Cisco | Networking Academy®
Mind Wide Open™

Cybersecurity Essentials v1.0

Instructor Packet Tracer Manual

Packet Tracer – Creating a Cyber World (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	255.255.255.0	Metropolis Bank HQ
Email/DNS Server	10.44.1.253	255.255.255.0	Metropolis Bank HQ
NTP/AAA Server	10.44.1.252	255.255.255.0	Metropolis Bank HQ
File Backup Server	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Objectives

Part 1: Configure the FTP Server

Part 2: Configure the Web Server

Part 3: Configure the Email Server

Part 4: Configure the DNS Server

Part 5: Configure the NTP Server

Part 6: Configure the AAA Server

Background / Scenario

In this activity, you will configure basic server components. The IP addressing configuration is already complete. You will use the Services tab on multiple servers to deploy FTP, Web, Email, DNS, NTP, and AAA services.

Part 1: Configure the FTP Server

Step 1: Activate the FTP Service.

a. Click the **Metropolis Bank HQ** and then click the **FTP/Web** server.

b. Click the **Services** tab and then click **FTP**.

c. Turn on the FTP service using the radial button at the top.

Step 2: Allow users' access to the FTP server.

a. Create user account names of **bob**, **mary**, and **mike**, each with the password of **cisco123**.

b. Each user account should have full permissions (RWDNL) on the FTP/Web server.

Part 2: Configure the Web Server

Step 1: Activate the HTTP Service.

a. Within the **Metropolis Bank HQ**, click the **FTP/Web** server.

b. Click the **Services** tab and then click **HTTP**.

c. Turn on both the HTTP and HTTPS services using the radial buttons at the top.

Step 2: Verify the HTTP Service.

a. Click the PC named Sally, and click the **Desktop** tab.

b. Click the **Web Browser**. Browse to the website **www.cisco.corp**.

c. Within the Web Browser, browse to the IP **10.44.1.254**.

Why would a user be able to browse to an IP address but not a FQDN?

____

____

The web browser does not know IP address without DNS to translate the domain name to the IP address.

Part 3: Configure the DNS Server

Step 1: Activate the DNS Service.

a. Within the **Metropolis Bank HQ**, click the **Email/DNS** server.

b. Click the **Services** tab and then click **DNS**.

c. Turn on the DNS service using the radial button at the top.

Step 2: Create the DNS A records.

a. Create the **A** record **email.cisco.corp** with IP address **10.44.1.253**. Click **Add** to save the record.

b. Create the **A** record **www.cisco.corp** with IP address **10.44.1.254**. Click **Add** to save the record.

Step 3: Verify the DNS Service.

a. Click the PC named Sally, and click the **Desktop** tab.

b. Click the **Web Browser**. Browse to the website **www.cisco.corp**.

Why is the user able to browse to an FQDN?

____

____

The DNS server translated the domain name to the associated IP address so the web browser can understand it.

Part 4: Configure the Email Server

Step 1: Activate the Email Services.

a. Within the **Metropolis Bank HQ**, click the **Email/DNS** server.

b. Click the **Services** tab and then click on **EMAIL**.

c. Turn on both the SMTP and POP3 services using the radial buttons at the top.

Step 2: Create Email accounts for users.

a. Create the domain name of **cisco.corp**.

b. Create user account names of **phil**, **sally**, **bob**, **dave**, **mary**, **tim** and **mike,** each with the password of **cisco123**.

Step 3: Configure user Email clients.

a. Click the PC named **Sally**, and click the **Desktop** tab.

b. Click **Email** and enter the following information:

   Name: **Sally**

   Email Address: **sally@cisco.corp**

   Incoming & Outgoing Email Server(s): **email.cisco.corp**

   Username: **sally**

   Password: **cisco123**

c. Repeat Step **3b** on the PC named **Bob** but replace the name **sally** with **bob** as needed.

   Why does the Email service require both SMTP and POP3 to be activated?

   ____

   ____

   SMTP is the protocol responsible for sending emails between servers, and POP is a protocol used by local email clients to retrieve emails from a server.

Part 5: Configure the NTP Server

Step 1: Activate the NTP Service.

a. Within the **Metropolis Bank HQ**, click the **NTP/AAA** server.

b. Click the **Services** tab and then click **NTP**.

c. Turn on the NTP service using the radial button at the top.

Step 2: Secure the NTP Service.

a. Enable the NTP authentication feature using the radial button.

b. Configure **Key 1** with a password of **cisco123**.

Part 6: Configure the AAA Server

Step 1: Activate the AAA Service.

a. Within the **Metropolis Bank HQ**, click the **NTP/AAA** server.

b. Click the **Services** tab and then click **AAA**.

c. Turn on the AAA service using the radial button at the top.

Step 2: Configure the AAA Network Configuration.

a. Configure the Client Name **HQ_Router** with the Client IP **10.44.1.1** with a secret of **cisco123**. Click **Add** to save the client information.

b. Configure the AAA user account of **admin** with a password of **cisco123**. Click **Add** to save the user information.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Configure the Web Server	Step 2	2	
Part 3: Configure the DNS Server	Step 3	2	
Part 4: Configure the Email Server	Step 3	2	
Questions		**6**	
Packet Tracer Score		**94**	
Total Score		**100**	

Packet Tracer – Communicating in a Cyber World (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Email/DNS Server	10.44.1.253	209.165.201.4	255.255.255.0	Metropolis Bank HQ
NTP/AAA Server	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ
File Backup Server	10.44.2.254	N/A	255.255.255.0	Gotham Healthcare Branch

Objectives

Part 1: Send Email between Users

Part 2: Upload and Download Files using FTP

Part 3: Remotely Access an Enterprise Router using Telnet

Part 4: Remotely Access an Enterprise Router using SSH

Background

In this activity, you will communicate across remote networks using common network services. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to connect to both servers and other client devices.

Part 1: Send Email between Users

Step 1: Access the email client on Mike's PC.

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

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

Step 2: Send an email to Sally.

a. Create an email by clicking the **Compose** button.

b. In the **To:** field, enter the email **sally@cisco.corp**

In the **Subject:** field, enter the string of text "**Urgent- Call me**".

In the **Message** section, enter. "**Call me when you are free today to discuss the new sale.**"

c. Click the **Send** button to transmit the email.

What protocol was used to send the email to the email server?

____

STMTP

Step 3: Have Sally check her email.

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

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

c. Click the **Receive** button to retrieve the email sent from Mike.

What protocol was used to retrieve the email from the email server?

____

POP

Part 2: Upload Files using FTP

Step 1: Set the packet sniffer to capture traffic on the correct port.

a. Enter the geographic (root) view to see all three remote sites.

b. Click the **Cyber Criminals Sniffer**.

c. Click **Port1** to capture packets on this port.

d. Leave the **Cyber Criminal Sniffer** open and visible for the rest of this part.

Step 2: Remotely connect to the FTP server.

e. Enter the **Healthcare at Home** site and then click the PC **Mary**.

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

g. Connect to the **FTP/Web** server at **Metropolis Bank HQ** by entering **ftp 209.165.201.3** in the command prompt.

h. Enter the username of **mary** and a password of **cisco123**.

Step 3: Upload a file to the FTP server.

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

b. Mary has a file containing sensitive information regarding new healthcare client information.

Upload the **newclients.txt** file to the FTP server by entering the command **put newclients.txt**.

c. At the **ftp>** prompt, enter the command **dir** and verify the **newclients.txt** file is now on the FTP server.

Why is FTP considered an insecure protocol for moving files?

____

FTP does not provide encryption and all data is sent in clear text.

Step 4: Analyze the FTP traffic.

a. Enter the geographic (root) view to see all three remote sites.

b. Click the **Cyber Criminals Sniffer**.

c. Under the GUI tab on the left, click the 1st FTP packet available to select it. Then scroll down to the bottom of the window displayed on the right.

What information is displayed in clear text from the FTP header?

____

The username used by the client to connect to the FTP server.

d. On the left, click the 2nd FTP packet available to select it. Then scroll down to the bottom of the window displayed on the right. Do this again for the 3rd FTP packet.

e. Besides the username, what other sensitive information is displayed in clear text from the FTP header?

____

The password used by the client to connect to the FTP server.

Part 3: Remotely Access an Enterprise Router Using Telnet

Step 1: Remotely connect to an enterprise router.

a. Enter the **Healthcare at Home** site and then click on the PC **Dave**.

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

c. Ping the enterprise router using the command **ping 209.165.201.2** to verify reachability.

d. Use the command **telnet 209.165.201.2** to telnet to the IP address of the enterprise router.

e. Authenticate to the enterprise router with the username of **admin** and the password of **cisco123**.

f. Use the command **show users** to view the active Telnet connection to the enterprise router.

Why is Telnet considered an insecure protocol for remotely managing a device?

____

Telnet does not provide encryption and all data is sent in clear text.

Part 4: Remotely Access an Enterprise Router Using SSH

Step 1: Remotely connect to an enterprise router.

a. Enter the **Gotham Healthcare Branch** site and then click the PC **Tim**.

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

c. Ping the enterprise router using the command **ping 209.165.201.2** to verify reachability.

d. Use the command **ssh -l admin 209.165.201.2** to SSH to the IP address of the enterprise router.

e. Authenticate to the enterprise router with the password of **cisco123**.

f. Use the command **show users** to view the active SSH connection to the enterprise router.

Why is SSH considered a secure protocol for remotely managing a device?

____

SSH provides encryption and all data is sent in a secure format.

g. Enter the global configuration mode using **configure terminal** command.

h. Create an **enable secret** password of **cisco** with the command **enable secret cisco**.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Send email between users	Step 2	2	
	Step 3	2	
Part 2: Upload and download files using FTP	Step 2	2	
	Step 3d	2	
	Step 3f	2	
Part 3: Remotely access an enterprise router using telnet	Step 1	2	
Part 4: Remotely access an enterprise router using SSH	Step 1	2	
Questions		**14**	
Packet Tracer Score		**86**	
Total Score		**100**	

Packet Tracer – Exploring File and Data Encryption (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
FTP/Web Server	10.44.1.254	209.165.201.3	255.255.255.0	Metropolis Bank HQ
Mary	10.44.3.101	N/A	255.255.255.0	Healthcare at Home
Bob	10.44.1.3	N/A	255.255.255.0	Metropolis Bank HQ

Objectives

Part 1: Locate the FTP Account Credentials for Mary's Laptop

Part 2: Upload Confidential Data using FTP

Part 3: Locate the FTP Account Credentials for Bob's PC

Part 4: Download Confidential Data using FTP

Part 5: Decrypt the Contents of the clientinfo.txt File

Background

In this activity, you will access the encrypted contents of multiple files and transfer a file across the Internet to a centralized FTP server. Another user will then download the file from the FTP server and decrypt the files' contents. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to transfer a file with encrypted data to another device.

Part 1: Locate the FTP Account Credentials for Mary's Laptop

Step 1: Access the text document on Mary's laptop.

a. Click the **Healthcare at Home** site and then click the laptop **Mary**.

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

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

d. Click the document **ftplogin.txt** and click **OK**.

Step 2: Decrypt Mary's FTP account information.

a. Highlight all the text from the **ftplogin.txt** file and copy it.

b. Open a web browser on your personal computer and browse to the website https://encipher.it

c. Click the **whitespace on the right of the website and paste in the encrypted text**.

Click the **Decipher It** button and use the decryption password **maryftp123** to decrypt the encrypted text. Click **Decrypt**.

What is the username and password for Mary’s FTP account?

____

username: mary password: cisco321

Part 2: Upload Confidential Data using FTP

Step 1: View the confidential document on Mary’s Laptop.

a. Click the **Healthcare at Home** site and then click the Laptop **Mary**.

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

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

d. Click on the document **clientinfo**.txt and click **OK**.

What form is the data in?

____

Encrypted form

Step 2: Remotely connect to the FTP server.

a. Within the **Healthcare at Home** site, click the Laptop **Mary**.

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

c. Connect to the **FTP/Web** server at **Metropolis Bank HQ** by entering **ftp 209.165.201.3** in the command prompt.

d. Enter the username/password credentials located in Part 1 Step 2

Step 3: Upload a file to the FTP server.

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

b. Mary has a file containing encrypted healthcare client information. Upload the **clientinfo.txt** file to the FTP server by entering the command **put clientinfo.txt**.

c. At the **ftp>** prompt, enter the command **dir** and verify the **clientinfo.txt** file is now on the FTP server.

If cyber criminals were to capture the file transfer crossing the Internet, what would be in clear text?

____

The username: mary password: cisco321 for the FTP connection are in clear text but the contents of the document are encrypted.

Part 3: Locate the FTP Account Credentials for Bob’s PC

Step 1: Access the text document on Bob’s PC.

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

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

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

d. Click the document **ftplogin.txt** and click **OK**.

Step 2: Decrypt Bob’s FTP account information.

a. Highlight all the text from **ftplogin.txt** file and copy it.

b. Open a web browser on your personal computer and browse to the website https://encipher.it

c. Click the **whitespace on the right of the website and paste in the encrypted text.**

d. Click **Decipher It** button and use the decryption password **bobftp123** to decrypt the encrypted text. Click **Decrypt**.

What is the username and password for Bob’s FTP account?

____

username: bob   password: ninja123

Part 4: Download Confidential Data using FTP

Step 1: Remotely connect to the FTP server.

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

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

c. Connect to the **FTP/Web** server within the **Metropolis Bank HQ** by entering **ftp 10.44.1.254** in the command prompt.

d. Enter the username/password credentials located in Part 3 Step 2

Step 2: Download the file to Bob’s PC.

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

b. Mary had uploaded the clientinfo.txt file containing encrypted healthcare client information.

Download the **clientinfo.txt** file to Bob’s PC by entering the command **get clientinfo.txt**.

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

d. At the **PC>** prompt, enter the command **dir** and verify the **clientinfo.txt** file is now Bob’s PC.

If cyber criminals were to capture the file transfer crossing the Internet, what would be in clear text?

____

The username: bob   password: ninja123 for the FTP connection are in clear text but the contents of the document are encrypted.

Part 5: Decrypt the Contents of the clientinfo.txt File

Step 1: Receive the decryption key from Mary.

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

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

c. In the Email window, click **Receive**.

d. Click on the Email with the subject “Decryption Key” and record the decryption key below.

What is the decryption key to access the confidential information in the clientinfo.txt file?

____

cisco123

Step 2: Decrypt the contents of the clientinfo.txt file.

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

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

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

d. Click the document **clientinfo.txt** and click **OK**.

e. Highlight all the text from the **clientinfo.txt** file and copy it.

f. Open a web browser on your personal computer and browse to the website https://encipher.it

g. Click the **whitespace on the right of the website and paste in the encrypted text**.

Click **Decipher It** button and use the decryption password from Mary's email to decrypt the encrypted text. Click **Decrypt**.

What is the first account name in the clientinfo.txt file?

____

Plato X. Riggs

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Locate the FTP account credentials for Mary's laptop	Step 2	2	
Part 2: Upload confidential data using FTP	Step 1	2	
	Step 3	2	
Part 3: Locate the FTP account credentials for Bob's PC	Step 2	2	
Part 4: Download confidential data using FTP	Step 2	2	
Part 5: Decrypt the contents of the clientinfo.txt file	Step 1	2	
	Step 2	2	
	Questions	**14**	
	Packet Tracer Score	**86**	
	Total Score	**100**	

Packet Tracer – Using File and Data Integrity Checks (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

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? ____________________ HTTP

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? ____________________
HTTPS

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

____

____

____

____

____

____

FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6

FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378

FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf

FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f

FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2

FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b

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? ____________________________________
SEclients.txt

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?

____

1b319bc7ba0adc63f2af2cafdc59f5279d46dd33

How is using HMAC more secure than general hashing?

____

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

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? ________________________________ Yes

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**	

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – WEP/WPA2 PSK/WPA2 RADIUS (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
NTP/AAA Server	10.44.1.252	209.165.201.5	255.255.255.0	Metropolis Bank HQ

Objectives

Part 1: Configure WEP for Healthcare at Home

Part 2: Configure WPA2 PSK for Gotham Healthcare Branch

Part 3: Configure WPA2 RADIUS for Metropolis Bank HQ

Background

In this activity, you will configure WiFi networks for all three geographic sites. This activity will utilize WEP, WPA2 PSK, and WPA2 RADIUS to demonstrate the varying configuration of WiFi networks and their security considerations. Healthcare at Home will be setup using WEP. Gotham Healthcare Branch will be configured with WPA2 PSK and Metropolis Bank HQ will be using WPA2 Radius. The IP addressing, network configuration, and service configurations are already complete. You will use the wireless routers and client devices in the differing geographic regions to setup multiple secure wireless networks.

Part 1: Configure WEP for Healthcare at Home

Step 1: Setup the Wireless SSID.

a. Click the **Healthcare at Home** site and click **PC0**.

b. Select **Desktop** tab. Click **Command Prompt**. At the prompt, enter **ipconfig**.

```
PC> ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: FE80::20B:BEFF:FEB4:1262
   IP Address......................: 10.44.3.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 10.44.3.1
```

What is the IP address for the default gateway?

____

The IP address for the default gateway is 10.44.3.1.

c. Navigate to the **Web Browser** and enter the IP address for the default gateway. Enter **admin** as the username and password when prompted. Click **OK**.

d. The **Wireless Router** is the default gateway for this network. Click **Wireless** tab.

e. Change the **SSID** from **DefaultWIFI** to **Home**.

f. Set the SSID to **Broadcast**.

g. Click **Save Settings**. Click **Continue**.

Step 2: Setup Wireless Security.

a. Within the Wireless Router, click **Wireless** > **Wireless Security**.

b. Click the drop down menu and set the Security Mode to **WEP**.

c. Keep the encryption option set to 40/64-bits and enter the key **0123456789** as Key 1.

d. Click **Save Settings**. Click **Continue**.

WEP and the key 0123456789 are not secure. Why is WEP not recommended for use in securing wireless networks?

____

____

WEP doesn’t provide key management and uses weak encryption keys.

Step 3: Connect the Clients.

a. Within the **Healthcare at Home** site, click **Dave’s** Laptop.

b. Click the **Desktop** tab and click **PC Wireless**.

c. Click the **Connect** tab and click **Refresh**.

d. Select the Wireless Network Name of **Home** and click **Connect**.

e. Enter the key **0123456789** as WEP Key 1 and click **Connect**.

a. Repeat steps **a - e** for **Mary’s** Laptop.

Part 2: Configure WPA2 PSK for Gotham Healthcare Branch

Step 1: Setup the Wireless SSID.

a. Click the **Gotham Healthcare Branch** site and click **PC1**.

b. Select **Desktop** tab. Click **Command Prompt**. At the prompt, enter **ipconfig**.

Record the IP address for the default gateway: ____ 10.44.2.1

c. Navigate to the **Web Browser** and enter the IP address for the default gateway. Enter **admin** as the username and password when prompted. Click **OK**.

d. Click **Wireless** tab.

e. Change the **SSID** from **DefaultWIFI** to **BranchSite**.

f. Change the Standard Channel to **6 – 2.437GHz**.

g. Set the SSID to **Broadcast**.

h. Click **Save Settings**. Click **Continue**.

Step 2: Setup Wireless Security.

a. Within the wireless router, click on **Wireless** > **Wireless Security**.

b. Click the drop down menu and set the Security Mode to **WPA2 Personal**.

c. Keep the encryption option set to **AES** and enter the passphrase **ciscosecure**.

d. Click **Save Settings**. Click **Continue**.

Step 3: Connect the Clients.

a. Within the **Gotham Healthcare Branch** site, click **Tim's** computer.

b. Click the **Desktop** tab and click on **PC Wireless**.

c. Click the **Connect** tab and click **Refresh**.

d. Select the Wireless Network Name of **BranchSite** and click the **Connect**.

e. Enter the Pre-shared Key **ciscosecure** and click **Connect**.

f. Repeat steps **a - e** for **Mike's** computer.

Part 3: Configure WPA2 RADIUS for Metropolis Bank HQ

Step 1: Setup the Wireless SSID.

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

b. Navigate to the **Web Browser** and enter the IP address for the wireless router (**10.44.1.251**). Enter **admin** as the username and password when prompted. Click **OK**.

c. Click the **Wireless** tab. Change the **SSID** from **DefaultWIFI** to **HQ**.

d. Change the Standard Channel to **11 – 2.462GHz**.

e. Set the SSID to **Broadcast**.

f. Click **Save Settings**. Click **Continue**.

Step 2: Setup Wireless Security.

a. Within the **Wireless Router**, click on **Wireless** > **Wireless Security**.

b. Click the drop down menu and set the Security Mode to **WPA2-Enterprise**.

c. Keep the encryption option set to **AES** and enter the following RADIUS server credentials:

RADIUS SERVER IP: **10.44.1.252**

Shared Secret: **ciscosecure**

d. Click **Save Settings**. Click **Continue**.

Step 3: Configure the RADIUS server.

a. Within the **Metropolis Bank HQ** site, click the **NTP/AAA** server.

b. Click the **Services** tab and click on **AAA**.

c. Enter the following information in **Network Configuration**:

Client Name:.... **HQ**

Client IP: **10.44.1.251**

Secret: .... **ciscosecure**

ServerType: ..... **Radius**

d. Click **Add**.

e. Enter the following information in **User Setup** and click **Add** to add the new username:

Username:	**bob**	Password:	**secretninjabob**
Username:	**phil**	Password:	**philwashere**

Step 4: Connect the Clients.

a. Within the **Metropolis Bank HQ** site, click **Bob's** computer.

b. Click the **Desktop** tab and click on **PC Wireless**.

c. Click the **Profiles** tab and click **New**.

d. Name the Profile **RADIUS** and click **OK**.

e. Click **Advanced Setup**.

f. Enter the Wireless Network Name **HQ** and click **Next**.

g. Do not modify the Network Settings and click **Next**.

h. Change the Wireless Security drop down menu to **WPA2-Enterprise** and click **Next**.

i. Enter the login name of **bob** and the password of **secretninjabob** and click **Next**.

j. Click **Save** and then **Connect to Network**.

k. **Bob's** computer will connect automatically.

l. Repeat steps **a-j** for **Phil's** laptop using the authentication information from Step 3e.

When considering a large organization, why is WPA2 RADIUS more beneficial than WPA2 PSK?

____

____

WPA2 RADIUS allows each user to have their own unique credentials to access the wireless network. When a single user is no longer employed their specific account can be disabled/removed.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Configure WEP for Healthcare at Home	Step 2	5	
Part 3: Configure WPA2 RADIUS for Metropolis Bank HQ	Step 4	5	
	Questions	**10**	
	Packet Tracer Score	**90**	
	Total Score	**100**	

Packet Tracer – Configuring VPN Transport Mode (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
Private_FTP server	10.44.2.254	N/A	255.255.255.0	Gotham Healthcare Branch
Public_FTP server	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	N/A	209.165.201.19	255.255.255.248	Gotham Healthcare Branch
Phil's computer	10.44.0.2	N/A	255.255.255.0	Metropolis Bank HQ

Objectives

Part 1: Sending Unencrypted FTP Traffic

Part 2: Configuring the VPN Client within Metropolis

Part 3: Sending Encrypted FTP Traffic

Background

In this activity, you will observe the transfer of unencrypted FTP traffic between a client and a remote site. You will then configure a VPN client to connect to the Gotham Healthcare Branch site and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use a client device within Metropolis Bank HQ to transfer unencrypted and encrypted FTP data.

Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

c. Minimize the **Cyber Criminals Sniffer**.

Step 2: Connect to the Public_FTP server using an insecure FTP connection.

a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

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

c. Use the **ipconfig** command to view the current IP address of **Phil's** computer.

d. Connect to the **Public_FTP** server at **Gotham Healthcare Branch** by entering **ftp 209.165.201.20** in the command prompt.

e. Enter the username of **cisco** and password of **publickey** to login to the **Public_FTP** server.

f. Use the **put** command to upload the file **PublicInfo.txt** file to the **Public_FTP** server.

Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

____

USER **cisco**   PASS **publickey** and the filename of **PublicInfo.txt**

c. Type **quit** to exit **Public_FTP** server.

Part 2: Configuring the VPN Client on Phil's Computer

a. From **Phil's** computer, use the **ping** command and target the IP address of the **Branch_Router**. The first few pings may timeout. Enter the **ping** to get four successful pings.

b. On the **Desktop** tab, click on **VPN**

c. Within the **VPN Configuration** window, enter the following settings:

GroupName: .... **VPNGROUP**

Group Key:............... **123**

Host IP (Server IP):.. **209.165.201.19**

Username: .... **phil**

Password: **cisco123**

d. Click **Connect** and Click **OK** on the next window.

What is the Client IP for the client-to-site VPN connection?

____

10.44.2.200 (this may vary between 10.44.2.200 to 10.44.2.230)

Part 3: Sending Encrypted FTP Traffic

Step 1: View the current IP addressing on Phil's computer.

a. Within the **Metropolis Bank HQ** site, click **Phil's** computer.

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

c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.

What extra IP address is now shown that was not shown before in Part 1 Step 2c?

____

Tunnel Interface IP Address: 10.44.2.200 (this may vary between 10.44.2.200 to 10.44.2.230)

Step 2: Send encrypted FTP traffic from Phil's computer to the Private_FTP server.

a. Connect to the **Private_FTP** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

b. Enter the username of **cisco** and password of **secretkey** to login to the **Private_FTP** server.

c. Upload the file **PrivateInfo.txt** file to the **Private_FTP** server.

Step 3: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages displaying the password of internal or the file upload of PrivateInfo.txt? Explain.

____

No, the client-to-site VPN is using encryption and the Cyber Criminals Sniffer cannot decrypt the traffic to view it.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Sending Unencrypted FTP Traffic	Step 3	20	
Part 2: Configure the VPN Client on Phil's Computer	Step 1	10	
Part 3: Send Encrypted FTP Traffic	Step 1	10	
	Step 3	20	
Questions		**60**	
Packet Tracer Score		**40**	
Total Score		**100**	

Packet Tracer – Configuring VPN Tunnel Mode (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Subnet Mask	Site
File Backup Server	10.44.2.254	255.255.255.0	Gotham Healthcare Branch

Objectives

Part 1: Sending Unencrypted FTP Traffic

Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

Part 3: Sending Encrypted FTP Traffic

Background

In this activity, you will observe the transfer of unencrypted FTP traffic between two geographic sites. You will then configure a VPN tunnel between two geographic sites and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to transfer FTP data securely and insecurely.

Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.

b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

c. Minimize the **Cyber Criminals Sniffer**.

Step 2: Connect to the FTP Backup server using an insecure FTP connection.

a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

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

c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

a. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server.

Step 3: View the traffic on the Cyber Criminals Sniffer.

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

____

USER cisco PASS cisco

Part 2: Configuring the VPN Tunnel between Metropolis and Gotham

a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.

b. Copy the IPSec VPN site-to site configuration below and paste it into **HQ_Router**.

```
enable
configure terminal
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
!
crypto isakmp key vpnpass address 209.165.201.19
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Branch_Router
 set peer 209.165.201.19
 set transform-set VPN-SET
 match address 110
!
interface GigabitEthernet0/1
crypto map VPN-MAP
!
access-list 110 permit ip 10.44.1.0 0.0.0.255 10.44.2.0 0.0.0.255
!
end
copy run start
```

c. The required mirror configuration of the IPSec VPN has already been implemented on the **Branch_Router** of the **Gotham Healthcare Branch** site.

Part 3: Sending Encrypted FTP Traffic

Step 1: Send FTP traffic from Sally's PC to the File Backup server.

a. Within the **Metropolis Bank HQ** site, click **Sally's** computer.

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

c. Use the **ipconfig** command to view the current IP address of **Sally's** PC.

d. Connect to the **File Backup** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt. (It may take 2-5 attempts)

e. Enter the username of **cisco** and password of **cisco** to login to the **File Backup** server

f. Use the **put** command to upload the file **FTPupload.txt** to the **File Backup** server.

Step 2: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages sourced from the IP of **Sally's** computer? Explain.

____

No, the IPSec VPN is using encryption and the Cyber Criminals Sniffer cannot decrypt the traffic to view it.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Send unencrypted FTP traffic	Step 3	20	
Part 3: Send encrypted FTP traffic	Step 2	30	
	Questions	**50**	
	Packet Tracer Score	**50**	
	Total Score	**100**	

Packet Tracer – Router and Switch Redundancy (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	IP Address	Subnet Mask	Default Gateway	Site
External Web Server	209.165.201.10	255.255.255.0	N/A	Internet
R1	10.44.1.2	255.255.255.0	N/A	Metropolis Bank HQ
R2	10.44.1.3	255.255.255.0	N/A	Metropolis Bank HQ
Phil's computer	10.44.1.12	255.255.255.0	10.44.1.1	Metropolis Bank HQ
Tim's computer	10.44.2.11	255.255.255.0	10.44.2.1	Gotham Healthcare Branch

Objectives

Part 1: Observe a Network Failover with Redundant Routers.

Part 2: Observe a Network Failover with Redundant Switches.

Background

In this activity, you will observe the successful failover of the Metropolis network utilizing multiple routers to provide default gateway redundancy. Afterwards across the world, you will observe the successful network failover of the Gotham network utilizing multiple switches to provide redundant network pathways. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the differing geographic regions to test the pathways before and after successful network failover.

Part 1: Observe a Network Failover with Redundant Routers.

Step 1: Access the command prompt on Phil's computer.

a. Click the **Metropolis Bank HQ** site and then click the laptop **Phil**.

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

Step 2: Trace the pathway to the External Web server.

a. Ping the **External Web** server on the **Internet** by entering **ping 209.165.201.10** in the command prompt.

b. Trace the pathway to the **External Web** server on the **Internet** by entering **tracert 209.165.201.10** in the command prompt.

c. Each IP address shown in the output of the **tracert** command is a network device that network traffic is crossing.

What are the IP addresses of the devices that the traffic from Phil's laptop is crossing to reach the External Web server?

____

10.44.1.2 > 10.45.2.2 > 209.165.201.1 > 209.165.201.10

The first address of the **tracert** output is the default gateway (exit point) of the network.

d. Comparing the output of the **tracert** command to the Addressing Table at the beginning of this lab, which router is operating as the current default gateway?

____

Router R1

Step 3: Cause a network failover.

a. Within the **Metropolis Bank HQ** site, click the switch **HQ_S1**.

b. Click the **CLI** tab.

c. Disable the uplink port Gig0/2 using the following commands:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

Step 4: Trace the pathway to the External Web server again.

a. Within the **Metropolis Bank HQ** site, click the laptop **Phil**.

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

c. Ping the **External Web** server on the **Internet** by entering **ping 209.165.201.10** in the command prompt.

d. Trace the pathway to the **External Web** server on the **Internet** by entering **tracert 209.165.201.10** in the command prompt.

Each IP address shown in the output of the **tracert** command is a network device that network traffic is crossing.

What are the IP addresses of the devices that the traffic from Phil’s laptop is crossing to reach the External Web server?

____

10.44.1.3 > 10.45.1.2 > 209.165.201.1 > 209.165.201.10

e. The first address of the **tracert** output is the default gateway (exit point) of the network.

Which router is now operating as the current default gateway?

____

Router R2

f. In the **Command Prompt** enter the command **ipconfig**. The default gateway is listed as 10.44.1.1 which is neither 10.44.1.2 from the first time the tracert command was given, nor 10.44.1.3 from the second time the tracert command was given. This shows that the default gateway of 10.44.1.1 is actually routed through redundant routers with different IP addresses, router R1 at 10.44.1.2 or router R2 at 10.44.1.3 if R1 is not available.

Part 2: Observe a Network Failover with Redundant Switches

Step 1: Access the command prompt on Tim’s computer.

a. Click the **Gotham Healthcare Branch** site and then click the computer **Tim**.

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

Step 2: Trace the pathway to the External Web server.

a. Ping the **External Web** server on the **Internet** by entering **ping 209.165.201.10** in the command prompt.

b. In order to observe the network failover, a constant ping can be used.

Ping the **External Web** server with a constant ping by entering **ping -t 209.165.201.10** in the command prompt.

Minimize the Tim computer window.

Step 3: Cause a network failover.

a. Within the **Gotham Healthcare Branch** site, click the switch **S3**.

b. Click on the **CLI** tab.

c. Disable the uplink port Gig0/2 using the following commands:

```
enable
configure terminal
interface GigabitEthernet0/2
shutdown
```

Step 4: Trace the pathway to the External Web server again.

a. Within the **Gotham Healthcare Branch** site, maximize the Tim computer window.

b. Wait about 30-60 seconds. You can also watch the switchport link lights in the Gotham Healthcare Branch network.

c. The output on Tim's computer should be similar to the following:

```
PC> ping -t 209.165.201.10
Pinging 209.165.201.10 with 32 bytes of data:

Reply from 209.165.201.10: bytes=32 time=47ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=43ms TTL=126
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 209.165.201.10: bytes=32 time=41ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
Reply from 209.165.201.10: bytes=32 time=42ms TTL=126
```

d. Close the window.

Which cable was the data crossing during the successful ping replies **before** the "Request timed out" messaged occurred?

____

Gigabit Ethernet 0/2, the cable connecting switch **S1** to switch **S3**

Which cable was the data crossing during the successful ping replies **after** the “Request timed out” messaged occurred?

____

Gigabit Ethernet 0/1, the cable connecting switch **S2** to switch **S3**

e. What does this scenario prove about switch failover redundancy when a Gigabit Ethernet port is shutdown all of a sudden?

____

____

It proves that another switchport can be turned on automatically and traffic can take a redundant path.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Observe a network failover with redundant routers	Step 2	10	
	Step 2	10	
	Step 4	10	
	Step 4	10	
Part 2: Observe a network failover with redundant switches	Step 4	5	
	Step 4	5	
	Step 4	10	
	Questions	**60**	
	Packet Tracer Score	**40**	
	Total Score	**100**	

Packet Tracer - Router and Switch Resilience (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	IP Address	Subnet Mask	Default Gateway	Site
HQ_Router	10.44.1.1	255.255.255.0	N/A	Metropolis Bank HQ

Objectives

Part 1: Hardening the IOS Configuration

Part 2: Activating the Cisco IOS Resilient Configuration Feature

Background

In this activity, you will harden the IOS configuration of a router within the Metropolis network. Afterwards, you will enable the IOS resiliency feature on a Cisco router. The IP addressing, network configuration, and service configurations are already complete. You will use the client devices in the Metropolis network to deploy the IOS resiliency configuration.

Part 1: Hardening the IOS configuration

Step 1: Access the command prompt on Sally's computer.

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

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

Step 2: Remotely connect to the router HQ_Router.

a. SSH to the **HQ_Router** by entering **ssh –l admin 10.44.1.1** in the command prompt. Use the password of **cisco12345** when prompted.

b. At the prompt, type **enable** and enter the enable password **class** when prompted.

Your prompt should display:

```
HQ_Router#
```

c. Were you prompted with any warning message preventing unauthorized users from accessing the HQ_Router?

____

No

Step 3: Create a legal notification message on the HQ_Router.

a. At the `HQ_Router#` prompt, enter global configuration mode using the **configure terminal** command.

b. At the `HQ_Router(config)#` prompt, paste in the following commands:

```
banner motd #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
You must have explicit, authorized permission to access or configure this
device.
```

```
Unauthorized attempts and actions to access or use this system may result in
civil and/or
criminal penalties.
All activities performed on this device are logged and monitored.
#
```

c. At the `HQ_Router(config)#` prompt use the **end** and **logout** command to end your connection to **HQ_Router**.

d. SSH into the **HQ_Router** again from the computer **Sally**. The SSH password is **cisco12345**.

Were you prompted with any additional text/information when you connected successfully to the **HQ_Router**? What is shown?

____

____

Yes, the MOTD banner configured in step 3.b is displayed after successfully forming an SSH connection with router **HQ_Router**.

Step 4: Enforce password security on the HQ_Router.

a. At the prompt, type **enable** and enter the enable password **class** when prompted.

b. Enter global configuration mode using the **configure terminal** command. At the `HQ_Router(config)#` prompt, paste in the following commands:

```
!encrypts plain-text passwords in the running-config
service password-encryption

!enforces any new configured passwords to have a minimum of 10 characters
security passwords min-length 10
```

Part 2: Activating the Cisco IOS Resilient Configuration Feature

Step 1: View the current IOS image.

a. While connected via SSH from **Sally's** computer, enter the **exit** command to return to the `HQ_Router#` prompt.

b. Enter the command **dir flash:** to view the current IOS.bin file.

What is the name of the current .bin file in flash?

____

c2900-universalk9-mz.SPA.151-4.M4.bin

Step 2: Secure the running image and configuration.

a. At the `HQ_Router#` prompt, enter global configuration mode using the **configure terminal** command.

b. Use the **secure boot-image** command within the `HQ_Router(config)#` prompt to activate IOS image resilience and prevent the IOS file from both showing in the directory output and prevents the deletion of the secured IOS file.

c. Use the **secure boot-config** command within the `HQ_Router(config)#` prompt to store a secure copy of the running configuration and prevent deletion of the secured configuration file.

d. Return to privileged EXEC mode by entering the **exit** command. Now enter the command **dir flash:** to view the current IOS.bin file.

   Are there any IOS.bin file listed? ____ No

e. At the `HQ_Router#` prompt, enter the command **show secure bootset** to view the status of the Cisco IOS image and configuration resilience.

f. Enter the command **reload** to reload the router. Press **Enter** to confirm the reload.

```
HQ_Router#reload
Proceed with reload? [confirm]
% Connection timed out; remote host not responding
C:\>
```

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Harden the IOS configuration	Step 2	10	
	Step 3	10	
Part 2: Activate the Cisco IOS resilient configuration feature	Step 1	10	
	Step 2	10	
Questions		**40**	
Packet Tracer Score		**60**	
Total Score		**100**	

Packet Tracer - Server Firewalls and Router ACLs (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
Web Server	N/A	209.165.201.10	255.255.255.0	Internet

Objectives

Part 1: Connect to the Web Server

Part 2: Prevent Unencrypted HTTP Sessions

Part 3: Access the Firewall on the Email Server

Background

In this activity, you will access a user within the Metropolis site and connect using HTTP and HTTPS to a remote Web Server. The IP addressing, network configuration, and service configurations are already complete. You will use a client device in the Metropolis site to test connectivity to a remote Web Server and then secure the Metropolis site by preventing unencrypted web sessions from connecting to the outside world.

Part 1: Connect to the Web Server

Step 1: Access the HQ Internet Web Server on Sally’s PC using HTTP.

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

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

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

d. Click the link **Login Page**.

Why would a user be concerned when submitting information using this website?

____

The webpage is accepting user authentication information via insecure unencrypted HTTP.

Step 2: Access the HQ Internet Web Server on Sally’s PC using HTTPS.

a. Access the **Web Browser** on Sally’s computer.

b. Enter the URL of **https://www.cisco.corp** and click Go.

c. Click on the link **Login Page**.

Why would a user be less concerned when submitting information using this website?

____

The webpage is securing the user authentication information with SSL/TLS via encrypted HTTPS.

d. Close **Sally’s** computer.

Part 2: Prevent Unencrypted HTTP Sessions

Step 1: Configure the HQ_Router.

a. Within the **Metropolis Bank HQ** site, click the **HQ_Router**.

b. Click the **CLI** tab and press **Enter**.

c. Use the password **cisco** to login to the router.

d. Use the **enable** command and then **configure terminal** command to access the global configuration mode.

In order to prevent unencrypted HTTP traffic from traveling through the HQ router, network administrators can create and deploy access control lists (ACLs).

The following commands are beyond this course but are used to demonstrate the ability to prevent unencrypted traffic from moving through the HQ_Router.

e. Within the global configuration mode **HQ_Router**(config)# copy the following access-list configuration below and paste it into the **HQ_Router**.

```
!
access-list 101 deny tcp any any eq 80
access-list 101 permit ip any any
!
int gig0/0
ip access-group 101 in
!
end
```

f. Close the **HQ_Router**.

Step 2: Access the HQ Internet Web Server on Sally's PC using HTTP.

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

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

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

Is **Sally's** computer able to access the HQ Internet Web Server using HTTP?

No, the HTTP request is not connecting to the server.

Step 3: Access the HQ Internet Web Server on Sally's PC using HTTPS.

a. Access the **Web Browser** on Sally's computer.

b. Enter the URL of **https://www.cisco.corp** and click Go.

Is Sally's computer able to access the HQ Internet Web Server using HTTPS?

Yes, the HTTPS request is connecting to the server.

c. Close **Sally's** computer.

Part 3: Access the Firewall on the Email Server

a. Within the **Metropolis Bank HQ** site, click the **Email** server.

b. Click the **Desktop** tab and then click on **Firewall**. There are no firewall rules implemented.

In order to prevent non-email related traffic from being sent or received from the Email server, network administrators can create firewall rules directly on the server, or as previously shown, they can use access control lists (ACLs) on a network device like a router.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Connect to the Web Server	Step 1	15	
	Step 2	15	
Part 2: Prevent Unencrypted HTTP Sessions	Step 2	15	
	Step 3	15	
Questions		**60**	
Packet Tracer Score		**40**	
Total Score		**100**	

Packet Tracer – Skills Integration Challenge (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ_Router	G0/0	10.44.1.1	255.255.255.0	N/A
	G0/1	209.165.201.2	255.255.255.248	N/A
VPN server	NIC	209.165.201.19	255.255.255.248	N/A
HQ_Wireless	LAN	10.44.0.254	255.255.255.0	10.44.1.1
FTP/Web server	NIC	10.44.1.252	255.255.255.0	10.44.1.1
BackupFiles server	NIC	10.44.2.10	255.255.255.0	10.44.2.1

Scenario

This culminating activity includes many of the skills that you have acquired during this course. You will configure a wireless router, upload and download files using FTP, connect securely to a remote site using a VPN, and secure a Cisco IOS router.

Implementation

Note: You only have access to the Metropolis HQ site. You can access all the servers and PCs within this site for testing purposes.

Implement to following requirements:

Sally's Computer – Metropolis Bank HQ

- Upload the **secure.txt** file to the **FTP/Web** server using FTP:
  - User **sally** with password **ftpaccess**
  - The file to upload is **secure.txt**
  - Use the IP address of the **FTP/Web server** located in the addressing table.
- Connect **Sally's** computer to the **Gotham Healthcare Branch** site via a client-to-site VPN:
  - Use the IP address of the VPN server located in the addressing table and ping the VPN server
  - Connect the client-to-site VPN with user **sally** and password **vpnsally**
  - Use the group **VPNGROUP** and key **123**
- Using the VPN connection, download the **data.txt** file from the **BackupFiles** server using FTP:
  - Use the IP address of the **BackupFiles** server located in the addressing table.
  - User **sally** with password **securesally**
  - The file to download is **data.txt**

Phil's Laptop – Metropolis Bank HQ

- Configure the **HQ_Wireless** router.
  - Use the IP address of the **HQ_Wireless** router located in the addressing table.
  - Use the Web Browser to configure the **HQ_Wireless** router from **Phil's** laptop.

    - User **admin** with password **p@ssword**
    - Change the SSID from **Default** to **HQwifi**
    - Set the SSID to be viewable (broadcasted) to wireless clients.
    - Configure wireless security of **WPA2 Personal** with the passphrase of **cisco321**.
- Secure the **HQ_Router**.
    - Use the IP address of **HQ_Router** router located in the addressing table.
    - Use the Command prompt to ssh to **HQ_Router** with the user **phil** and password **securessh**
    - Use the **enable** command and password **cisco.**
    - Configure a banner motd message that includes the phrase **Authorized Access Only**
    - Activate the Cisco IOS resilient configuration feature and reload the router.

Gina's Laptop – Metropolis Bank HQ

- Connect **Gina's** laptop to the wireless network.
    - Connect to the SSID of **HQwifi**
    - Use the Pre-shared Key of **cisco321**
    - Verify that the laptop uses **DHCP**

Suggested Scoring Rubric

Packet Tracer scores 100 points.

Final Config for HQ_Router

```
enable
config t
banner motd "Authorized Access Only"
secure boot-image
exit
```