Packet Tracer - Configure Wireless Router Hardening and Security

Objectives

Part 1: Configure Basic Security Settings for a Wireless Router

Part 2: Configure Wireless Router Network Security

Part 3: Configure Wireless Clients Network Security

Part 4: Verify Connectivity and Security Settings

Background / Scenario

In this Packet Tracer activity, you will configure wireless security on a wireless router. During installation of the router, it was partially configured but has some security issues that need to be addressed. You will also harden the router to help mitigate potential attacks. After the security configuration is complete, you will verify connectivity and security settings.

Note: Most tasks in this activity are graded. Click **Check Results** at any time to view your correct and incorrect **Assessment Items**.

Note: Switching to **Logical** mode is disabled in this activity. Also, the **Data Center** and **ISP/Telco** locations are locked.

Instructions

Part 1: Configure Basic Security Settings for a Wireless Router

The initial settings on a home wireless router can pose a security risk. For example, if threat actors know your public facing IP address, they can search the internet for your router's default login credentials and remotely access your router. In this Part, you will change the router's password and disable remote login.

Step 1: Change the default router password.

It is important to set a very strong password or lengthy passphrase to prevent unauthorized users from changing configurations on the router.

a. Click the **Home**, and then click **Home Office PC** > **Desktop** tab > **Web Browser**.

b. Connect to the **Home Wireless Router** at **192.168.0.1**.

c. Enter **admin** for both the username and password.

d. Click the **Administration** tab, and then enter **cisconetacadrocks!** for both password fields.

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

f. The router requests that you re-authenticate. Log back in with the username **admin** and the new password, and then click **Continue**.

Step 2: Disable remote management.

Home wireless routers typically ship with remote configuration enabled. This allows technicians from your service provider to access your device to help setup your home network or troubleshoot issues. However, this can be a security risk because a port must be open and listening in order for the technician to connect to the router. It is often possible to change the port and only permit HTTPS access, but this does not afford any real measure of security because a threat actor could detect open ports and launch a password attack against the router. If remote management is truly needed, it would be far more secure to set up a VPN solution instead.

The Home Wireless Router in this Packet Tracer activity does not support VPN. Therefore, you will disable remote management.

a. From the **Administration** tab, click the **Disabled** next to **Remote Management**.

b. Click **Save Settings**.

Note: This change will cause **Home Wireless Router** to reset. Close the **Web Browser** and click **Fast Forward Time** (Alt+D). Return to **Home Office PC** and click **IP Configuration** to check if IP addressing is reassigned. If necessary, toggle between **DHCP** and **Static** until **Home Office PC** receives IP addressing from the 192.168.0.1/24 network. Close **IP Configuration**, and then click **Web Browser**. Navigate to **192.168.0.1**, and re-authenticate in preparation for the next part of the activity.

Part 2: Configure Wireless Router Network Security

Right now, anyone that has a wireless device in range of the **Home Wireless Router** could connect easily and possibly access devices on the network. To prevent this from happening, in this Part, you will secure the wireless networks so that only devices with the correct configuration will be able to connect to the networks.

Step 1: Configure and broadcast the HomeNet SSID.

Currently, the router is not broadcasting the SSID of the networks that are configured. This is not a generally accepted security measure mostly because if a threat actor were looking for a network to attack, they would still see the nameless network. There are tools available to sniff the traffic to determine the SSID. In fact, the practice of turning off the SSID broadcast could potentially make the network a higher target for attack because the administrator is trying to hide it.

a. Click the **Wireless** tab, and then for each of the three networks, click the **Enabled** for **SSID Broadcast**.

b. For each of the three networks, change the SSID from **default** to **HomeNet**.

c. Click **Save Settings**.

Step 2: Configure security for the HomeNet wireless networks.

Perhaps the most important security measure outside of changing the router password is encrypting the traffic between the router and wireless clients. Without encryption, a threat actor can use easy-to-get and often free tools to simply intercept communications with very little effort. This can lead to further attacks as the threat actor gains knowledge about you and your networks.

a. From the **Wireless** tab, click **Wireless Security**.

b. For each of the three networks, configure the following:

- Security Mode: **WPA2 Personal**
- Encryption: **AES**
- Passphrase: **ciscorocks**

c. Click **Save Settings**.

Step 3: Configure security for the GuestNet wireless network.

This router allows for two independent wireless networks to be configured for each radio. This can be useful when you wish to keep guest traffic separated from traffic on your other networks.

a. From the **Wireless** tab, click **Guest Network**.

b. For each of the three networks, click **Enable Guest Profile,** and then configure the following:

- SSID: **GuestNet**
- Broadcast SSID: **Enabled**

- Security Mode: **WPA2 Personal**
- Encryption: **AES**
- Passphrase: **guestpass**

c. Click **Save Settings**.

Part 3: Configure Wireless Clients

The **Home Wireless Router** has been hardened and wireless security has been configured. In this Part, you will safely connect wireless clients to the network.

Step 1: Configure wireless connectivity for the laptops.

a. Click **Home Laptop 1** located in the living room, and then click **Desktop** tab > **PC Wireless**.

b. Click the **Connect** tab.

c. Click the first entry for **HomeNet**, and then click **Connect**.

d. Security is already set to **WPA2-Personal**. Enter **ciscorocks** for the **Pre-shared Key**, and then click **Connect**.

e. Click the **Link Information** tab. You should see message "You have successfully connected to the access point". If you are still not connected, check the configuration of the **Home Wireless Router** and try this Step again.

f. Close the **PC Wireless** window and click **IP Configuration**. If the laptop still has an address from the "169" network, toggle between **DHCP** and **Static** until it receives IP addressing from the 192.168.0.0/24 network.

g. Repeat this Step for **Home Laptop 2** in the home office, but use the first entry for **GuestNet**. Enter **guestpass** as the **Pre-shared Key**.

Step 2: Configure wireless connectivity for the IoT devices.

a. In the home office, on the top shelf of the bookcase, click the **Home_Webcam**

b. Click the **Config** > **Wireless0**.

c. Enter **HomeNet** for the **SSID**.

d. Choose **WPA2-PSK** for the **Authentication**, and then enter **ciscorocks** for the **PSK Pass Phrase**.

e. Under **IP Configuration**, click **DHCP** and verify the device received IP addressing from the 192.168.0.0/24 network. Toggle between **DHCP** and **Static**, if necessary.

f. Repeat this Step for both the **Home_Siren**, located in the living room above the bookcase, and **Home Doors**.

Part 4: Verify Connectivity and Security Settings

In this Part, you will test your configurations and security settings to make sure that the devices are communicating with each other, and that they can reach the internet.

Step 1: Test internet connectivity for wireless laptops.

a. Click **Home Laptop 1** > **Desktop** tab > **Web Browser**.

b. Navigate to **www.ptsecurity.com**. Packet Tracer may take several seconds to converge. You can click **Fast Forward Time** (Alt+D) to speed up the process until the **Data Center Public Web** page loads.

c. Repeat this step for **Home Laptop 2**.

Step 2: Configure security for GuestNet and HomeNet interconnectivity.

The **GuestNet** and the **HomeNet** should not normally be able to connect or share resources. Recall that Home Laptop 2 is configured for the guest network and should not normally have access to devices on the home network.

a. Use any method you wish to determine the IP address for **Home Laptop 1**.

b. Click **Home Laptop 2** > **Desktop** tab > **Command Prompt**.

c. Enter **ping** command followed by the IP address for **Home Laptop 1**.

Home Laptop 1 responds to the pings indicating that **Home Laptop 2** can access devices on the home network. You will need to set the router to prevent hosts on different networks from communicating with each other.

d. From **Home Office PC**, if necessary, log back into the **Home Wireless Router** configuration web page at 192.168.0.1.

e. Click the **Wireless** tab, and then the **Guest Network** submenu.

f. Uncheck the box next to **Allow guests to see each other and access the local network**, and then click **Save Settings**.

g. From **Home Laptop 2**, attempt to ping **Home Laptop 1** again. The pings should now fail. This indicates that the hosts are not allowed to communicate between the two networks.