

INTERNSHIP-THE RED USERS

NAME: Obinna Emere

Task 1: Introduction to Network Security Basics

Different types of network threat:

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.

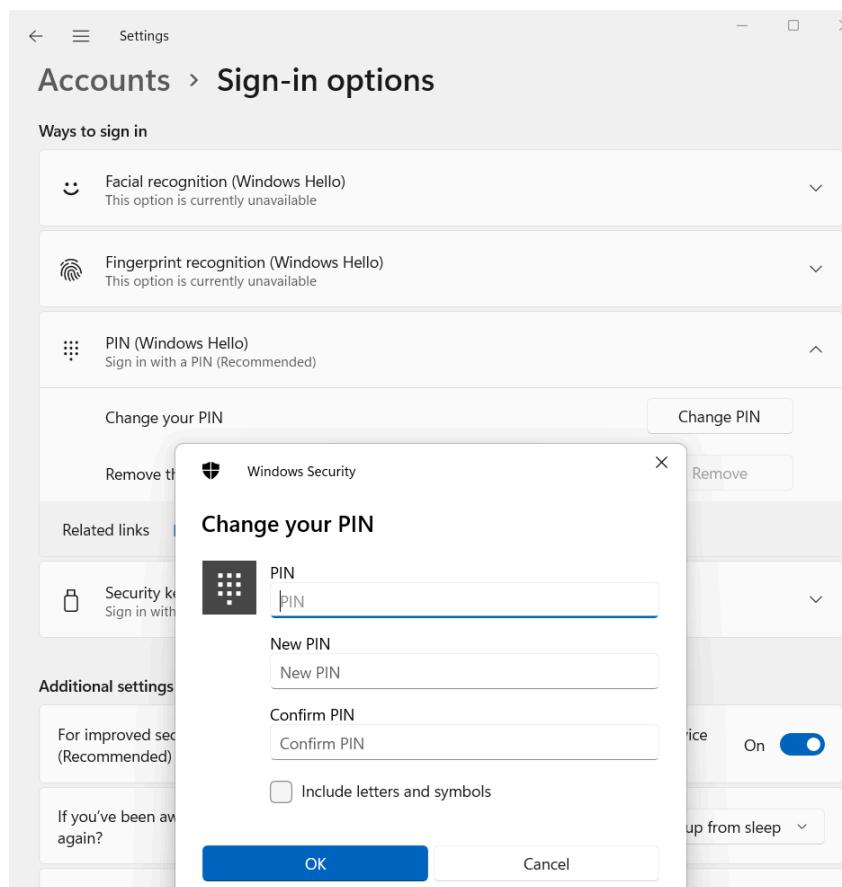
2. **Go to Accounts:** Click on **Accounts**.

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)

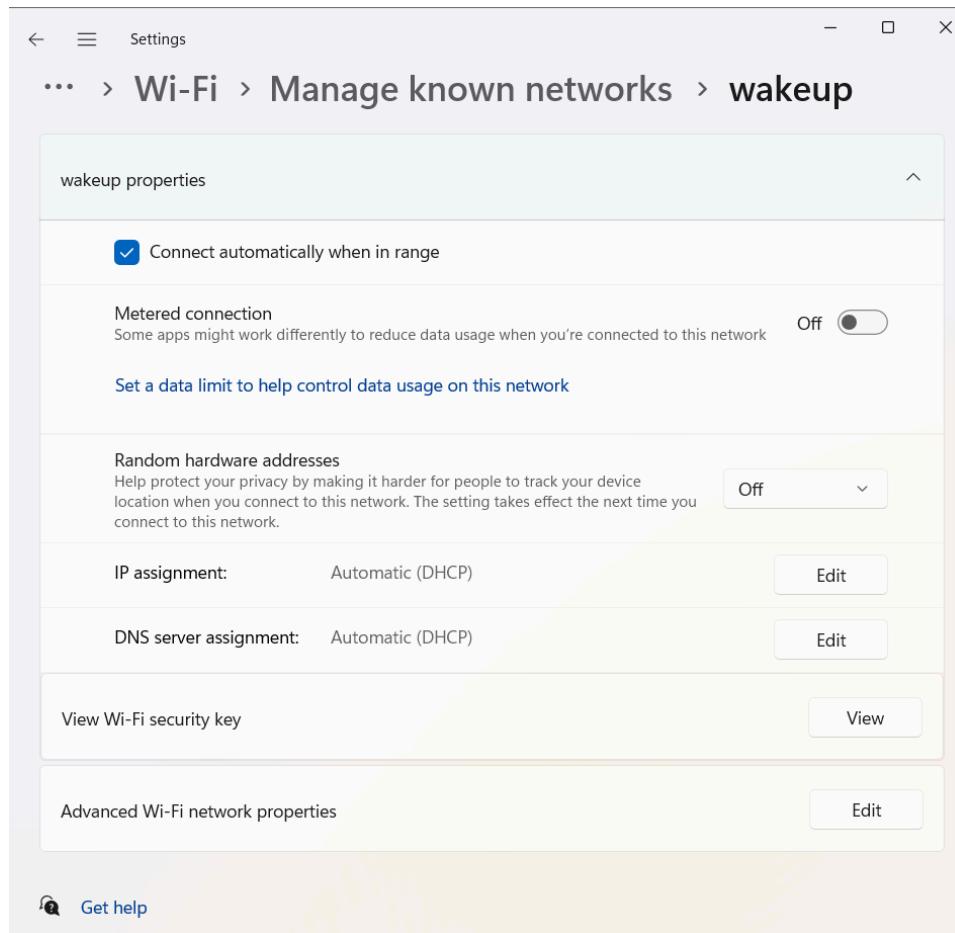
WPA2/WPA3 encryption is generally set up on a **router** to secure wireless networks. However, if you're connecting to a Wi-Fi network on your laptop, you can ensure that you're connecting to a network with proper encryption.

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

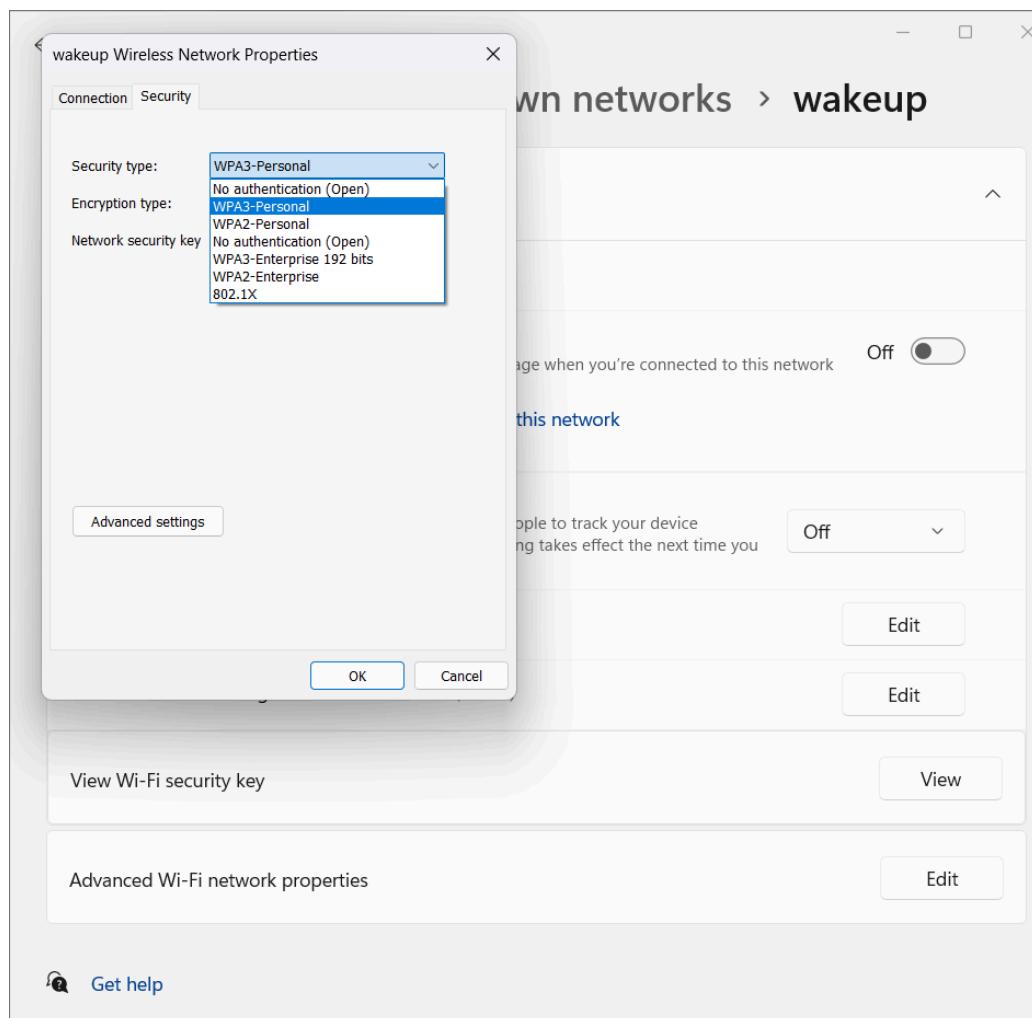


Connect to Secured Networks: Select a network and make sure it's using **WPA2** or **WPA3** encryption

(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

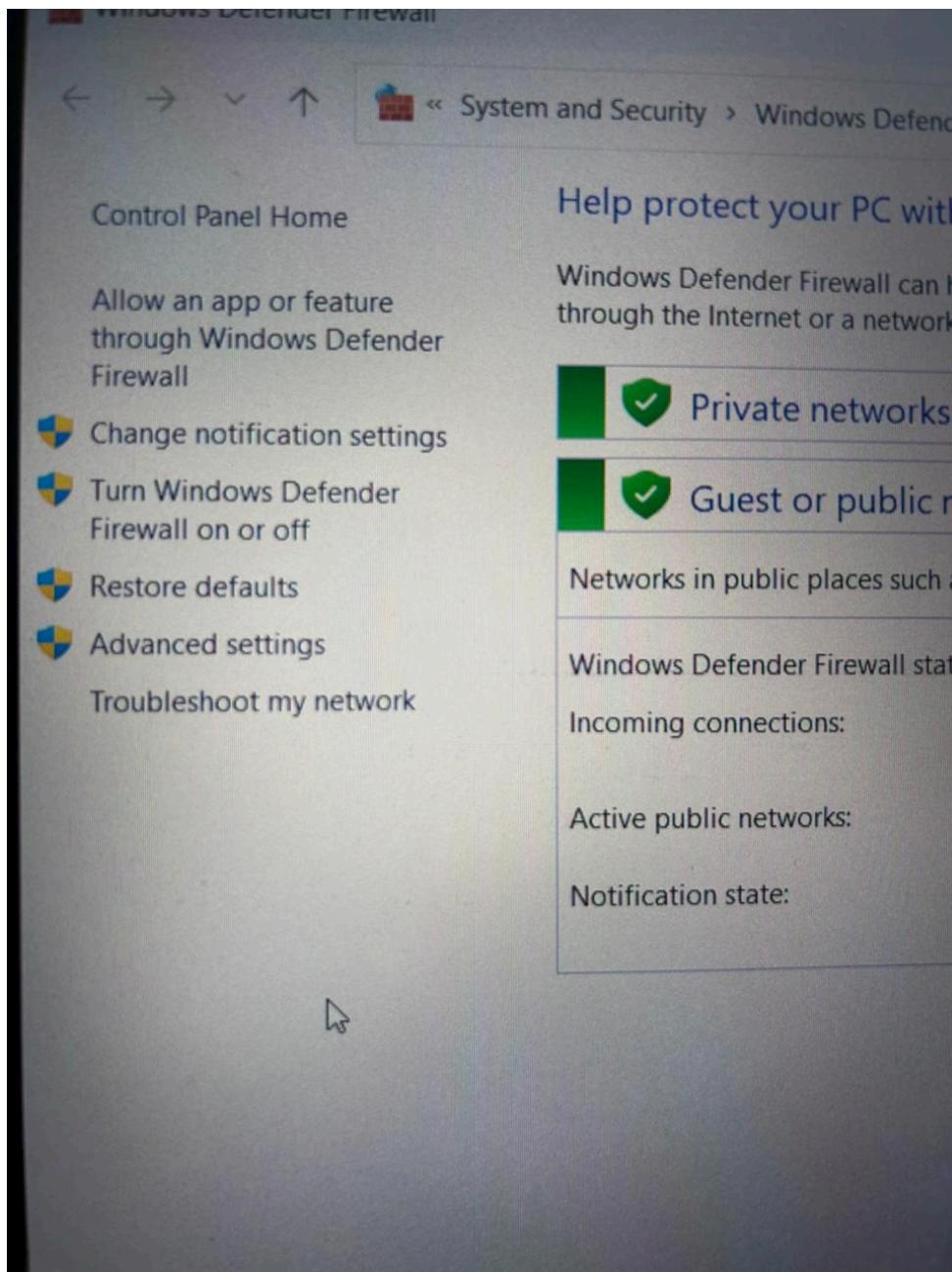
connecting to it or consider reaching out to your network administrator to upgrade security



Steps to block unused ports using Windows Firewall:

Open Windows Defender Firewall:

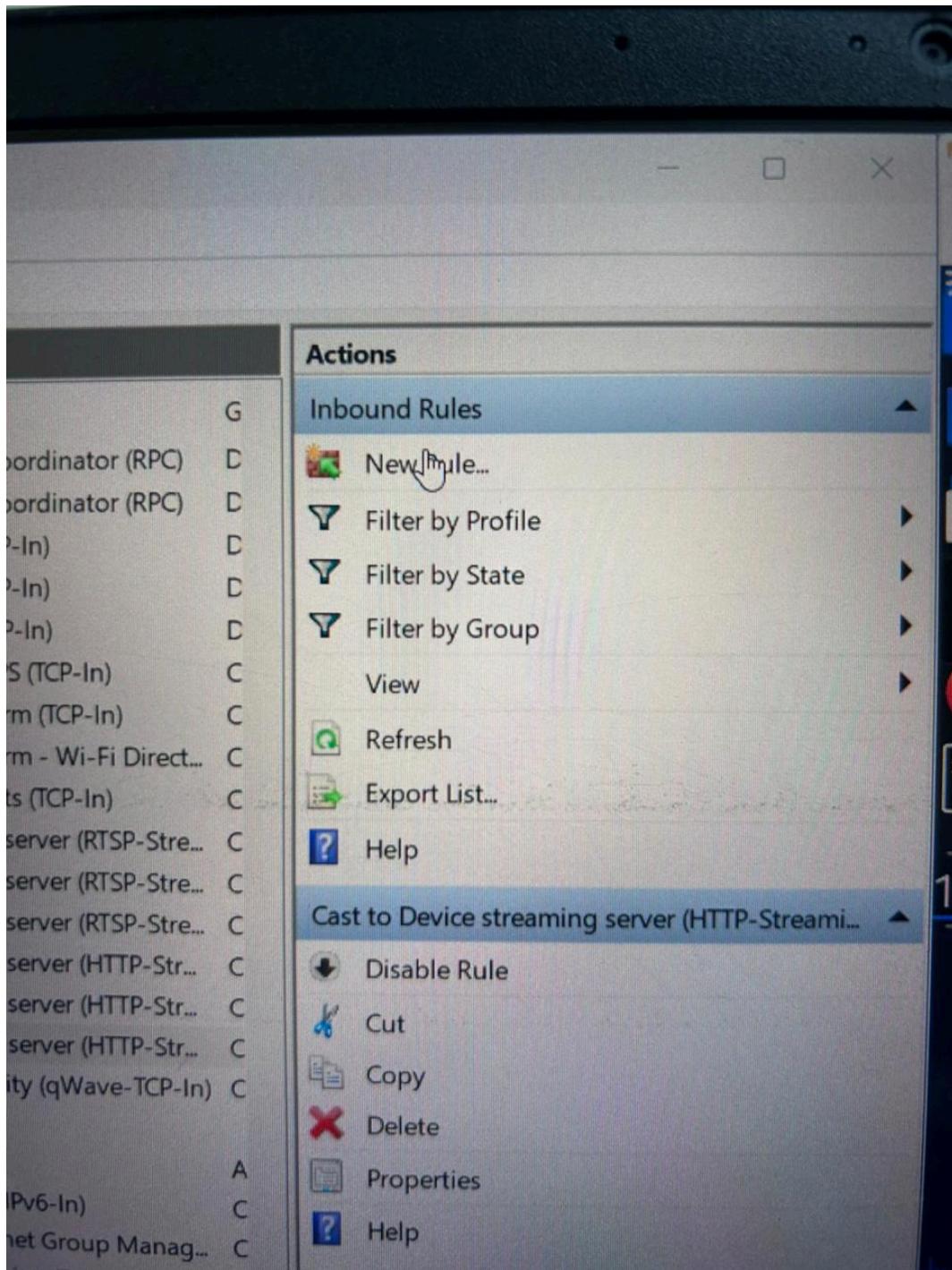
Search for "Windows Defender Firewall" in the Start menu and select **Advanced settings** on the left.



Create a New Inbound Rule:

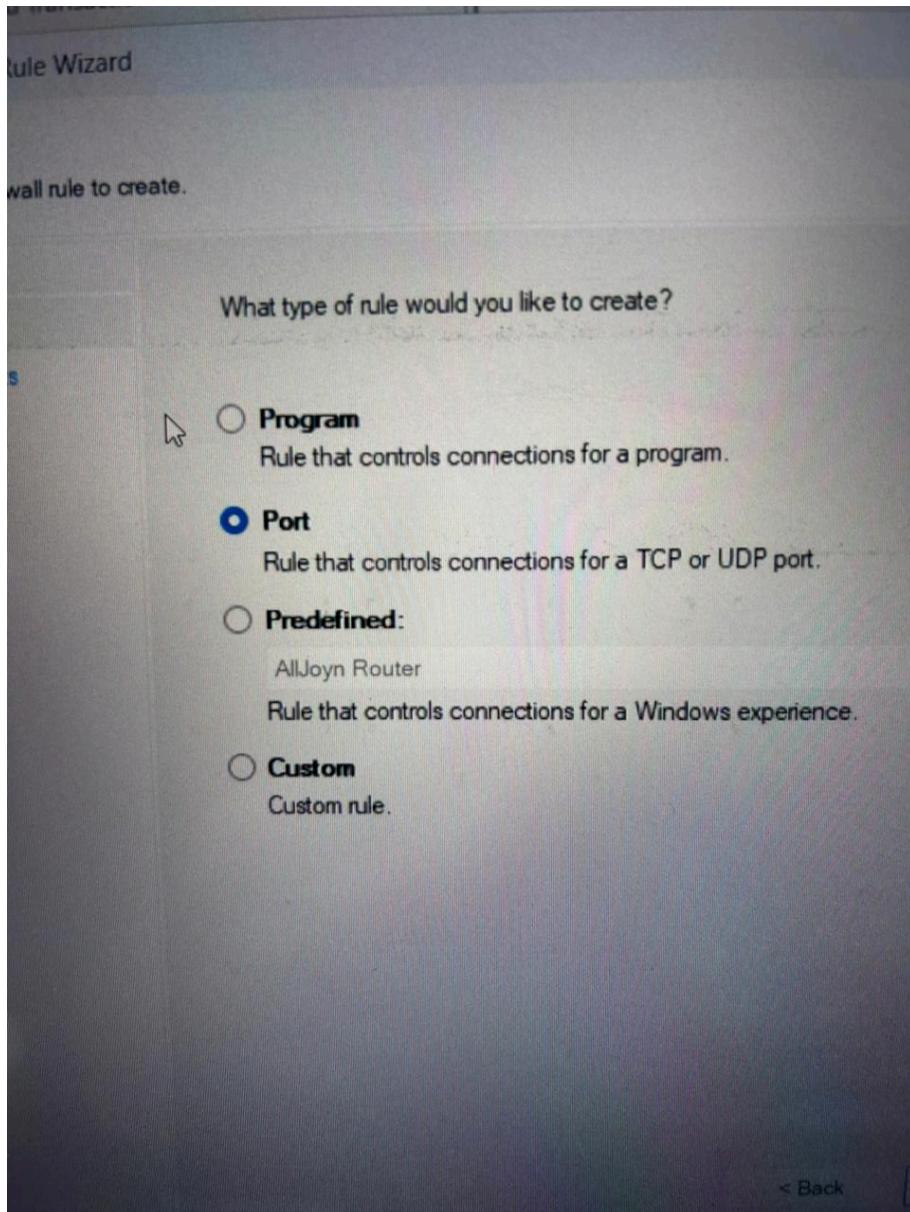
Click **Inbound Rules** on the left panel.

On the right, select **New Rule**.



Select Port:

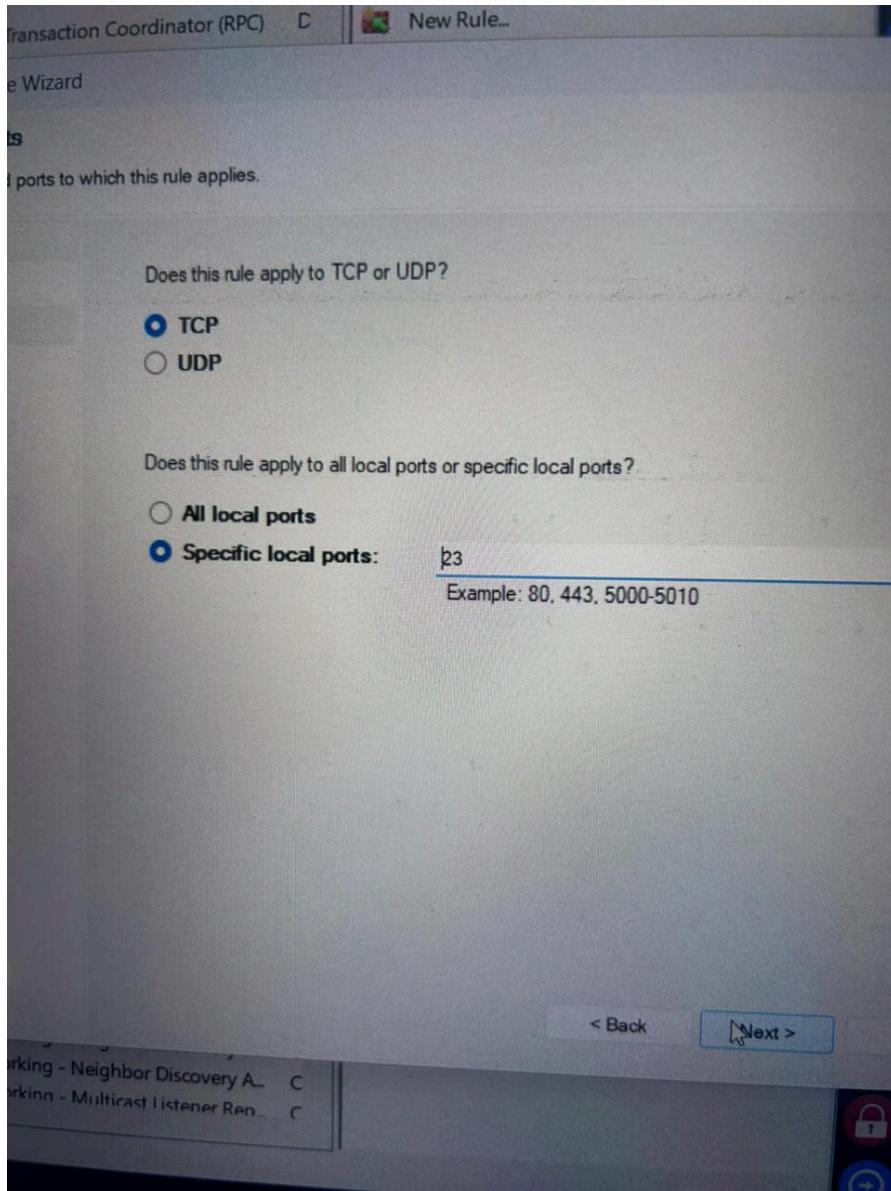
Choose **Port** and click **Next**.



Specify Ports to Block:

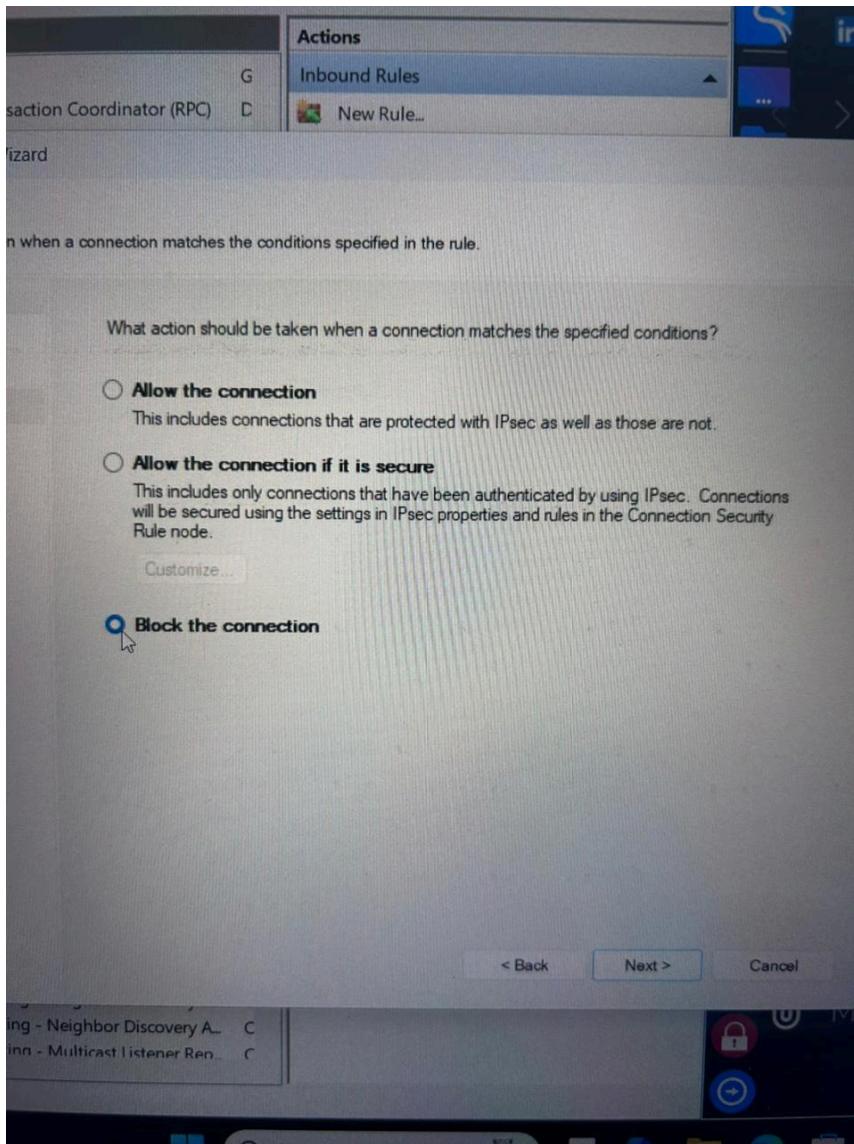
Select whether to block **TCP** or **UDP** ports and then specify the port number(s) you want to block.

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:

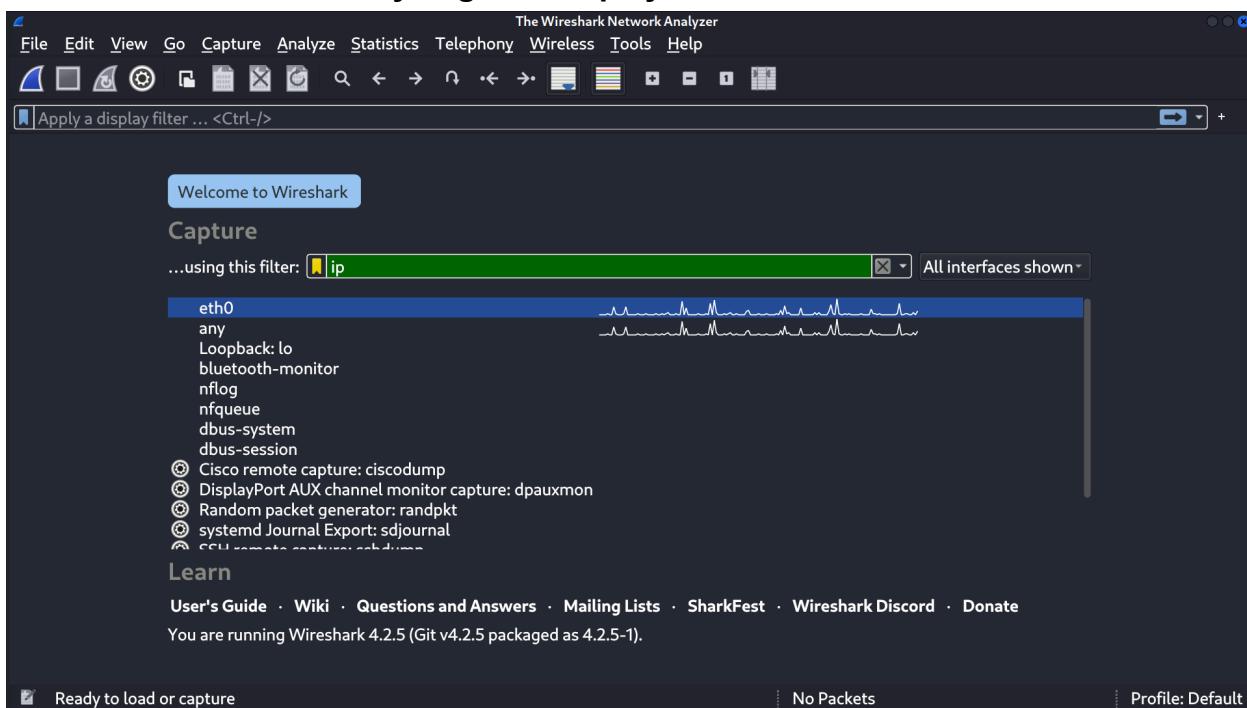
1. Open Wireshark.
2. Select a network interface to monitor (e.g., your Wi-Fi or Ethernet interface).

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.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
239	17.246498	172.20.10.2	44.228.249.3	HTTP	397	GET / HTTP/1.1
245	17.565229	44.228.249.3	172.20.10.2	HTTP	1233	HTTP/1.1 200 OK (text/html)
293	22.335564	172.20.10.2	44.228.249.3	HTTP	444	GET /login.php HTTP/1.1
296	22.649502	44.228.249.3	172.20.10.2	HTTP	1422	HTTP/1.1 200 OK (text/html)
558	37.599885	172.20.10.2	44.228.249.3	HTTP	582	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
562	37.926599	44.228.249.3	172.20.10.2	HTTP	207	HTTP/1.1 200 OK (text/html)
722	83.978462	172.20.10.2	102.132.101.35	HTTP	390	GET / HTTP/1.1
728	84.031218	102.132.101.35	172.20.10.2	HTTP	250	HTTP/1.1 301 Moved Permanently
751	84.455275	172.20.10.2	192.229.221.95	OCSP	470	Request
753	84.619150	192.229.221.95	172.20.10.2	OCSP	791	Response
3211	144.100621	172.20.10.2	196.49.32.6	HTTP	435	GET /phf/d/dod/ph/prod5/msdownload/update/software/defu/2024/11/1024/am_delta_4198b01cec4bd...
3216	145.003857	196.49.32.6	172.20.10.2	HTTP/J...	77	HTTP/1.1 200 OK (JSON application/json)
3271	146.984879	172.20.10.2	196.49.32.6	HTTP	399	GET /d/msdownload/update/software/defu/2024/11/am_delta_4198b01cec4bd9c9495133c232725cec727...
3285	147.048380	196.49.32.6	172.20.10.2	HTTP	707	HTTP/1.1 206 Partial Content

```

Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 20\r\n
Origin: http://testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Referer: http://testphp.vulnweb.com/login.php\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Response in frame: 562]
[Full request URL: http://testphp.vulnweb.com/userinfo.php]
File Data: 20 bytes
  Form item: "uname" = "test"
  Form item: "pass" = "test"
  
```

HTML Form URL Encoded: application/x-www-form-urlencoded

Packets: 6462 - Displayed: 20 (0.3%) - Dropped: 0 (0.0%) | Profile: Default

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
1660	124.658888	172.20.10.2	40.78.107.254	TLSv1.2	265	Client Hello (SNI=fe2cr.update.microsoft.com)
1662	124.959179	40.78.107.254	172.20.10.2	TLSv1.2	1102	Server Hello, Certificate, Server Key Exchange, Server Hello Done
1664	124.978034	172.20.10.2	40.78.107.254	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1665	125.273742	40.78.107.254	172.20.10.2	TLSv1.2	185	Change Cipher Spec, Encrypted Handshake Message
1666	125.273742	40.78.107.254	172.20.10.2	TLSv1.2	123	Application Data
1668	125.27452	172.20.10.2	40.78.107.254	TLSv1.2	141	Application Data
1669	125.274612	172.20.10.2	40.78.107.254	TLSv1.2	337	Application Data
1670	125.274675	172.20.10.2	40.78.107.254	TLSv1.2	92	Application Data
1671	125.274712	172.20.10.2	40.78.107.254	TLSv1.2	638	Application Data
1673	125.566984	40.78.107.254	172.20.10.2	TLSv1.2	92	Application Data
1676	125.906744	40.78.107.254	172.20.10.2	TLSv1.2	505	Application Data
1678	126.730280	172.20.10.2	40.78.107.254	TLSv1.2	194	Application Data
1691	127.025805	172.20.10.2	40.78.107.254	TLSv1.2	1434	Application Data
1692	127.025808	172.20.10.2	40.78.107.254	TLSv1.2	890	Application Data

```

> 010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xdbb2 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.20.10.2
Destination Address: 40.78.107.254
[Stream index: 35]
> Transmission Control Protocol, Src Port: 50269, Dst Port: 443, Seq: 212, Ack: 212
> Transport Layer Security
  > TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  > TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  > TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
  
```

0000 ce 66 0a a9 c1 64 f6 dd 23 df 69 20 08 00 45 00 f...d # i E...
0010 00 c5 d4 1c 49 00 08 06 db b2 ac 14 0a 02 28 4e ...@.....(N
0020 6b fa c4 5d 01 bb 49 71 d4 8e b1 c8 53 6c 50 18 k-]`@q SLP...
0030 02 00 ad 05 00 00 16 03 03 00 66 10 00 00 62 61 ..f...ba
0040 04 ad 62 9e 5b 07 bf ed 42 65 28 8b a2 12 36 35 b;...Be(...65
0050 10 35 dd a5 a9 8d 20 92 f5 c5 86 47 c2 8a 5e 64 5...G...d
0060 37 b7 a3 ee 07 25 1c 36 6a e2 61 3c ad 76 94 38 7...% 6 j.ac< v.8
0070 db f4 82 a6 56 84 68 0e 6c 86 46 61 c5 d9 bdV...1.Fa...
0080 be f9 66 de 58 c9 0f 4d b1 e2 15 e4 75 d7 03 37 ..f X-M...u.7
0090 f1 17 5f 6c 98 e0 fe d7 18 44 3c 19 b9 fb f4 c2 ..1...Dc.....
00a0 df 14 03 03 00 01 16 03 03 00 28 00 00 00 00R 1..j...&
00b0 00 00 00 bc 0e 52 ee 31 89 ce 6a c3 b2 26 aeX-7...(r...xz
00c0 65 7e c1 84 58 0d ab 37 b5 df 28 72 17 f4 78 7a e...\$ fe 13 eb 24
00d0

Packets: 6462 - Displayed: 510 (7.9%) - Dropped: 0 (0.0%) | Profile: Default

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.

