Packet Tracer – Communicating in a Cyber World

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?

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?

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?

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?

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?

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?

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?

   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**	