Investigate a Threat Landscape

Objectives:

Part 1: Investigate a Network Configuration Vulnerability

Part 2: Investigate a Phishing Malware Vulnerability

Part 3: Investigate a Wireless Network and DNS Vulnerability

Background / Scenario

The threat landscape consists of all the vulnerabilities that can be exploited by threat actors. Every cybersecurity incident involves the exploitation of vulnerabilities by different types of threat actors. Some threat actors want money, others want to be famous, and yet others want to destroy information and infrastructure.

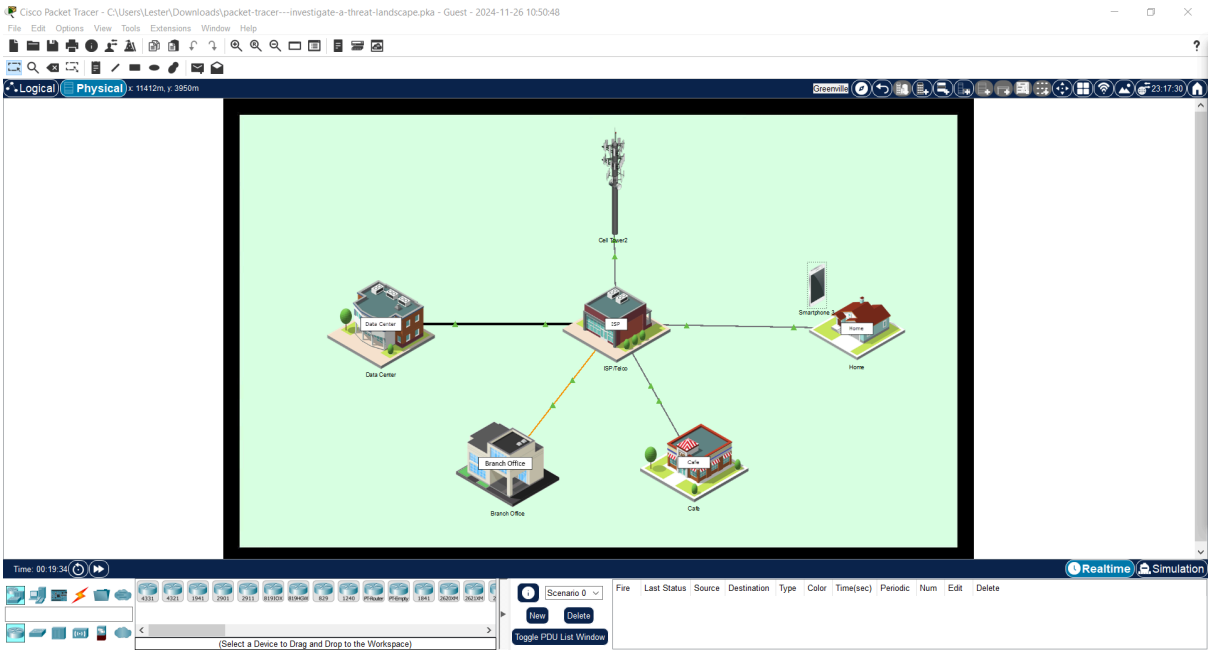
In this activity, you will investigate three vulnerabilities that can be exploited by threat actors.

Note: In this activity, both the Data Center and ISP/Telco sites are locked.

Instructions

Part 1: Investigate a Network Configuration Vulnerability

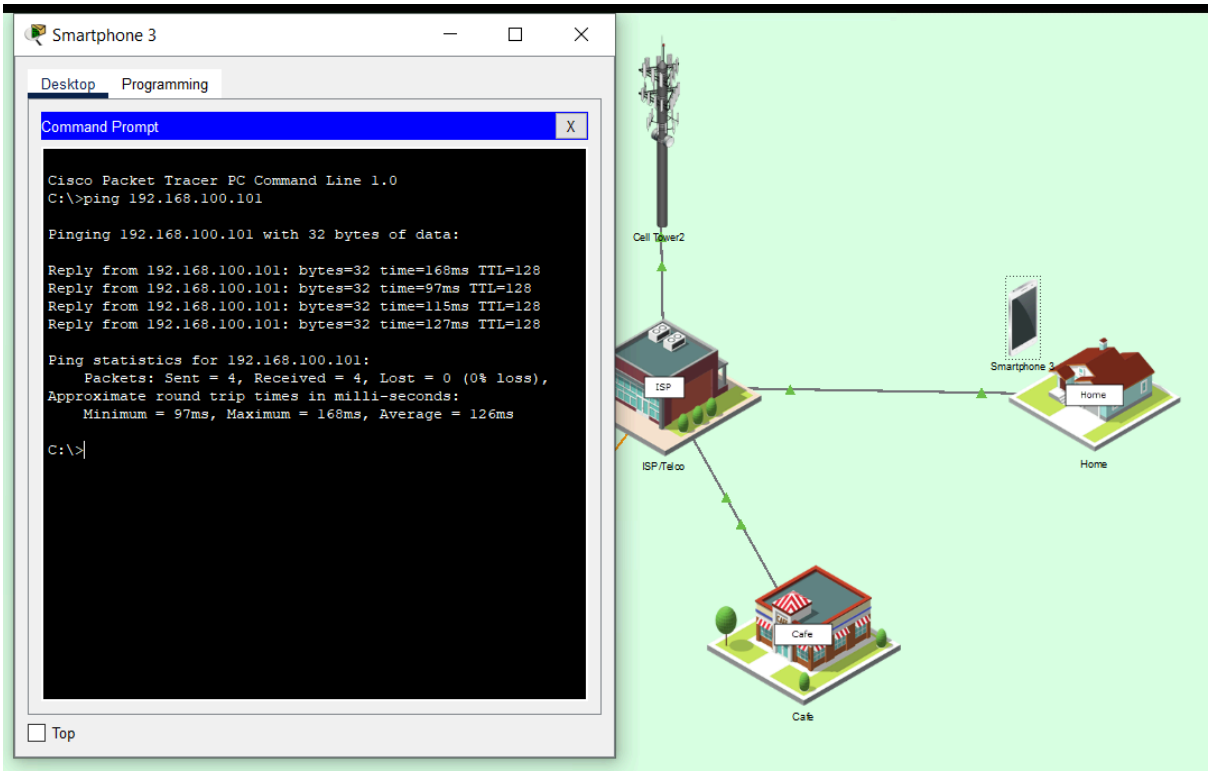
Sometimes network security vulnerabilities can happen by accident. For example, forgetting to update server or host software may expose known vulnerabilities that could easily be mitigated with a simple update. Similarly, vulnerabilities may be introduced when a network device is not configured properly, or a device is defective. In this part, you will explore a vulnerability that results from a device that is not properly configured with security best practices.



Step 1: Use a guest network to gain access to other devices on the network.

a. In **Greenville**, locate **Smartphone 3** just outside of the Home location.
   i. Mary is the owner of this smartphone. She is a friend of Bob who lives in the house. Mary is studying to eventually get a job in cybersecurity defense and is familiar with network penetration testing. She noticed that a guest wireless network is open and accessible by anyone. She connected to the guest network and used Nmap to run a scan, which can identify and discover details about all the active devices. One of the devices appears to be a webcam. Its IP address is 192.168.100.101.

b. Click **Smartphone 3**, and then click **Command Prompt**. Enter the command **ping 192.168.100.101**. After one or two "Request timed out" messages, the remaining pings should be successful.
   i. Mary informs Bob that the network is very vulnerable to attack. Someone could take control of the webcam, for example, and watch video from inside the house. Bob invites Mary to come in, investigate the issue, and propose a solution.



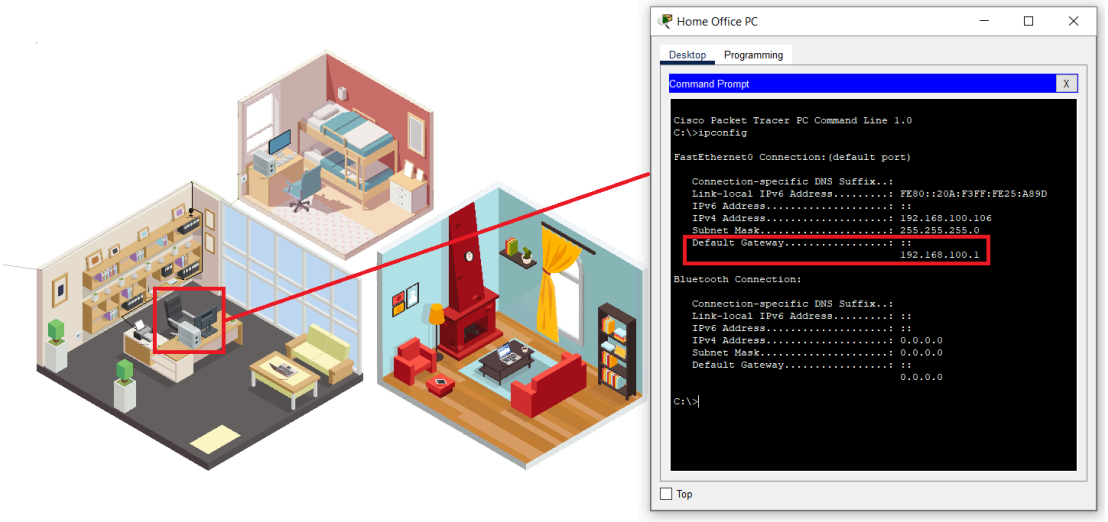
Step 2: Explore the Home network to identify the vulnerability.

a. Click **Home**. Knowing that home routers typically control home wireless networks, Mary heads straight for the home office and sits behind the desk. She will use the **Home Office PC** to connect to the router. But first she needs to determine the IP address.

b. Click **Home Office PC** > **Desktop tab** > **Command Prompt**, and then enter the command **ipconfig**.

The default gateway is the IP address for the **Home Wireless Router**.

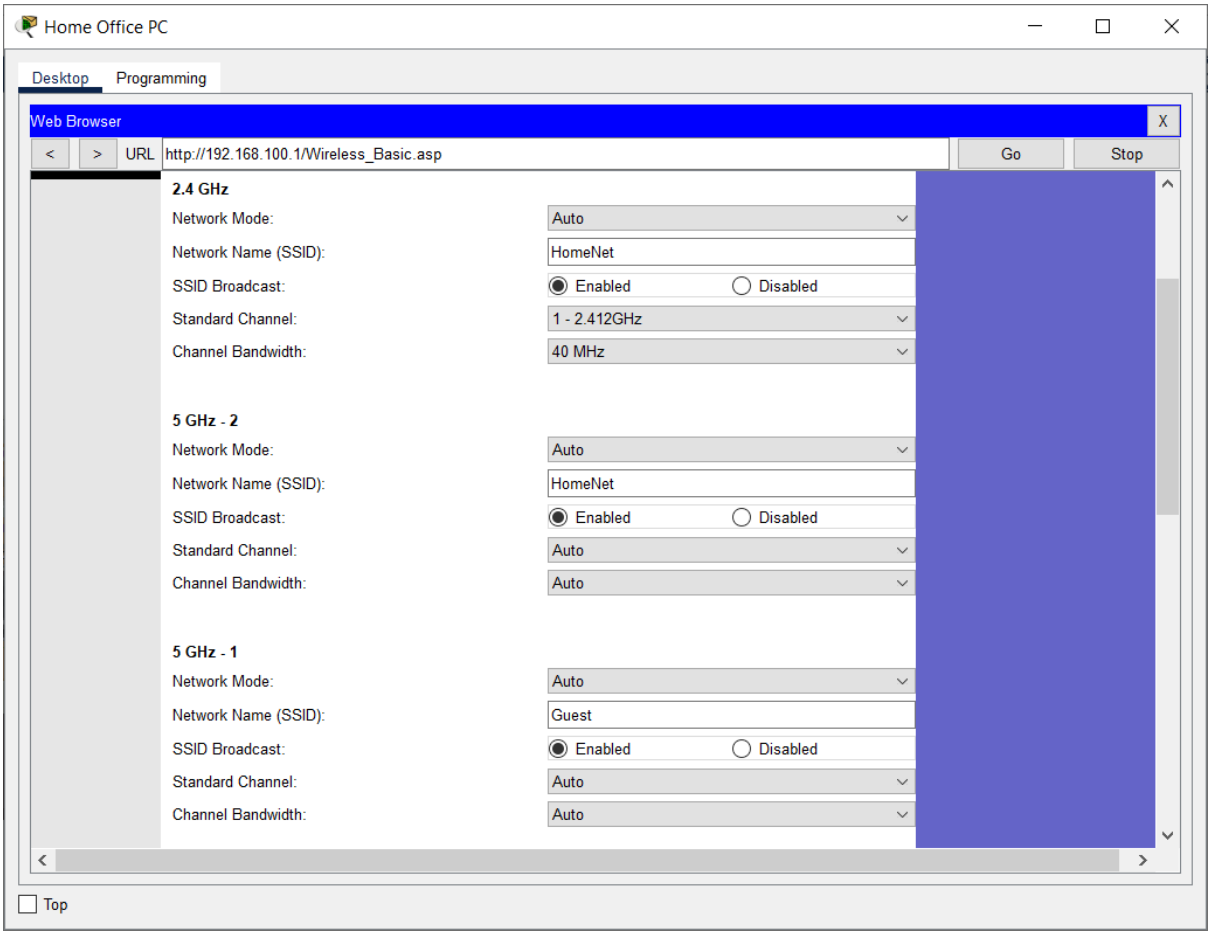
What is the IP address?
R: 192.168.100.1



c. Next, Mary uses the Web Browser to connect to the Home Wireless Router. Close the Command Prompt and click Web Browser. Enter the default gateway IP address.

d. Bob does not have the documentation for the router nor does he know the login credentials. Mary looks up the router model on the internet and discovers that the default credentials use ***admin*** for both the username and password. Login to Home Wireless Router.

e. Click **Wireless**. Review the **Basic Wireless Settings** for each of the three radios that are part of the wireless router.



Which of the radios are active?
R: All three of them are active.

What are the SSIDs that are assigned to these radios?
R: For the 2.4 GHz and 5 GHz-2 radios, the SSID is HomeNet. For the 5 GHz-1 radio, the SSID is Guest.

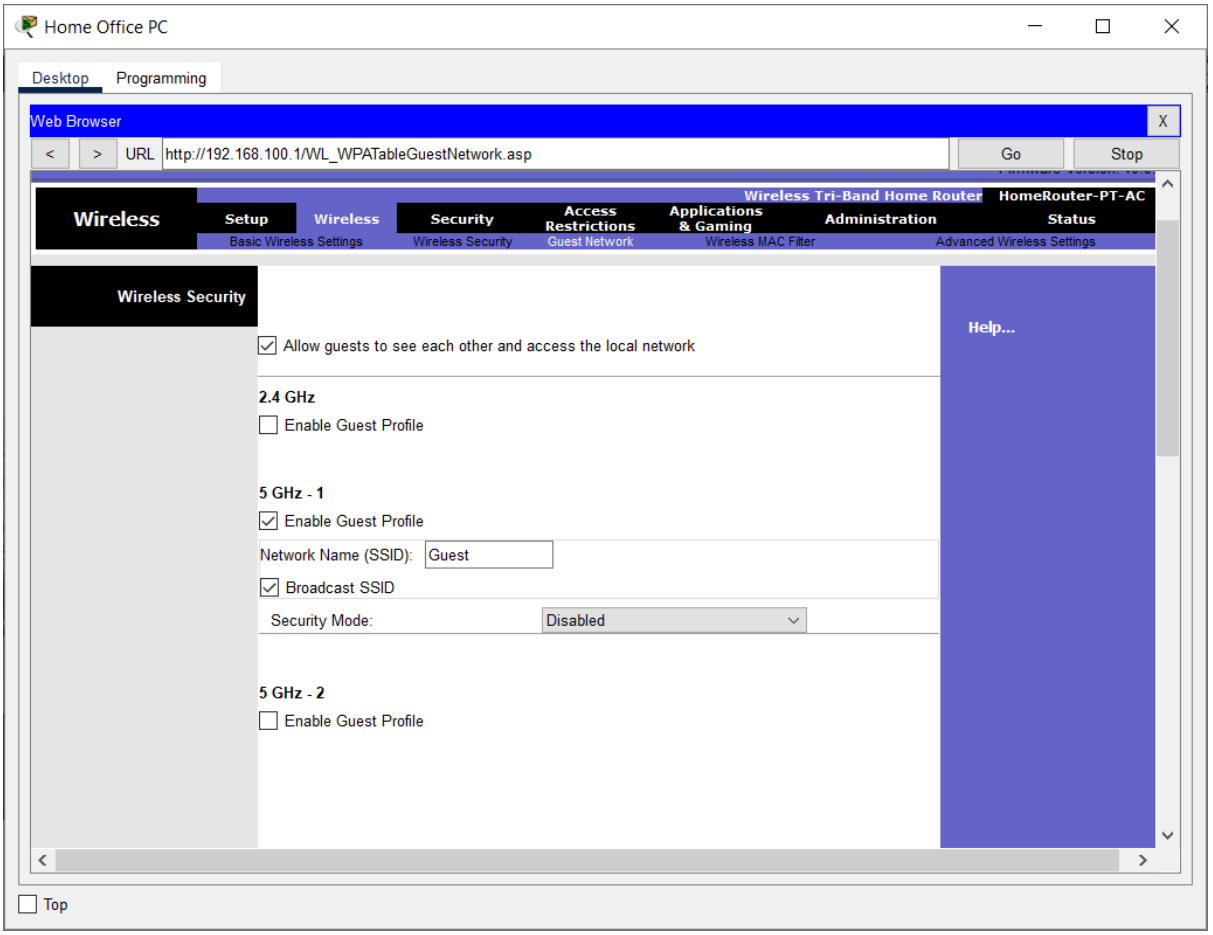
f. Click the Wireless Security submenu.

Is security activated for each of the radios? Are passphrases set?
R: Security is activated for the 2.4 GHz and 5 GHz-2 radios. Passphrases are set for those radios but security is not set for the 5 GHz-1 radio.

g. Mary was able to access the network from outside without logging in; therefore, she investigates further. Click the Guest Network submenu and investigate the settings.

Is the Guest network active? If so, on which radio?
R: The Guest network is active. It is configured on the 5 GHz-1 radio.

A wireless Guest network should only provide access to the internet for guests. It should not permit guests to access the devices on the local network inside the house. In this case, guests can access the local network. This indicates that the home router is misconfigured.



What would you propose Bob do to secure this network?

R: The guest network should be deactivated or configured with basic security such as strong authentication, SSID broadcast disabled, and access to local network devices disabled.

Part 2: Investigate a Phishing Malware Vulnerability

Phishing is a type of social engineering attack where a threat actor disguises themself as being a legitimate, trusted source in order to trick you into installing malware on your device, or sharing personal or financial information. Phishing attacks typically come through emails or phone calls. Unlike other network vulnerabilities, the primary vulnerability in phishing attacks is the users of the network. For this reason, an important defense against phishing is training users on how to prevent phishing exploits.

In this part, you will simulate and investigate a phishing attack.

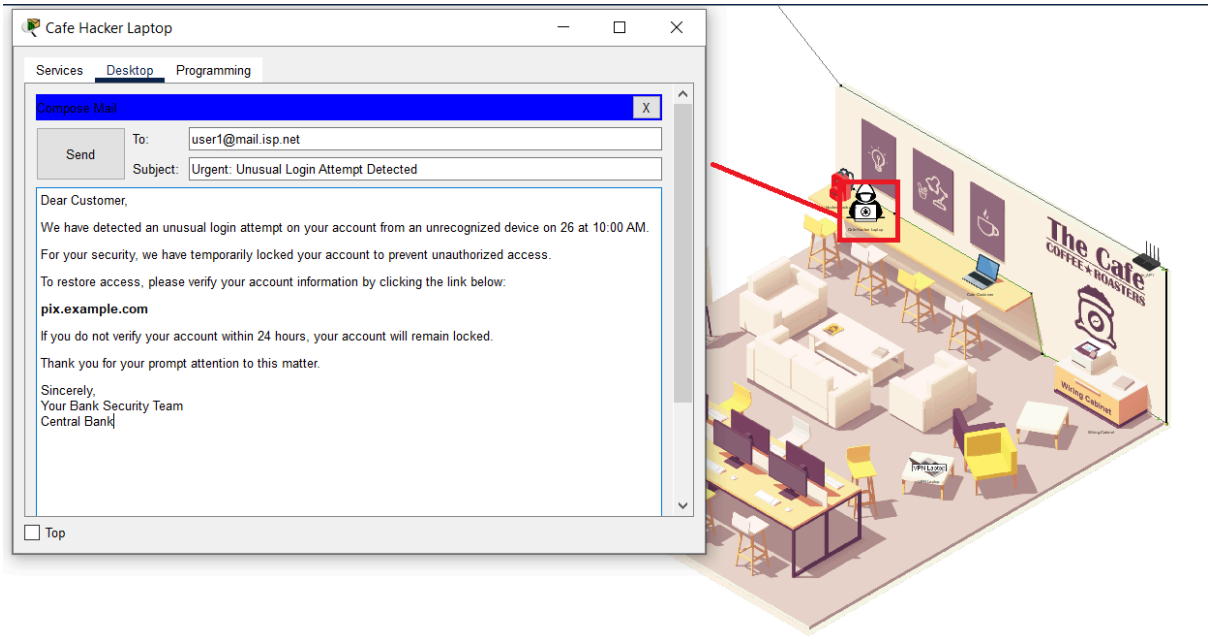
Step 1: Pose as a threat actor and create a phishing email.

a. Navigate to the Cafe network

b. Click the Cafe Hacker Laptop > Desktop tab > Email.

c. Click Compose.

Use your imagination to write a phishing email. Your objective is to persuade the user to copy and paste a URL from your email message into their browser. Include the link pix.example.com in the email. You can look for example phishing emails online to see how threat actors write this type of email.



Note: Links in phishing emails are typically active or "hot" links. All the victim has to do is click it. However, Packet Tracer does not support the use of active links inside the email client.

d. Send your email to three people inside the Branch Office network. Their email addresses are as follows:
   i. user1@mail.isp.net
   ii. user2@mail.isp.net
   iii. user3@mail.isp.net

Step 2: Open the emails received from the threat actor.

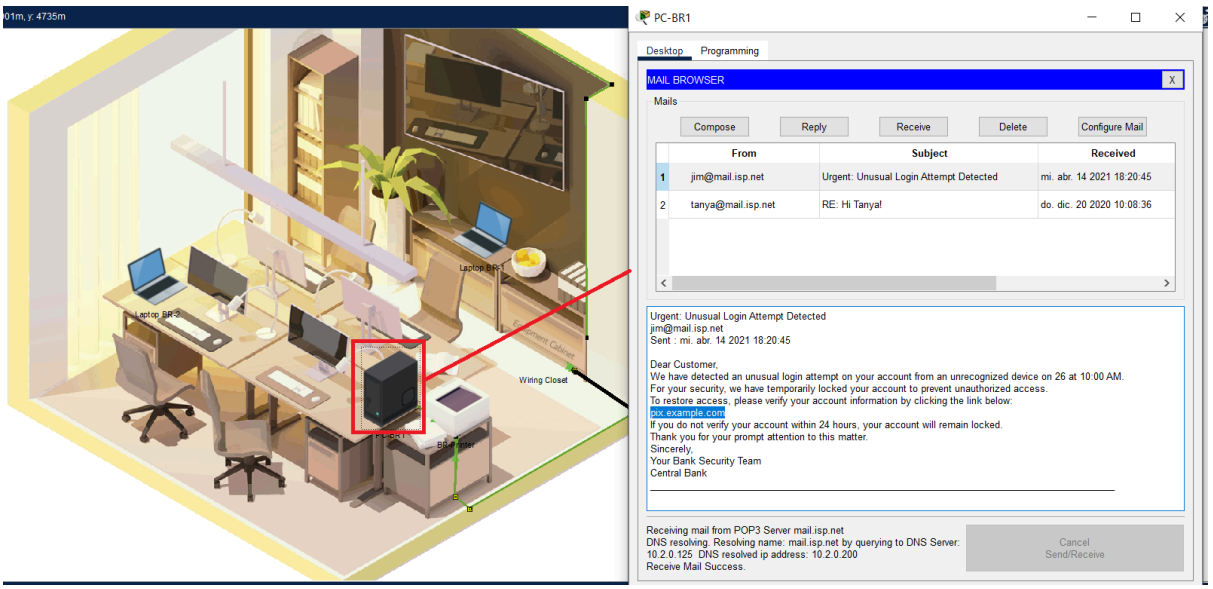
a. Navigate to the **Branch Office**.

b. Click one of the devices, either PC-BR1, Laptop BR-1, or Laptop BR-2.

c. Click Desktop tab > Email, and then click Receive. You should receive the email that you just sent.

Note: Packet Tracer may take up to a minute to converge. You may need to click Receive several times if the email is not successfully retrieved.

d. Optional: Go to the other victim devices, open their Email client, and click Receive to verify that they also received your phishing email.



Step 3: Pose as a victim and follow the phishing instructions.

a. Read the email and copy the website address.

b. Close the Mail Browser window, and then click Web Browser.

c. Paste the URL into the URL field, and then Go.

Note: Packet Tracer may take up to a minute to converge. You can click Fast Forward Time (Alt+D) to speed up the process.

What happened when the webpage loaded?
R: A message appeared that says that the hard drive has been encrypted and pay money to recover the files.

What is this type of attack called?
R: This is a ransomware attack. In a real world situation, this email is typically spread by a virus that automatically sends malicious emails to all the addresses in your contact list.

Describe the damage this type of attack can cause within an organization?
R: Hard drives could be encrypted and a lot of data could potentially be lost. In some cases, companies and other organizations have paid thousands of dollars in hopes of recovering the encrypted data.

Employees should be trained how to identify phishing emails and the actions that should be taken to prevent damage from them. In addition, organizations can configure firewalls, intrusion prevention systems, and other security devices and software, to block phishing emails before entering the network. Some businesses subscribe to services that compile and maintain lists of malicious websites. The security devices in the organization can then use these lists to automatically update filters for blocking malicious traffic.

Part 3: Investigate a Wireless Network and DNS Vulnerability

Your average network user tends to trust open Wi-Fi networks out in public places. Using Wi-Fi instead cellular data services can provide faster data rates and be more cost effective. However, threat actors can configure a laptop with a Wi-Fi interface that can act as both a Wi-Fi access point and a Wi-Fi client. This means that threat actors can create their own wireless networks and broadcast a convincing SSID to potential victims in public places. Threat actors use these rogue access points to create main-in-the-middle attacks. In this attack, threat actors can capture and read all the wireless traffic from devices that associate with the rogue access point, potentially learning usernames, passwords, and other confidential information.

In this part, you will investigate how a rogue access point can be used to entice users to connect to a fake wireless network. When combined with network services such as DHCP and DNS, users can become victims of malicious website attacks through DNS hijacking.

Step 1: Connect to the threat actor's wireless network.

a. Navigate to the **Cafe**. Notice the threat actor sitting in the corner.

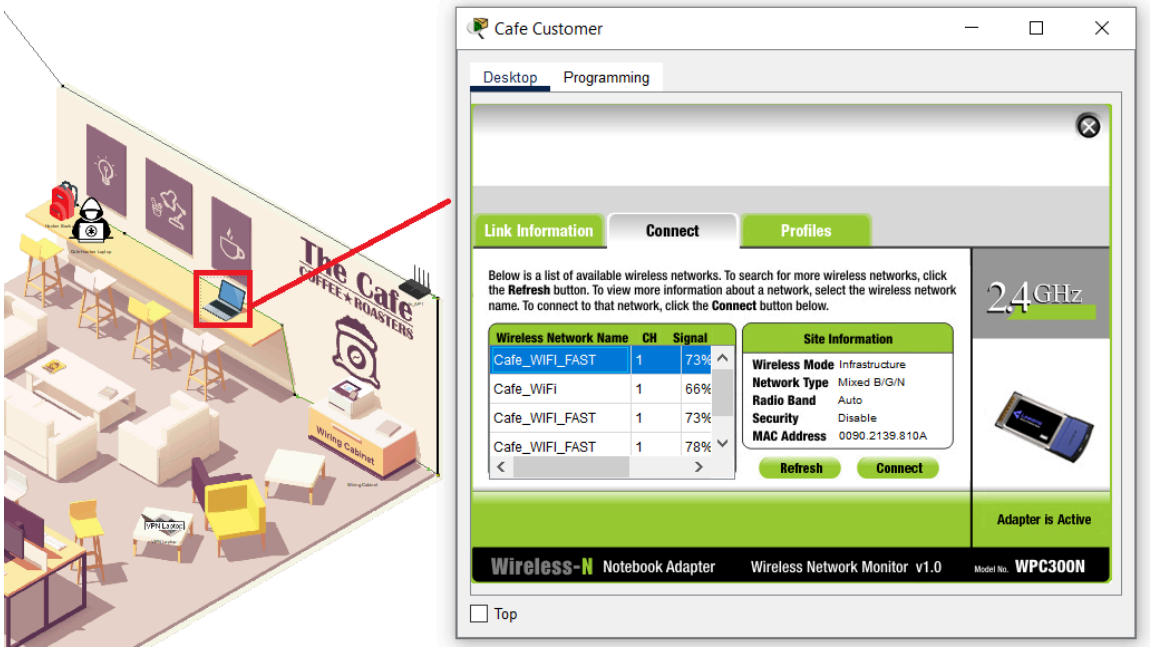
b. Click the **Hacker Backpack** and investigate the contents. In his backpack, he has a wireless router and a network sniffer. His goal is to intercept user traffic and direct it to a malicious server.

c. Return to the Cafe and click the Cafe Customer laptop > Desktop tab > PC Wireless application.

d. Click the Connect tab. You may need to click Refresh to see the list of available wireless networks.

If you were in the Cafe, which wireless network would you choose to connect to?
R: The Cafe_WI-FI_FAST network is very tempting. It is named to look legitimate, but better than the real network. The Cafe_WiFi network is the only one with security enabled so I need to ask for the password instead of doing a quicker connection using the other.

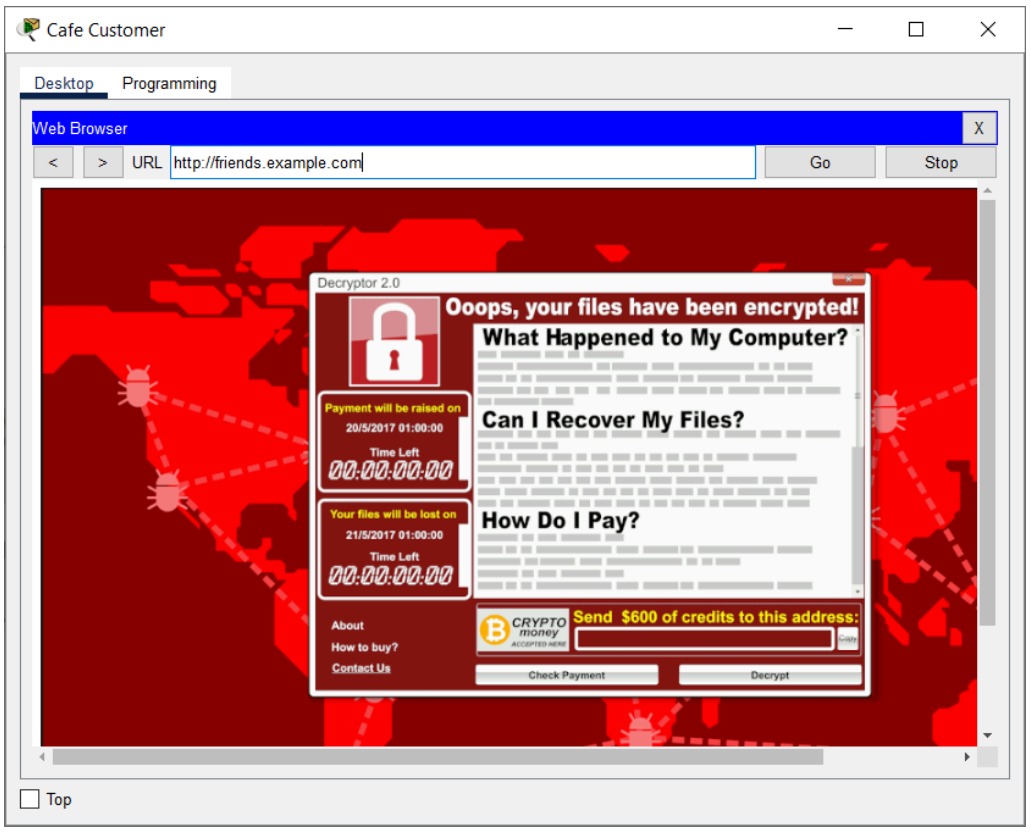
e. Click any of the **Cafe_WI-FI_FAST** network names and then click Connect.



Step 2: Visit your favorite social media site.

a. Close the PC Wireless application and click Web Browser.

b. In the URL field, enter ***friends.example.com***, and then click Go. This website is supposed to be a legitimate social network in this simulation.



What happened?
R: Although the URL was friends.example.com, it was taken to the malware server.

What was the URL for the malware server that was used in the phishing attack scenario? Is it the same?
R: The URL for the previous scenario was pix.example.com. It is a different URL but looks like the same server.

Step 3: Investigate the source of the attack.

a. Close the Web Browser and click IP Configuration.

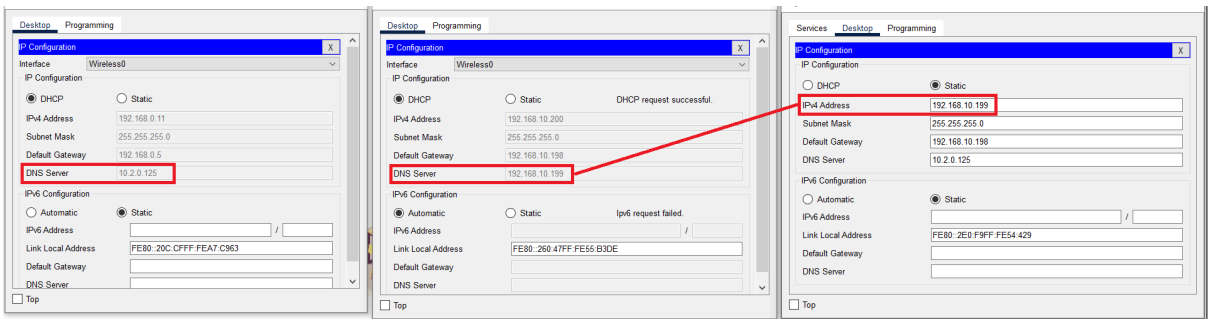
b. In the Cafe, click VPN Laptop > Desktop tab > IP Configuration.

c. Click Cafe Customer from your task bar to bring it back into view and then arrange the two IP Configuration windows side by side. Compare the values between the two devices.

What are the differences between the addresses of the two laptops?
R: The host IP addresses are different, but this is normal. Each host on a LAN needs a unique IP address. The subnet masks are the same but he DNS server addresses are different.

d. Investigate the Cafe Hacker Laptop.

What is its IP address? Why is this significant?
R: 192.168.10.199. Is it the same as the DNS server address that is configured on the Cafe Customer laptop.



On the Cafe Hacker Laptop, click the **Services** tab > **DNS**.

e. Locate the Name for the friends.example.com website. Note that the IP address is the same IP address as is associated with pix.example.com from the phishing attack earlier.

f. Under Services, click **DHCP**. Notice that the DNS server address distributed to the hosts over DHCP is the same one assigned to Cafe Customer.

What are the steps in this attack?
R: When Cafe Customer connected to the rogue access point's wireless network, it received an IP address configuration from DHCP. The DHCP server is configured to distribute the hacker laptop address as the DNS server address. The DNS server on the Cafe Hacker Laptop associates the IP address of a malicious server, 10.6.0.250, with the name of a popular website, friends.example.com. When the user of the Cafe Customer laptop tries to visit the website, traffic is redirected to the malicious server instead. Ransomware is then installed on the Cafe Customer laptop and the user's files are encrypted.

Summary

In this activity, you have looked at three different ways in which vulnerabilities can lead to exploits. As an informed network user or cybersecurity professional, it is your responsibility to think about the different ways in which such vulnerabilities can be detected and mitigated before a cyber attack occurs.