

# Packet Tracer – Using File and Data Integrity Checks, Rymbayeva Anelya, 20B030299

## Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3 <a href="http://www.cisco.corp">http://www.cisco.corp</a>	255.255.255.0	Metropolis Bank HQ
Backup File Server	N/A	209.165.201.10 <a href="https://www.cisco2.corp">https://www.cisco2.corp</a>	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**

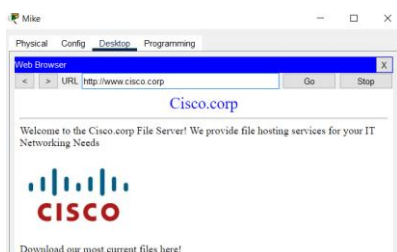
## Background

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.

- Click the **Gotham Healthcare Branch** site and then click the PC **Mike**.
- Click the **Desktop** tab and then click **Web Browser**.
- Enter the URL **<http://www.cisco.corp>** and click **Go**.
- Click the link to download the most current files.





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

**HTTP**

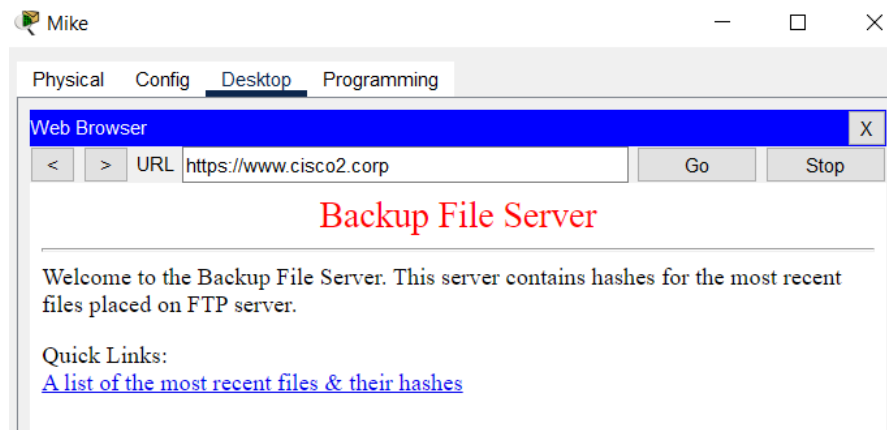
## Step 2: The file server has been hacked, notify Sally.

- Within the **Gotham Healthcare Branch** site, click the PC **Mike**.
- Click the **Desktop** tab and then click **Email**.
- Create an email and send it to [Sally@cisco.corp](mailto: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

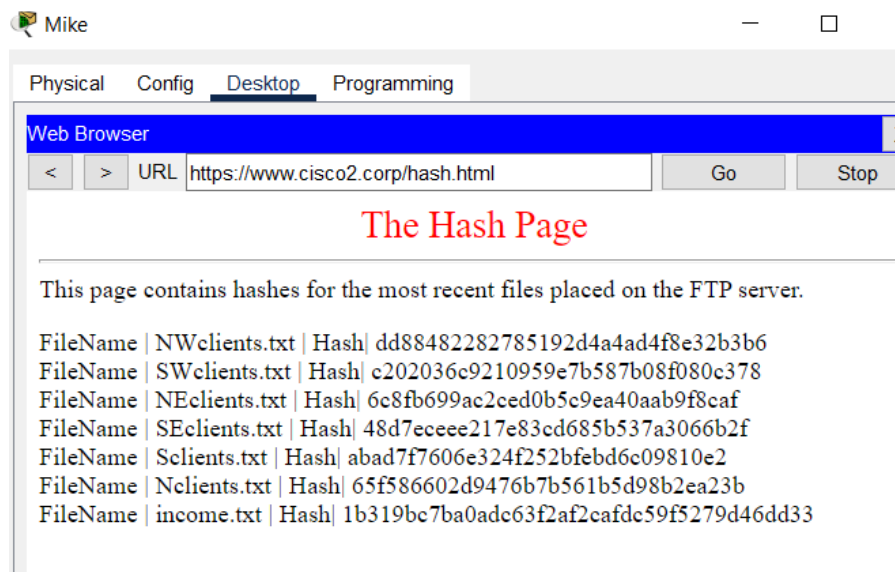
### Step 1: Access the offsite FTP server from Mike's PC.

- Within the **Gotham Healthcare Branch** site, click the **PC Mike**.
- Click the **Desktop** tab and then click **Web Browser**.
- Enter the URL **https://www.cisco2.corp** and click **Go**.
- 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? **HTTPS(secured)**

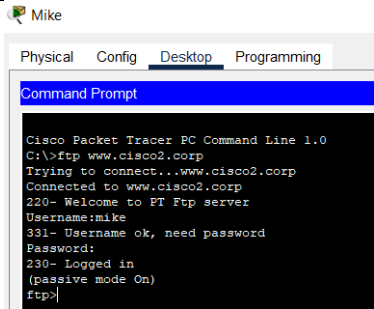
What are the file names and hashes of the client files on the backup server? (copy and paste them below)



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

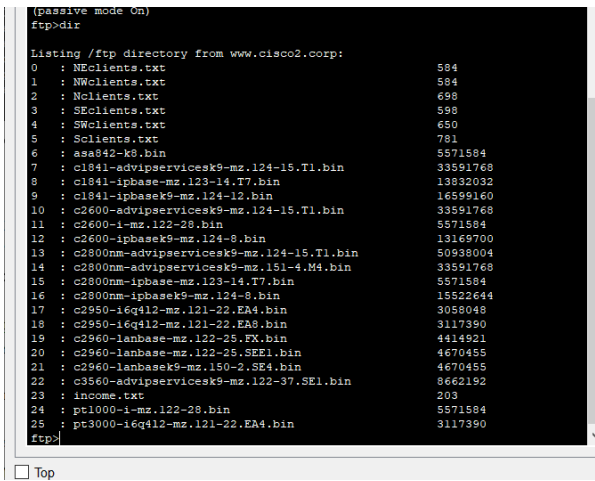
- Within the **Gotham Healthcare Branch** site, click the **PC Mike**.
- Click the **Desktop** tab and then click **Command Prompt**.
- Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.
- Enter the username of **mike** and a password of **cisco123**.

## Packet Tracer – Using File and Data Integrity Checks



```
Mike
Physical Config Desktop Programming
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp www.cisco2.corp
Trying to connect...www.cisco2.corp
Connected to www.cisco2.corp
220- Welcome to PT Ftp server
Username:mike
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

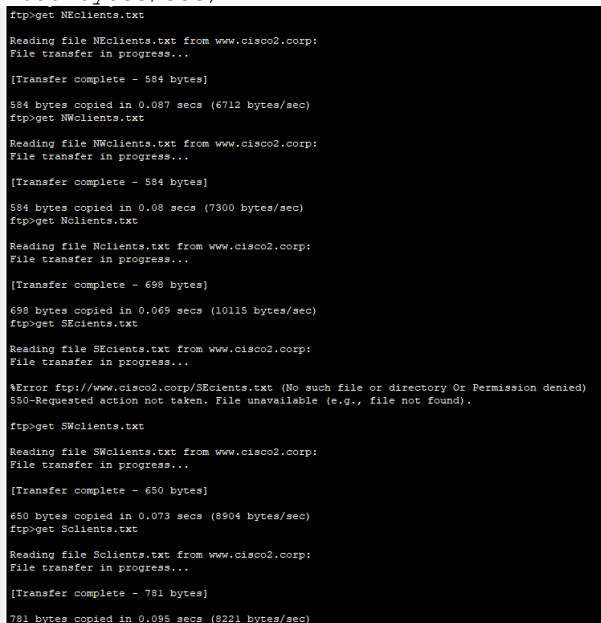
- e. At the **ftp>** prompt, enter the command **dir** to view the current files stored on the remote FTP server.



```
(passive mode On)
ftp>dir
Listing /ftp directory from www.cisco2.corp:
 0 : NEclients.txt                584
 1 : NWclients.txt                584
 2 : Nclients.txt                 698
 3 : SEclients.txt                 650
 4 : SWclients.txt                 781
 5 : Sclients.txt                 781
 6 : asa842-k8.bin                5571584
 7 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 8 : c1841-ibase-mz.123-14.T7.bin 13832032
 9 : c1841-ibasek9-mz.124-12.bin 16599160
10 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
11 : c2600-i-mz.122-28.bin        5571584
12 : c2600-ibasek9-mz.124-8.bin 13169700
13 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
14 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
15 : c2800nm-ibase-mz.123-14.T7.bin 5571584
16 : c2800nm-ibasek9-mz.124-8.bin 15522644
17 : c2950-16q412-mz.121-22.EA4.bin 3058048
18 : c2950-16q412-mz.121-22.EA8.bin 3117390
19 : c2960-lanbase-mz.122-35.FX.bin 4414921
20 : c2960-lanbase-mz.122-35.S2E1.bin 4670455
21 : c2960-lanbasek9-mz.150-2.SF4.bin 4670455
22 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
23 : income.txt                  203
24 : pt1000-i-mz.122-28.bin      5571584
25 : pt3000-16q412-mz.121-22.EA4.bin 3117390
ftp>
```

- 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)
```



```
ftp>get NEclients.txt
Reading file NEclients.txt from www.cisco2.corp:
File transfer in progress...
[Transfer complete - 584 bytes]
584 bytes copied in 0.087 secs (6712 bytes/sec)
ftp>get NWclients.txt
Reading file NWclients.txt from www.cisco2.corp:
File transfer in progress...
[Transfer complete - 584 bytes]
584 bytes copied in 0.08 secs (7300 bytes/sec)
ftp>get Nclients.txt
Reading file Nclients.txt from www.cisco2.corp:
File transfer in progress...
[Transfer complete - 698 bytes]
698 bytes copied in 0.069 secs (10115 bytes/sec)
ftp>get SEclients.txt
Reading file SEclients.txt from www.cisco2.corp:
File transfer in progress...
!Error ftp://www.cisco2.corp/SEclients.txt (No such file or directory Or Permission denied)
550-Requested action not taken. File unavailable (e.g., file not found).
ftp>get SWclients.txt
Reading file SWclients.txt from www.cisco2.corp:
File transfer in progress...
[Transfer complete - 650 bytes]
650 bytes copied in 0.073 secs (8904 bytes/sec)
ftp>get Sclients.txt
Reading file Sclients.txt from www.cisco2.corp:
File transfer in progress...
[Transfer complete - 781 bytes]
781 bytes copied in 0.095 secs (8221 bytes/sec)
```

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

## Packet Tracer – Using File and Data Integrity Checks

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

```
C:\>dir

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

1/1/1970    6:0 PM                584      NEclients.txt
1/1/1970    6:0 PM                584      NWclients.txt
1/1/1970    6:0 PM                698      Nclients.txt
1/1/1970    6:0 PM                650      SWclients.txt
1/1/1970    6:0 PM                781      Sclients.txt
2/7/2106    12:28 PM               26      sampleFile.txt
               3323 bytes           6 File(s)
```

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

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

- Within the **Gotham Healthcare Branch** site, click the PC **Mike**.
- Click the **Desktop** tab and then click **Text Editor**.
- In the Text Editor window, click **File > Open**.
- Click on the first document **NEclients.txt** and click **OK**.
- Copy the entire text document contents.
- Open a web browser on your personal computer and browse to the website [https://www.tools4noobs.com/online\\_tools/hash/](https://www.tools4noobs.com/online_tools/hash/)
- Click the whitespace and paste in the text document contents. Make sure the algorithm is set to md2. Click **Hash this!**.

Filename: C:\Users\mike\Documents\NEclients.txt

Rhannon B. Langley|46872|fermentum@cursusnon.co.uk|9781  
Nigel Ward|3584|convallis.erat.eget@luctusvulputatenisi.org|4896  
Alvin Farley|69508|lectus@volutpat.co.uk|5358  
Clark U. Pratt|23441|tincidunt.neque@nisi.co.uk|9273  
Robin Randall|10108|faucibus.lectus.a@nonarcu.net|4232  
Stacey L. Kirby|Y4B 8Z5|euismod.enim@mauris.org|4200  
Joan Pearson|1867VB|convallis.erat@accumsannequeet.net|5002  
Herman Lambert|09774|vitae.velit.egestas@tinciduntaliquamarcu.com|1220  
Quentin Blankenship|48315-746|augue@consequat.edu|3387

Algorithm:

**Result:** 6c8fb699ac2ced0b5c9ea40aab9f8caf

- 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.
- 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?

**SEclients.txt**

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

- Click the **Metropolis Bank HQ** site, and then click the PC **Sally**.
- Click the **Desktop** tab and then click **Command Prompt**.
- Connect to the **Backup File** server by entering **ftp www.cisco2.corp** in the command prompt.
- Enter the username of **sally** and a password of **cisco123**.

## Packet Tracer – Using File and Data Integrity Checks

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

```
ftp>dir
Listing /ftp directory from www.cisco2.corp:
 0 : NEclients.txt                584
 1 : NWclients.txt                584
 2 : Nclients.txt                698
 3 : SEclients.txt                598
 4 : SWclients.txt                650
 5 : Sclients.txt                781
 6 : asa842-k8.bin               5571584
 7 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 8 : c1841-ipbase-mz.123-14.T7.bin 13832032
 9 : c1841-ipbasek9-mz.124-12.bin 16599160
10 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
11 : c2600-i-mz.122-28.bin        5571584
12 : c2600-ipbasek9-mz.124-8.bin  13169700
13 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
14 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
15 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
16 : c2800nm-ipbasek9-mz.124-8.bin 15522644
17 : c2950-i6q412-mz.121-22.EA4.bin 3058048
18 : c2950-i6q412-mz.121-22.EA8.bin 3117390
19 : c2960-lanbase-mz.122-25.FX.bin 4414921
20 : c2960-lanbase-mz.122-25.SEE1.bin 4670455
21 : c2960-lanbasek9-mz.150-2.SE4.bin 4670455
22 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
23 : income.txt                  203
24 : pt1000-i-mz.122-28.bin       5571584
25 : pt3000-i6q412-mz.121-22.EA4.bin 3117390
ftp>
```

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

```
25 : pt3000-i6q412-mz.121-22.EA4.bin
ftp>get SEclients.txt

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

[Transfer complete - 598 bytes]

598 bytes copied in 0.101 secs (5920 bytes/sec)
ftp>
```

- 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.

```
C:\>dir

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

1/1/1970    6:0 PM                598      SEclients.txt
              598 bytes              1 File(s)
C:\>
```

## Part 4: Verify the Integrity of Critical Files using HMAC

### Step 1: Compute the HMAC of a critical file.

- Within the **Metropolis Bank HQ** site, click the PC **Bob**.
- Click the **Desktop** tab and then click **Command Prompt**.
- At the **PC>** prompt, enter the command **dir** and verify the critical file named **income.txt** is on Bob's PC.

## Packet Tracer – Using File and Data Integrity Checks

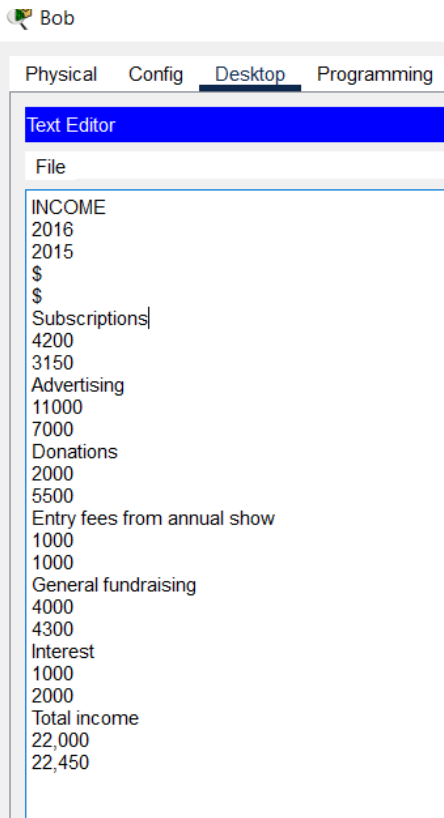
```
Cisco Packet Tracer PC Command Line 1.0
C:\>dir

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

1/1/1970    6:0 PM             701      clientinfo.txt
1/1/1970    6:0 PM             203      income.txt
2/7/2106    12:28 PM           26       sampleFile.txt
               930 bytes              3 File(s)

C:\>
```

- 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?

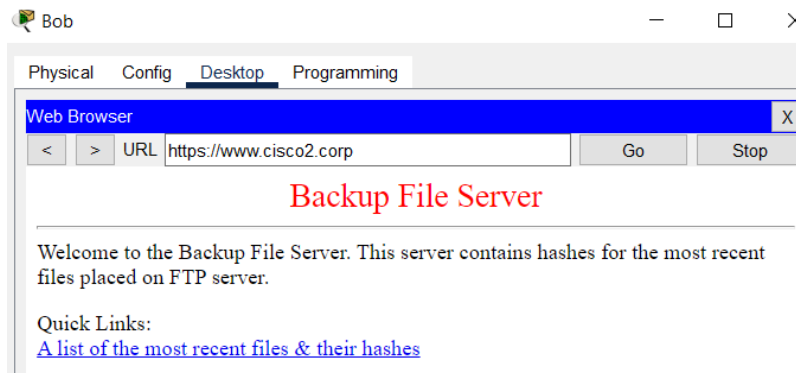
```
1b319bc7ba0adc63f2af2cafdc59f5279d46dd33
```

## How is using HMAC more secure than general hashing?

Need both the original message and a secret key.

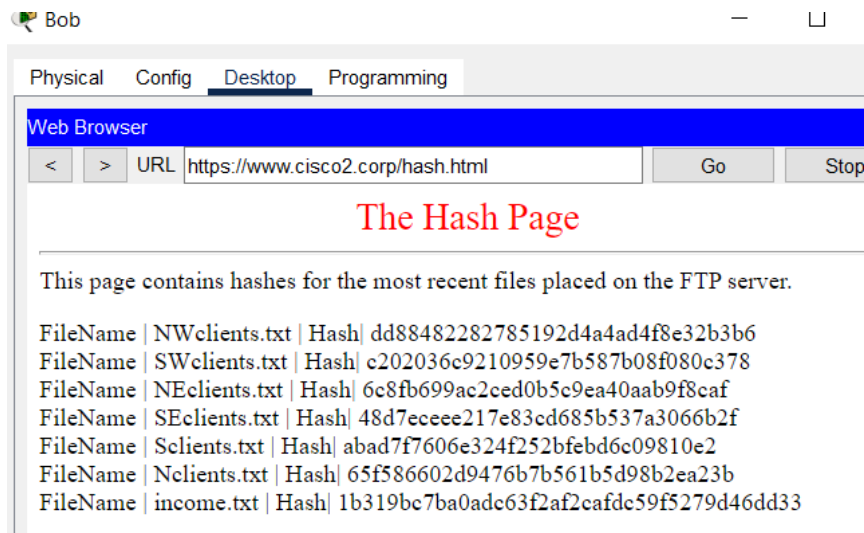
## Step 2: Verify the computed HMAC.

- Within the **Metropolis Bank HQ** site, click the **PC Bob**.
- Click the **Desktop** tab and then click **Web Browser**.
- 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 Results

Time Elapsed: 00:31:50

Congratulations Anelya! You completed the activity.

Overall Feedback

Assessment Items

Connectivity Tests

Expand/Collapse All

Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
<div>Network</div> <div> <div>Mike</div> <div>Files</div> <div> <div>C Directory</div> <div> <div>✓ Nclients.txt Correct</div> <div>✓ NEclients.txt Correct</div> <div>✓ NWclients.txt Correct</div> <div>✓ Sclients.txt Correct</div> <div>✓ SEclients.txt Correct</div> <div>✓ SWclients.txt Correct</div> </div> </div> </div>				
<div>Sally</div> <div>Files</div> <div> <div>C Directory</div> <div> <div>✓ SEclients.txt Correct</div> </div> </div>				

Score

: 70/70

Item Count

: 7/7

Component	Items/Total	Score
lp	7/7	70/70



## Packet Tracer – Using File and Data Integrity Checks

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	
<b>Questions</b>		<b>30</b>	
<b>Packet Tracer Score</b>		<b>70</b>	
<b>Total Score</b>		<b>100</b>	