Packet Tracer - File and Data Integrity Checks

Objectives

Part 1: Recover Files after a Cyber Attack

Part 2: Using Hashing to Verify File Integrity

Part 3: Using HMAC to Verify File Integrity

Background

In this Packet Tracer (PT) activity, you will verify the integrity of multiple files using hashes to ensure files have not been tampered with. If any files are suspected of being tampered with, they are to be sent to Sally's PC so that she can further analyze the contents. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices to verify and transfer any suspect files.

Resources

The **CSE-LABVM** installed in VirtualBox

Note: It is recommended that you use the **CSE-LABVM** to check file MD5 files hashes in this activity. The **CSE-LABVM** was installed during the **Lab - Install a Virtual Machine on a Personal Computer**.

Instructions

Part 1: Recover Files after a Cyber Attack

Client data must be secured and remain unchanged by unauthorized personnel. By hashing data before and after it is archived, you can tell if it has changed even by one character or even one bit because the hashes will not match. In this Part, you will attempt to recover files from a backup after a cyber attack.

Step 1: Access the BR Server from Mike's PC.

a. Click **Branch Office** and then click **Laptop BR-1**.

b. Click the **Desktop** tab and then click **Web Browser**.

c. Enter the URL **http://branch.corp** and click **Go**.

Note: Packet Tracer may take up to a minute to converge. You can click **Fast Forward Time** (Alt+D) to speed up the process.

d. Click the link to download the most current files.

Step 2: Copy the hash values from the last time the files were archived.

You need to restore the missing files from a backup server located in HQ. But first, you need the hashes for the stored files to ensure their integrity.

a. Enter the URL **http://hq.corp** and click **Go**.

b. Click the link to view the most recent files and their hashes.

c. Select and copy all the content.

d. Open the **CSE-LABVM**, and then click **Menu** > **Text Editor Pluma**.

e. Paste the contents of your clipboard into the blank document. You will use these hashes to validate if a file is corrupted.

Step 3: Download the backup files to Mike's PC.

a. Back in Packet Tracer, close the **Web Browser** one Mike's PC.

b. Click **Command Prompt**. Connect to the **HQ FTP Server** by entering **ftp hq.corp** at the prompt.

c. Enter the username of **mike** and a password of **cisco123**.

d. At the **ftp>** prompt, enter the command **dir** to view the current files stored on FTP server.

e. Download the six client files (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt, and Sclients.txt) to Mike's PC. Example for the first file is shown here:

```
ftp> get NEclients.txt

Reading file NEclients.txt from hq.corp:
File transfer in progress...

[Transfer complete - 584 bytes]

584 bytes copied in 0.05 secs (11680 bytes/sec)
```

f. After downloading all the files, **quit** the FTP command line.

g. Enter the command **dir** and verify the client files are now on **Laptop BR-1**.

Part 2: Use Hashing to Verify File Integrity

In this Part, use the **CSE-LABVM** to hash the contents of the files you downloaded. You will then compare the new hash to the old hash to see if the data has changed. Any files that have changed since they were archived will be sent to Sally so that she can investigate the changes at a later time.

Step 1: Check the hashes on the client files on Mike's PC.

a. Close the **Command Prompt**, and then click **Text Editor**.

b. Click **File** > **Open**, select first document **NEclients.txt**, and then click **OK**.

c. Copy the entire text document content.

d. Open the **CSE-LABVM**.

e. Double click the **Terminal** icon to open a terminal window.

f. Use the **echo -n '**file-contents**' | md5 sum** command to create a hash to validate the data in the **NEclients.txt** file. Paste you clipboard content between the single quotes.

```
cisco@labvm:~$ echo -n 'file-contents' | md5sum
```

g. Compare the hash value created here with the hash values you copied to the text document earlier.

Are the two hash values for **NEclients.txt** the same?

h. Hash the contents of the remaining five files until one of the values does not match the computed hash.

Which file has been tampered with and has an incorrect hash?

Step 2: Escalate the cyber attack to Mike's supervisor, Sally.

a. Return to Packet Tracer and close the **Text Editor**.

b. Click **Email**, and then **Compose**. Write an email and send it to **sally@branch.corp** to tell her that the file server has been hacked.

Step 3: Download the suspected file to Sally's PC.

a. Navigate to the **HQ** site, and then click **HQ-Laptop-1**.

b. Click **Desktop** tab > **Command Prompt**, and then enter **ftp hq.corp** to connect to the **HQ FTP Server**.

c. Enter the username of **sally** and a password of **cisco321**.

d. At the **ftp>** prompt, enter the **dir** command to view the current files stored on the remote **HQ FTP Server**.

e. Download the file that was found to have been tampered with in Part 3 Step 1.

f. At the **ftp>** prompt, enter the command **quit**.

g. At the **C:\>** prompt, enter the command **dir** and verify the tampered client file is now on **HQ-Laptop-1** for analysis by Sally in the future.

Part 3: Use HMAC to Verify File Integrity

Bob is the CFO for a small business and keeps track of all the finances. In this Part, you will compute and verify a hash-based message authentication code (HMAC) of a critical file to ensure that it is the same data since the last time the file was used. HMAC requires a secret key before file integrity can be validated.

a. Click Bob's laptop, which is **HQ-Laptop-2**.

b. Click the **Desktop** tab > **Command Prompt**, and then enter the **dir** command and verify the critical file named **income.txt** is on the laptop. Close the command prompt window when done.

c. Click **Text Editor**, and then **File** > **Open**.

d. Select the document **income.txt** and click **OK**.

e. Select and copy all the document contents.

f. In the **CSE-LABVM**, click the **Menu** button, and then click **Text Editor Pluma**. Click **Edit** and click **Paste**.

g. Click **File** and click **Save**. Save the file with the name **income.txt**. Close the file.

h. In a terminal window in the **CSE-LABVM** VM, use the following command to create an HMAC for the file **income.txt**. The secret key is **cisco123**.

```
cisco@labvm:~$ openssl dgst -sha256 -hmac cisco123 income.txt
```

What is the computed HMAC for the contents of the file?

How is using HMAC more secure than general hashing?

Does the HMAC hash for the **income.txt** file match the original hash you copied to the text file on the **CSE-LABVM**?

Answer Key

Part 1: Recover Files after a Cyber Attack

Step 1: Access the BR Server from Mike's PC.

Step 2: Copy the hash values from the last time the files were archived.

Step 3: Download the backup files to Mike's PC.

Part 2: Use Hashing to Verify File Integrity

Step 1: Check the hashes on the client files on Mike's PC.

Are the two hash values for **NEclients.txt** the same?

Yes

Which file has been tampered with and has an incorrect hash?

SEclients.txt

Step 2: Escalate the cyber attack to Mike's supervisor, Sally.

Step 3: Download the suspected file to Sally's PC.

Part 3: Use HMAC to Verify File Integrity

What is the computed HMAC for the contents of the file?

b138706cb55787d2a01934b224edad32203f87470ff6c7ffb9bd126786d1830d

How is using HMAC more secure than general hashing?

To produce a specific hash, you need both the original message and a secret key.

Does the HMAC hash for the **income.txt** file match the original hash you copied to the text file on the **CSE-LABVM**?

Yes