Packet Tracer - Network Security Exploration - Physical Mode

Objectives

Part 1: Explore the Networks

Part 2: Implement Security Measures

Background / Scenario

In this Packet Tracer Physical Mode (PTPM) activity, you will explore and implement several security procedures in different locations within the city of Greenville, North Carolina. Included are networks in a Data Center, an ISP, a Coffee Shop, and a Home.

The Data Center is provisioned for environmental and physical security. There is also software included to maintain access control. You will install an Internet of Things (IoT) smoke detector.

The Coffee Shop offers free wireless access to their patrons. You will implement a VPN to secure traffic.

The Home includes an office, a student's bedroom, and a living room. You will configure two home wireless LANs (WLANs) to require authentication for two different user types: family members and guests. These networks will also be configured with MAC address filtering to restrict access.

Note: This activity is not graded. However, you will use a variety of methods to verify the configurations you implement.

Instructions

Part 1: Explore the Networks

In this part, you will explore the networks in the Data Center, ISP, Coffee Shop, and Home.

Step 1: Explore Greenville.

The activity opens with a view of North Carolina, USA. All the tasks in this activity occur in Greenville. Click **Greenville** to enter city view. There are four locations to explore: **Data Center**, **ISP**, **Home**, and **Coffee Shop**.

Step 2: Explore the rooms in the Data Center.

a. There are two rooms and a variety of devices to explore including a server room, the POP, an IoT server, two access points, a laptop, and several IoT devices connected to the network.

b. Click **Data Center Server Room**. Notice the majority of devices are servers. In a real data center, there would be hundreds of racks filled with servers. Switches are linking the servers together with redundant connections. A router is providing connectivity to the POP, which then connects to the ISP.

What is the name of the router that is located in this wiring closet?

c. Navigate up one level to the **Data Center**.

Step 3: Investigate the devices in the Data Center POP.

a. Click **Data Center POP**. What cable type is used to connect the **DC_Edge-Rtr1** to the ISP?

b. What device is doing the translation of private Data Center addresses into public addresses?

c. Click **DC_Edge-Rtr1** > **CLI**. Enter the **show access-list** command to view the access list. This access list permits only specific traffic into the Data Center. In this simulation, HTTP, HTTPS, IPsec, and FTP traffic are permitted. All other traffic is blocked.

d. Investigate the interfaces. What interface and in which direction is this access list applied?

Note: The **access-list** commands in this simulation are limited. On a real edge router the access lists would be much more complex and even more restrictive to protect all networking devices and data within the **Data Center**.

Step 4: Investigate the IoT devices configured to connect to the DC IoT Server.

a. Navigate to the Data Center. In the **Data Center POP** room, click the laptop on the desk, and then **Desktop** > **Web Browser**.

b. Enter the IP address 172.31.0.2, which is the **DC IoT Server**.

c. For username and password, enter **admin** and **ciscorocks**.

d. What devices are currently being used to protect the networking equipment in the Data Center from environmental factors and physical security?

e. In the list of IoT devices, click **Humidity Monitor** to expand it. What is the current humidity level?

Step 5: Investigate the monitored door and siren.

a. In the list of IoT devices, click **Door** to expand it. Notice the **Open** indicator is Red. This means that the door is closed.

b. In the list of IoT devices, click **Siren**. Notice the **On** indicator is Red. This means that the siren is not on.

c. Keep the **Web Browser** window in view and locate the **Siren** next to the **Door** in the **Data Center POP**.

d. To open the **Door**, click **Unlock** in the list of IoT devices and then hold the **ALT** key down and **Left Click** the **Door**. When the **Door** opens the Siren turns **Red**.

e. In the **Web Browser** window, the **Open** indicator turned Green, meaning that the door is open. The Siren **On** indicator is also **Green**, meaning that the **Siren** is going off. Close the **Door** again by holding down the **ALT** key and left clicking the **Door**.

f. In the **Web Browser** window, under **Door**, click **Lock**. Try to open the door again by holding the **ALT** key down and left clicking the **Door**. The **Door** should not open.

Step 6: Investigate the thermostat.

a. In the list of IoT devices, click **Thermostat** to expand the available features and variables. At what temperature will the air conditioner turn on?

b. In the **Data Center**, click the **Thermostat** > **Config**, and then **Wireless0** under **INTERFACE**. What is the IP address for the **Thermostat**?

c. On the **DC_Laptop**, close the **Web Browser**, if necessary. Click **Command Prompt** and ping the **Thermostat**. The ping should be successful.

Step 7: Explore the ISP, Coffee Shop, and Home networks.

a. Navigate to the **ISP**. The ISP contains two routers, a DNS server, and a Central Office router that connects the **Coffee Shop** and **Home** to the internet.

b. Navigate to the **Coffee Shop**. How do clients connect to the Coffee Shop network?

What type of media is used to connect the café to the internet?

What devices are used to create the **Coffee Shop** network? Click the **Wiring Cabinet** to see additional devices.

c. Click each laptop in the **Coffee Shop**. Click the **Config** tab, and then **Wireless0** under **INTERFACE**. What IP addresses do they have?

d. Navigate to the **Home** network. You will configure the network later in this activity. Investigate the devices in the network. How does the **Home** connect to the **ISP**?

What devices require connectivity within the house?

Part 2: Implement Security Measures

In this part, you configure wireless security for the smoke detector in the **Data Center**, a virtual private network (VPN) in the **Coffee Shop**, and two wireless networks in the **Home**.

Step 1: Configure an IoT smoke detector in the Data Center.

a. Navigate back to the **Data Center**. Click the **Smoke Detector** on the wall in the **Data Center Server Room**, and then click the **Config** tab. Complete the following configurations:

1) Modify the **Display Name** to **Smoke Detector-DC1**.

2) In the **Gateway/DNS IPv4** section, enable DHCP.

3) In the **IoT Server** section, modify the **Remote Server** to have the IP address **172.31.0.2**. The username is **admin**, and the password is **ciscorocks**.

b. Click **Wireless0** under **INTERFACE** and complete the following configurations:

1) Modify the **SSID** to **DC_WLAN**.

2) Change the **Authentication** to **WPA2-PSK** and set the **PSK Pass Phrase** to **ciscorocks**.

3) Return to **Settings**. In the **IoT Server** section, click **Connect**. The registration server will update the default gateway and IP address of the smoke detector through DHCP.

Note: The **Connect** button changes to **Refresh** after you have successfully connected.

c. Close the **Smoke Detector-DC1**, and then click the laptop in the **Data Center POP**. If you closed the **Web Browser** previously, reopen it now and authenticate with the **IoT Server** at **172.3.1.0.2** with the username **admin** and password **ciscorocks**.

d. Notice the **Smoke Detector-DC1** is now added to the list of IoT devices. Click **Smoke Detector-DC1** in the Web browser. The **Alarm** indicator should be red, meaning that the alarm is not activated.

Step 2: Create a VPN on a laptop in the Coffee Shop to secure traffic.

Free Wi-Fi in businesses like the coffee shop is usually “open”, meaning that there is no privacy and traffic can be easily captured. To avoid that issue, you will use a VPN client on one of the laptops to connect to an FTP server in the Data Center. The tunnel created by the VPN will encrypt any data transferred between the laptop and the server. The edge router in the Data Center is already configured for VPN.

a. Navigate to the **Coffee Shop**, and then click the **VPN Laptop**.

b. Click **Desktop** > **Command Prompt** and enter the **ipconfig** command. What is the IP address assigned to this laptop?

c. To speed up convergence in Packet Tracer, ping the VPN server which is provided by the **DC_Edge-Rtr1** at 10.0.0.2.

d. Close the **Command Prompt** window, and then click **VPN**. Enter the following configuration:

GroupName: **REMOTE**

Group Key: **CISCO**

Host IP (Server IP): **10.0.0.2**

Username: **VPN**

Password: **ciscorocks**

e. Click **Connect**. Click OK to the **VPN is connected** message. If you have any issues, be sure your configuration is correct and that you previously successfully pinged 10.0.0.2. The **VPN Configuration** window now displays the **Client IP**. What is the IP address?

f. Navigate to the **Data Center**, and then click **Data Center POP** > **DC_Edge-Rtr1**.

g. Click the **CLI** tab. In privileged EXEC mode, enter the **show crypto isakmp sa** command to display active IPsec security associations. What status is listed in the output of the command?

What destination IP address is listed in the output? Can you determine to which device this IP address belongs?

h. To test the VPN, return to the **VPN Laptop**. In the **Command Prompt** window, enter the **ftp 172.19.0.3** command to connect to the FTP server in the **Data Center**. When prompted, enter the username **remote** and the password **ciscorocks**.

Note: If the connection fails, verify that the VPN is still connected.

```
C:\> ftp 172.19.0.3
Trying to connect...172.19.0.3
Connected to 172.19.0.3
220- Welcome to PT Ftp server
Username: remote
331- Username ok, need password
Password: ciscorocks
230- Logged in
(passive mode On)
ftp>
```

i. At the **ftp>** prompt enter the **dir** command to view the contents of the FTP server. What is the name of the file listed?

j. Enter the **get** *filename* command replacing *filename* with the name of the file to download to the laptop.

k. Enter the **quit** command to exit your FTP session.

l. To view the contents of the file, close the **Command Prompt** window and open the **Text Editor**.

m. Click the **File** > **Open**. Click the downloaded file and then click **Open**. What is the first word in the message?

n. In the **Coffee Shop**, click the other laptop, and then click **Desktop** > **Command Prompt**. Attempt to ping the FTP server at 172.19.0.3. Was it successful? Why or why not?

o. On real equipment, you would require a VPN service and their VPN client software loaded on the laptop. Use the internet to research different VPN services/applications available for laptops, tablets, and smartphones. What are three examples of VPN services/applications that you could use on an open wireless network to protect your data?

Step 3: Configure secure WLANs in the Home network.

For the Home network, you will do the initial wireless setup, create separate networks for the home office and guests, secure each network with strong authentication, and include MAC address filtering.

a. Navigate to the **Home**. Investigate the cabling. Notice that the two PCs, one in the home office and the other in the bedroom, use a wired connection. The laptop in the office will use the home office WLAN and laptop in the living room will use the guest WLAN.

b. Use the zoom tool (or **Ctrl** + scroll middle mouse wheel) to zoom in on the home office.

c. Click the **Home Router**. It is the left device sitting on the shelf behind the desk. Then click the **GUI** tab. The router is using DHCP to automatically receive IP addressing from the ISP.

d. In the **Network Setup** section, configure the following setting:

IP Address: **192.168.0.254**

Subnet Mask: 255.255.255.0

DHCP: Enabled

Start IP Address: 192.168.0.10

Maximum number of Users: 25

Static DNS 1: 10.2.0.125

e. Scroll to the bottom and click **Save Settings**.

f. Scroll back to the top and click **Wireless**. Under the **Basic Wireless Settings** submenu, configure **HomeNet** as the SSID for each of WLAN and disable all SSID broadcasts.

g. Scroll to the bottom and click **Save Settings**.

h. Scroll back to the top and click the **Wireless Security** submenu. Configure the following settings for all three WLANs.

Security Mode: **WPA2 Personal**

Encryption: **AES**

Passphrase: **ciscorocks**

i. Scroll to the bottom and click **Save Settings**.

j. Scroll back to the top and click the **Guest Network** submenu. Configure the following settings for all three WLANs:

Enable Guest Profile

Network Name (SSID): **GuestNet**

Enable Broadcast SSID

Security Mode: **WPA2 Personal**

Encryption: **AES**

Passphrase: **guestpass**

k. Scroll to the bottom and click **Save Settings**.

l. Scroll back to the top and click the **Wireless MAC Filter** submenu. Permit the MAC address for the laptop in the Home Office, which is **00:01:42:2B:9E:9D**. Be sure to permit the MAC address for all three WLANs. There is a dropdown menu at the top next to **Wireless Port** where you can switch from **2.4G** to **5G(1)** and **5G(2)**.

m. Scroll to the bottom and click **Save Settings**.

n. In the **Home Office**, click the laptop on the table in front of the couch, and then click the **Config** tab. Configure the wireless settings necessary to access the **HomeNet** WLAN.

o. Click **Desktop** tab > **Web Browser**. Enter the URL **www.ptsecurity.com** and click **Go**. It may take a few seconds for the web page to display. If you get a Request Timeout message, click **Go** again.

p. Navigate back to the **Home** and zoom in on the living room. Click the **Guest Laptop**, and then **Wireless0** under the **INTERFACE** section. Configure the wireless settings necessary to access the **GuestNet** WLAN. Under IP Configuration, make sure **DHCP** is selected. Did the laptop receive IP addressing from the **Home Router**? Why or why not?

q. Navigate back to the **GUI** tab for the **Home Router** and correct the issue.

r. Navigate back to the **Guest Laptop**. In the **Wireless0** > **IP Configuration** section, you should now see IP addressing from the pool you configured earlier on the **Home Router**. If not, toggle between **DHCP** and **Static** to refresh the DHCP requests.

s. Click **Desktop** > **Command Prompt** and ping the DNS server in the ISP at 10.2.0.125 to test access to external devices. The ping should be successful.

t. Test access to any other device in the Home network. Are these pings successful? Why or why not?

u. Close the **Command Prompt** and click **Web Browser**. Test access to **www.ptsecurity.com**. Access should be successful.

Reflection

a. List all of the different security approaches that were used in this situation.

b. In a situation where real equipment is used, list other suggestions that could be added to this scenario to make it more secure.