

File and Data Integrity Checks

Objectives

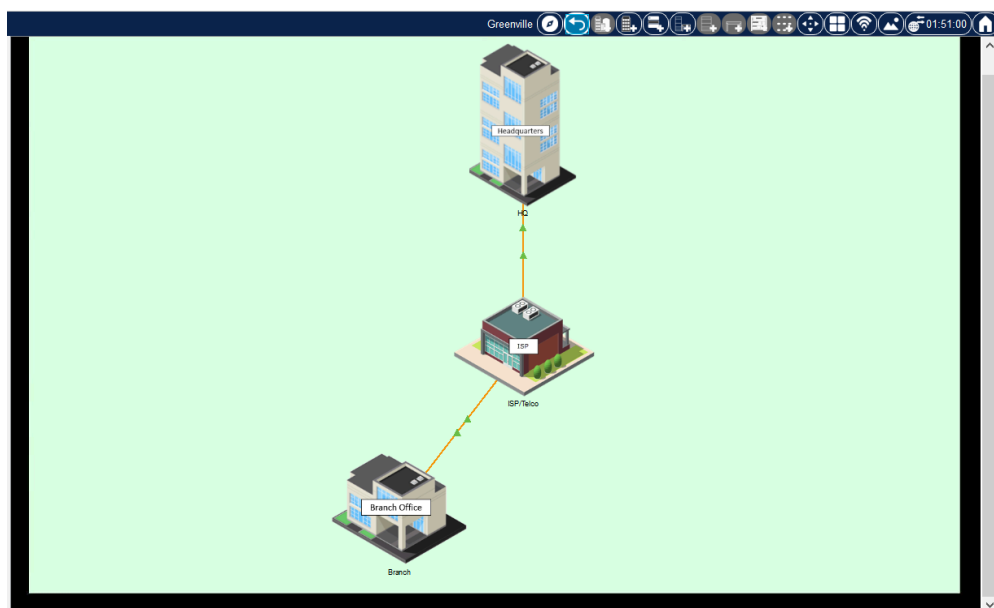
Part 1: Recover Files after a Cyber Attack

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

- Cisco Packet Tracer
- CSE-LABVM installed in VirtualBox

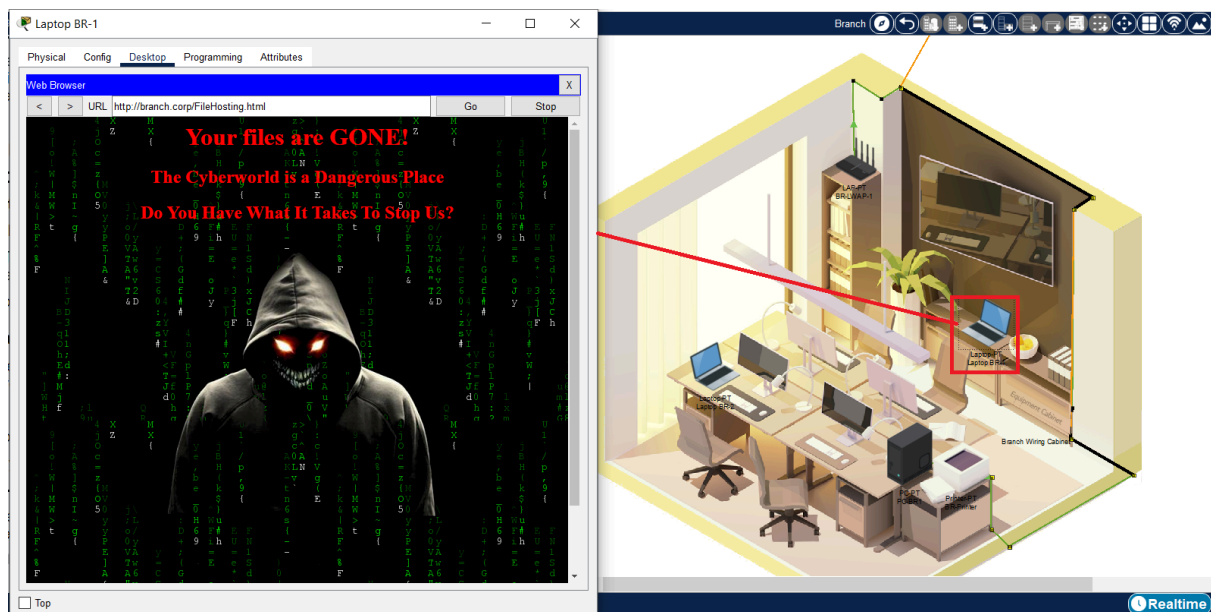
Instructions

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.

- Click Branch Office and then click Laptop BR-1.
- Click the Desktop tab and then click Web Browser.
- Enter the URL `http://branch.corp` and click Go.
- Click the link to download the most current files.

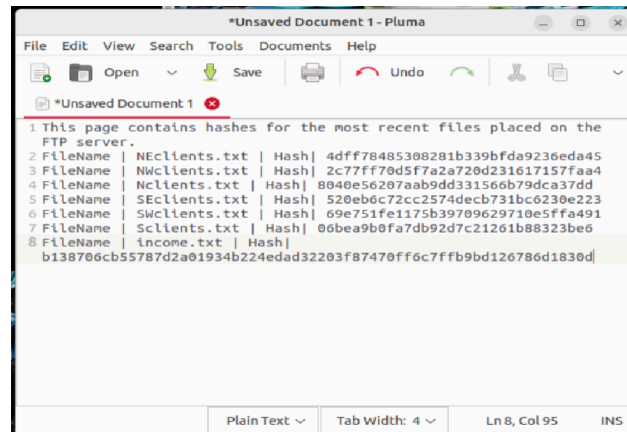


Step 2: Copy the hash values from the last time the files were archived.

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.

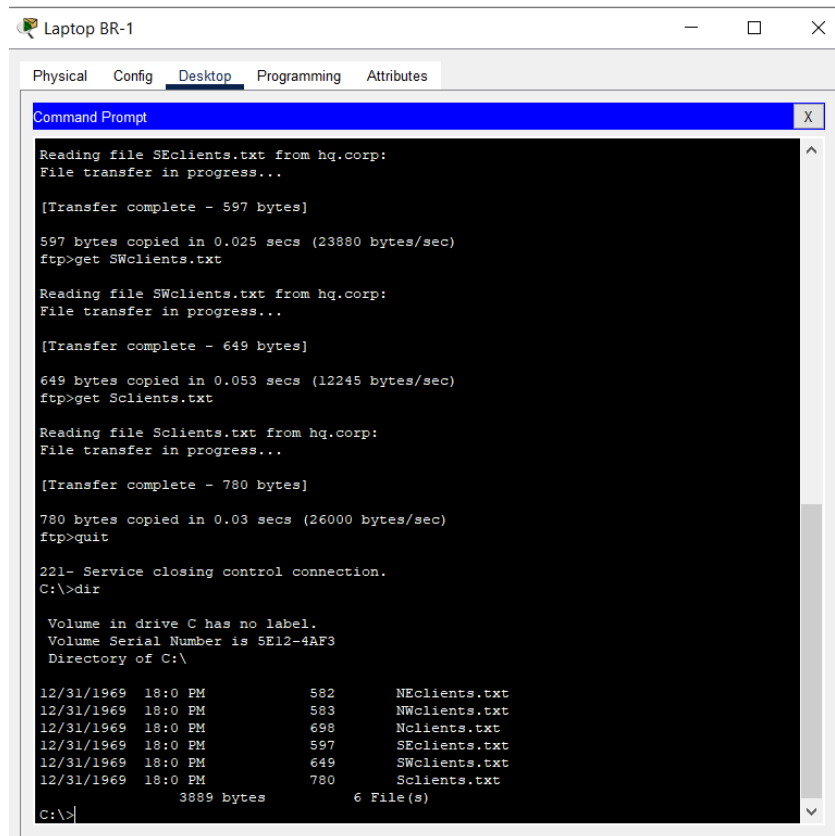
- Enter the URL `http://hq.corp` and click Go.
- Click the link to view the most recent files and their hashes.

- 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 on 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.
- 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.



```
Laptop BR-1
Physical Config Desktop Programming Attributes
Command Prompt
Reading file SEclients.txt from hq.corp:
File transfer in progress...

[Transfer complete - 597 bytes]

597 bytes copied in 0.025 secs (23880 bytes/sec)
ftp>get SWclients.txt

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

[Transfer complete - 649 bytes]

649 bytes copied in 0.053 secs (12245 bytes/sec)
ftp>get Sclients.txt

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

[Transfer complete - 780 bytes]

780 bytes copied in 0.03 secs (26000 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>dir

Volume in drive C has no label.
Volume Serial Number is 5E12-4AF3
Directory of C:\

12/31/1969  18:0 PM             582      NEclients.txt
12/31/1969  18:0 PM             583      NWclients.txt
12/31/1969  18:0 PM             698      Nclients.txt
12/31/1969  18:0 PM             597      SEclients.txt
12/31/1969  18:0 PM             649      SWclients.txt
12/31/1969  18:0 PM             780      Sclients.txt
               3889 bytes          6 File(s)

C:\>
```

Part 2: Use Hashing to Verify File Integrity

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.

- Close the Command Prompt, and then click Text Editor.
- Click File > Open, select first document NEclients.txt, and then click OK.
- Copy the entire text document content.
- Open the CSE-LABVM.
- Double click the Terminal icon to open a terminal window.
- Use the `echo -n '<file-content>' | md5sum` command to create a hash to validate the data in the NEclients.txt file.
- 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?

R: Yes

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?

R: NEclients.txt, Nclients.txt, SEclients.txt, SWclients.txt have incorrect hashes.

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 files that were 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 files are now on HQ-Laptop-1 for analysis by Sally in the future.

```
HQ-Laptop-1
Physical Config Desktop Programming Attributes
Command Prompt
Reading file NWclients.txt from hq.corp:
File transfer in progress...

[Transfer complete - 583 bytes]

583 bytes copied in 0.064 secs (9109 bytes/sec)
ftp>get Nclients.txt

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

[Transfer complete - 698 bytes]

698 bytes copied in 0.014 secs (49857 bytes/sec)
ftp>get SEclients.txt

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

[Transfer complete - 597 bytes]

597 bytes copied in 0.05 secs (11940 bytes/sec)
ftp>get SWclients.txt

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

[Transfer complete - 649 bytes]

649 bytes copied in 0.027 secs (24037 bytes/sec)
ftp>quit

221- Service closing control connection.
C:\>dir

Volume in drive C has no label.
Volume Serial Number is SE12-4AF3
Directory of C:\

12/31/1969  18:0 PM           583      NWclients.txt
12/31/1969  18:0 PM           698      Nclients.txt
12/31/1969  18:0 PM           597      SEclients.txt
12/31/1969  18:0 PM           649      SWclients.txt
                2527 bytes      4 File(s)

C:\>|
```

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.

- Click Bob's laptop, which is HQ-Laptop-2.
- 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.
- Click Text Editor, and then File > Open.
- Select the document `income.txt` and click OK.
- Select and copy all the document contents.
- In the CSE-LABVM, click the Menu button, and then click Text Editor Pluma. Click Edit and click Paste.
- 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?

R: HMAC-SHA2-256(income.txt)=
`b138706cb55787d2a01934b224edad32203f87470ff6c7ffb9bd126786d1830d`

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

R: Yes