Packet Tracer – Using File and Data Integrity Checks

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3 http://www.cisco.corp	255.255.255.0	Metropolis Bank HQ
Backup File Server	N/A	209.165.201.10 https://www.cisco2.corp	255.255.255.248	Internet
Mike	10.44.2.101	N/A	255.255.255.0	Healthcare at Home
Sally	10.44.1.2	N/A	255.255.255.0	Metropolis Bank HQ
Bob	10.44.1.3	N/A	255.255.255.0	Metropolis Bank HQ

Objectives

Part 1: Download the Client Files to Mike's PC

Part 2: Download the Client Files from the Backup File Server to Mike's PC

Part 3: Verify the Integrity of the Client Files using Hashing

Part 4: Verify the Integrity of Critical Files using HMAC

Background

In this 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 for further analysis. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to verify and transfer any suspect files.

Part 1: Download the Client Files to Mike's PC

Step 1: Access the FTP server from Mike's PC.

a. Click the **Gotham Healthcare Branch** site and then click the PC **Mike**.

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

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

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

What protocol was used to access this webpage on the backup file server?

Step 2: The file server has been hacked, notify Sally.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Email**.

c. Create an email and send it to Sally@cisco.corp and tell her about the File Server.

Part 2: Download the Client Files from the Backup File Server to Mike's PC

Step 1: Access the offsite FTP server from Mike's PC.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

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

c. Enter the URL **https://www.cisco2.corp** and click **Go**.

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

What protocol was used to access this webpage on the backup file server?

What are the file names and hashes of the client files on the backup server? (copy and paste them below)

Step 2: Download the client files to Mike's PC.

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.

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

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

f. Download the six client files (NEclients.txt, NWclients.txt, Nclients.txt, SEclients.txt, SWclients.txt, and Sclients.txt) to Mike's PC by entering the command **get FILENAME.txt**, replace FILENAME with one of the six client filenames.

```
ftp> get NEclients.txt

Reading file NEclients.txt from www.cisco2.corp:
File transfer in progress...

[Transfer complete - 584 bytes]

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

g. After downloading all the files, enter the command **quit** at the **ftp>** prompt.

h. At the **PC>** prompt, enter the command **dir** and verify the client files are now on Mike's PC.

Part 3: Verify the Integrity of the Client Files using Hashing

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

a. Within the **Gotham Healthcare Branch** site, click the PC **Mike**.

b. Click the **Desktop** tab and then click **Text Editor**.

c. In the Text Editor window, click **File** > **Open**.

d. Click on the first document **NEclients.txt** and click **OK**.

e. Copy the entire text document contents.

f. Open a web browser on your personal computer and browse to the website https://www.tools4noobs.com/online_tools/hash/

g. Click the whitespace and paste in the text document contents. Make sure the algorithm is set to md2. Click **Hash this!**.

h. To make sure a file has not been tampered with, you will compare the resulting hash with the filename/hash information you found in Part 2 Step 1.

i. Repeat Steps d through h for each client file and compare the generated hash with the original hash shown in Part 2 Step 1.

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

Step 2: Download the suspected file to Sally's PC.

a. Click the **Metropolis Bank HQ** site, and then click the PC **Sally**.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.

d. Enter the username of **sally** and a password of **cisco123**.

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

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

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

h. At the **PC>** prompt, enter the command **dir** and verify the tampered client file is now on Sally's PC for analysis at a later time.

Part 4: Verify the Integrity of Critical Files using HMAC

Step 1: Compute the HMAC of a critical file.

a. Within the **Metropolis Bank HQ** site, click the PC **Bob**.

b. Click the **Desktop** tab and then click **Command Prompt**.

c. At the **PC>** prompt, enter the command **dir** and verify the critical file named **income.txt** is on Bob's PC.

d. Within the **Desktop** tab, click **Text Editor**.

e. In the Text Editor window, click **File** > **Open**.

f. Click the document **income.txt** and click **OK**.

g. Copy the entire text document contents.

h. Open a web browser on your personal computer and browse to the website http://www.freeformatter.com/hmac-generator.html

i. Click the whitespace and paste in the text document contents. Enter the secret key of **cisco123**. Make sure the algorithm is set to **SHA1**. Click **Compute HMAC**.

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

How is using HMAC more secure than general hashing?

Step 2: Verify the computed HMAC.

a. Within the **Metropolis Bank HQ** site, click the PC **Bob**.

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

c. Enter the URL **https://www.cisco2.corp** and click **Go**.

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

Does the HMAC hash for the income.txt file match?

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Download the client files to Mike's PC	Step 1	2	
Part 2: Download the client files from the backup file server to Mike's PC	Step 1	2	
	Step 1	6	
Part 3: Verify the integrity of the client files using hashing	Step 1	5	
Part 4: Verify the integrity of critical files using HMAC	Step 1	5	
	Step 1	5	
	Step 2	5	
Questions		**30**	
Packet Tracer Score		**70**	
Total Score		**100**	