INTERNSHIP-THE RED USERS

NAME: Obinna Emere

Task 1: Introduction to Network Security Basics

Different types of network thread:

When it comes to network threats, it's essential to understand how they target systems and networks to steal
data, cause damage, or disrupt services. Some of the most common types of network threats, including
malware, viruses, Trojans, worms, phishing, and a few more are.

1. Malware (Malicious Software)
Malware is a broad term for any software designed to harm, exploit, or gain unauthorized access to a
computer or network. It's like an unwanted guest that sneaks into your system, often without you even
knowing. It comes in many forms, and each has its own way of causing trouble.
2. Virus
A virus is a type of malware that attaches itself to legitimate programs or files. Just like how a biological
virus spreads by infecting cells, a computer virus spreads when you unknowingly run an infected file,
allowing it to replicate and cause damage. It can slow down your system, delete important files, or even
corrupt your entire device. It needs human action (like running a program) to spread.
3. Trojan Horse (Trojan)
Named after the famous Greek myth, a Trojan disguises itself as something harmless or useful—like a free
app or an email attachment. Once you let it in by downloading or opening the file, it can grant hackers
access to your system, steal your data, or even control your computer remotely. It's one of the most
deceptive forms of attack because it relies on you trusting the wrong thing.
4. Worm
Unlike a virus, a worm doesn't need a host file or program to spread. It's like a fast-moving bug that

replicates itself and spreads from one device to another, all by exploiting vulnerabilities in your network.
Worms can infect an entire network quickly, using up resources and potentially bringing down systems or
networks without needing user interaction.

5. Phishing Attacks

Ever gotten an email that looks real, asking you to click a link and log in to your bank account or social
media? That’s phishing. These attacks try to trick you into giving away sensitive information—like your
passwords, credit card details, or even Social Security number—by pretending to be someone you trust.
Phishing is all about deceiving people into handing over their private information.

6. Ransomware

Ransomware is a particularly nasty type of malware. It locks you out of your files or entire system until
you pay a ransom (usually in cryptocurrency). Imagine waking up one day and realizing you can't access
any of your important documents or photos unless you pay the attacker. It's a very stressful form of
attack that’s increasingly common in both personal and business environments.

7. Spyware

As the name suggests, spyware is software that sneaks onto your device to gather information about you
without your consent. It can track your browsing habits, collect your login credentials, or even record your
keystrokes (keylogging). The worst part? You might not even know it's there, quietly collecting your
private data.

8. Adware

Adware is less harmful but still annoying. It bombards you with unwanted ads, slowing down your system
and affecting your browsing experience. Sometimes, adware can come bundled with legitimate software
and sneak its way onto your computer, making it a frustrating type of malware to deal with.

9. Denial of Service (DoS) Attacks

In a DoS attack, hackers flood a network or website with so much traffic that it can’t handle the load and

crashes. Imagine trying to drive home during rush hour, but the streets are so packed that you can't even
move an inch—that's what a DoS attack does to websites and networks. There's also a more powerful
version called a DDoS (Distributed Denial of Service) Attack, where the traffic comes from many different
sources, making it even harder to stop.

10. Man-in-the-Middle (MitM) Attack

In a Man-in-the-Middle Attack, a hacker secretly intercepts communication between two parties (like you
and your bank). The attacker can steal sensitive information, alter communication, or impersonate one of
the parties. It's like having someone secretly eavesdrop on your conversation and manipulate it without
either side knowing.

11. SQL Injection

An SQL injection attack happens when attackers insert malicious code into a database through a website's
input fields. For example, they might enter harmful commands into a login form to gain unauthorized
access to a website's data, like usernames and passwords. This type of attack is particularly dangerous for
websites and web applications.

Firewalls, encryption, and secure network configurations—three foundational concepts in network security:

1. Firewall

A firewall is like a security guard for your network. It sits between your network and the outside world,
controlling what comes in and goes out. It monitors and filters the incoming and outgoing network traffic based on a set of predefined security rules. Firewalls can be either hardware (a physical device that protects
an entire network) or software (a program on your computer or device).

How it works:

Think of it as a gatekeeper—only allowing trusted or authorized connections through while blocking
harmful or suspicious traffic.

For example, if a hacker tries to access your computer, the firewall can block their attempts.

Why it's important:
It helps prevent unauthorized access to your network.
It can block malware, viruses, and other types of cyber attacks before they even reach your devices.

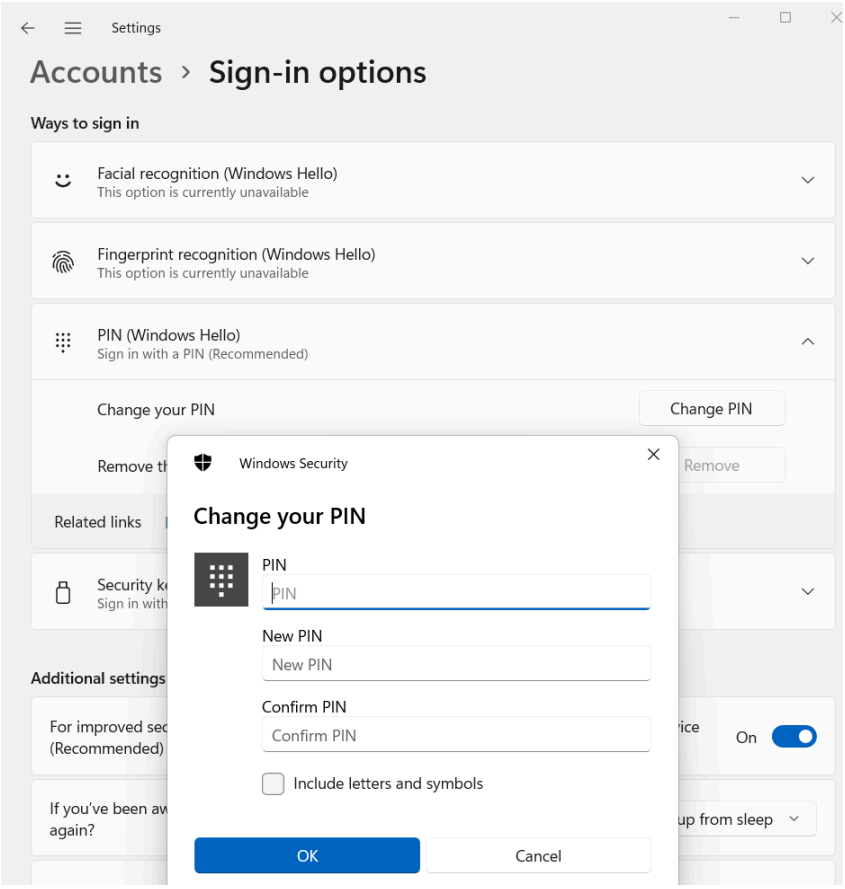
2. **Encryption**

Encryption is like converting your data into a secret code to keep it safe. When you send data over a
network, encryption scrambles that data so that even if someone intercepts it, they won't be able to
understand it without the key to decrypt it. Only authorized users who have the key can decode (or
decrypt) the information.
How it works:
Imagine writing a letter and locking it in a box. Only the person with the correct key can unlock and
read it.
Encryption is used to protect sensitive data like passwords, credit card numbers, or personal messages.
Why it's important:
Encryption ensures **confidentiality**—only the intended recipient can read the information.
It's widely used in **Wi-Fi networks (WPA2, WPA3)** to prevent others from eavesdropping on your
internet traffic.

3. **Secure Network Configuration**

Secure network configuration is all about setting up your network in a way that minimizes vulnerabilities
and reduces the risk of attacks. It's the process of securing various components of your network, like
routers, devices, and software, by following best practices.
Examples of secure configurations:
Changing default passwords: Default usernames and passwords (e.g., admin/admin) are often easy to
guess and can make your network vulnerable. Always change these to strong, unique passwords.
Enabling network encryption (WPA2/WPA3): These encryption protocols are essential for securing
wireless networks. They help prevent unauthorized access to your Wi-Fi network by ensuring that

only trusted devices can connect.
Disabling unused services and ports: Every open port or running service on your network is a potential
entry point for attackers. Disable those that are not needed to reduce the attack surface.**Why it's important**:
Misconfigurations or weak settings can open the door for cyber attacks.
Secure configurations ensure that your network is less likely to be exploited, making it much harder
for hackers to find vulnerabilities.
Steps to change user account password:
1. **Open Settings**: Press Windows Key + I to open the Settings window.
2. **Go to Accounts**: Click on **Accounts**.
3. **Select Sign-in Options**: On the left panel, click **Sign-in options**.
4. **Change Password**: Under the **Password** section, click **Change**.
Enter your current password.
Enter and confirm your new password. Make sure it’s strong (use a mix of upper/lowercase letters,



Enable Network Encryption (WPA2/WPA3)

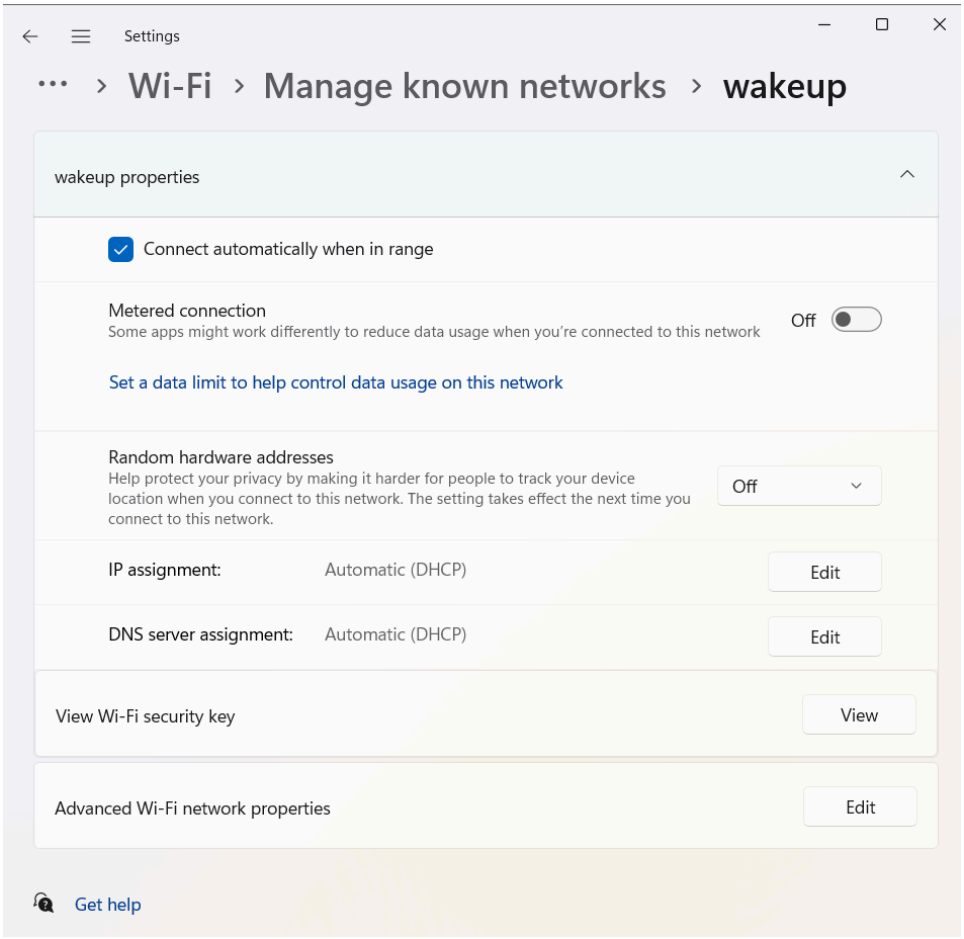
WPA2/WPA3 encryption is generally set up on a **router** to secure wireless networks. However, if you're
connecting to a Wi-Fi network on your laptop, you can ensure that you're connecting to a network with
proper encryption.

Steps to ensure you're using a secure Wi-Fi connection (WPA2/WPA3):

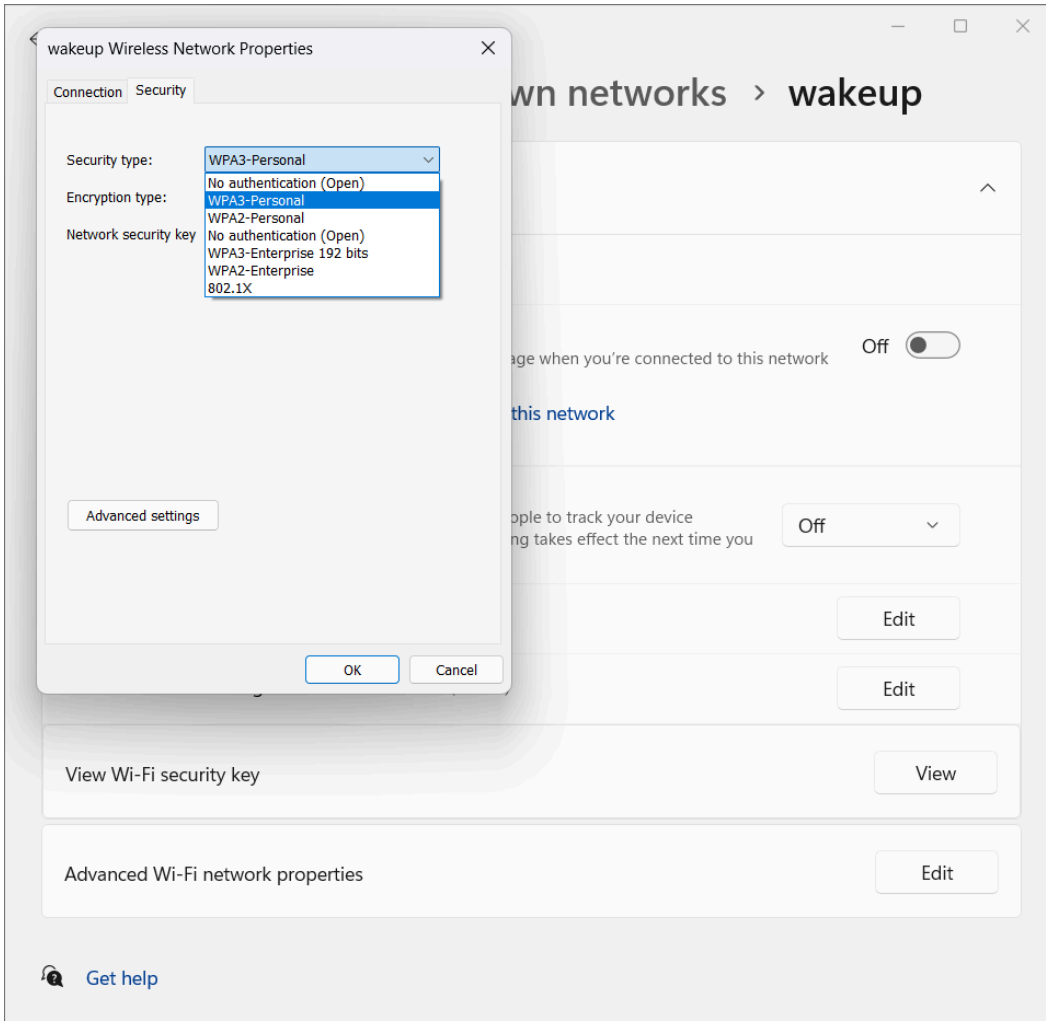
Open Network Settings: Click on the **Wi-Fi icon** in the taskbar and select **Network & Internet settings**.

Select Wi-Fi: From the left panel, select **Wi-Fi**.

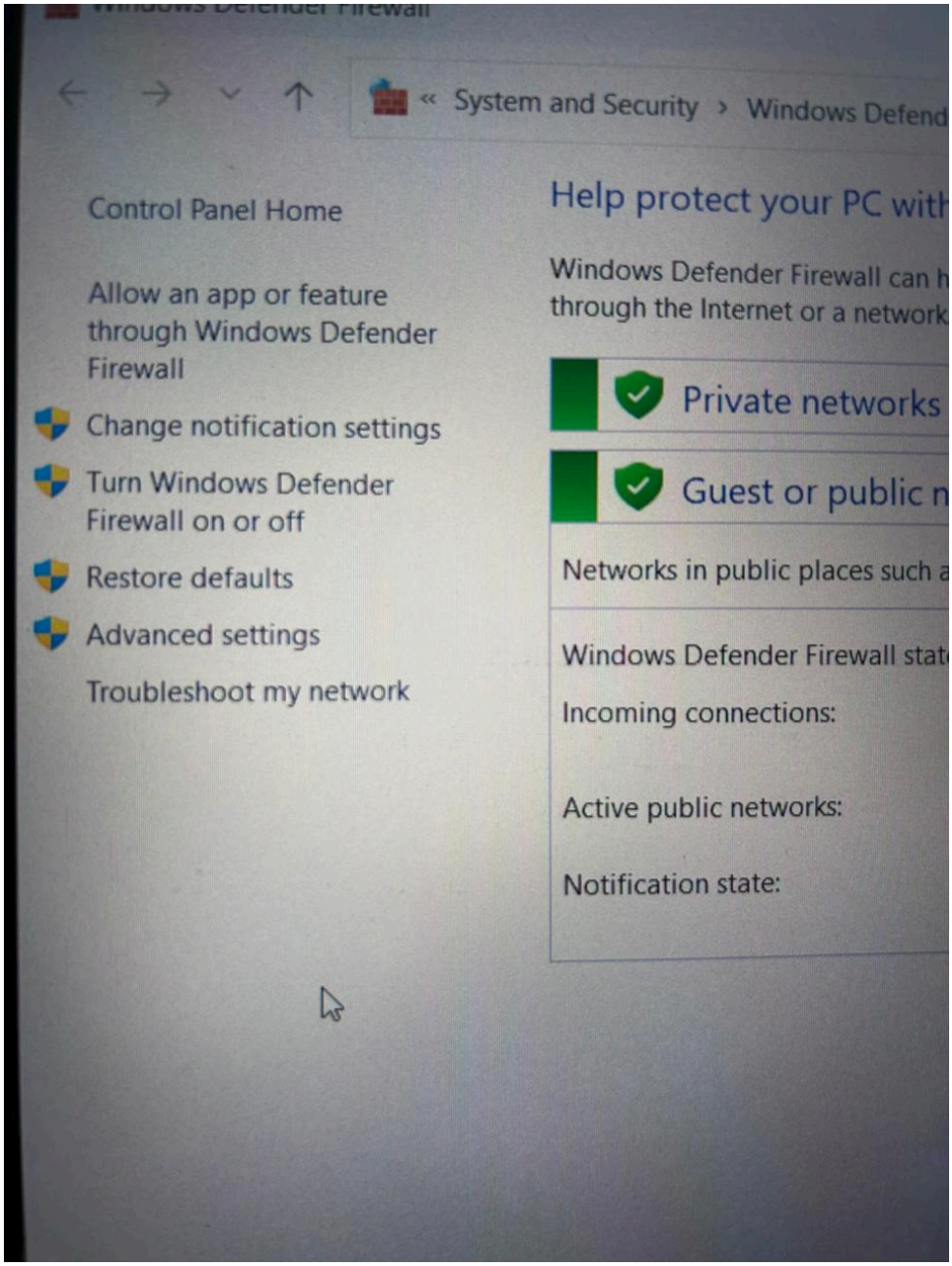
View Available Networks: Click on **Manage known networks** to see all saved networks



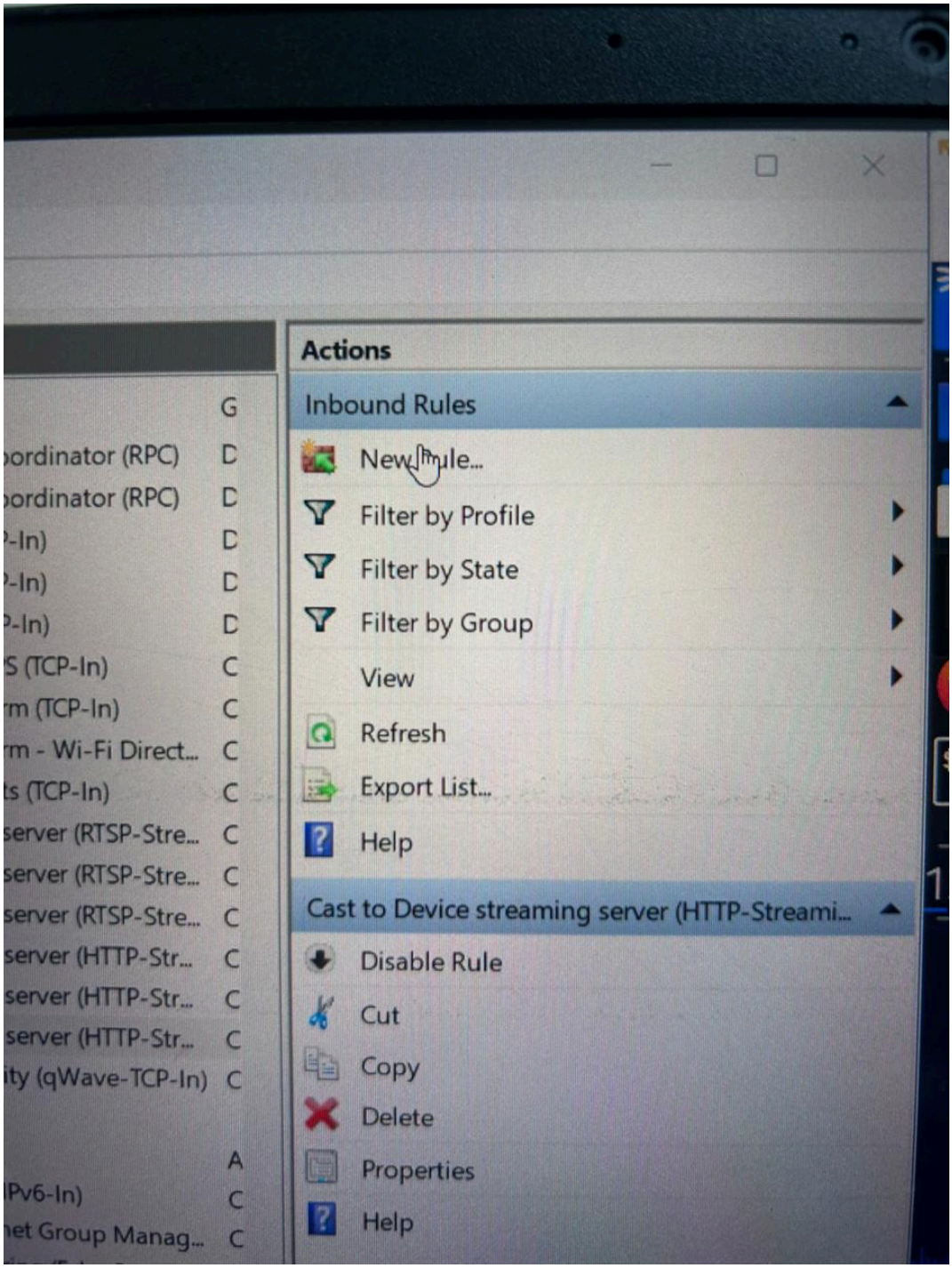
Connect to Secured Networks: Select a network and make sure it’s using **WPA2** or **WPA3**encryption
(this is usually displayed next to the network name).
If your Wi-Fi connection is unsecured or using WEP (a weaker form of encryption), avoid
connecting to it or consider reaching out to your network administrator to upgrade security



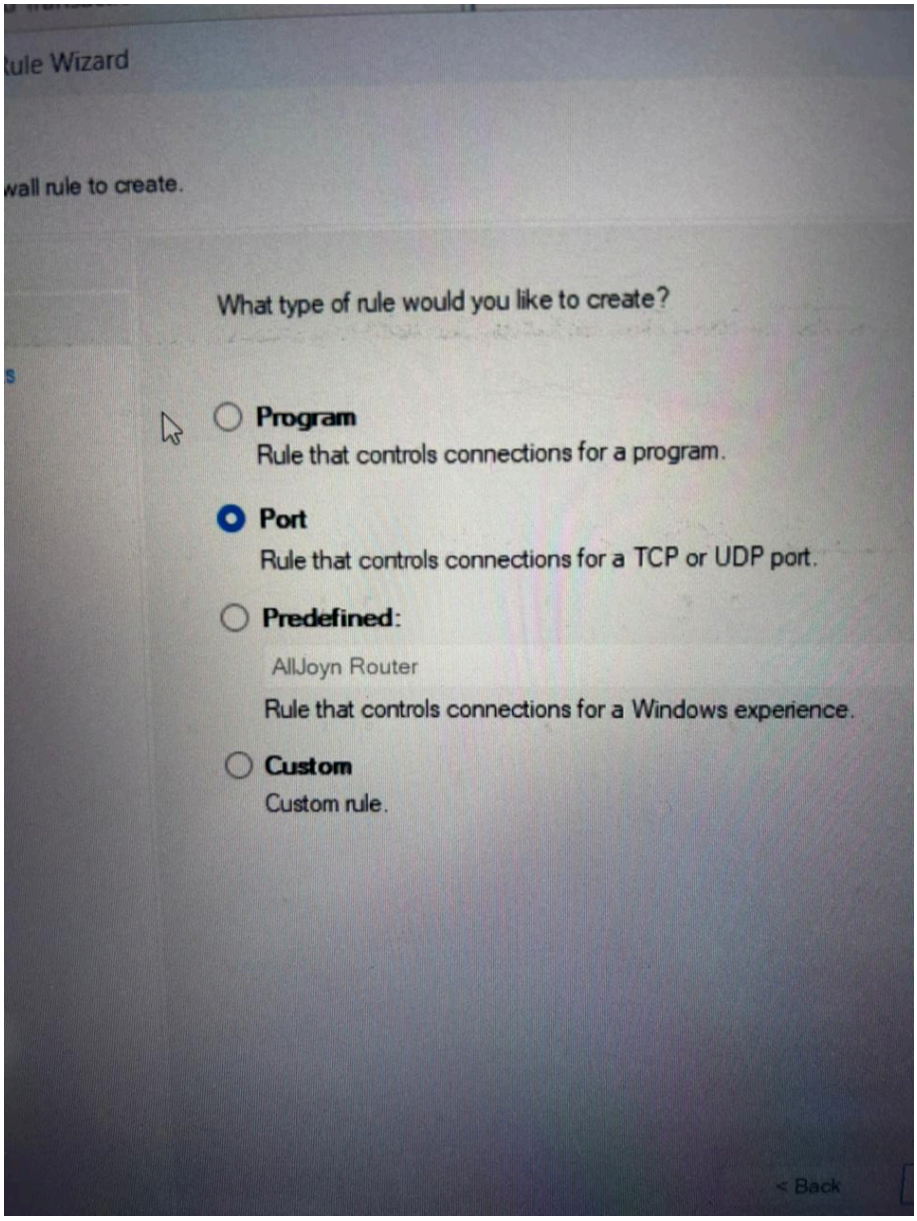
Steps to block unused ports using Windows Firewall:
Open Windows Defender Firewall:
Search for "Windows Defender Firewall" in the Start menu and select **Advanced settings** on the
left.



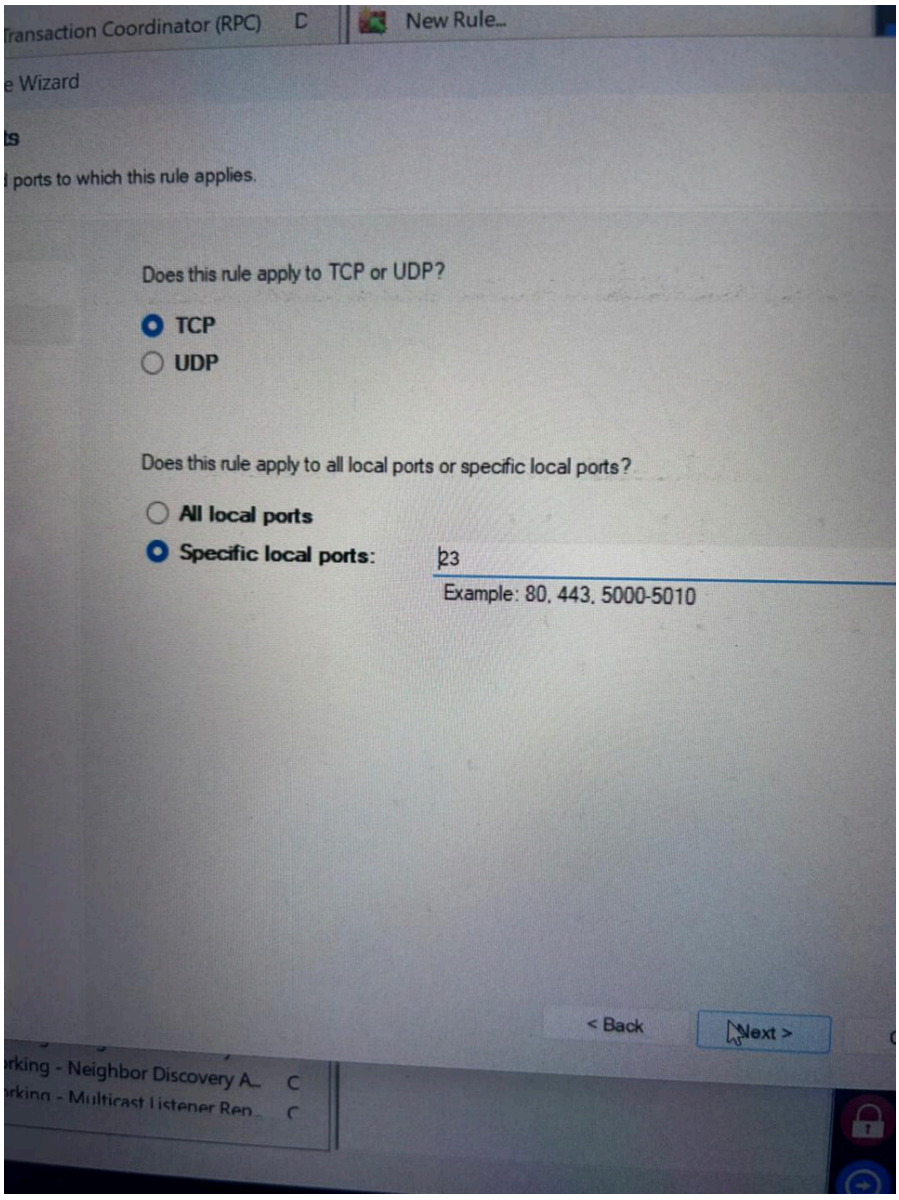
Create a New Inbound Rule:
Click **Inbound Rules** on the left panel.
On the right, select **New Rule**.



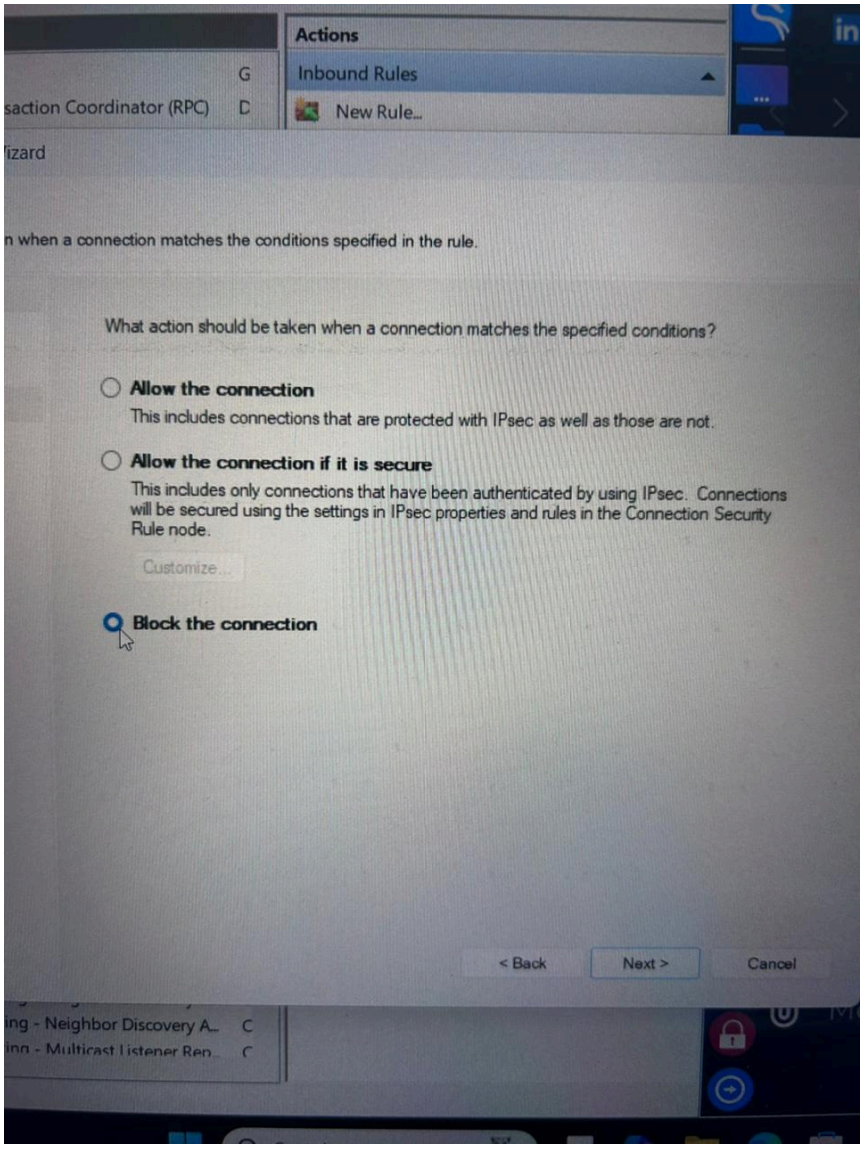
Select Port:
Choose **Port** and click **Next**.



Specify Ports to Block:
Select whether to block **TCP** or **UDP** ports and then specify the port number(s) you want to
block.
For example, you could block **port 445 (SMB)** if you don't use file sharing or **port 23 (Telnet)** if
you don't use remote access.



Action:
Choose **Block the connection** and click **Next**



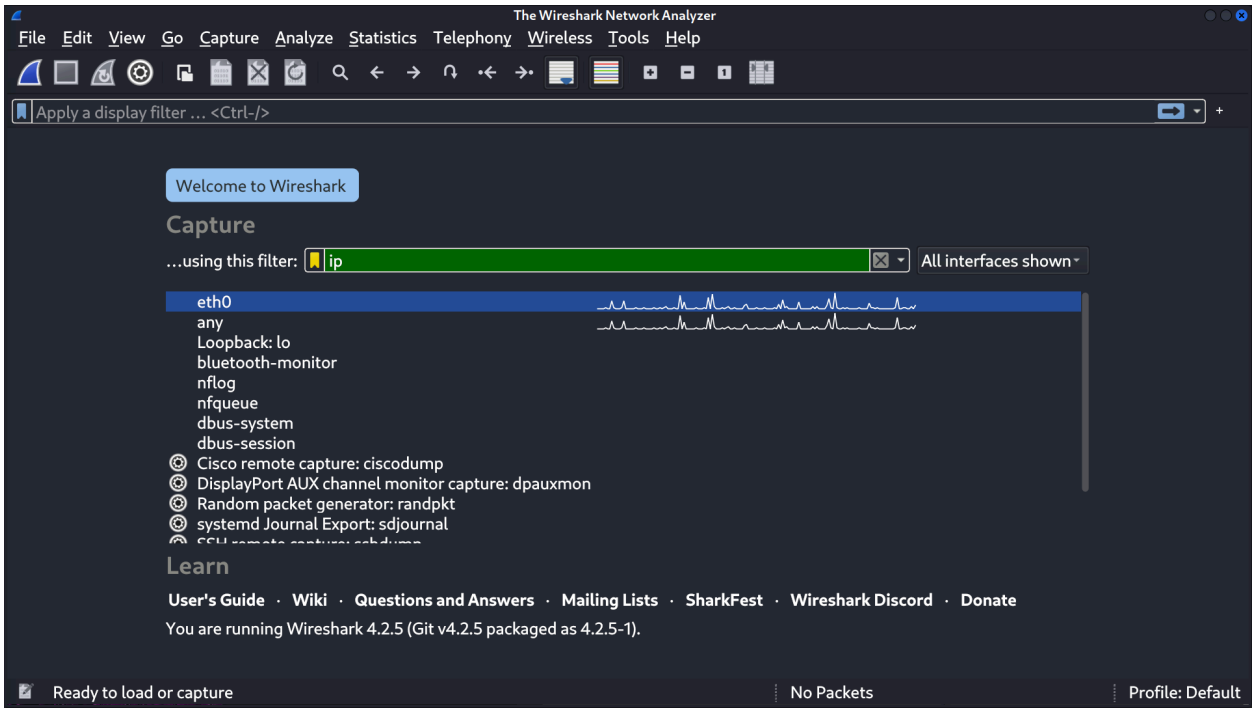
Apply Rule:
Give your rule a name, like "Block Unused Ports," and click Finish.
Commonly unused ports to block:
Port 23 (Telnet): Often targeted in attacks.
Port 135 (RPC): Used by malicious actors for remote code execution.
Port 445 (SMB): Can be exploited for spreading malware like ransomware

Monitoring Network Traffic with Wireshark

Wireshark is a powerful, free tool that allows you to capture and analyze network traffic in real-time. It
helps you understand the various types of traffic passing through your network and spot potential security

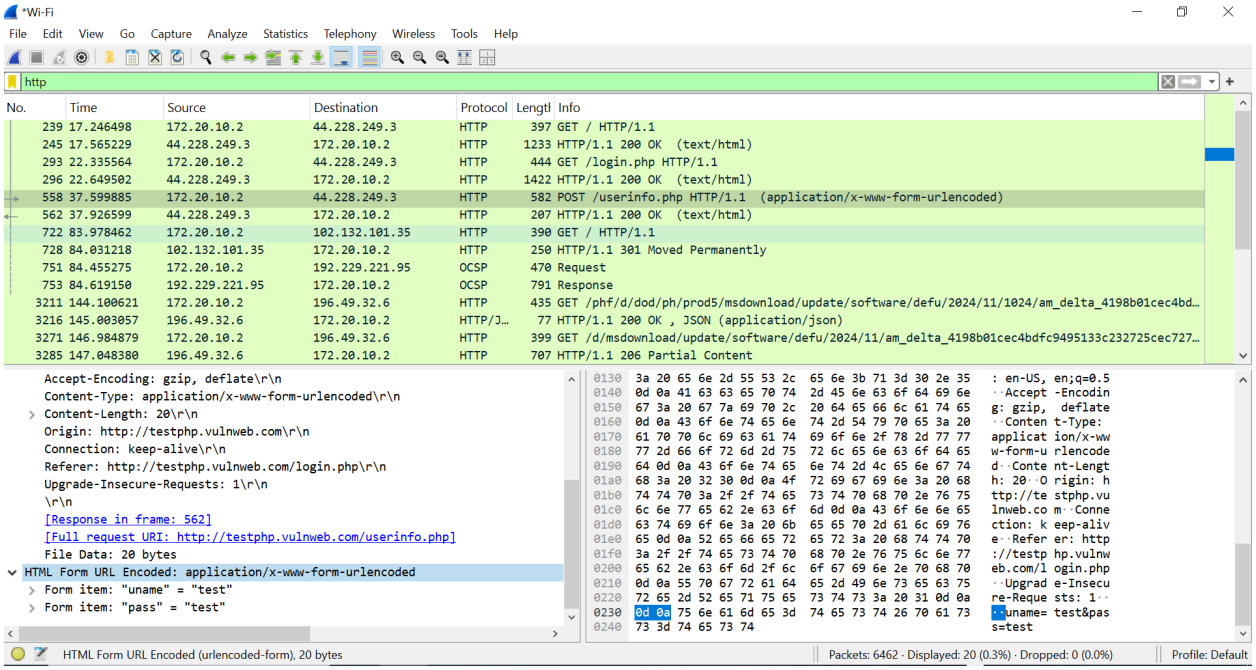
threats.I'll show how to use Wireshark to monitor network traffic, identify different types of traffic, and
detect unusual or suspicious activity.

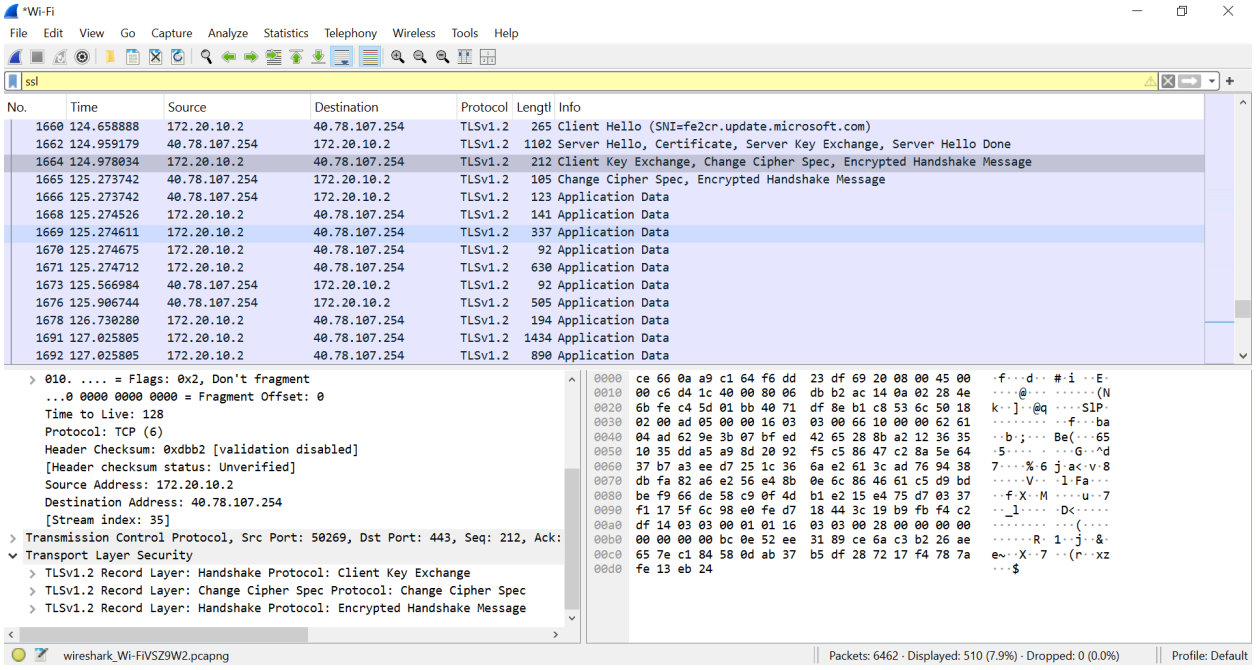
To start capturing traffic:
1. Open Wireshark.
2. Select a network interface to monitor (e.g., your Wi-Fi or Ethernet interface). Wireshark will display
all available interfaces on your machine. Click the one you want to monitor.3. Start Capturing: Press the shark fin icon to start capturing packets. Wireshark will immediately begin to display the traffic in real-time



Identify Different Types of Network Traffic

As Wireshark captures packets, you'll see various types of traffic flowing through the network. Each
protocol serves a different function, and understanding them helps identify what's normal versus
suspicious activity.





Reflecting on Security Best Practices for Larger Networks:

In a larger, more complex network, additional security measures become crucial to protecting data and
maintaining system integrity. Beyond basic firewalls and encryption, you'd need tools like **intrusion

detection systems (IDS), **virtual private networks (VPNs)** for secure remote access, **multi-factor
authentication (MFA)** to strengthen login security, and **network segmentation** to limit the spread
of threats. Implementing **regular vulnerability assessments** and **security patches** ensures that the
network stays protected from emerging threats. Automating these processes with advanced monitoring and
logging systems will help detect unusual behavior in real time, allowing quicker responses to security
incidents.**

Educating Others on the Importance of Network Security:

**Network security is like locking the front door of your house—essential, but often overlooked in the
digital world. I'd explain to others that every time they use the internet, they're exposed to potential risks,
from phishing scams to malware. Simple actions, like using strong passwords, enabling two-factor
authentication, and avoiding public Wi-Fi for sensitive tasks, can drastically reduce these risks. I'd remind
them that protecting their devices and personal information is not just a matter of convenience but
essential to keeping their digital lives secure in a world where threats are constantly evolving.**

CONCLUSION:

**This task has helped me to dive deep into Network Security Task and how to spot Potential Network Anomalies on a Network i have also been able to equip myself with measures on how to protect my Network from being hacked into
This will help me protect my organisation from future Network Incidents and Attacks.
My Advice for Future Interns will be for them to Take Network Security Seriously because the Network is a very critical component in Cyber Security because if it is being compromised a lot of Departments in the Organization will suffer from it.**

CLOSING REMARKS:

**I want to thank the Red Users for giving me this opportunity and this task on Network Security it has really helped me to learn about Network Security and to know how to keep them secured from Attackers.
Thank you.**