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

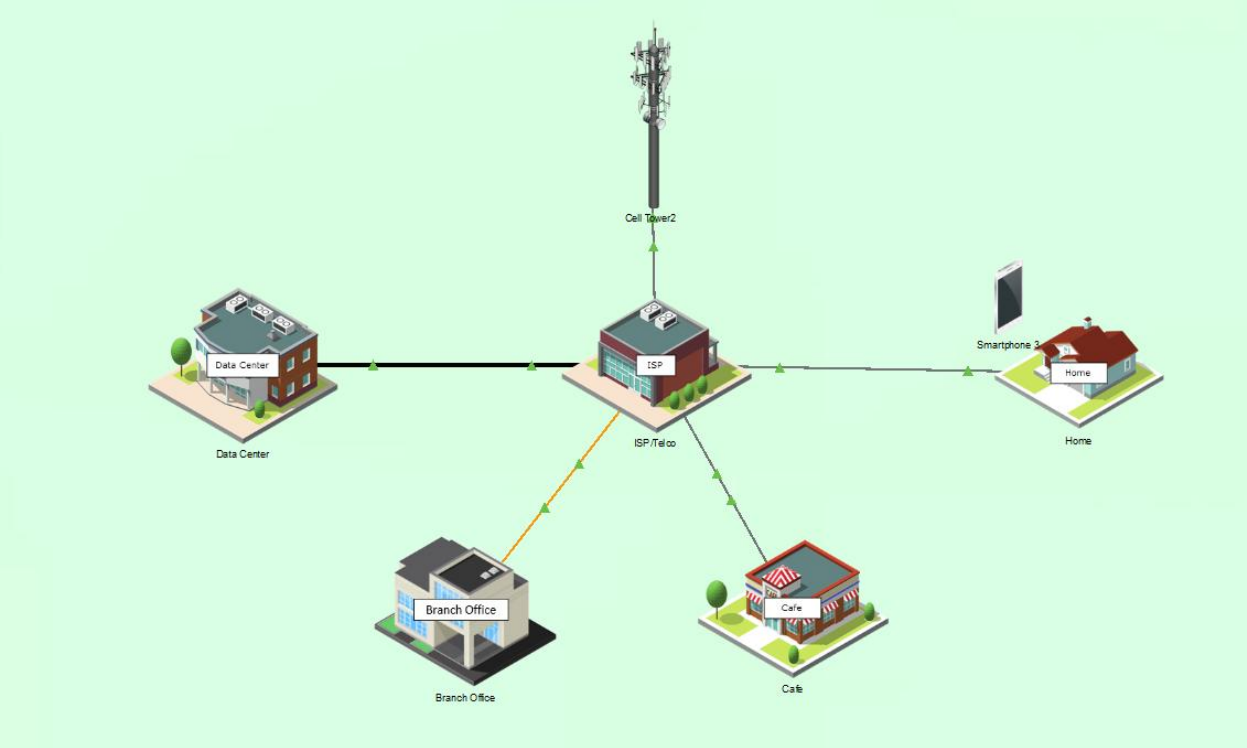
Table of Contents

1. Introduction

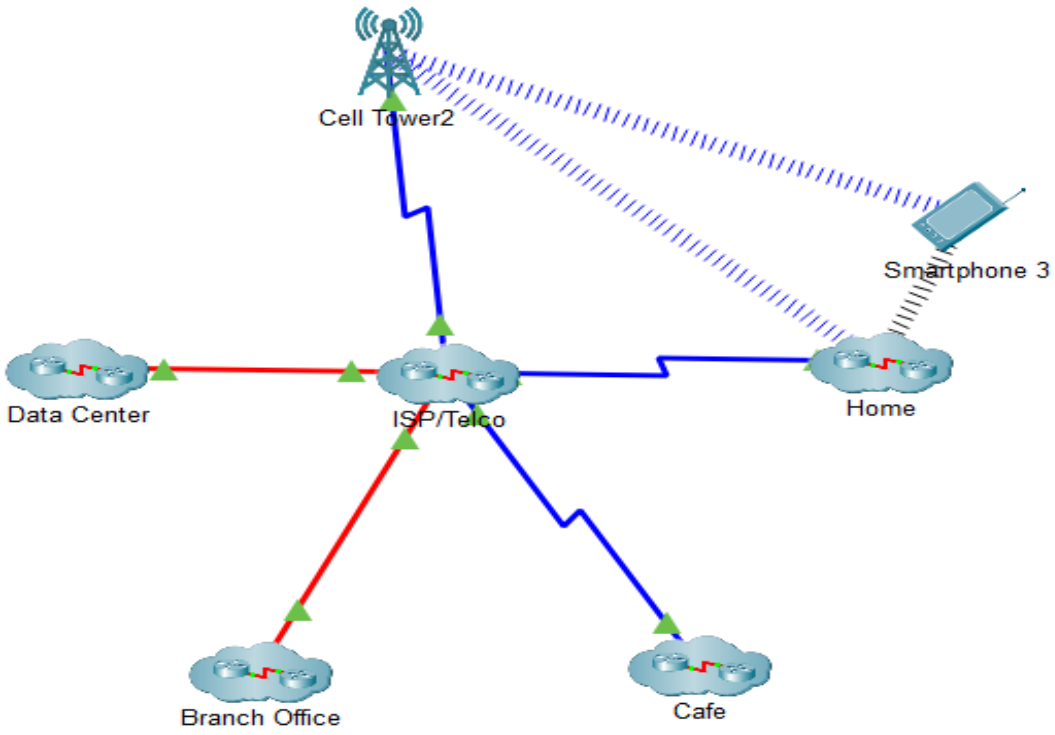
In today's cybersecurity environment, threats can come from anywhere misconfigured home routers, careless user actions, or malicious actors setting up fake networks. This lab demonstrates **three real-world vulnerabilities**:

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

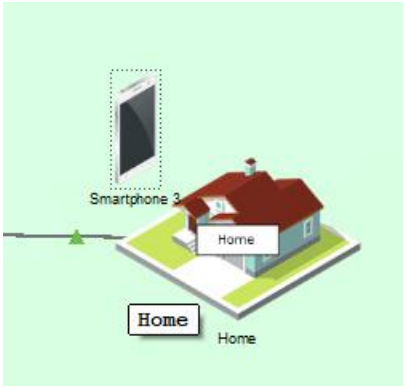


Logical Topology

2. Part 1 – Network Configuration Vulnerability

2.1 Connecting to the Guest Network

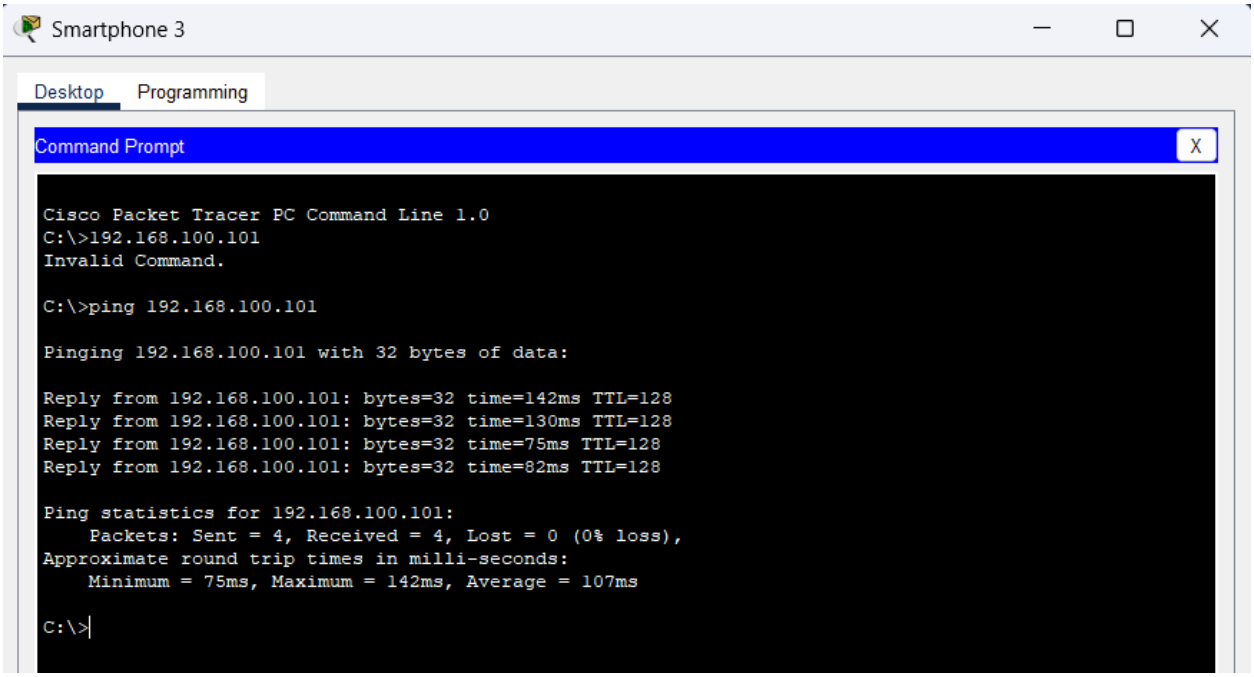
Mary uses *Smartphone 3* and notices an **open guest Wi-Fi network**.
No password → anyone can join → major security risk.



Smartphone 3 connecting to guest network

She then pings the suspicious device:

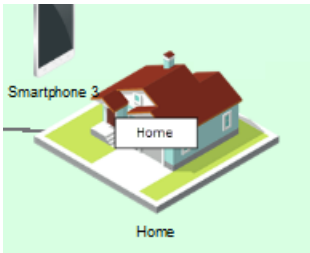
ping 192.168.100.101



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

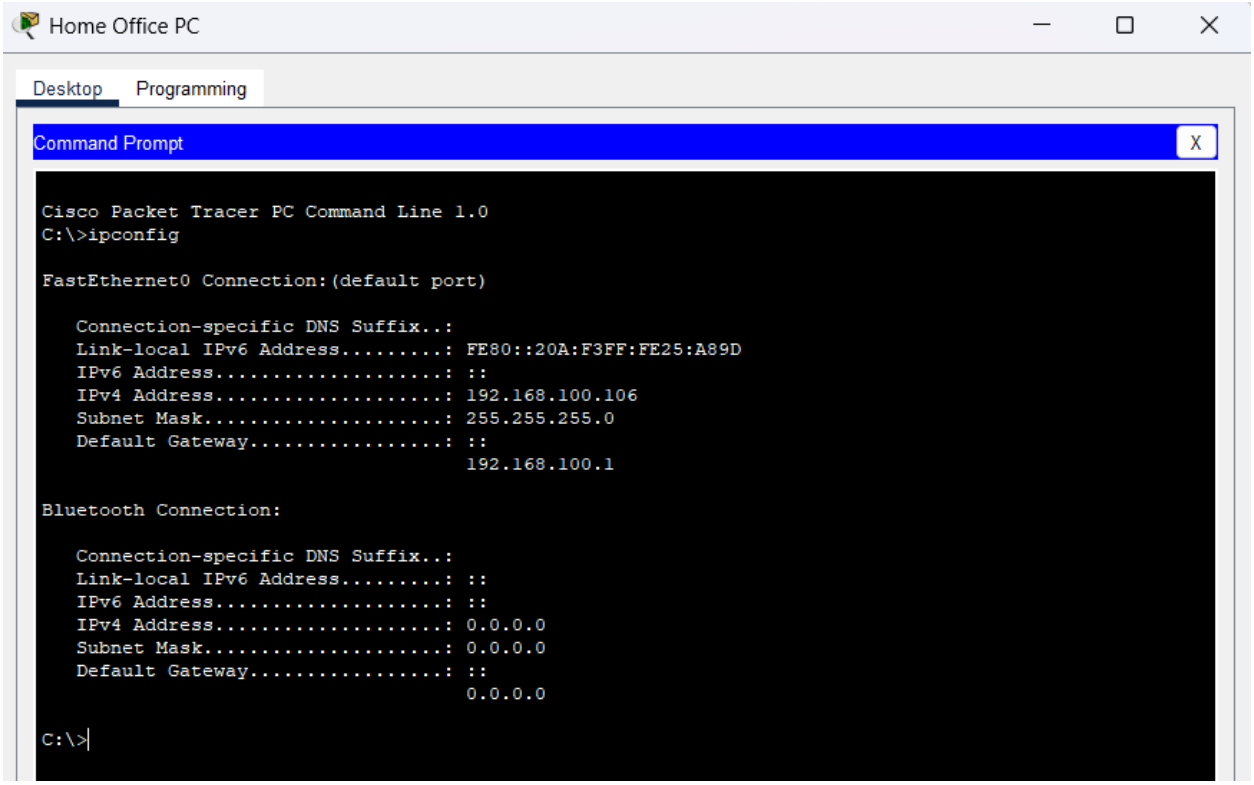
2.2 Discovering the Router's IP Address

Click **Home**:



From the **Home Office PC**:

Ipconfig



Ipconfig output

Default Gateway:

192.168.100.1

This is the router's login address.

2.3 Logging into the Router

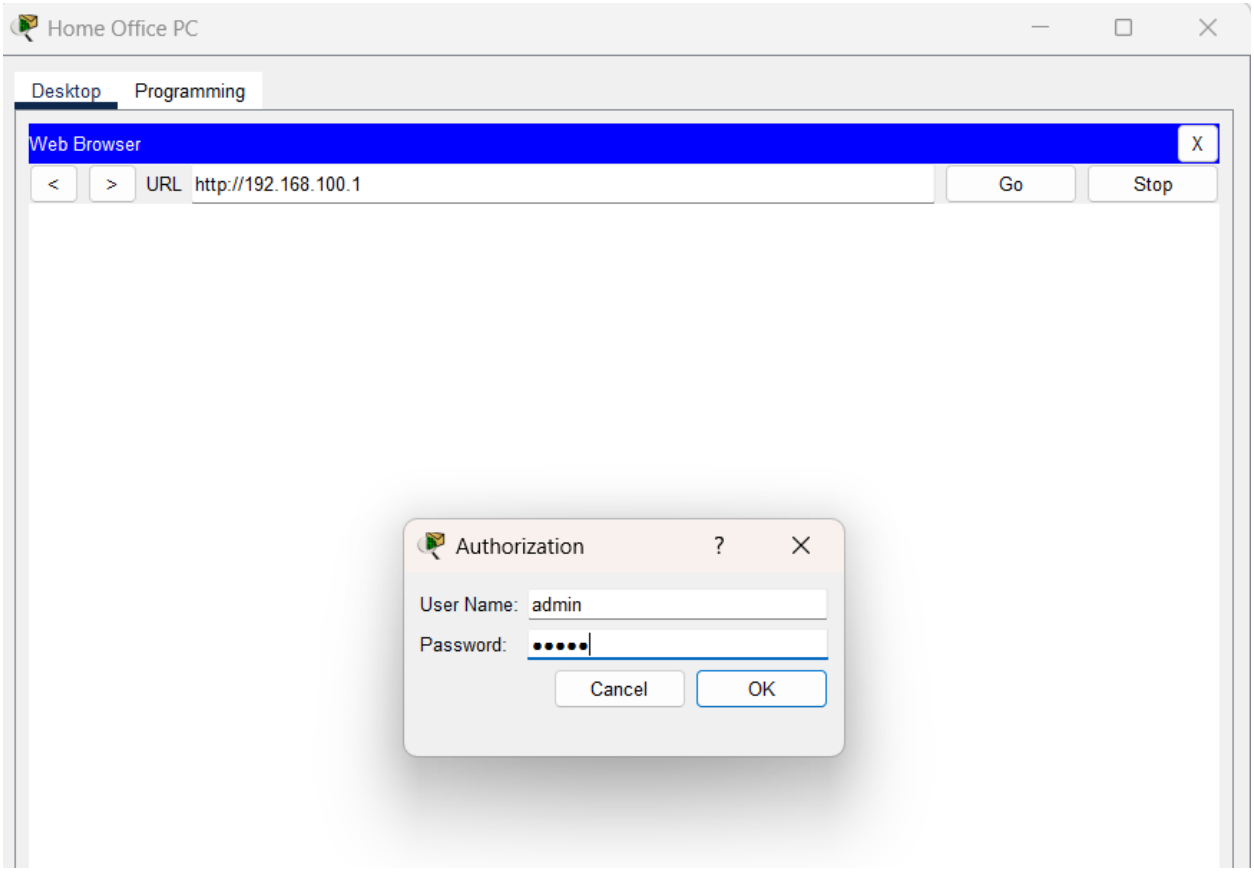
Mary opens the browser → enters the default gateway IP.

Router login appears.

Most home routers use:

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

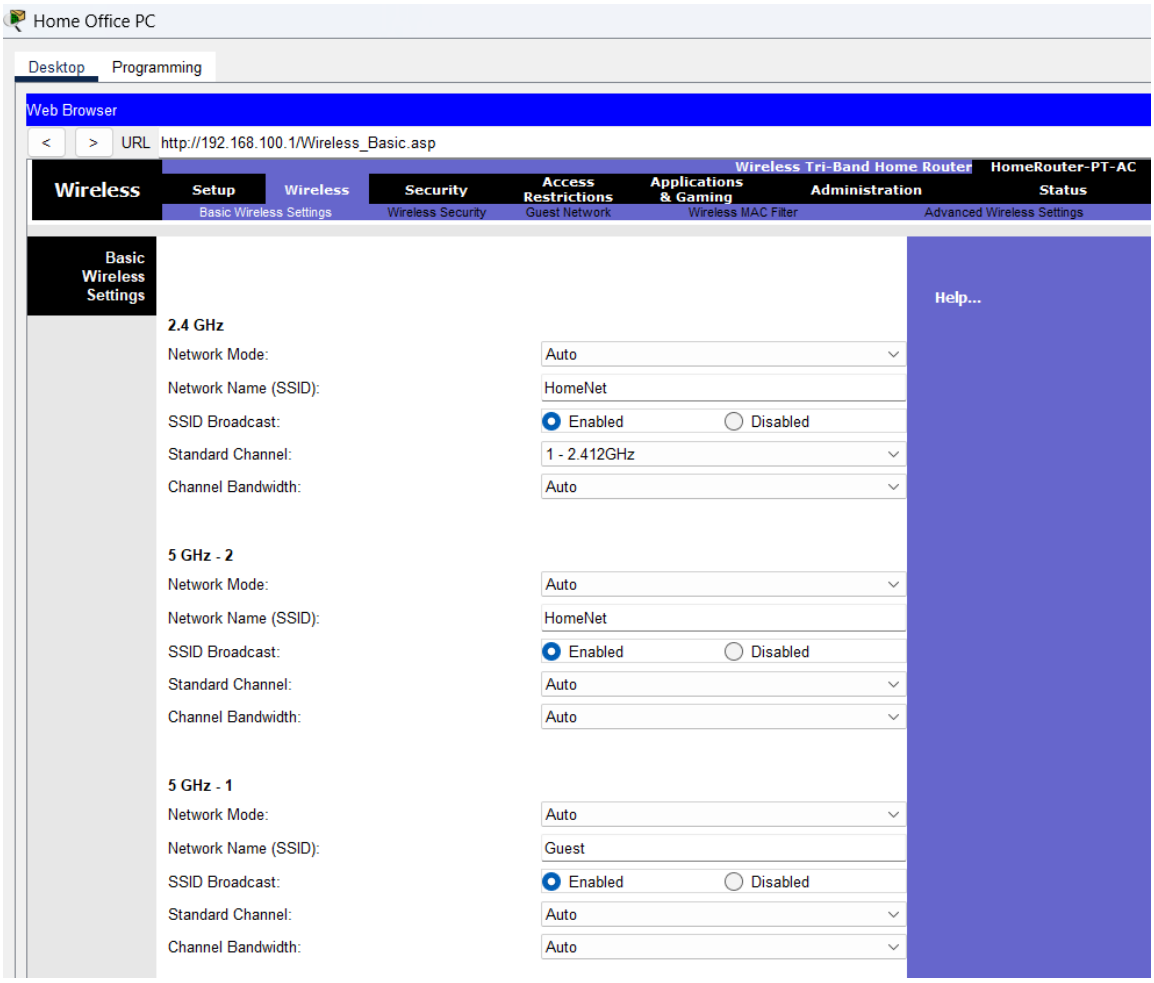
This is extremely insecure.



router login screen

2.4 Wireless Settings Review

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



Which radios are active?

- 2.4 GHz → Active
- Guest Network Radio → Active

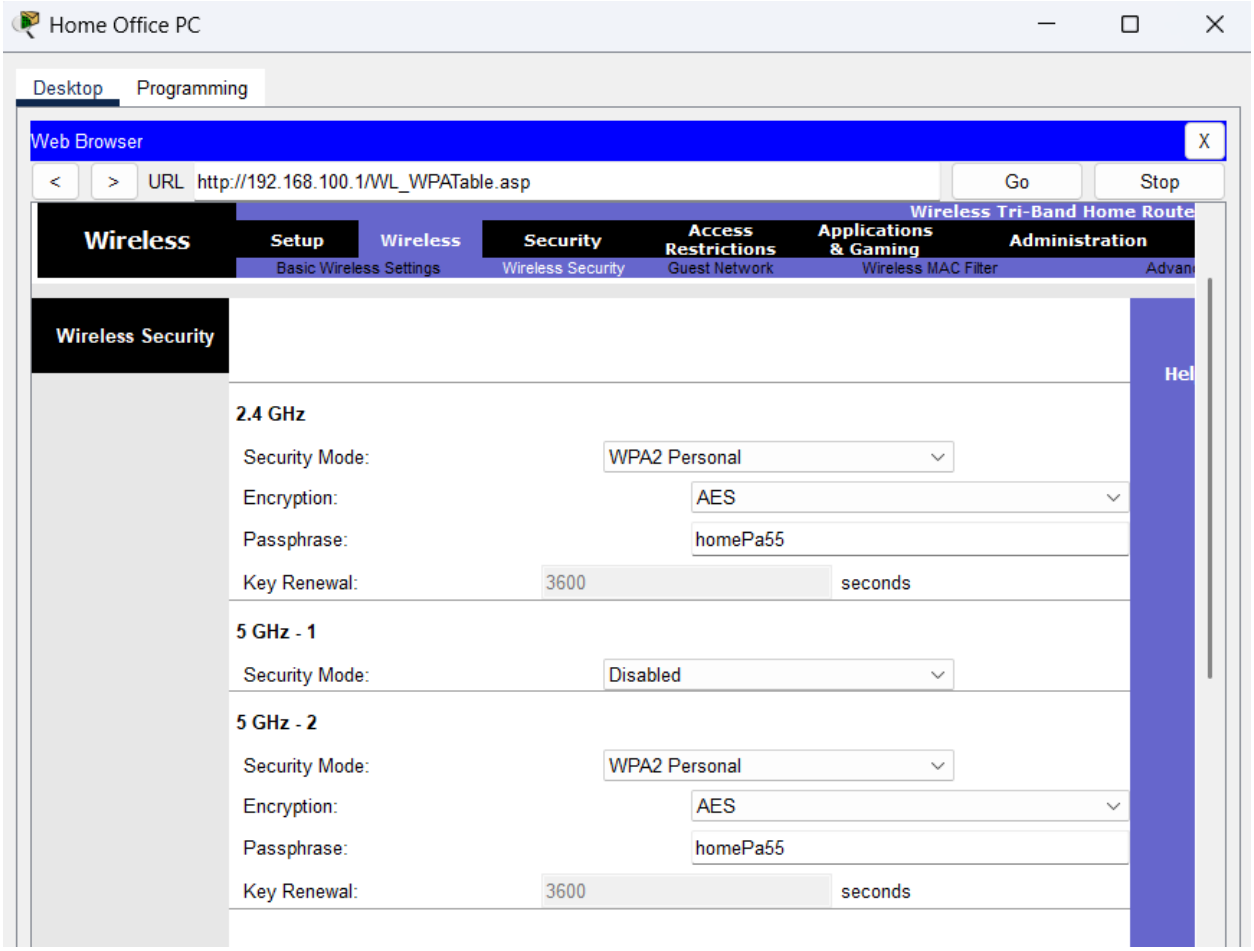
SSIDs:

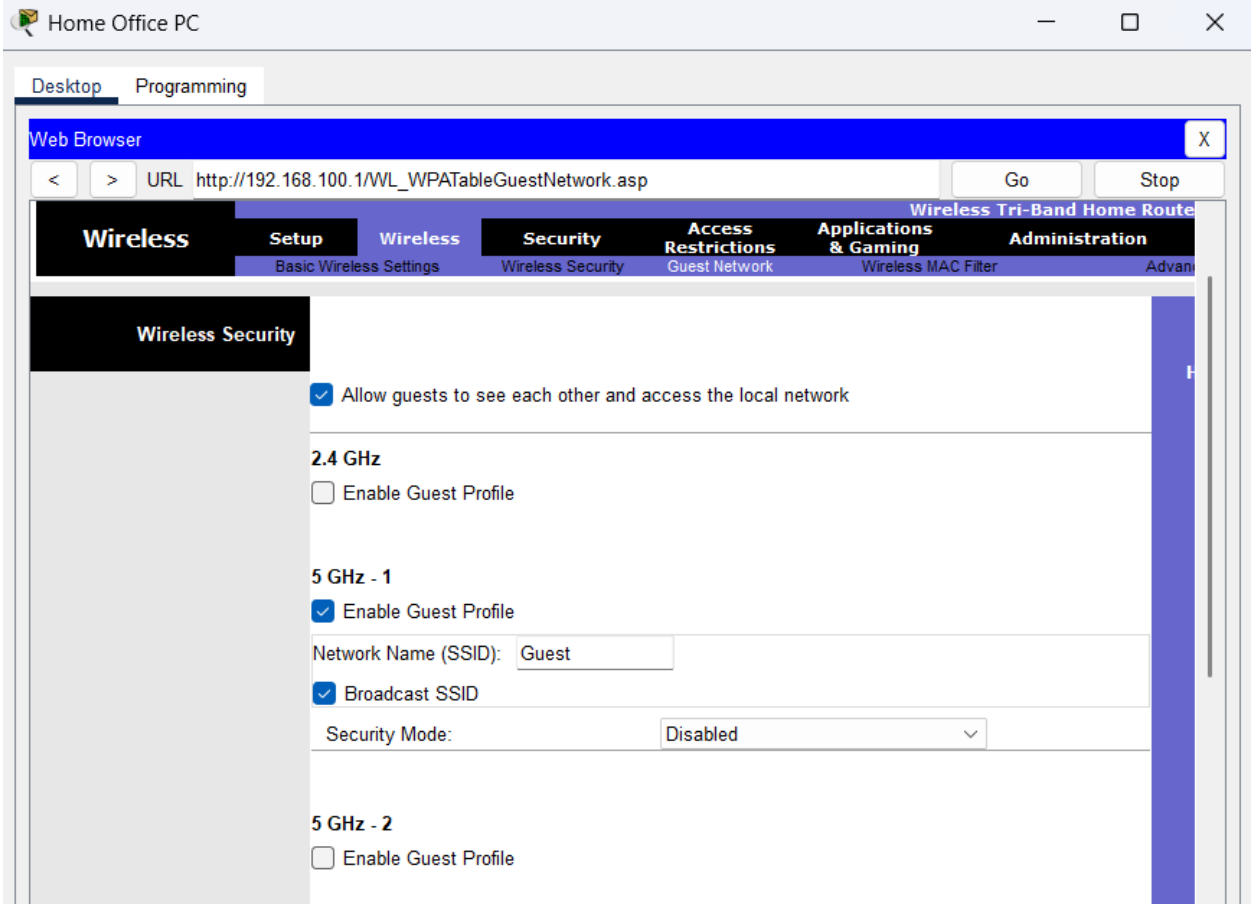
- Home_Network
- Home_5G
- **Guest_Network (open)**

2.5 Wireless Security Review

Under **Wireless Security**:

- Home_Network → WPA2 enabled
- Guest Network → **No security**
- Guest network **allowed LAN access** → huge vulnerability





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

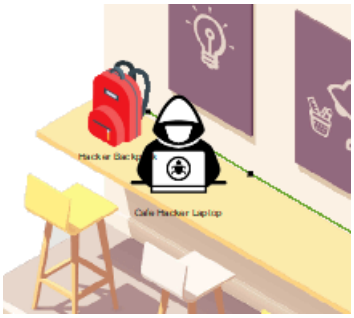
3. Part 2 – Phishing Malware Vulnerability

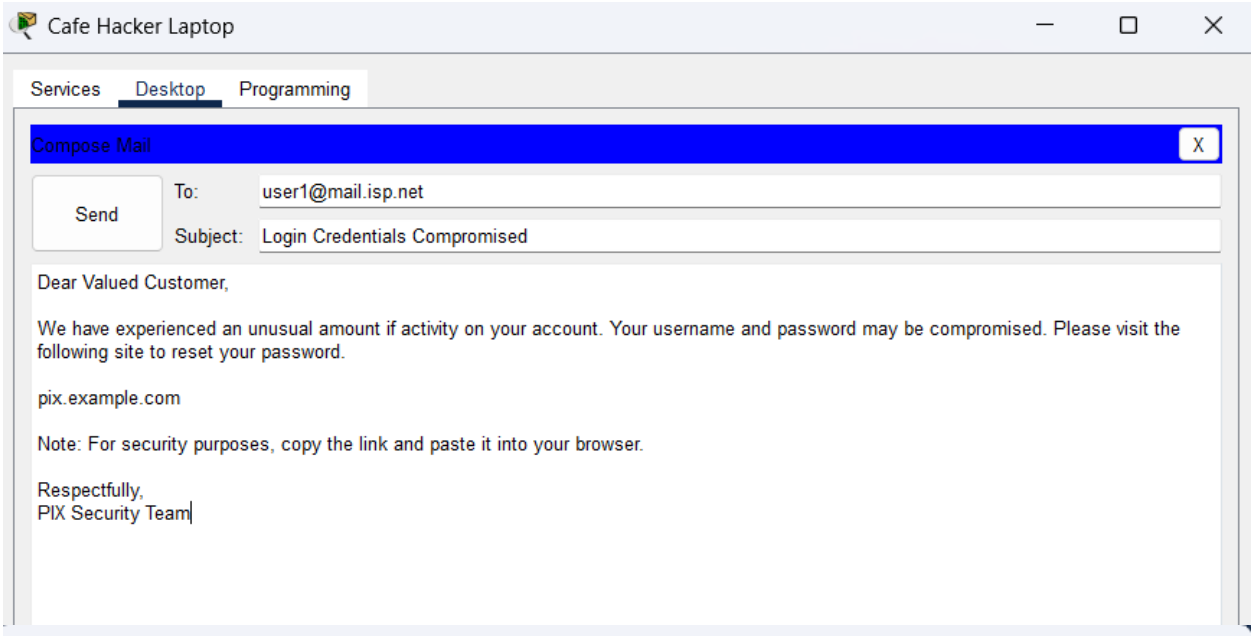
3.1 Threat Actor Writes a Phishing Email

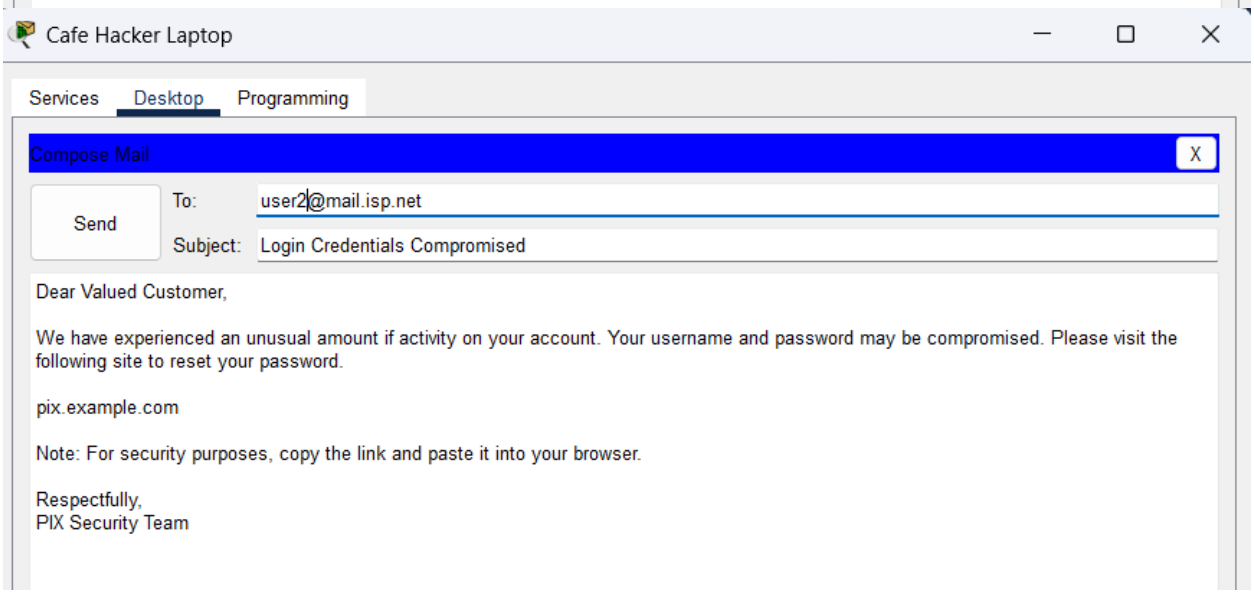
Click Café:

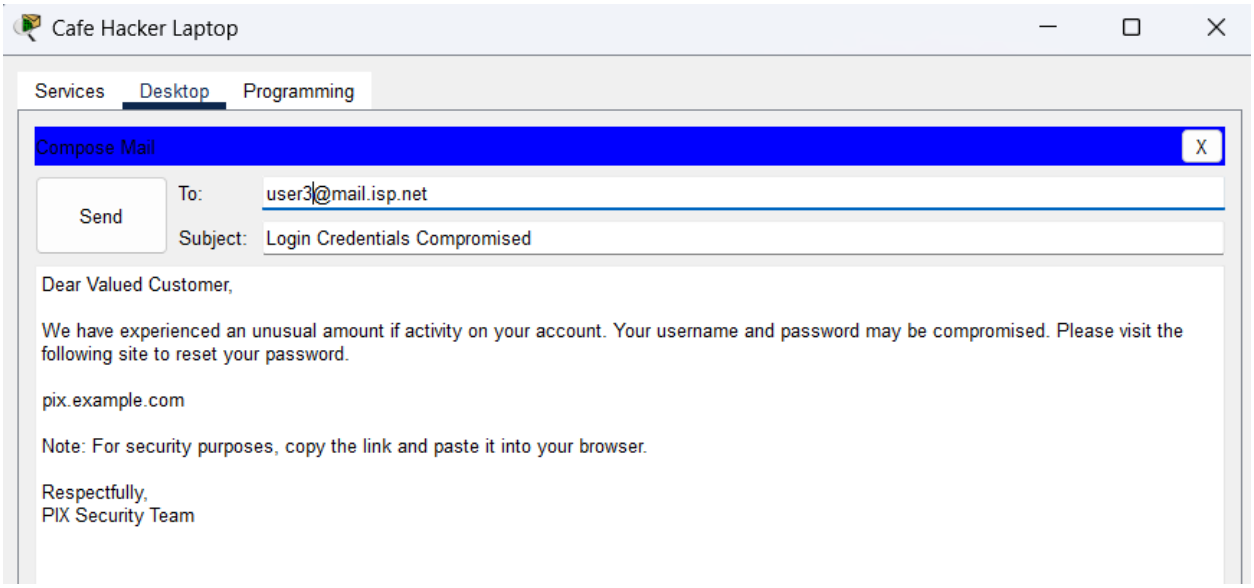
On the **Cafe Hacker Laptop → Email → Compose**, the attacker writes a fake email convincing users to visit:

pix.example.com




Cafe Hacker Laptop
Services
Desktop
Programming
Compose Mail
X
Send
To:
user1@mail.isp.net
Subject:
Login Credentials Compromised
Dear Valued Customer,
We have experienced an unusual amount if activity on your account. Your username and password may be compromised. Please visit the following site to reset your password.
pix.example.com
Note: For security purposes, copy the link and paste it into your browser.
Respectfully,
PIX Security Team

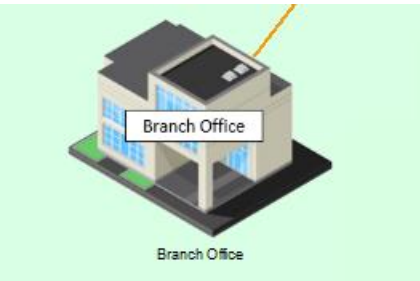

Cafe Hacker Laptop
Services
Desktop
Programming
Compose Mail
X
Send
To:
user2@mail.isp.net
Subject:
Login Credentials Compromised
Dear Valued Customer,
We have experienced an unusual amount if activity on your account. Your username and password may be compromised. Please visit the following site to reset your password.
pix.example.com
Note: For security purposes, copy the link and paste it into your browser.
Respectfully,
PIX Security Team



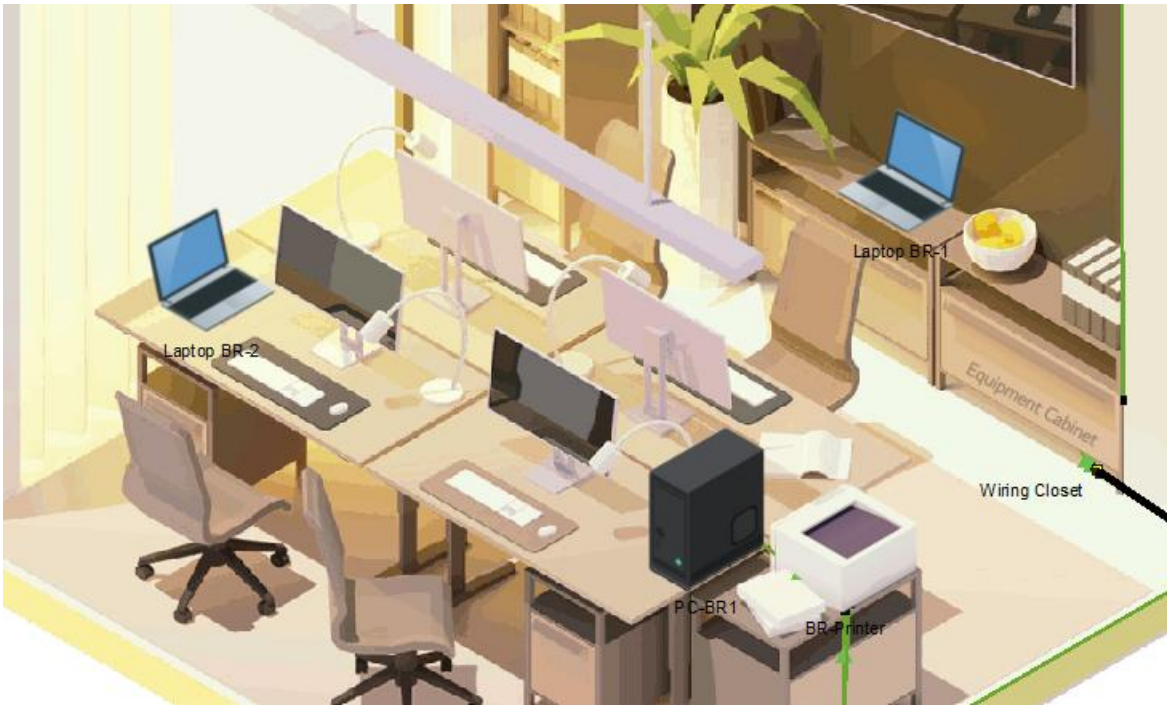
phishing email

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.



Laptop BR-2

Desktop | Programming

MAIL BROWSER

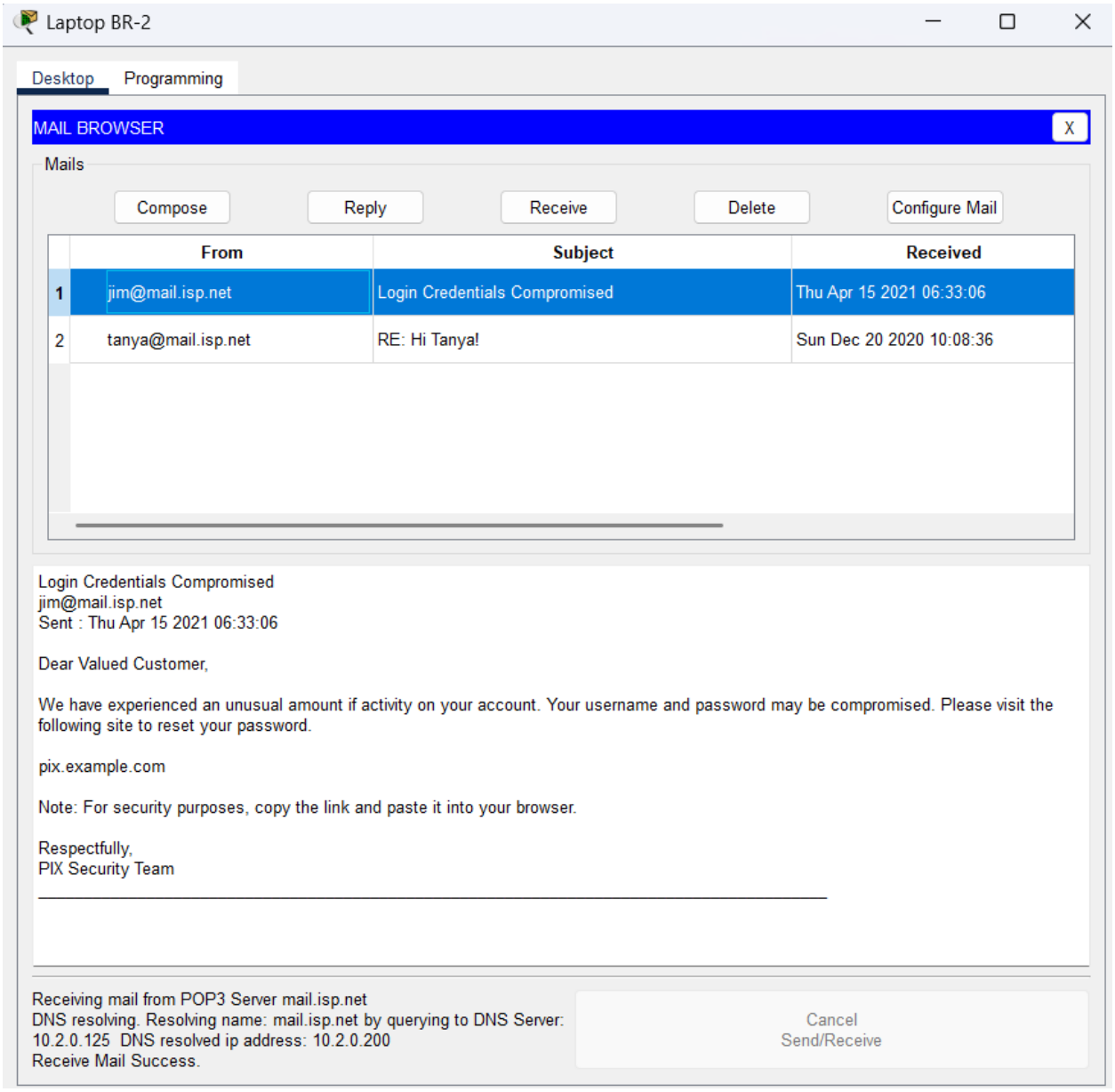
Mails

Compose | Reply | Receive | Delete | Configure Mail

	From	Subject	Received
1	jim@mail.isp.net	Login Credentials Compromised	Thu Apr 15 2021 06:33:06
2	tanya@mail.isp.net	RE: Hi Tanya!	Sun Dec 20 2020 10:08:36

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

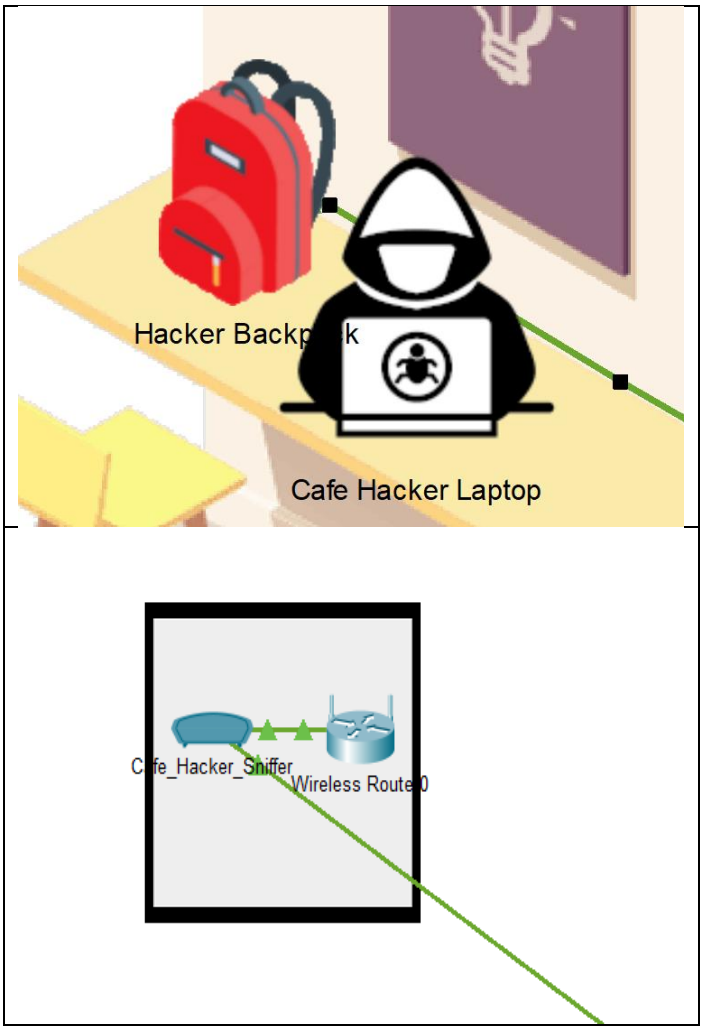
4. Part 3 – Rogue Wi-Fi & DNS Hijacking Vulnerability

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

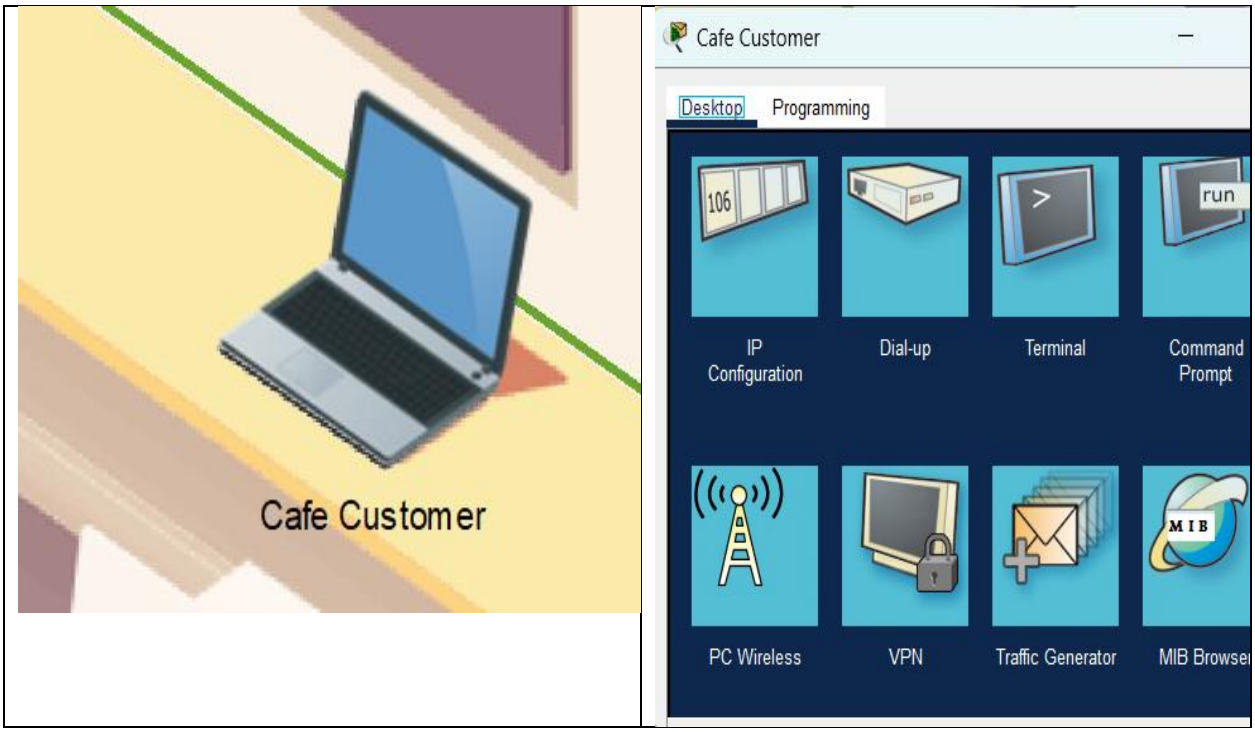


Hacker Backpack contents

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)

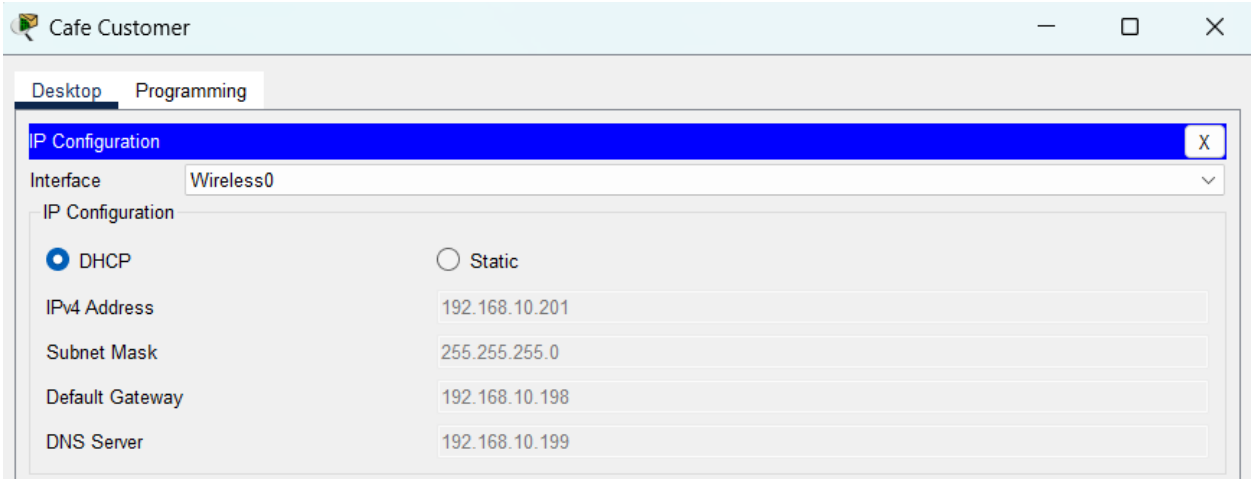
This is a crucial part of understanding DNS hijacking.

5.1 Open IP Configuration on Victim

Cafe Customer Laptop → Desktop → IP Configuration

Record:

- IP Address
- Default Gateway
- DNS Server

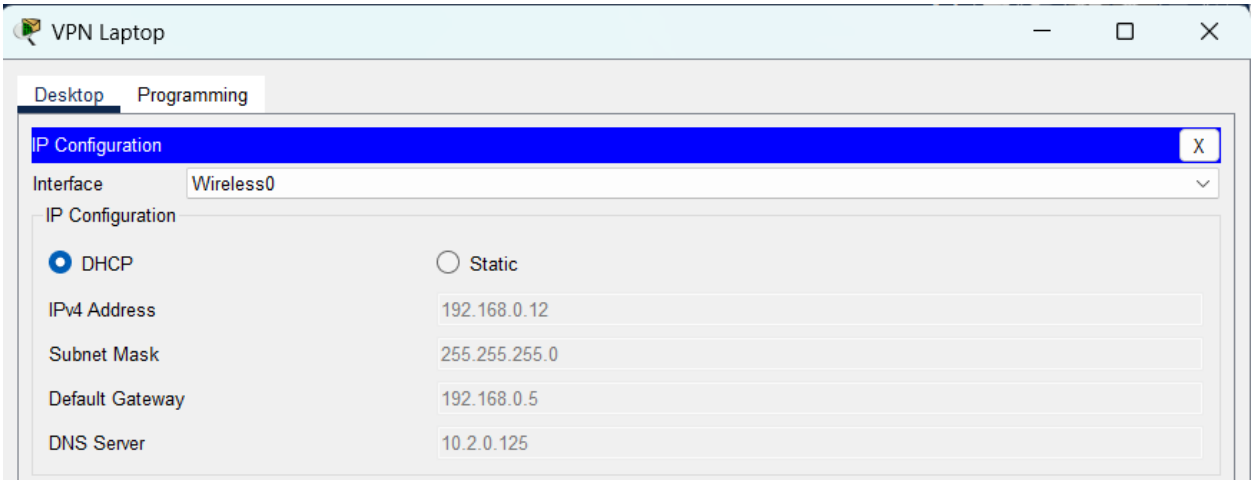


victim's IP configuration window

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:

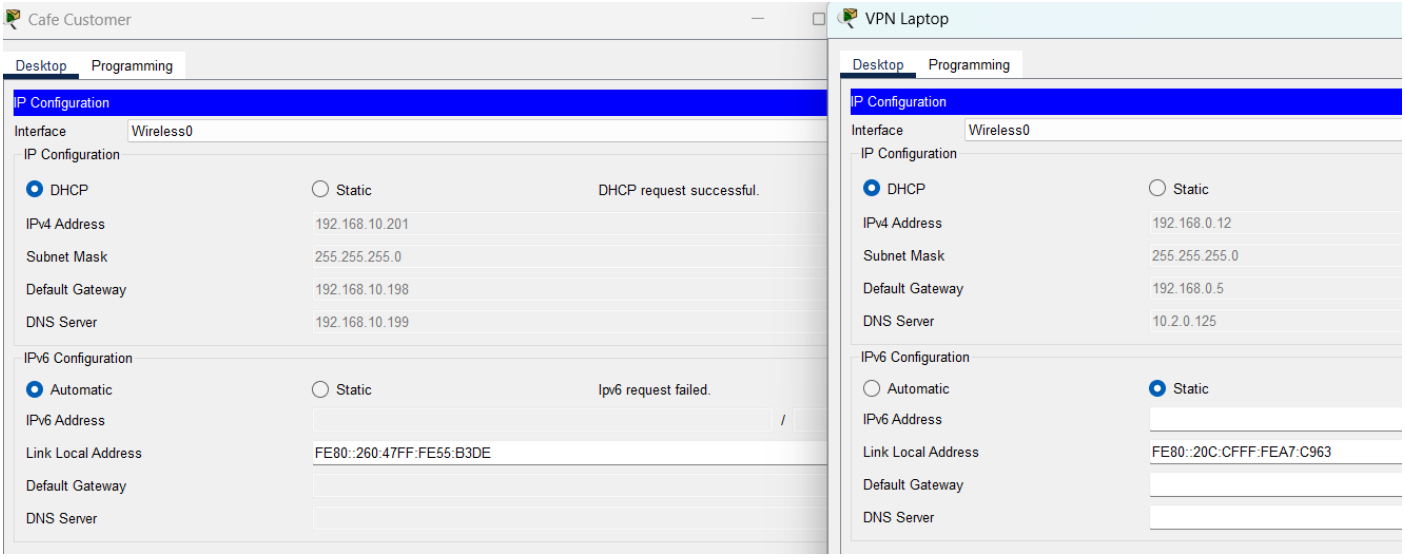
Victim Laptop:

- **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

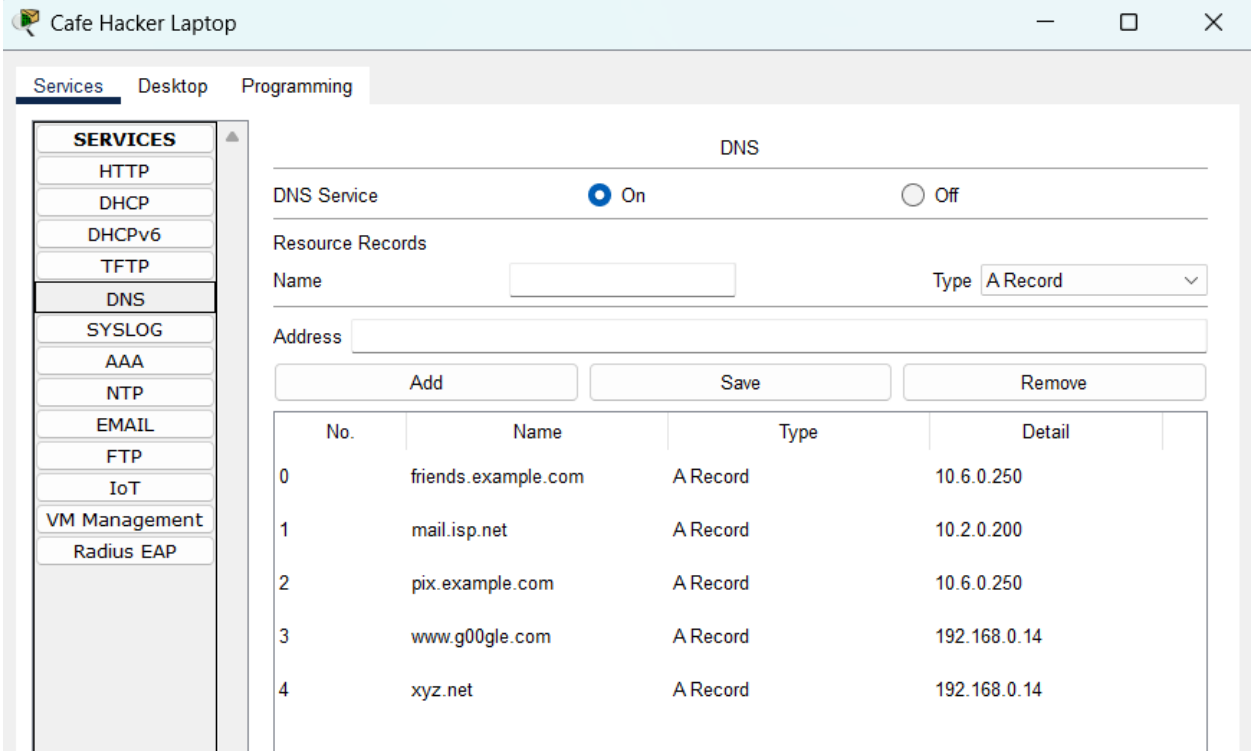
Here you will see:

- 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

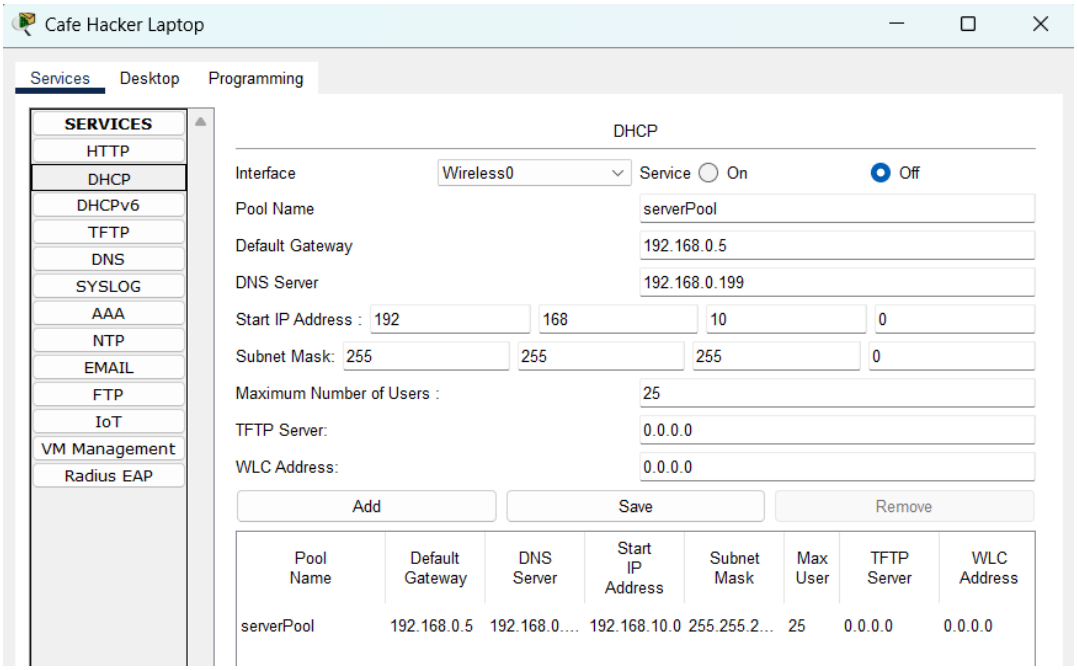
Step 7: Inspect the Rogue DHCP Server

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