

## **VxLEARN Networks**

Networking & Cybersecurity Track  
Simulated Employment Program

### **Lab Report: Investigate a Threat Landscape**

Prepared by:  
Kudzaishe Majeza  
Junior Network Engineer – VxLEARN Networks

Mentor:  
Titus Majeza  
Senior Network Engineer

Date: 05 December 2025

## Table of Contents

<b>1. Introduction.....</b>	<b>4</b>
<b>2. Part 1 – Network Configuration Vulnerability .....</b>	<b>5</b>
<b>2.1 Connecting to the Guest Network.....</b>	<b>5</b>
<b>2.2 Discovering the Router’s IP Address.....</b>	<b>7</b>
<b>2.3 Logging into the Router .....</b>	<b>8</b>
<b>2.4 Wireless Settings Review.....</b>	<b>9</b>
<b>2.5 Wireless Security Review.....</b>	<b>10</b>
<b>2.6 Recommended Fixes .....</b>	<b>11</b>
<b>3. Part 2 – Phishing Malware Vulnerability .....</b>	<b>12</b>
<b>3.1 Threat Actor Writes a Phishing Email .....</b>	<b>12</b>
<b>3.2 Victims Receive the Email.....</b>	<b>14</b>
<b>3.3 Victim Opens the Malicious URL.....</b>	<b>16</b>
<b>3.4 Attack Type.....</b>	<b>17</b>
<b>3.5 Potential Organizational Damage .....</b>	<b>18</b>
<b>4. Part 3 – Rogue Wi-Fi &amp; DNS Hijacking Vulnerability .....</b>	<b>18</b>
<b>Step 1: Inspect the Threat Actor’s Setup.....</b>	<b>18</b>
<b>1.1 View the Hacker Backpack.....</b>	<b>18</b>
<b>Step 2: Scan Available Wi-Fi Networks.....</b>	<b>19</b>
<b>2.1 Open the PC Wireless App on the Café Customer Laptop .....</b>	<b>19</b>
<b>2.2 Explain which SSID is suspicious .....</b>	<b>22</b>
<b>Step 3: Connect the Victim to the Rogue Wi-Fi Network .....</b>	<b>22</b>
<b>3.1 Connect to “Cafe_WI-FI_FAST” .....</b>	<b>22</b>
<b>Step 4: Victim Visits Social Media Website .....</b>	<b>23</b>

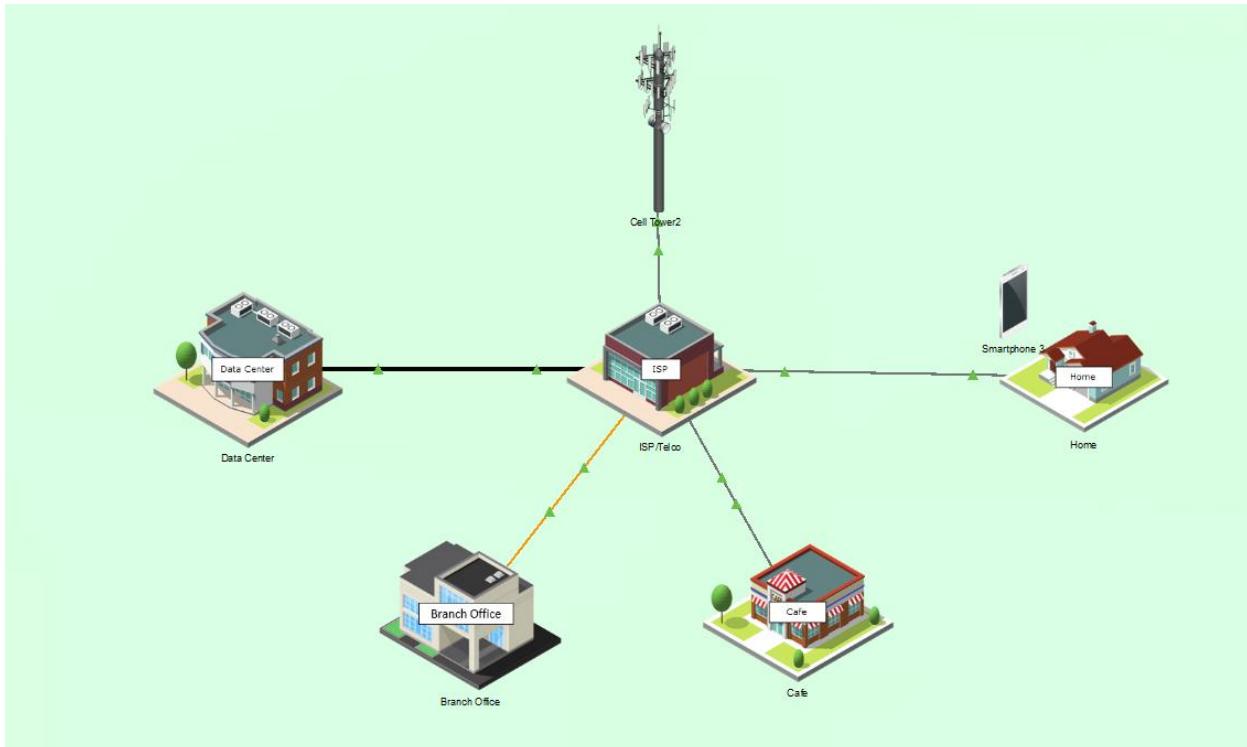
4.1 Open the Browser on the Victim Laptop Type:.....	23
Step 5: Compare Network Settings (Victim vs. Legit Laptop) .....	24
5.1 Open IP Configuration on Victim .....	24
5.2 Open IP Configuration on the VPN Laptop (legitimate device) ..	25
5.3 Compare the Two Laptops.....	25
Step 6: Investigate the Hacker’s DNS Server .....	26
6.1 Open Café Hacker Laptop → Services → DNS.....	26
Step 7: Inspect the Rogue DHCP Server .....	27
7.1 Open Café Hacker Laptop → Services → DHCP.....	27
Steps of the Attack .....	28
5. Summary of Findings.....	29
6. Recommendations .....	29

# 1. Introduction

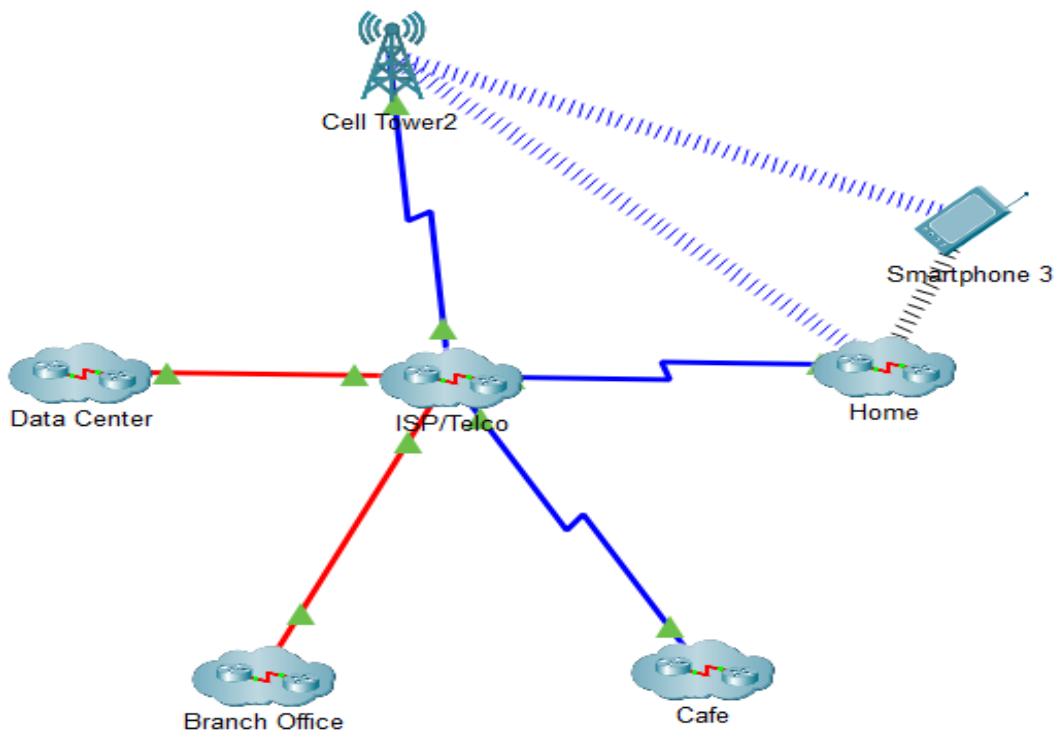
In today's cybersecurity environment, threats can come from anywhere misconfigured home routers, careless user actions, or malicious actors setting up fake networks. This lab demonstrates **three real-world vulnerabilities**:

1. A home router misconfiguration that exposes internal devices
2. A phishing attack that installs malware
3. A rogue Wi-Fi access point performing DNS hijacking

This report explains each vulnerability step-by-step, shows the attack flow, and provides professional recommendations to prevent these risks.



Physical Topology



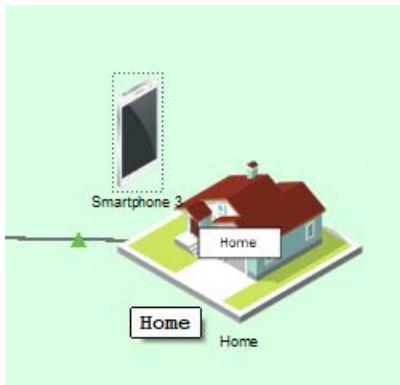
Logical Topology

## 2. Part 1 – Network Configuration Vulnerability

### 2.1 Connecting to the Guest Network

Mary uses *Smartphone 3* and notices an **open guest Wi-Fi network**.

No password → anyone can join → major security risk.



Smartphone 3 connecting to guest network

She then pings the suspicious device:

`ping 192.168.100.101`

The screenshot shows a Cisco Packet Tracer window titled 'Smartphone 3'. Inside, a 'Command Prompt' window is open. The user has typed 'ping 192.168.100.101' and is receiving responses from the target IP address. The output is as follows:

```

Cisco Packet Tracer PC Command Line 1.0
C:>192.168.100.101
Invalid Command.

C:>ping 192.168.100.101

Pinging 192.168.100.101 with 32 bytes of data:

Reply from 192.168.100.101: bytes=32 time=142ms TTL=128
Reply from 192.168.100.101: bytes=32 time=130ms TTL=128
Reply from 192.168.100.101: bytes=32 time=75ms TTL=128
Reply from 192.168.100.101: bytes=32 time=82ms TTL=128

Ping statistics for 192.168.100.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 75ms, Maximum = 142ms, Average = 107ms

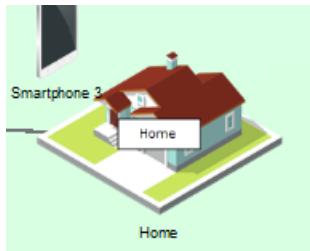
C:>

```

After ARP completes, replies come back → meaning the webcam is accessible.

## 2.2 Discovering the Router's IP Address

Click **Home**:



From the **Home Office PC**:

**Ipconfig**

A screenshot of a Windows-style Command Prompt window titled "Command Prompt". The window is running on a virtual machine named "Home Office PC". The title bar also shows tabs for "Desktop" and "Programming". The command "ipconfig" was entered, and the output shows network configuration for two connections: "FastEthernet0 Connection: (default port)" and "Bluetooth Connection".

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::20A:F3FF:FE25:A89D
IPv6 Address.....: ::
IPv4 Address.....: 192.168.100.106
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                           192.168.100.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
                           0.0.0.0

C:\>
```

**Ipconfig output**

**Default Gateway:**

**192.168.100.1**

This is the router's login address.

## 2.3 Logging into the Router

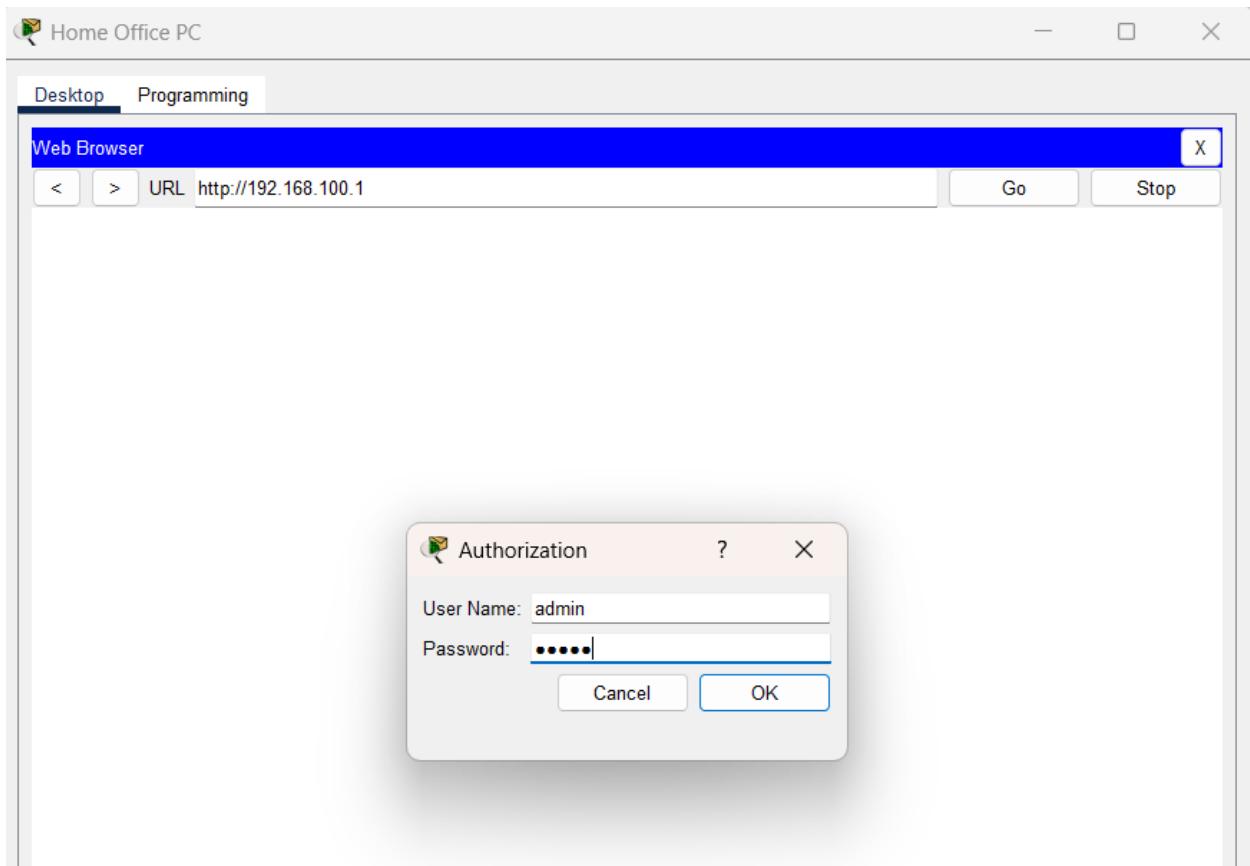
Mary opens the browser → enters the default gateway IP.

Router login appears.

Most home routers use:

- **Username:** admin
- **Password:** admin

**This is extremely insecure.**



router login screen

## 2.4 Wireless Settings Review

Under **Wireless → Basic Settings**, Mary checks all radios.

The screenshot shows a web browser window titled "Home Office PC" with the URL [http://192.168.100.1/Wireless\\_Basic.asp](http://192.168.100.1/Wireless_Basic.asp). The page is titled "Basic Wireless Settings". The top navigation bar includes tabs for Wireless, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The Wireless tab is selected, and its sub-tab "Basic Wireless Settings" is also selected. The main content area is divided into three sections: 2.4 GHz, 5 GHz - 2, and 5 GHz - 1. Each section contains fields for Network Mode (Auto), Network Name (SSID) (e.g., HomeNet), SSID Broadcast (Enabled or Disabled), Standard Channel, and Channel Bandwidth. In the 2.4 GHz section, the SSID Broadcast is set to Enabled. In the 5 GHz - 2 section, it is also set to Enabled. In the 5 GHz - 1 section, it is set to Enabled. A "Help..." link is located in the top right corner of the content area.

**Which radios are active?**

- 2.4 GHz → Active
- Guest Network Radio → Active

**SSIDs:**

- Home\_Network
- Home\_5G
- **Guest\_Network (open)**

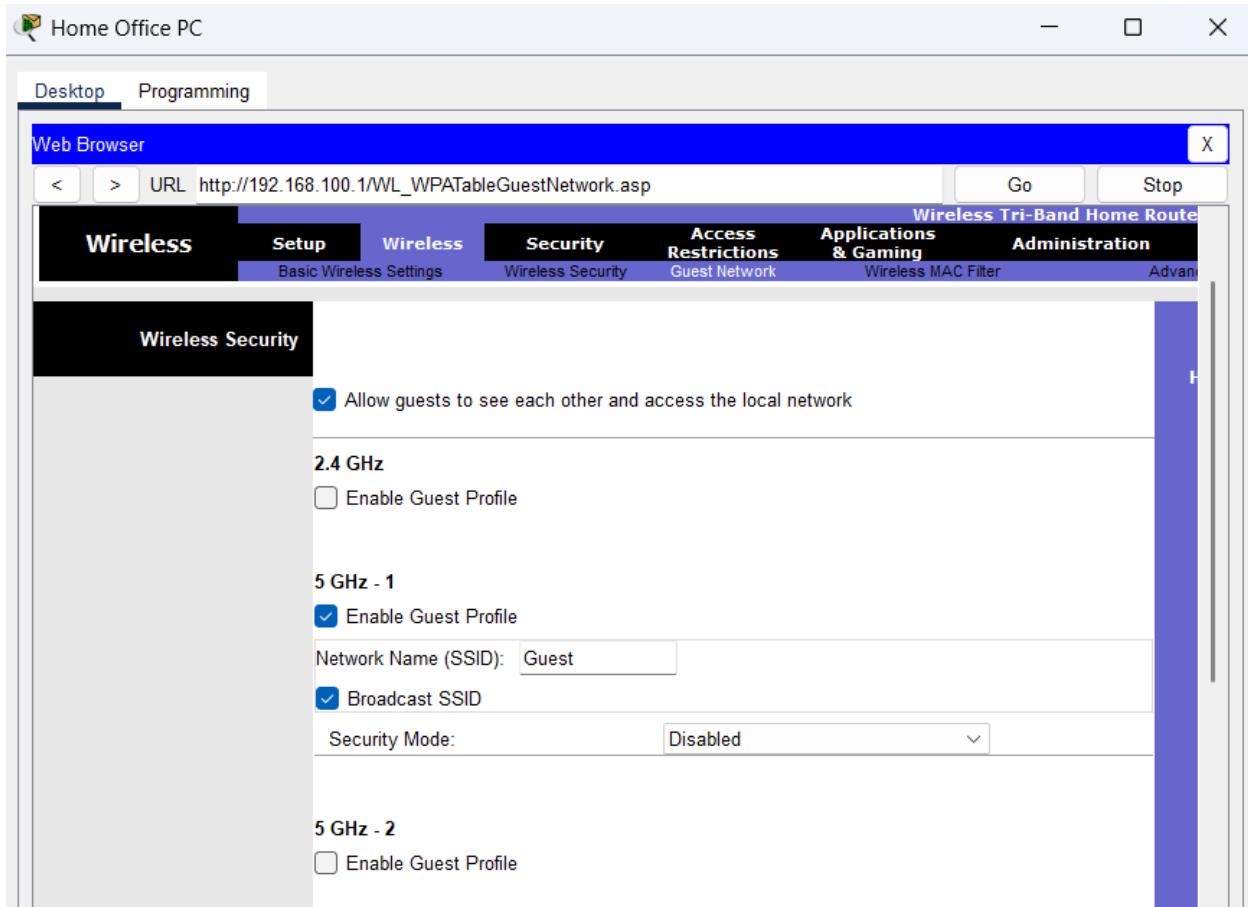
## 2.5 Wireless Security Review

### Under Wireless Security:

- Home\_Network → WPA2 enabled
- Guest Network → **No security**
- Guest network **allowed LAN access** → huge vulnerability

The screenshot shows a web browser window titled "Web Browser" with the URL [http://192.168.100.1/WL\\_WPATable.asp](http://192.168.100.1/WL_WPATable.asp). The page is titled "Wireless Tri-Band Home Router". The navigation bar includes tabs for Desktop, Programming, Web Browser, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Advanced. The "Security" tab is selected. The main content area is titled "Wireless Security". It displays configuration for three bands: 2.4 GHz, 5 GHz - 1, and 5 GHz - 2.

Band	Security Mode	Encryption	Passphrase	Key Renewal
2.4 GHz	WPA2 Personal	AES	homePa55	3600 seconds
5 GHz - 1	Disabled			
5 GHz - 2	WPA2 Personal	AES	homePa55	3600 seconds



This is how Mary accessed the webcam without logging in.

## 2.6 Recommended Fixes

Bob should immediately:

- Disable or secure the Guest Network
- Enable WPA2/WPA3 encryption
- Block guest access to LAN devices
- Change the default router password
- Update router firmware

### 3. Part 2 – Phishing Malware Vulnerability

#### 3.1 Threat Actor Writes a Phishing Email

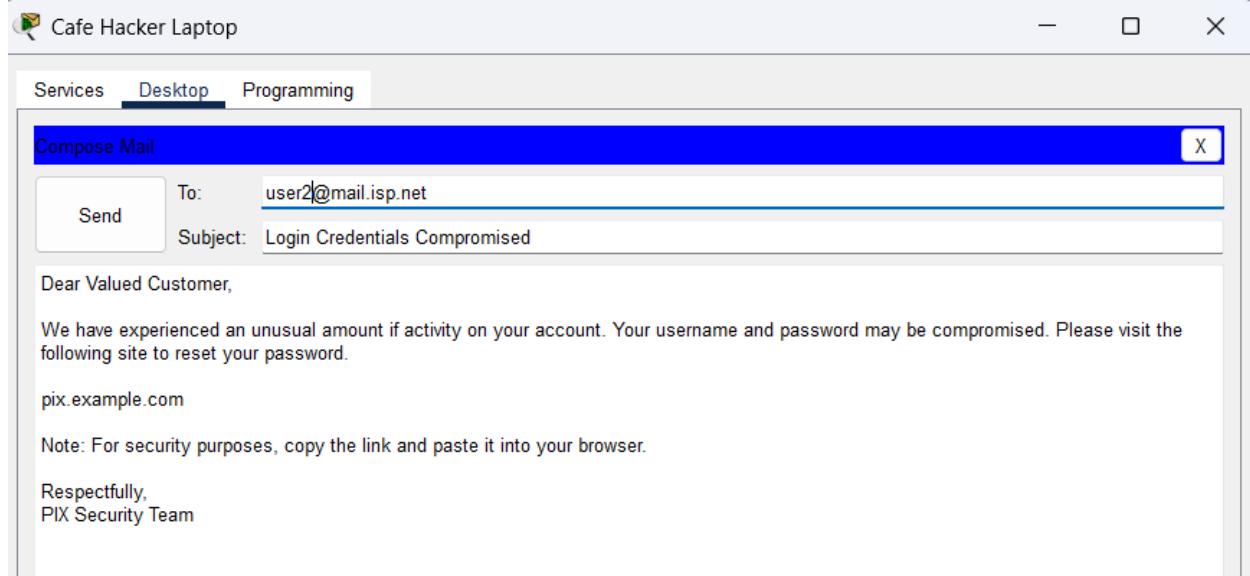
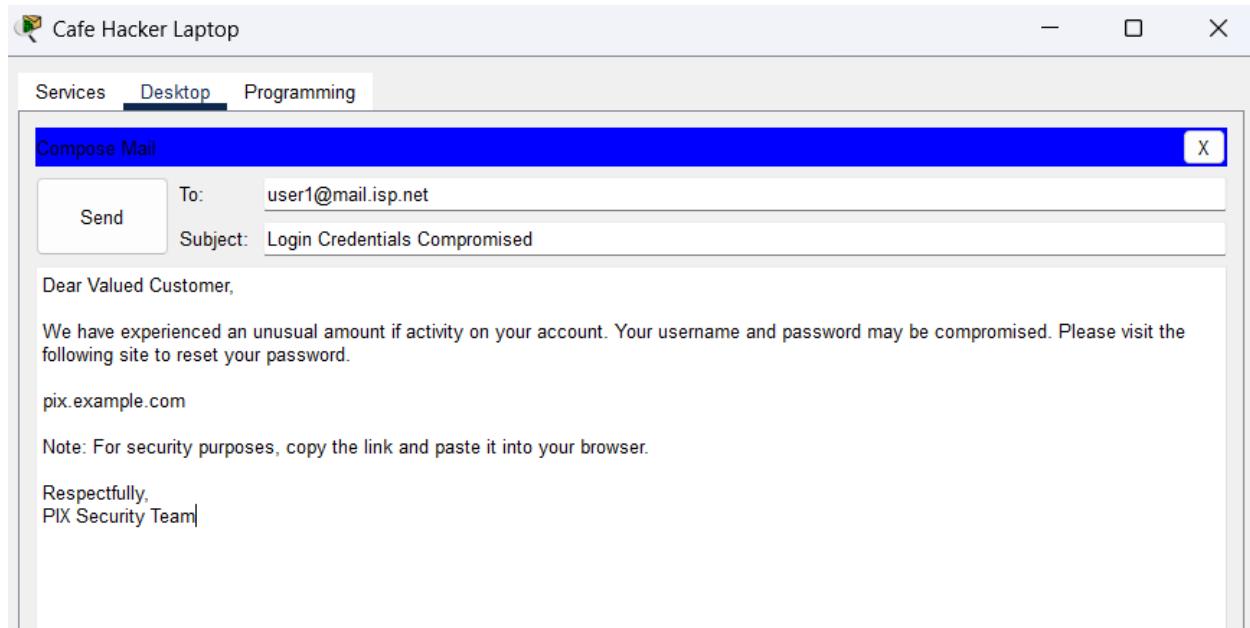
Click Café:

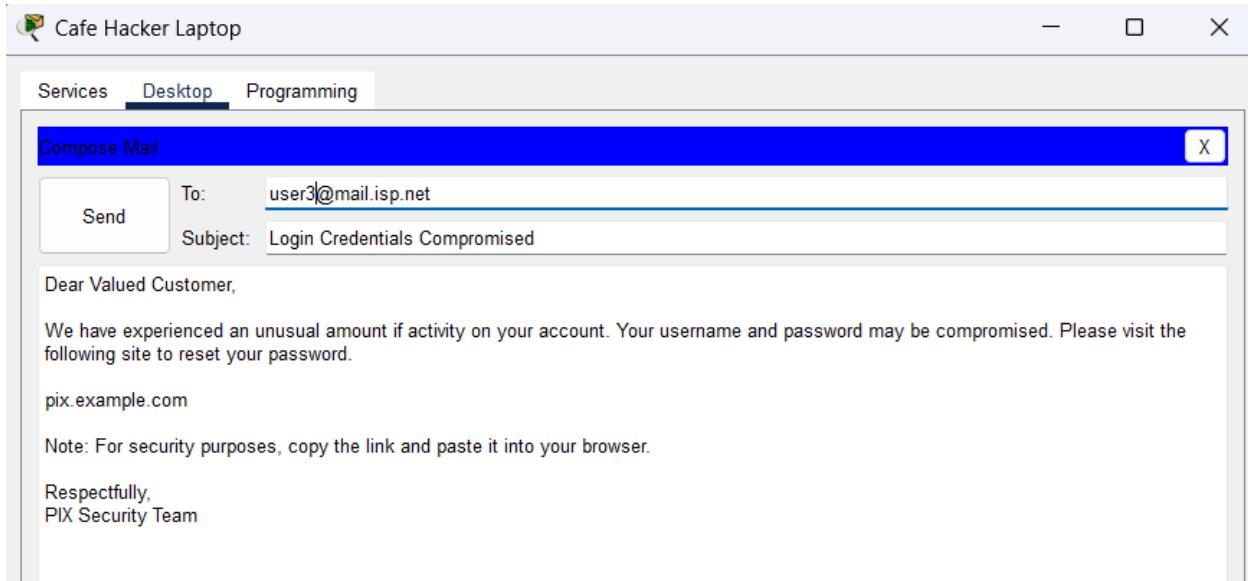


On the **Cafe Hacker Laptop** → **Email** → **Compose**, the attacker writes a fake email convincing users to visit:

`pix.example.com`



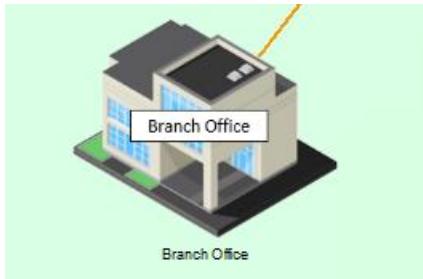




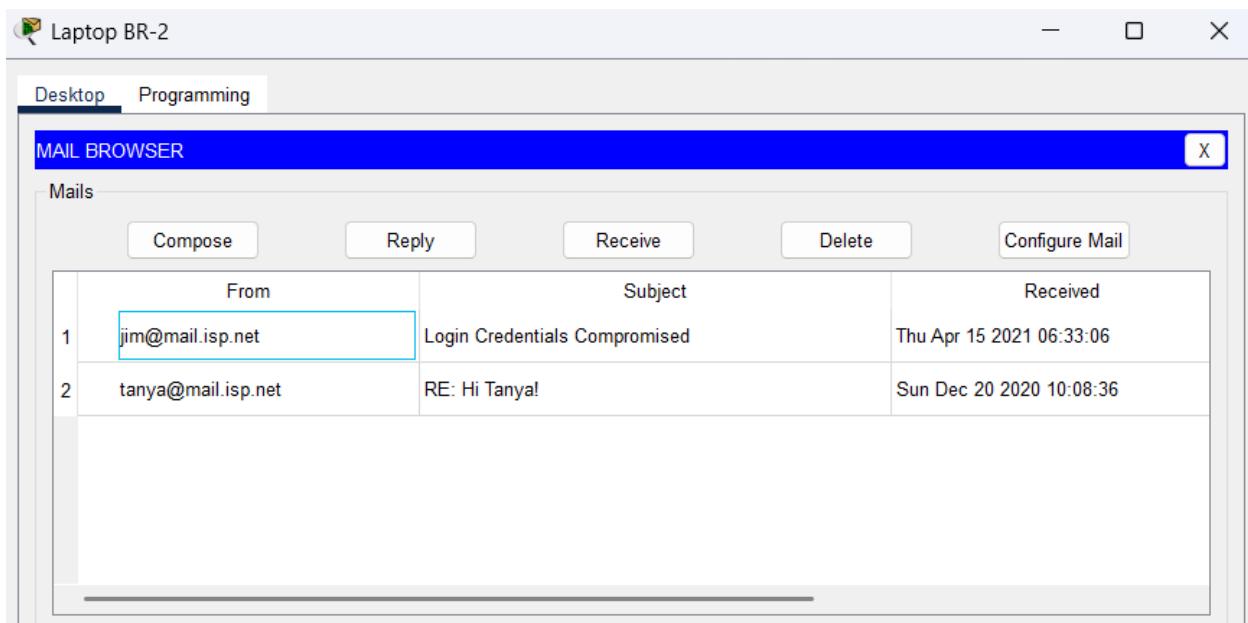
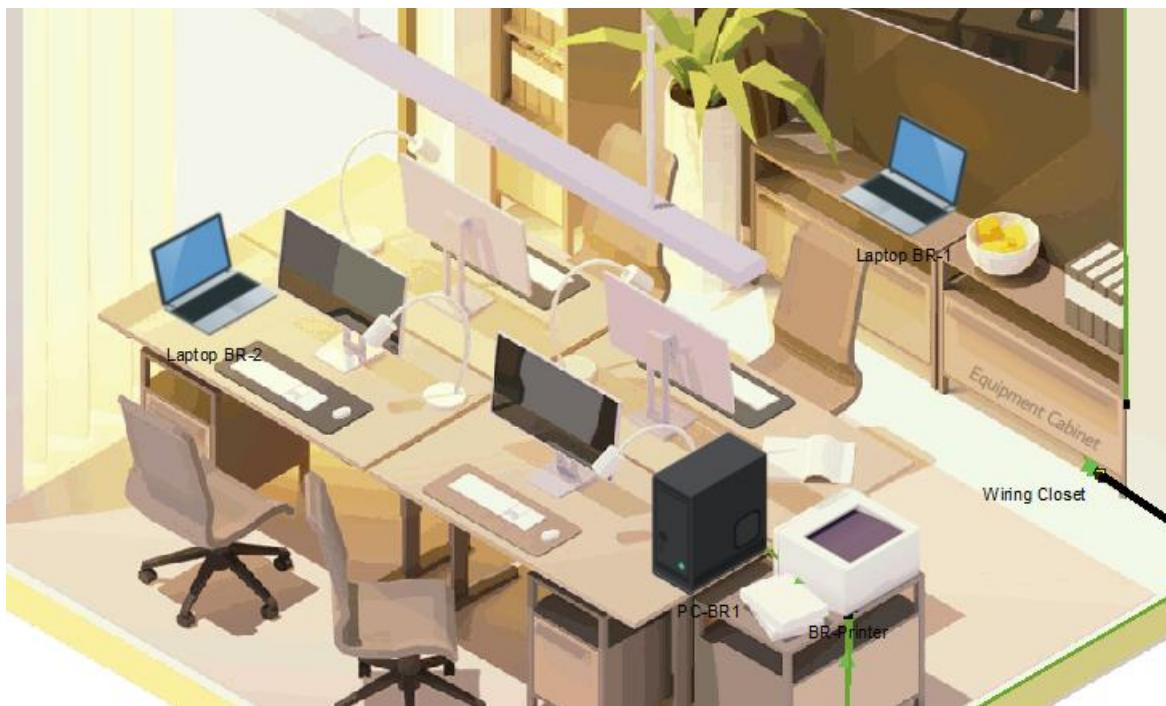
## phishing email

### 3.2 Victims Receive the Email

Click Branch Office:

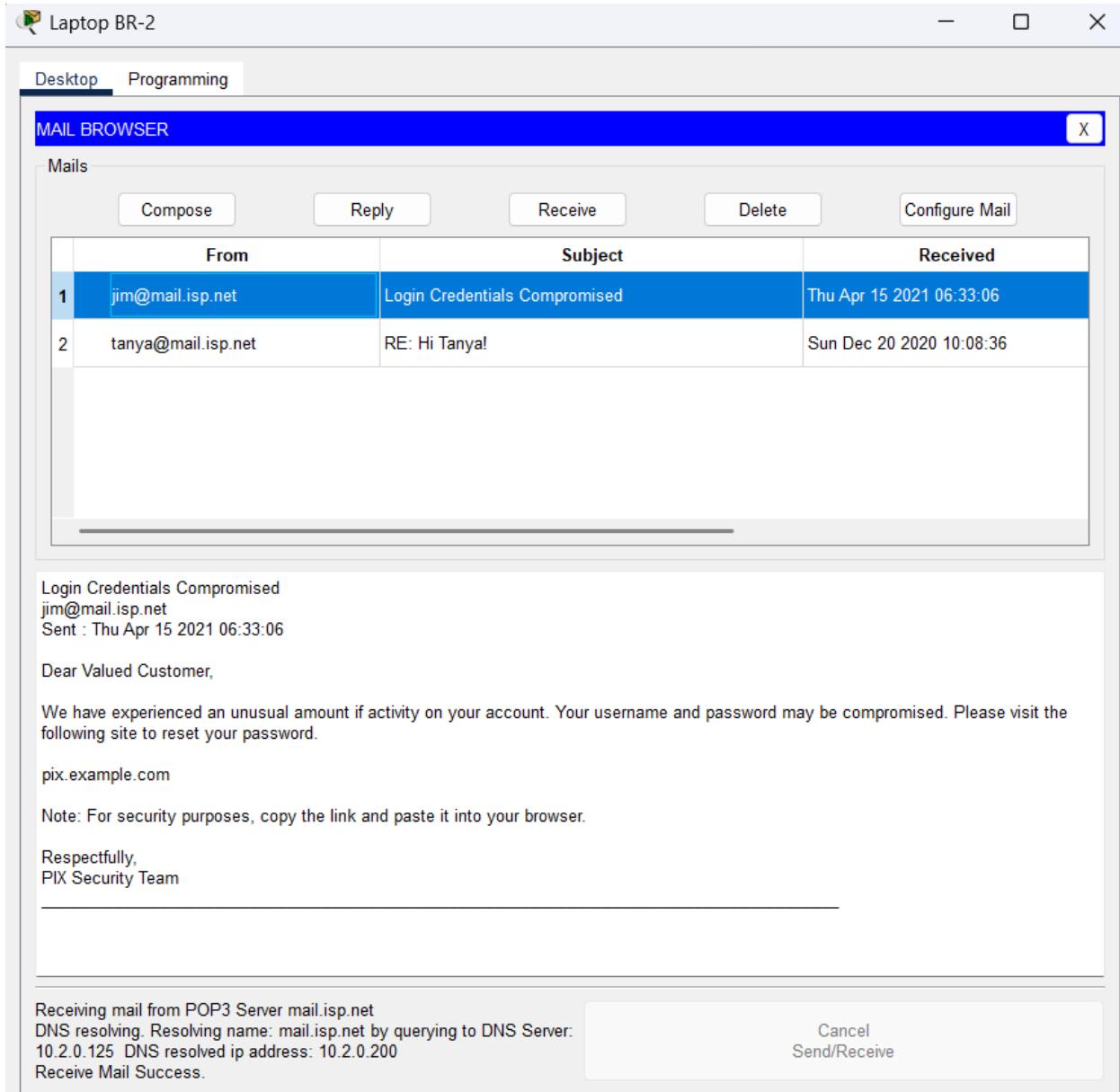


On PC-BR1, BR-Laptop 1, BR-Laptop 2 → Email → Receive, users get the phishing message.



### 3.3 Victim Opens the Malicious URL

User copies the URL → pastes into Web Browser → **malware website loads.**





What happened?

- The link redirected to a malicious site.
- The webpage loads a "compromised" page meant to infect the system.

### 3.4 Attack Type

This is a **phishing attack** leading to **malware installation**.

### 3.5 Potential Organizational Damage

A phishing attack like this can:

- Steal login credentials
- Spread malware to all contacts
- Encrypt company files (ransomware)
- Install backdoors
- Cause financial + reputational damage

## 4. Part 3 – Rogue Wi-Fi & DNS Hijacking Vulnerability

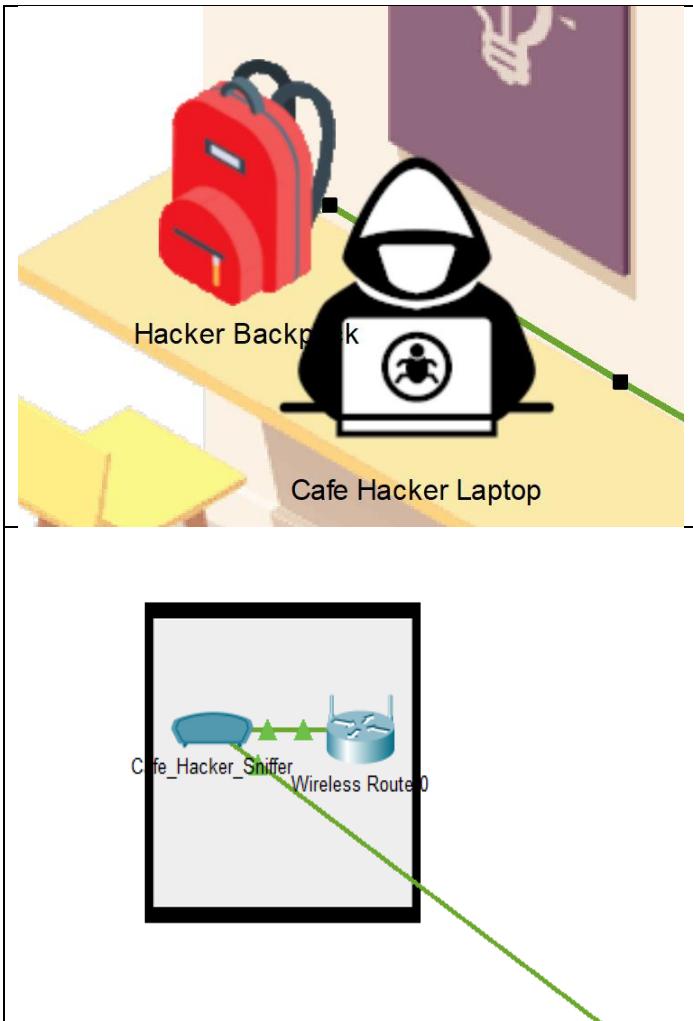
### Step 1: Inspect the Threat Actor's Setup

#### 1.1 View the Hacker Backpack

Click **Hacker Backpack** in the Café.

Inside, you will see:

- A portable wireless router
- A laptop with malicious services
- A network sniffer

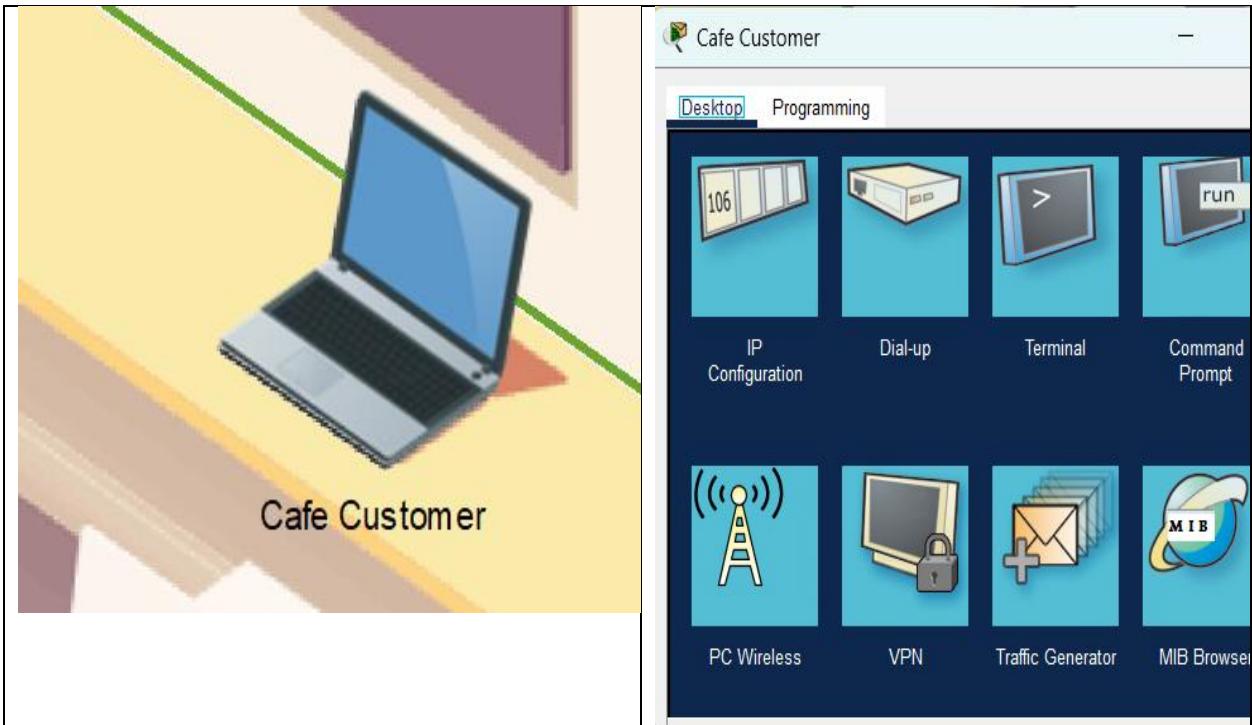


Hacker Backpack contents

## Step 2: Scan Available Wi-Fi Networks

### 2.1 Open the PC Wireless App on the Café Customer Laptop

- Click **Cafe Customer Laptop → Desktop → PC Wireless**



- Click the **Connect** tab
- Hit **Refresh**

You will see:

- Legit networks
- **Fake networks created by the attacker**

The rogue networks will look like:

Cafe\_WI-FI\_FAST

These names are intentionally appealing.



multiple Café Wi-Fi networks including the fake ones

## 2.2 Explain which SSID is suspicious

Examples of suspicious signs:

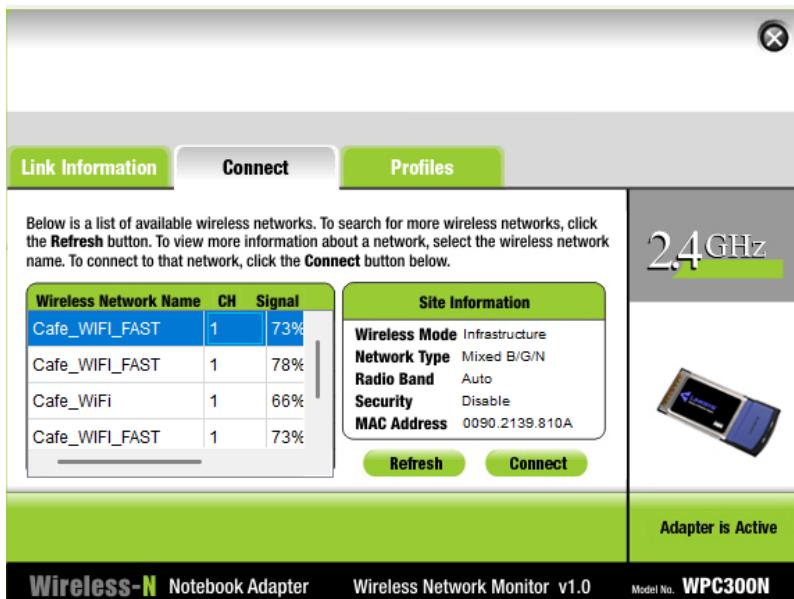
- Too many networks with similar names
- “FAST” marketing language
- Strong signal even when far away
- Open (no password)

## Step 3: Connect the Victim to the Rogue Wi-Fi Network

### 3.1 Connect to “Cafe\_WI-FI\_FAST”

Click the SSID → Press **Connect**

The victim is now joining the attacker’s fake network.



connection success to Cafe\_WI-FI\_FAST

# Step 4: Victim Visits Social Media Website

## 4.1 Open the Browser on the Victim Laptop

Type:

friends.example.com

Instead of loading the REAL page, the victim is redirected to:

- The attacker's malicious server
- The same server used in the phishing attack in Part 2
- A fake login/malware page



browser loading the malicious page instead of friends.example.com

# Step 5: Compare Network Settings (Victim vs. Legit Laptop)

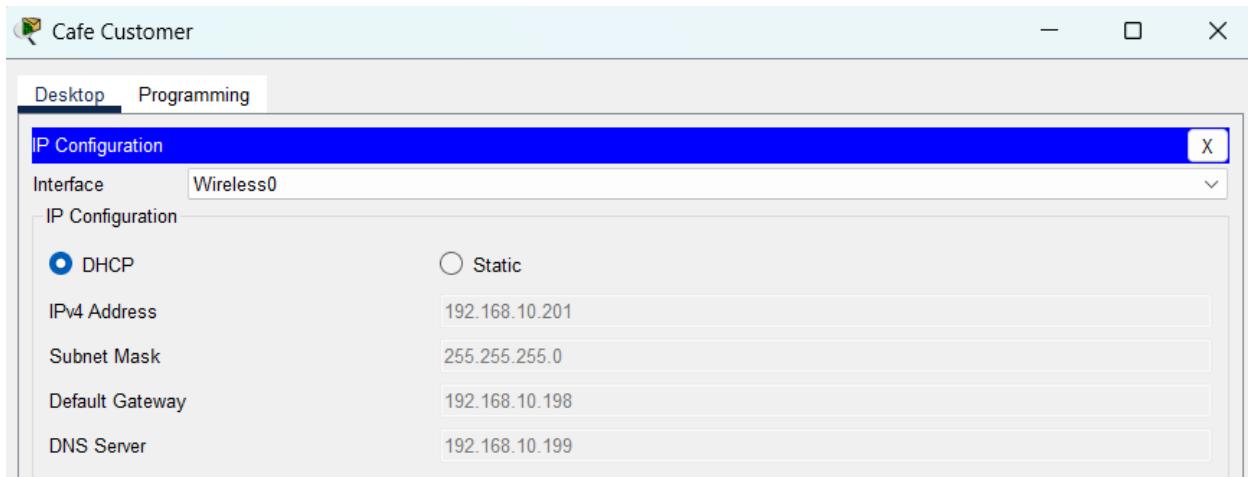
This is a crucial part of understanding DNS hijacking.

## 5.1 Open IP Configuration on Victim

Cafe Customer Laptop → Desktop → IP Configuration

Record:

- IP Address
- Default Gateway
- DNS Server

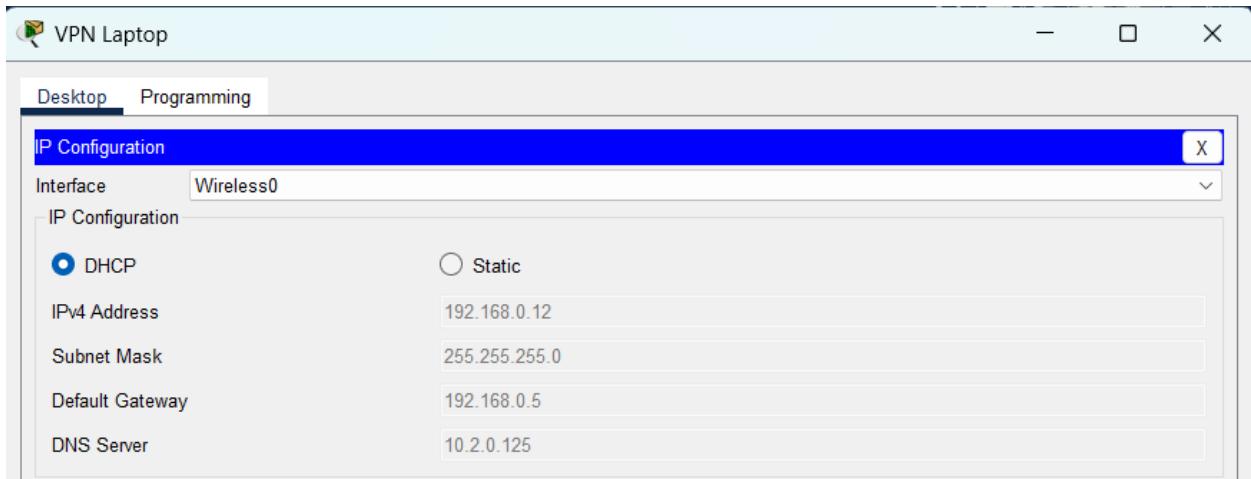


victim's IP configuration window

## 5.2 Open IP Configuration on the VPN Laptop (legitimate device)

Cafe VPN Laptop → Desktop → IP Configuration

This laptop uses the real / legitimate café network.



VPN Laptop's IP configuration

## 5.3 Compare the Two Laptops

Explain the differences:

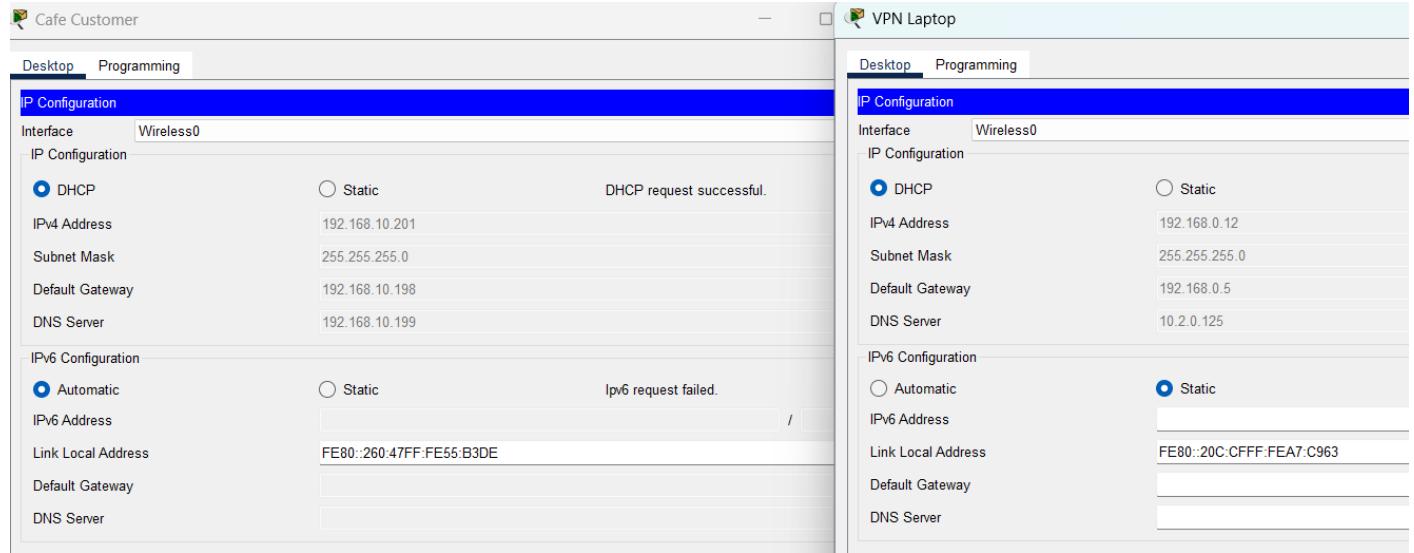
Victim Laptop:

- **IP range:** Same as attacker's network
- **Default Gateway:** Attacker's laptop/router
- **DNS Server:** Attacker's fake DNS

Legit Café Laptop:

- Normal café IP

- Legit gateway
- Legit DNS (safe)



A side-by-side of both IP configs for comparison

## Step 6: Investigate the Hacker's DNS Server

### 6.1 Open Café Hacker Laptop → Services → DNS

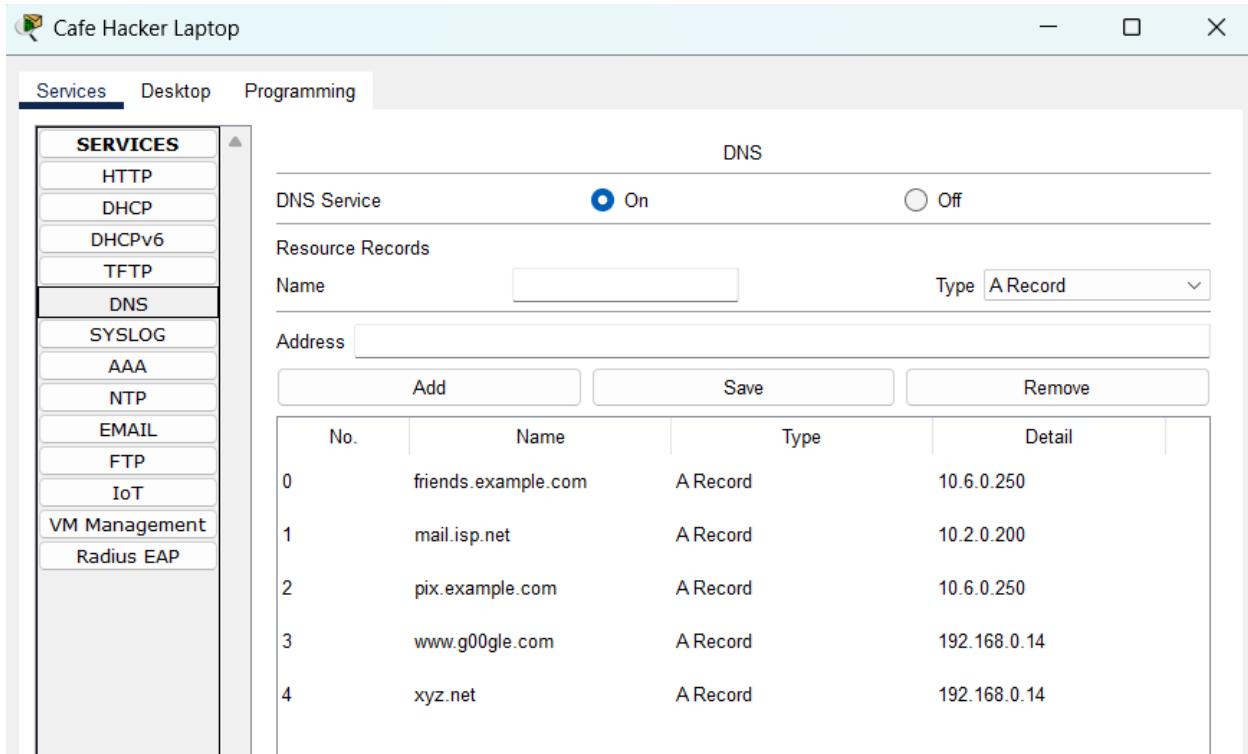
Here you will see:

- Fake DNS entries
- A malicious record for:

friends.example.com

Mapped to the same malicious IP used earlier:

pix.example.com



malicious DNS entries on the Hacker Laptop

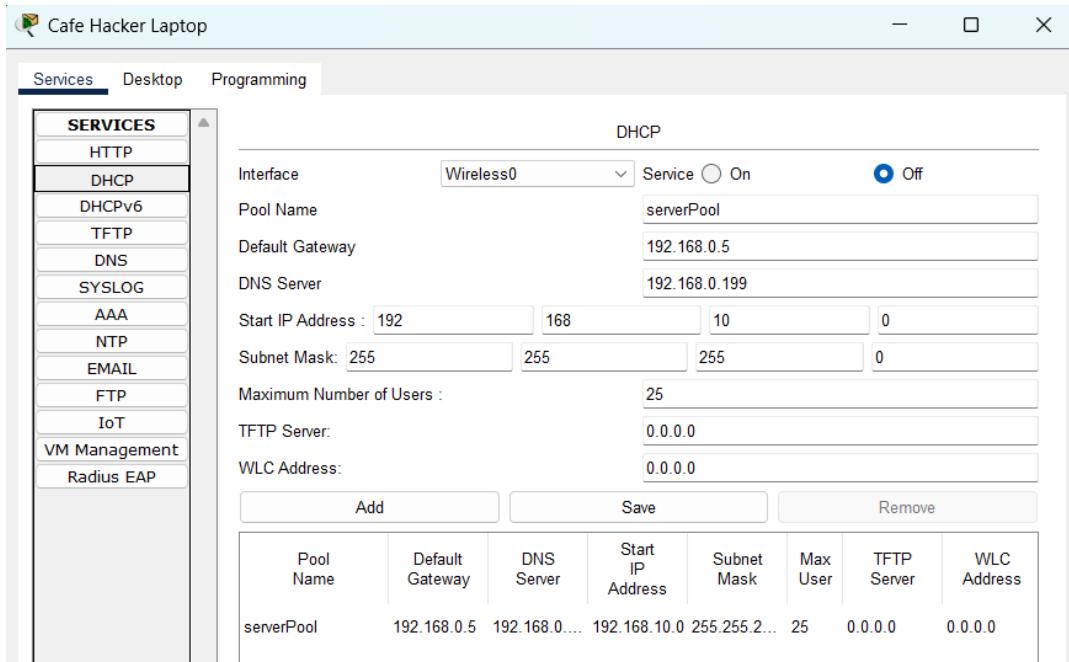
## Step 7: Inspect the Rogue DHCP Server

7.1 Open Café Hacker Laptop → Services → DHCP

You will notice:

- DNS Server field = attacker's DNS
- Gateway = attacker's Wi-Fi router
- DHCP scope = attacker's custom network

This is how the attacker controls ALL victim traffic.



rogue DHCP server settings

## Steps of the Attack

1. Hacker sets up a fake Wi-Fi
2. Victim connects
3. Hacker's DHCP assigns fake DNS server
4. Victim requests a normal website
5. DNS server returns attacker-controlled IP
6. Victim is redirected to malware
7. Credentials or data are stolen

## **5. Summary of Findings**

This lab demonstrates how:

- Even simple misconfigurations expose internal devices
- Human error (phishing) can bypass all firewalls
- Fake Wi-Fi access points can intercept and redirect traffic

These are realistic cybersecurity threats that happen every day.

## **6. Recommendations**

To prevent these attacks:

- Enable strong Wi-Fi encryption
- Separate guest networks from internal networks
- Train employees to detect phishing
- Use DNS filtering and firewalls
- Disable default credentials
- Keep firmware updated
- Avoid public Wi-Fi or use a VPN