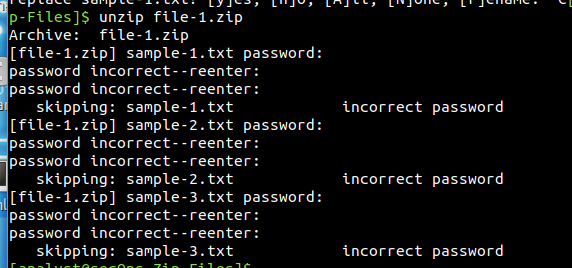
skipping: sample-2.txt incorrect password

[file-1.zip] sample-3.txt password:

password incorrect--reenter:

password incorrect--reenter:

skipping: sample-3.txt incorrect password



**Part 2: Recover Encrypted Zip File Passwords**

In this part, you will use the **fcrackzip** utility to recover lost passwords from encrypted zipped files. Fcrackzip searches each zip file given for encrypted files and tries to guess the password using brute-force methods.

The reason we created zip files with varying password lengths was to see if password length influences the time it takes to discover a password.

**Step 1: Introduction to fcrackzip**

From the terminal window, enter the **fcrackzip –h** command to see the associated command options.

In our examples, we will be using the **–v**, **-u**, and **-l** command options. The -l option will be listed last because it specifies the possible password length. Feel free to experiment with other options.

**Step 2: Recovering Passwords using fcrackzip**

a.     Now attempt to recover the password of the **file-1.zip** file. Recall, that a one-character password was used to encrypt the file.Therefore, use the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip -vul 1-4 file-1.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

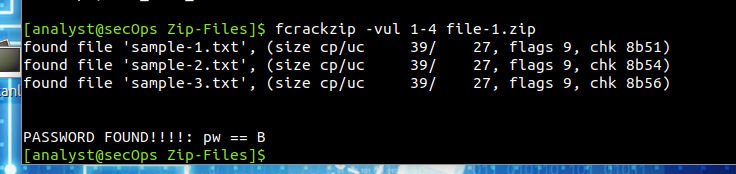
found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == B

**Note**: The password length could have been set to less than 1 – 4 characters.

Question:

How long does it take to discover the password?

***Type your answers here.*** ******

b.     Now attempt to recover the password of the **file-2.zip** file. Recall, that a two-character password was used to encrypt the file.Therefore, use the following **fcrackzip** command:

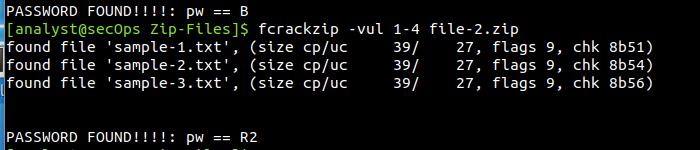
[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-2.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == R2



Question:

How long does it take to discover the password? Instant

***Type your answers here.***

c.     Repeat the procedure and recover the password of the **file-3.zip** file. Recall, that a three-character password was used to encrypt the file.Time to see how long it takes to discover a 3-letter password.Use the following **fcrackzip** command:

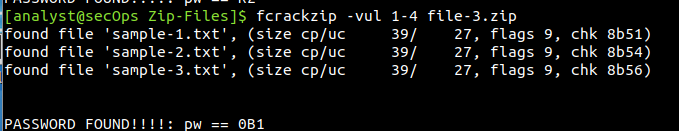
[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-3.zip**

found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

PASSWORD FOUND!!!!: pw == 0B1



Question:

How long does it take to discover the password? Instantly

***Type your answers here.***

d.     How long does it take to crack a password of four characters? Repeat the procedure and recover the password of the **file-4.zip** file. Time to see how long it takes to discover the password using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-4 file-4.zip**

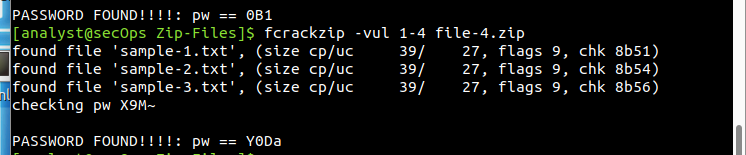
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

checking pw X9M~

PASSWORD FOUND!!!!: pw == Y0Da



Question:

How long does it take to discover the password? A bit longer but it worked

***Type your answers here.***

e.     How long does it take to crack a password of five characters? Repeat the procedure and recover the password of the **file-5.zip** file. The password length is five characters, so we need to set the **-l** command option to **1-5**. Again, time to see how long it takes to discover the password using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-5 file-5.zip**

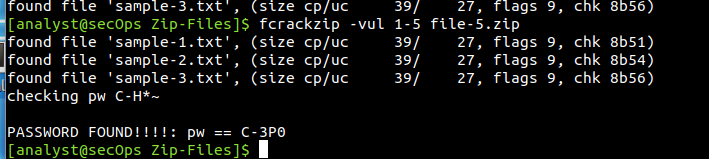
found file 'sample-1.txt', (size cp/uc 39/ 27, flags 9, chk 5754)

found file 'sample-2.txt', (size cp/uc 39/ 27, flags 9, chk 5756)

found file 'sample-3.txt', (size cp/uc 39/ 27, flags 9, chk 5757)

checking pw C-H\*~

PASSWORD FOUND!!!!: pw == C-3P0



Question:

How long does it take to discover the password? Quite long but inititally it did

***Type your answers here.***

f.      Recover a 6 Character Password using fcrackzip

It appears that longer passwords take more time to discover and therefore, they are more secure. However, a 6 character password would not deter a cybercriminal.

Question:

How long do you think it would take fcrackzip to discover a 6-character password?

***Type your answers here.***

To answer that question, create a file called **file-6.zip** using a 6-character password of your choice. In our example, we used **JarJar**.

[analyst@secOps Zip-Files]$ **zip –e file-6.zip sample\***

g.     Repeat the procedure to recover the password of the **file-6.zip** file using the following **fcrackzip** command:

[analyst@secOps Zip-Files]$ **fcrackzip –vul 1-6 file-6.zip**

Question:

How long does it take fcrackzip to discover the password? Long…

***Type your answers here.***

The simple truth is that longer passwords are more secure because they take longer to discover.

Question:

How long would you recommend a password needs to be for it to be secure?

For strong security, I recommend passwords be **at least 12–16 characters long**. Longer passwords (20+ characters) provide even better protection, especially against brute-force attacks

***Type your answers here.***

*End of document*

*End of document*

**Lab 6.3 - 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?**  
A program that identifies and catalogs publicly disclosed cybersecurity vulnerabilities.

**What is a CVE Numbering Authority (CNA)?**  
An organization authorized to assign CVE IDs to vulnerabilities.

**What is an Authorized Data Publisher (ADP)?**  
An entity approved to publish and manage CVE Records in the CVE database.

**What is the CVE List?**  
A public registry of known cybersecurity vulnerabilities, each assigned a unique CVE ID.

**What is a CVE Record?**  
A detailed entry describing a specific cybersecurity vulnerability.

**What is a CVE ID?**  
A unique identifier assigned to a publicly disclosed vulnerability.

***Type your answer here.***

**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?

“Cisco Meeting Management REST API Privilege Escalation Vulnerability”

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

CVE-2025-20156

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?



***Type your answer here.***

**Step 3: Return to the CVE website and research more about your chosen Cisco CVE.**

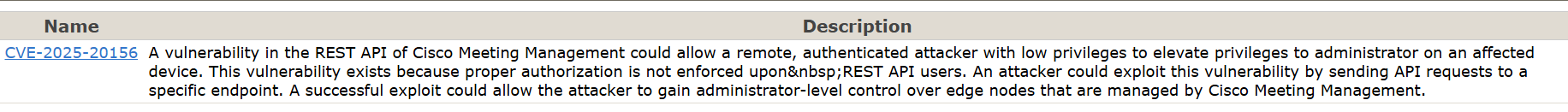
a.     Navigate back to the website cve.mitre.org website, which should still be open in a browser tab.

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.



A vulnerability in the REST API of Cisco Meeting Management could allow a remote, authenticated attacker with low privileges to elevate privileges to administrator on an affected device. This vulnerability exists because proper authorization is not enforced upon&nbsp;REST API users. An attacker could exploit this vulnerability by sending API requests to a specific endpoint. A successful exploit could allow the attacker to gain administrator-level control over edge nodes that are managed by Cisco Meeting Management.

**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:

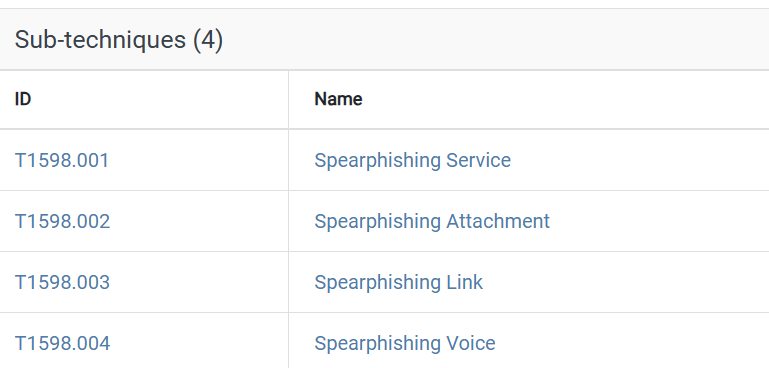
How many techniques are attributed to the **Reconnaissance** tactic? 10

***Type your answer here.***

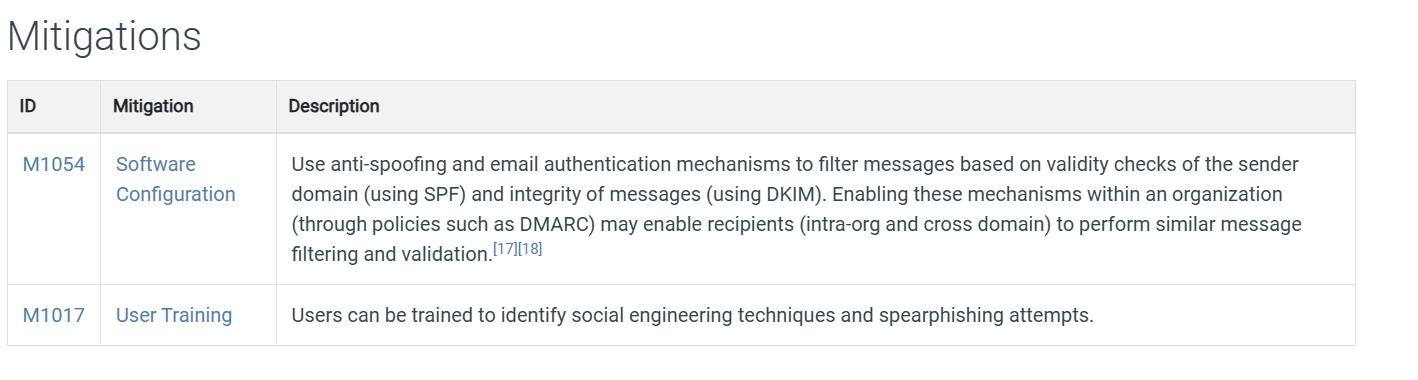
Under **Reconnaissance**, click **Phishing for Information** and read the description. Briefly describe how a threat actor could gather reconnaissance information using phishing techniques?

A threat actor can gather reconnaissance information using phishing by sending deceptive emails, messages, or calls to trick victims into revealing sensitive data. They may pose as a trusted entity (e.g., IT support, a colleague, or a service provider) and request credentials, financial details, or personal information. Spearphishing targets specific individuals or organizations, while broader phishing campaigns aim to collect mass data. Attackers may also use spoofed identities and social engineering tactics to bypass security measures and make their requests seem legitimate.

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?

******

What steps could you take to mitigate these techniques?

**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? 18

***Type your answer here.***

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?

A threat actor could use data encoding for command and control (C2) to obfuscate malicious communication and evade detection by security tools. By encoding C2 traffic using **Base64, ASCII, Unicode, or MIME**, they can disguise commands and exfiltrated data to appear as legitimate traffic. Additionally, **non-standard encoding** methods or compression (e.g., gzip) can further obscure the data, making it harder for security solutions to detect or analyze malicious activity.

What could you do to mitigate this technique?

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.

***Type***

***your answer here.***

**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? 14

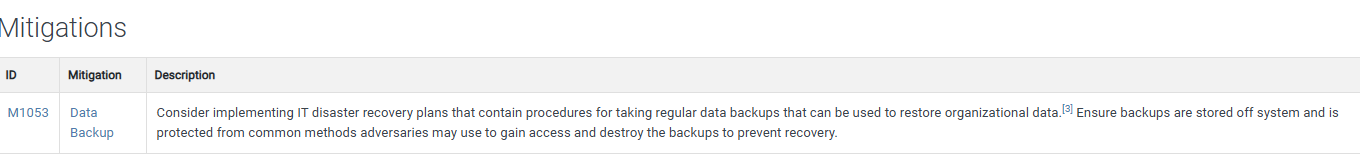
***Type your answer here.***

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

A **disk wipe** by a threat actor can cause severe **data loss, system downtime, and operational disruption**. By overwriting disk sectors or wiping critical structures like the **Master Boot Record (MBR)**, the attacker can render systems **unbootable** and destroy valuable files. If executed across a network, especially with worm-like propagation, it can **cripple an organization’s infrastructure**, leading to costly recovery efforts, business interruptions, and potential reputational damage.

***Type your answer here.***

What could you do to mitigate this technique?

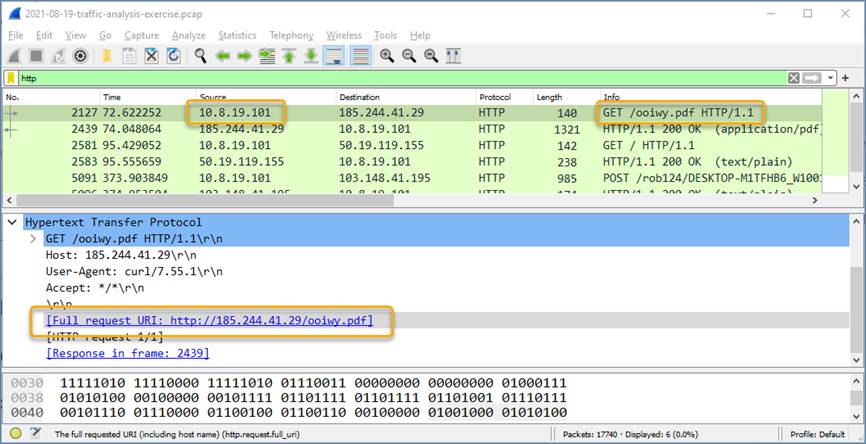
****Part 3: Investigate Potential Malware**

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.

a.     Search for "Cisco Talos" and click the first link to access the Cisco Talos Intelligence Group website.

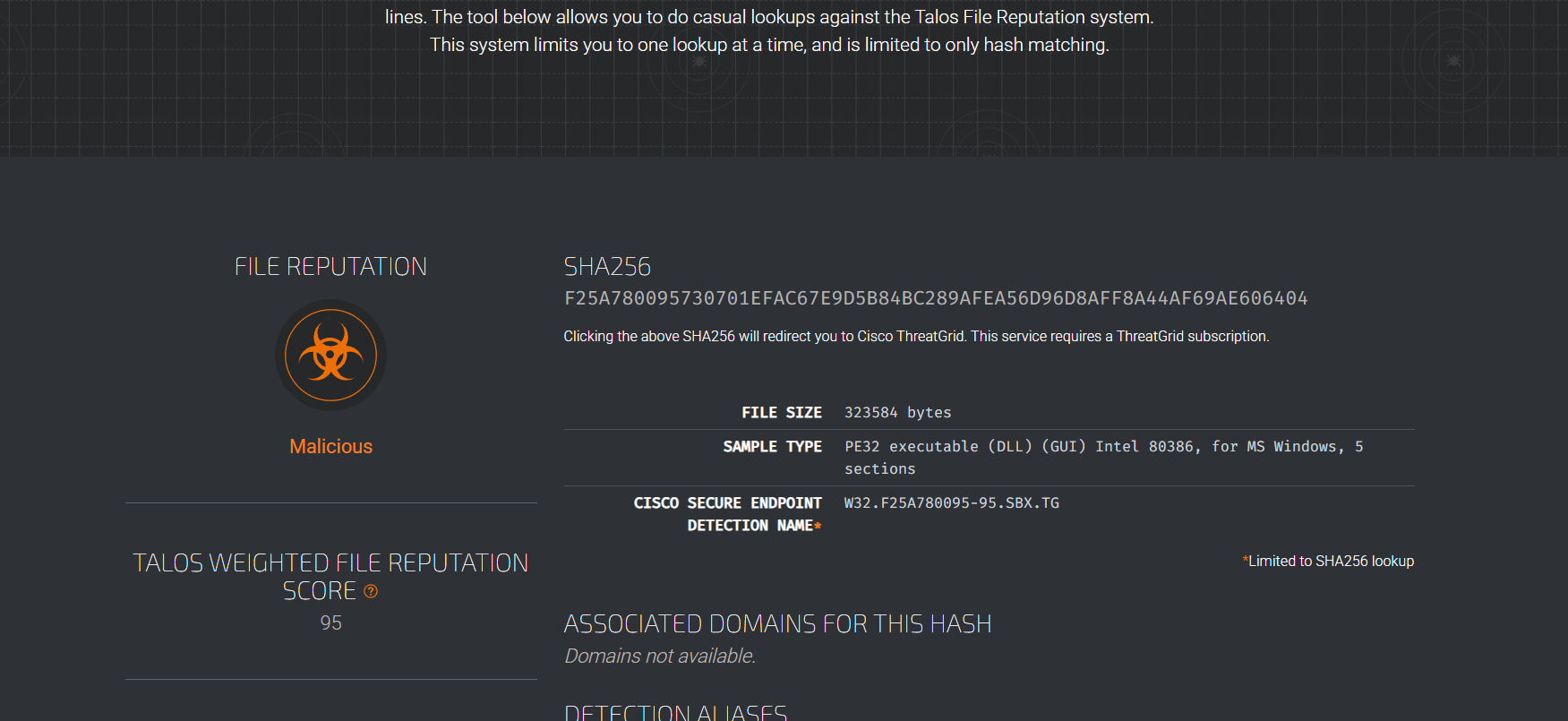
b.     Locate the menus at the top and over the **Reputation Center** to dropdown a submenu. Click the link for the **Talos File Reputation** search page.

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.

Questions:

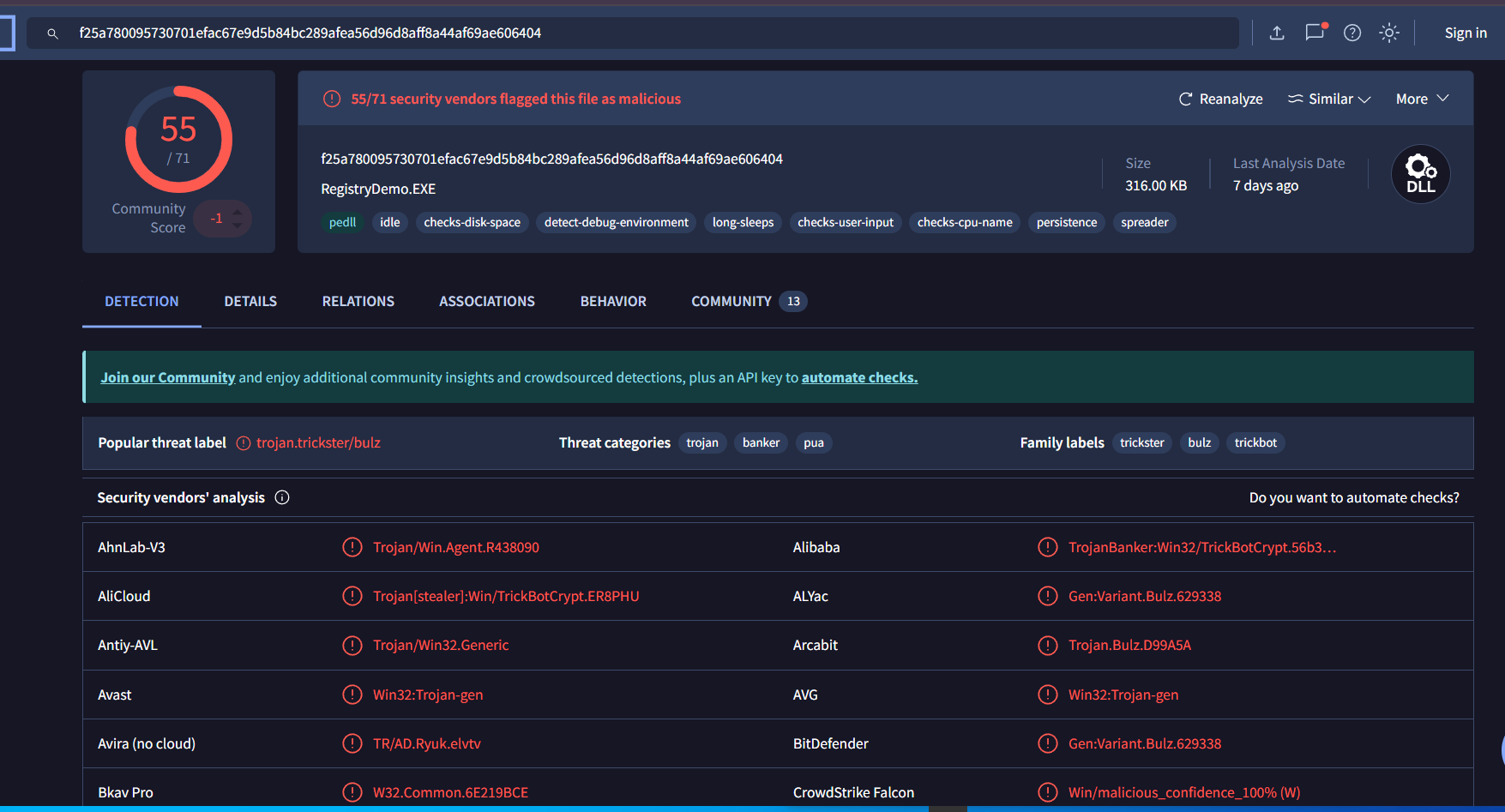
What is the Talos Weighted File Reputation Score? Is that good or bad?



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? 2021-07-06

***Type your answer here.***

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

* ooiwy.pdf
* RegistryDemo
* RegistryDemo.EXE
* malware.pdf
* virus
* sus.pdf
* ooiwy.pdf.defang
* bdreadmejt.dmo
* suspicious1
* ooiwyinf.pdf

***Type your answer here.***

What is the target machine?

Intel 386 or later processors and compatible processors ***here.***

*End of document*

**Lab 6.4 - Document Enterprise Cybersecurity Issues**

**Objectives**

**Part 1: Record your assessment of Athena's cybersecurity issues.**

**Part 2: Record the different types of assets owned by Athena.**

**Part 3: List the threats for each asset type.**

**Part 4: Recommend mitigation techniques to address each threat.**

**Note**: This lab assumes you have basic knowledge of vulnerabilities, threats, and mitigation techniques.

**Scenario**

Athena Learning Incorporated is an educational service provider. Athena has two major lines of business: course content creation and online learning services. Athena creates learning content and hosts learning content. Athena also provides internet sales services that enable its partners to charge their students to attend their courses.

Athena employs about 100 people in its headquarters office, and about 5 people each in its London and Singapore offices. Because it provides content and delivery services globally, Athena must comply with diverse privacy and security standards.

Athena serves as custodian for its own content and content that belongs to its partners. That content includes text, graphic, video, and interactive assets. This content is the essential intellectual property of the company. It also manages student account information including student registration, authentication, records, and payment information. Athena manages its own SQL databases, some of which are connected to web portals.

The Athena network consists of mostly MS Windows and Apple IOS clients with a mix of Microsoft and Linux servers to store business and employee records, learning content assets, and financial information, including customer data. The hosts include various PC brands and models of varying age. Different versions of operating systems are in use. Athena uses cloud services to deliver courses to the public, but must house assembled courses on the internal network for creation and editing. When the courses become available, they are mirrored to the cloud. Employees are permitted to use their personal phones and tablets for work. In addition, some employees work from home, but require full network access to do so. Athena also hosts its own DNS, email, and intranet services.

Athena employees use common office application software, custom applications, and tools that have been created internally.

Athena provides access to parts of its internal network to its partners through a secure web portal. Clients are able to preview their course content and deliver course assets to Athena for assembly in the Athena learning management system. Students interact with the cloud-managed learning platform through their web account logins.

In this lab, you will apply your knowledge of cybersecurity threats and mitigation techniques to a corporate setting. You will read about a business, classify its assets, and then list the potential vulnerabilities and threats that the business faces. Finally, you will recommend threat mitigation measures for the threats that you identify.

**Required Resources**

   Devices with internet access

**Instructions**

**Part 1: Record your assessment of Athena's cybersecurity issues.**

Study the **Scenario** above about Athena Learning Incorporated. Focus on identifying the data, software, hardware, and network assets that need to be protected to ensure that company is not impacted by various types of threats that have been discussed in the course so far.

Use the tables below to record your answers.

| **Information/Data Assets** | **Threats** | **Mitigation** |
| --- | --- | --- |
| Student registration, authentication, and payment information | Data breaches, phishing, unauthorized access | Implement strong encryption, multi-factor authentication (MFA), and regular security audits |
| Intellectual property (course content, videos, interactive assets) | Data leaks, insider threats, unauthorized duplication | Access control policies, digital rights management (DRM), and data loss prevention (DLP) tools |
| SQL databases (customer and financial data) | SQL injection, ransomware, unauthorized modifications | Regular security patches, input validation, and database access controls |
| Employee records | Insider threats, credential theft | Role-based access control (RBAC), employee cybersecurity training |
| Student records (grades, progress tracking) | Data integrity issues, unauthorized access | Implement secure backup procedures and audit logs for data changes |

*Blank Line, No additional information*

*Blank Line, No additional information*

| **Software Assets** | **Threats** | **Mitigation** |
| --- | --- | --- |
| Microsoft and Linux servers | OS vulnerabilities, malware, denial-of-service (DoS) attacks | Regular OS updates, endpoint detection and response (EDR), and firewall configurations |
| Custom internally developed applications | Zero-day exploits, software bugs | Secure coding practices, penetration testing, and patch management |
| Office productivity software | Phishing attacks, macro-based malware | Email filtering, user awareness training, and endpoint protection |
| Web portal for partners | Cross-site scripting (XSS), unauthorized access | Secure authentication mechanisms, web application firewall (WAF) |
| Learning management system (LMS) | Distributed denial-of-service (DDoS) attacks, unauthorized API access | Traffic monitoring, rate limiting, and secure API management |

*Blank Line, No additional information*

*Blank Line, No additional information*

| **Physical Assets** | **Threats** | **Mitigation** |
| --- | --- | --- |
| Employee workstations and laptops | Theft, unauthorized physical access | Laptop encryption, biometric authentication, and physical locks |
| On-premises servers | Physical tampering, power failures | Secure server rooms, backup power supplies, and surveillance cameras |
| Employee personal devices (BYOD) | Data leakage, insecure applications | Mobile device management (MDM), remote wipe capabilities |
| Office facilities | Unauthorized access, social engineering attacks | Security guards, access control systems, and visitor logs |

*Blank Line, No additional information*

*Blank Line, No additional information*

| **Network Assets** | **Threats** | **Mitigation** |
| --- | --- | --- |
| Internal network (corporate LAN) | Man-in-the-middle (MITM) attacks, unauthorized access | Network segmentation, VPN for remote access, and intrusion detection systems (IDS) |
| Cloud-based learning platform | Data interception, unauthorized API usage | End-to-end encryption, API gateway security, and cloud security audits |
| Email servers | Phishing, spam, malware delivery | Email filtering, DMARC/SPF/DKIM policies |
| DNS hosting | DNS poisoning, denial-of-service attacks | DNSSEC implementation, traffic monitoring |

*Blank Line, No additional informationBlank Line, No additional information*

**Part 2: Record the different types of assets owned by Athena.**

From the information in the **Scenario**, and your knowledge of business in general, fill in the first columns of each table with the relevant assets that are owned by Athena. You should have at least three entries in each table.

The different types of assets are defined as follows:

   **Information/Data Assets** - any data that is used by the company, in any of the three states of data. This data could be Athena’s business data, Athena’s learning content, student sales and learning data, or partner data.

   **Software Assets** - any software that is used by Athena, including commercial business applications, operating systems, server software, database software, and custom software.

   **Physical Assets** - the physical devices, equipment, and other property that are used by Athena in the course of their business.

   **Network Assets** - the types of networks and network connections that are hosted or used by Athena in the course of its business.

|  |  |  |  |
| --- | --- | --- | --- |
| **Information/Data Assets** | **Software Assets** | **Physical Assets** | **Network Assets** |
| Information/Data Assets | Software Assets | Physical Assets | Network Assets |
| Student registration, authentication, and records | Microsoft Windows and Apple iOS clients | Office workstations (HQ, London, Singapore) | Internal corporate network |
| Partner course content (text, graphics, videos) | Microsoft and Linux servers | Employee personal phones and tablets | Cloud-hosted course delivery system |
| Customer payment information | SQL databases | Servers hosting business and employee records | Partner web portal |
| Business financial records | Custom learning management system | Network hardware (routers, switches) | DNS, email, and intranet services |
| Internal proprietary course development data | Cloud-based learning platform | Employee home-office equipment | Remote access VPN |

**Part 3: List the threats for each asset type.**

a.     Review the information that you have learned in this pathway regarding vulnerabilities and threats.

Question:

What is the difference between a threat and a vulnerability? A **threat** refers to a potential danger or event that can exploit a vulnerability, causing harm or damage to an asset. It is typically something external, like a hacker, natural disaster, or malicious software, that could lead to a security breach.

A **vulnerability**, on the other hand, is a weakness or flaw in a system, process, or asset that could be exploited by a threat to cause harm. It could be a software bug, poor system configuration, or lack of proper access controls.***e your answers here.***

**Part 4: Recommend mitigation techniques to address each threat.**

Review the information that you have learned so far about ways to mitigate various cybersecurity threats. Complete the third column of the table with mitigation techniques that can be done to avoid or limit the damage caused by each potential threat.

**Reflection**

1.     Why is it useful to categorize assets when identifying threats and mitigation techniques?

Categorizing assets helps prioritize security efforts and allocate resources more efficiently. By understanding the value and criticality of each asset, you can better assess the risks associated with specific threats. This enables organizations to tailor mitigation techniques to protect the most valuable or vulnerable assets first, ensuring a more strategic and effective security posture.

2.     Do some threats have the same or similar mitigation measures? Why is it important to note this?

Yes, some threats share similar mitigation measures, such as using firewalls, encryption, or access control policies to protect against a range of attacks (e.g., malware, unauthorized access, data breaches). Noting this is important because it helps organizations avoid redundant or ineffective measures, optimize resources, and create scalable security solutions that can address multiple risks with a single approach, streamlining efforts and ensuring comprehensive protection.

3.     What have you learned about the application of knowledge of cybersecurity threats and mitigation techniques to the context of a simulated organization?

Applying cybersecurity knowledge in a simulated organization context helps to understand how theoretical concepts translate into real-world scenarios. It reinforces the importance of proactive threat identification, risk assessment, and applying the right mitigation strategies to safeguard critical assets. It also highlights the dynamic nature of cybersecurity, where new threats can emerge, requiring continuous monitoring and adaptation of security measures to maintain the integrity of the organization's systems.

***Type your answers here.***