INTERNSHIP-THE RED USERS

NAME-MAYUR KIRAN ERANDE

Task 1 : Introduction to Network Security

Basics Different Types Of Network Threats:

Network threats are malicious activities or events that can compromise the integrity, confidentiality, or availability of a network and its resources.some of most common network threats like malware, viruses, trojans, worms, phishing and etc.

1.Malware: Malicious software designed to harm or exploit devices and networks. Common types include: Viruses: Attach to files and spread when the files are shared. Worms: Self-replicating programs that spread across networks. Trojan Horses: Disguised as legitimate software but perform malicious actions. Ransomware: Encrypts data and demands payment for decryption. Spyware: Collects user data without consent. Adware: Displays unwanted ads, potentially containing malicious links.

2. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks DoS: Overloads a network or system with excessive requests, causing service disruption. DDoS: Uses multiple systems to amplify the attack, making it harder to mitigate.

3. Phishing and Social Engineering

Manipulation of individuals to obtain sensitive information:

Phishing: Fraudulent emails or websites designed to steal credentials. Spear Phishing: Targeted attacks on specific individuals or organizations.

Pretexting: Creating a fabricated scenario to trick users into divulging information.

4. Man-in-the-Middle (MITM) Attacks: An attacker intercepts and manipulates communication between two parties Common in unsecured Wi-Fi networks. Exploits weak encryption or session vulnerabilities.

5. Insider Threats

Malicious or accidental actions by employees or trusted individuals

Data theft: Stealing sensitive company information.

Sabotage: Deliberately damaging systems or networks.

Negligence: Weak passwords or ignoring security protocols.

6. Exploitation of Vulnerabilities

Exploiting software, hardware, or configuration weaknesses.

Examples: Buffer overflows, SQL injection, and cross-site scripting (XSS).

7. Wireless Network Threats Rogue Access Points: Malicious Wi-Fi hotspots.

Evil Twin Attacks: Mimics legitimate Wi-Fi networks to intercept data.

WEP/WPA Attacks: Exploiting weak encryption standards.

8.SQL Injection

SQL Injection specifically target databases, enabling the extraction of private information.

By injecting malicious SQL code, attackers illegally access and compromise private data.

1. Firewalls

A firewall acts as a barrier between a trusted internal network and untrusted external networks (like the internet). Its primary function is to monitor and control incoming and outgoing traffic based on predefined security rules.

Key Functions: Traffic Filtering: Blocks unauthorized or suspicious data packets.

Access Control: Regulates which services or users can access the network.

Threat Prevention: Protects against attacks such as port scanning and unauthorized access.

Types of Firewalls: Packet Filtering Firewalls: Inspects packets' source, destination, and protocol but doesn’t analyze payloads.

Stateful Inspection Firewalls: Tracks the state of active connections and makes decisions based on the context of traffic.

Proxy Firewalls: Acts as an intermediary between users and the internet, adding an extra layer of security.

Next-Generation Firewalls (NGFWs): Includes advanced features like intrusion prevention, deep packet inspection, and application filtering.

Use Cases: Blocking unauthorized access to servers. Preventing malware from reaching internal systems. Restricting access to specific websites or applications.

2. Encryption

Encryption ensures the confidentiality of data by converting it into an unreadable format that can only be decrypted with the correct key. It protects sensitive information in transit and at rest.

Types of Encryption:

Symmetric Encryption: Uses the same key for encryption and decryption. Example: AES (Advanced Encryption Standard).

Use Case: File storage, database encryption. Asymmetric Encryption: Uses a pair of keys: a public key for encryption and a private key for decryption. Example: RSA, Elliptic Curve Cryptography (ECC).

Use Case: Secure communication (e.g., TLS/SSL for HTTPS). Applications of Encryption: Data in Transit: Encrypts traffic between clients and servers (e.g., HTTPS, VPNs). Prevents eavesdropping and MITM (Man-in-the-Middle) attacks.

Data at Rest: Encrypts stored data to prevent unauthorized access, even if storage devices are stolen.

Email Encryption: Ensures sensitive emails remain private (e.g., using PGP or S/MIME).

3. Secure Network Configurations

A secure network configuration minimizes vulnerabilities and reduces the attack surface. It involves setting up network devices, systems, and policies to ensure robust protection.

Key Aspects of Secure Network Configurations:

Segmentation: Divides the network into smaller segments to isolate sensitive data or systems. Example: Separating public-facing servers (DMZ) from internal networks.

Access Control: Implements policies to restrict access to network resources.

Tools: Role-Based Access Control (RBAC), Network Access Control (NAC). Secure Device Configurations: Change default usernames and passwords. Disable unnecessary services or ports. Regularly update firmware and software. Use of VPNs (Virtual Private Networks): Encrypts connections for remote access, ensuring secure communication over untrusted networks.

Intrusion Detection and Prevention Systems (IDS/IPS): IDS monitors for suspicious activities. IPS actively blocks detected threats. Wireless Security: Use strong encryption protocols (e.g., WPA3). Disable SSID broadcasting and use MAC address filtering.

Logging and Monitoring: Track network activity to identify and respond to potential threats. Use tools like SIEM (Security Information and Event Management).

Steps to change password of user account

1. Open Settings: Press Windows Key + I to open the Settings window.

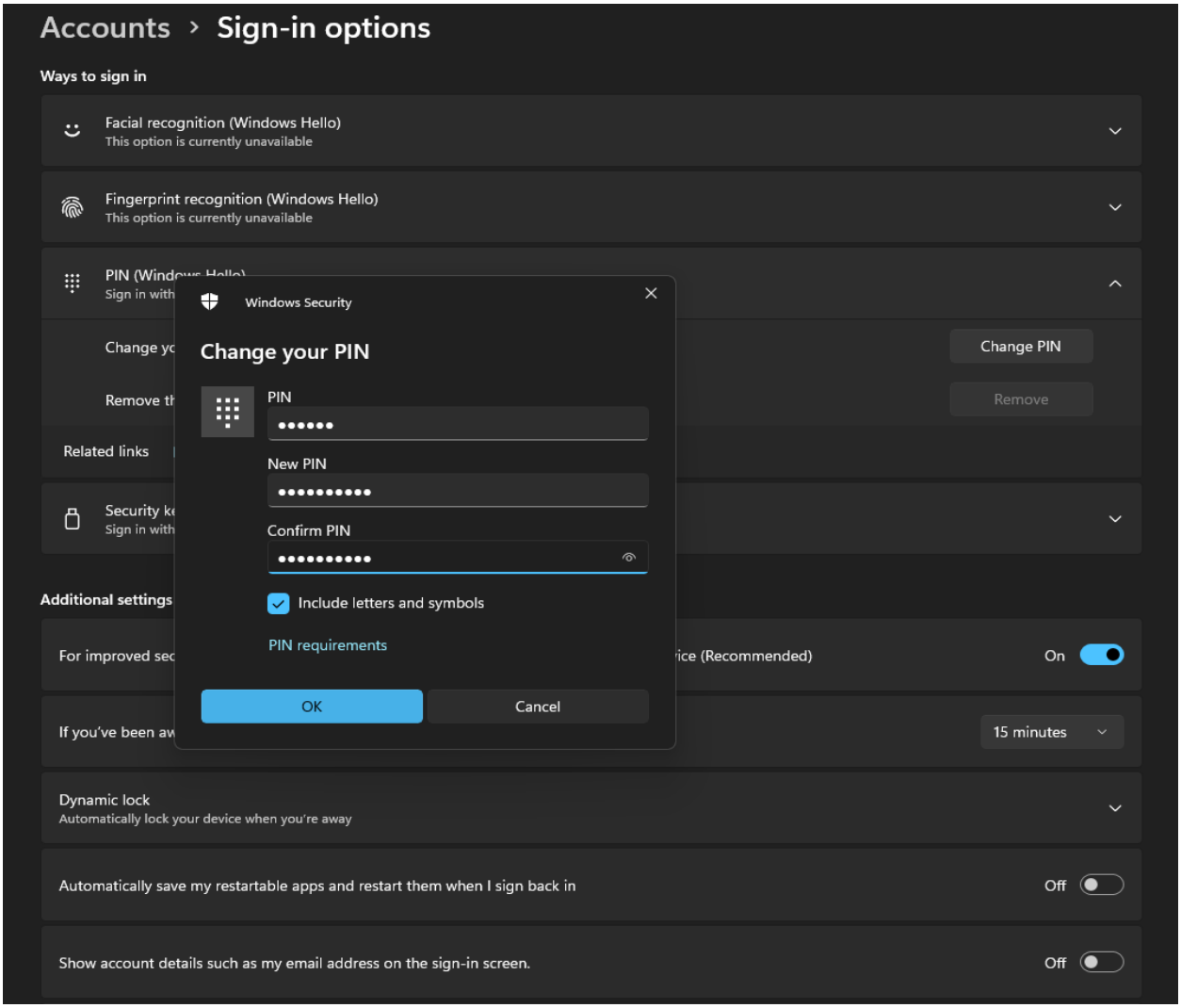
2. Go to Accounts: Click on Accounts.

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, numbers, and symbols).



Enable Network Encryption (WPA2/WPA3)

Network encryption (WPA2/WPA3) is a wireless security protocol that protects data transmitted between a client device and a wireless access point. WPA3 is the latest version of the protocol and offers stronger encryption and attack defense than its predecessor, WPA2.

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

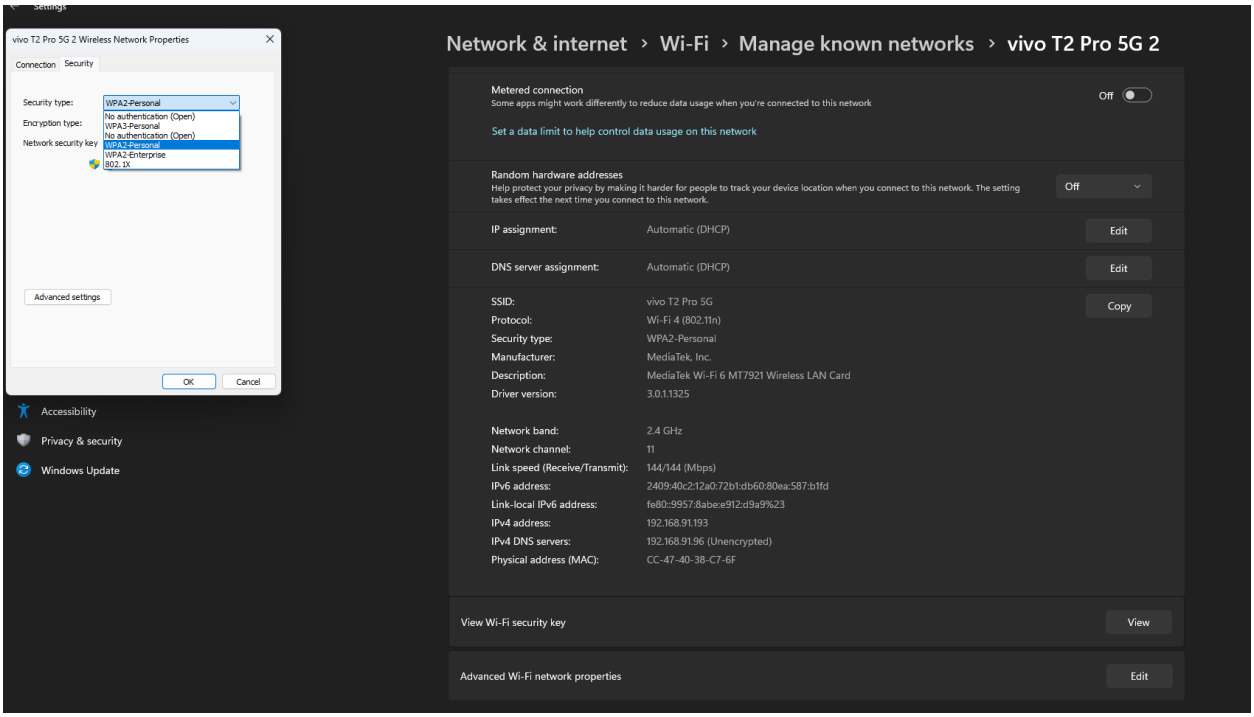
1.Open Network Settings: Click on the Wi-Fi icon in the taskbar and select Network & Internet settings.

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

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

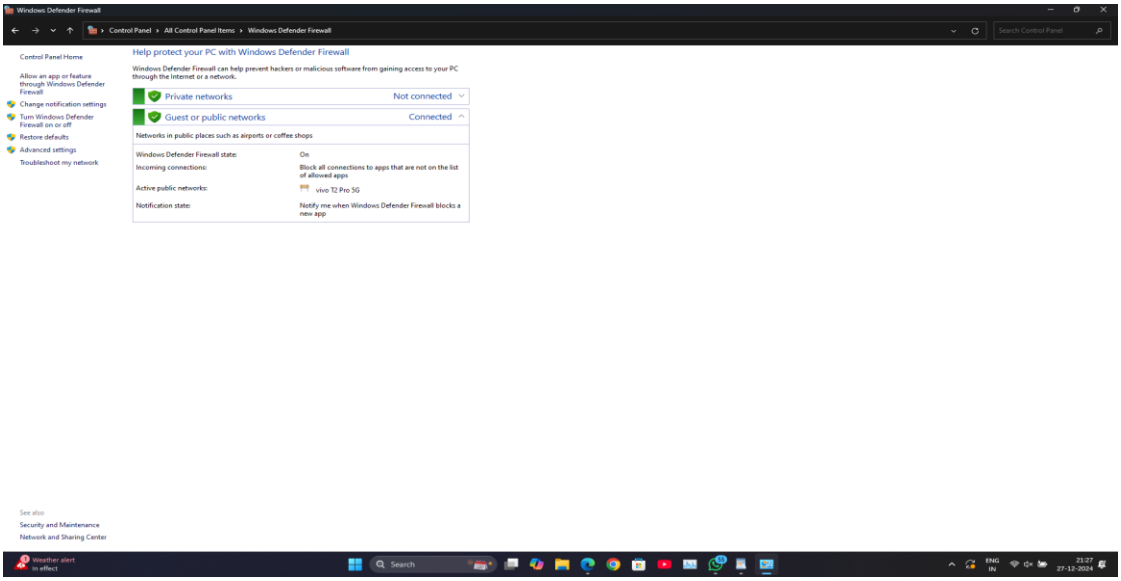
Connect to Secured Networks: Select a network and make sure it’s using WPA2 or WPA3encryption (this is usually displayed next to the network name).

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:

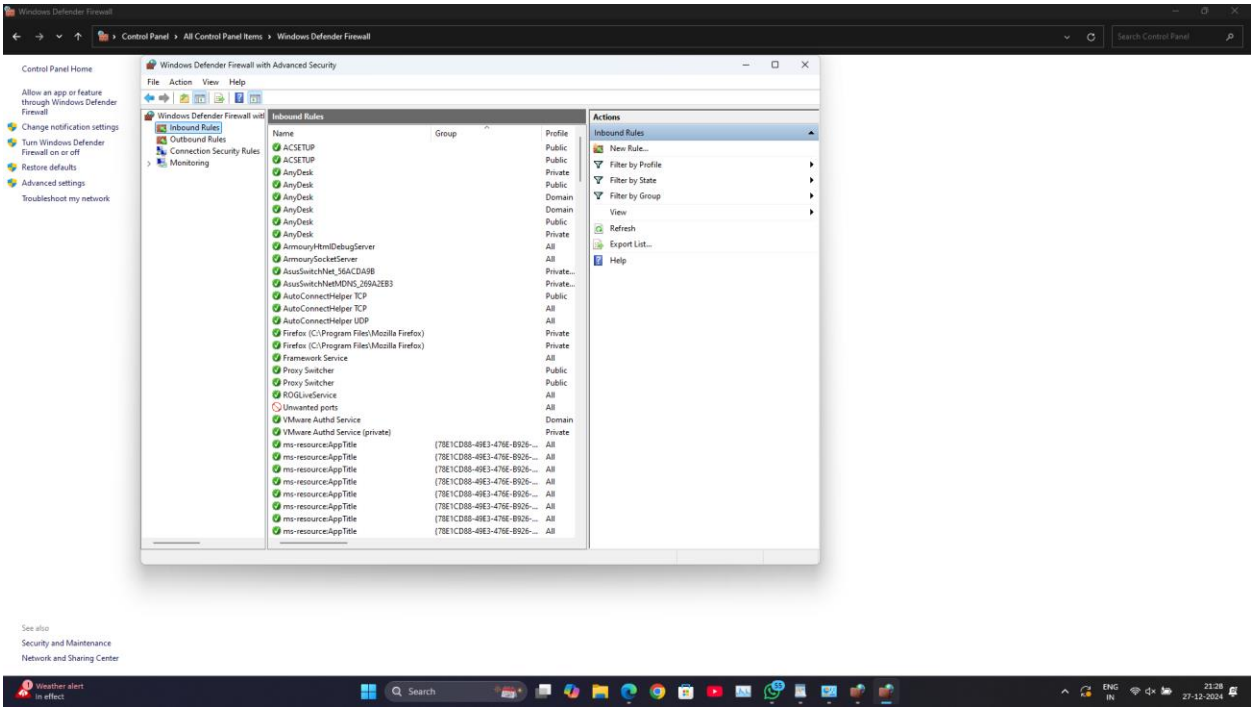
• Open Windows Defender Firewall: -Search for "Windows Defender Firewall" in the Start menu and select Advanced settings on the left.



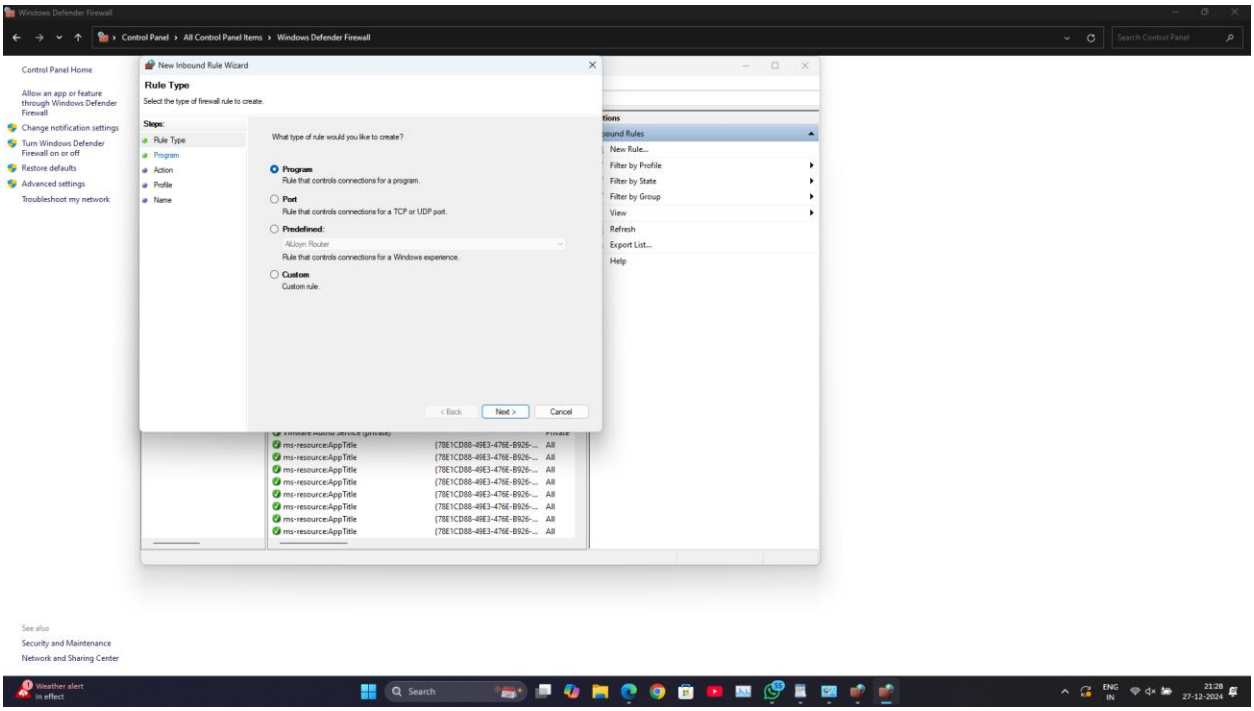
- Create a New Inbound Rule:

  Click Inbound Rules on the left panel.

  On the right, select New Rule.



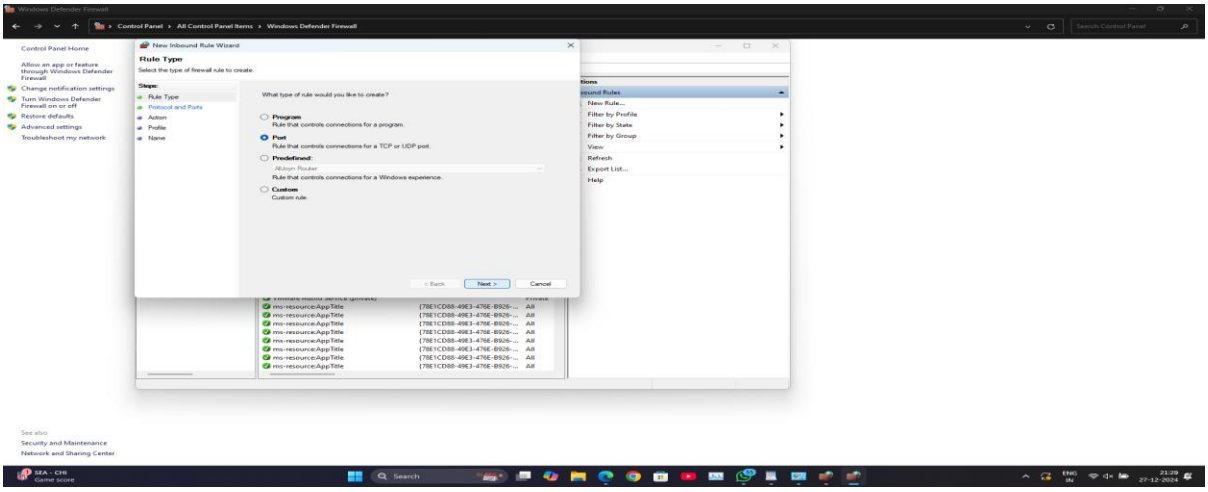
- Select Port:- Choose Port and click Next.



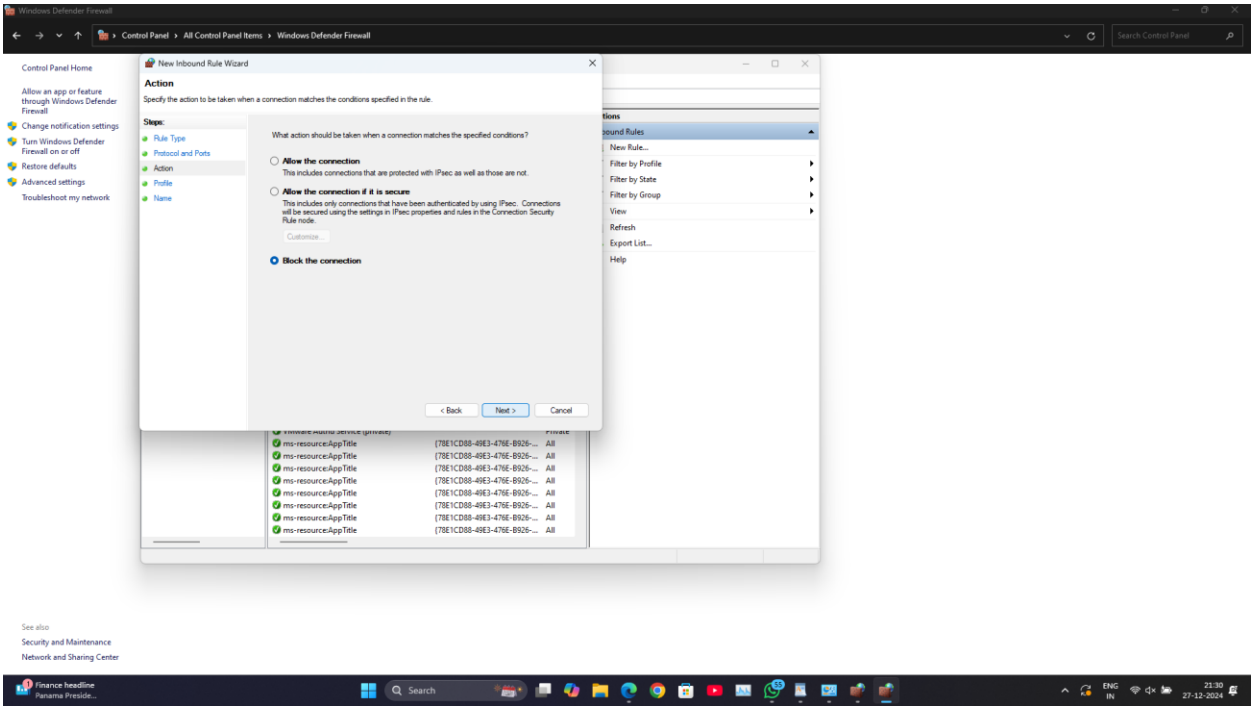
• Specify Port to Block:

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.

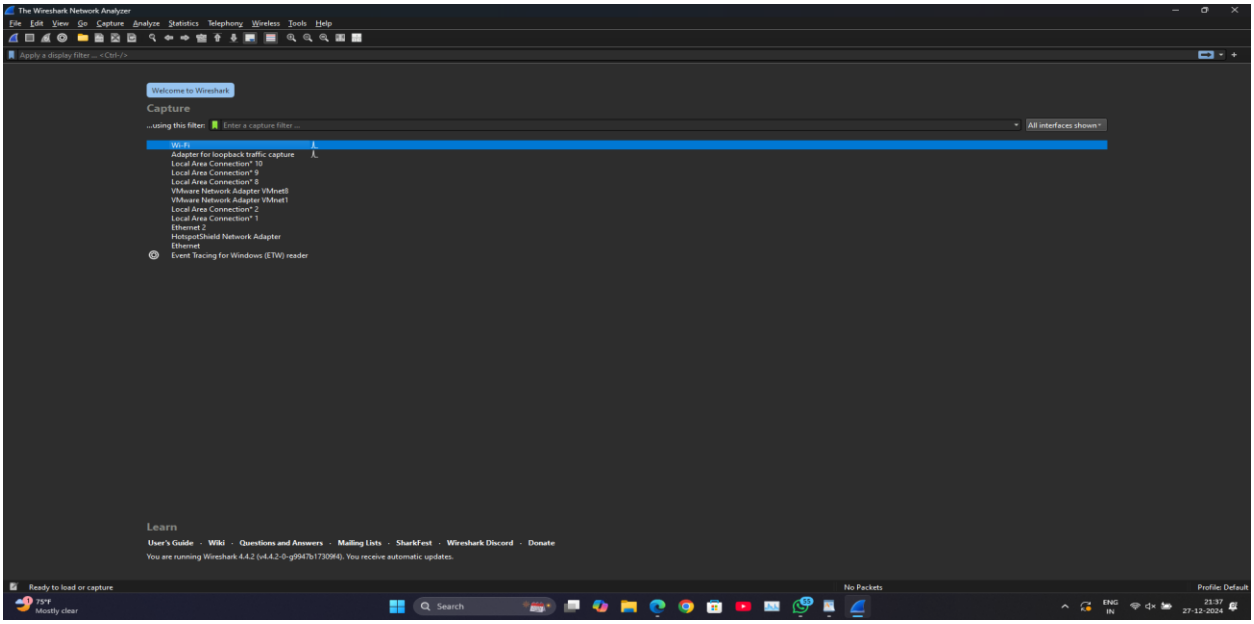
Monitor Network Traffic using Wireshark

Wireshark is a free open source tool that analyzes network traffic in real-time for Windows, Mac, Unix, and Linux systems. It captures data packets passing through a network interface (such as Ethernet, LAN, or SDRs) and translates that data into valuable information for IT professionals and cybersecurity teams.

Steps for Capturing Traffic:

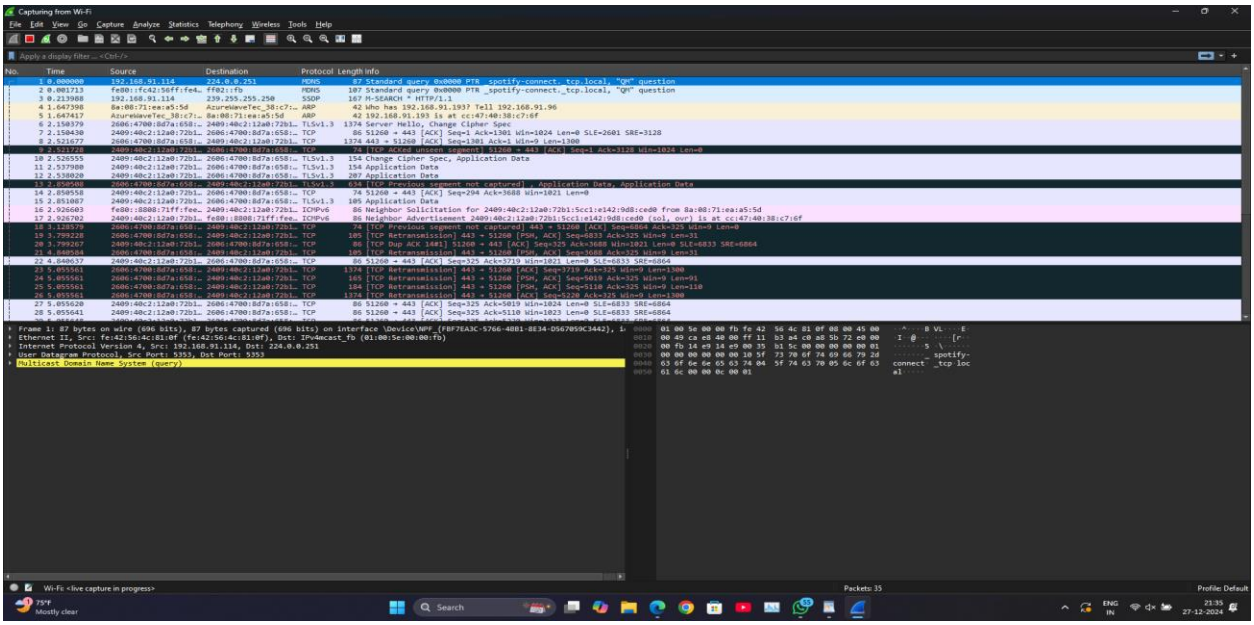
1.Open Wireshark.

2.Select a network interface for monitoring. Wireshark will display all available interfaces at network. Click on the Shark Fin Icon left side on the Windows or Press Ctrl + E Key to start capturing the Packets.



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.



Spotting Suspicious or Unusual Traffic

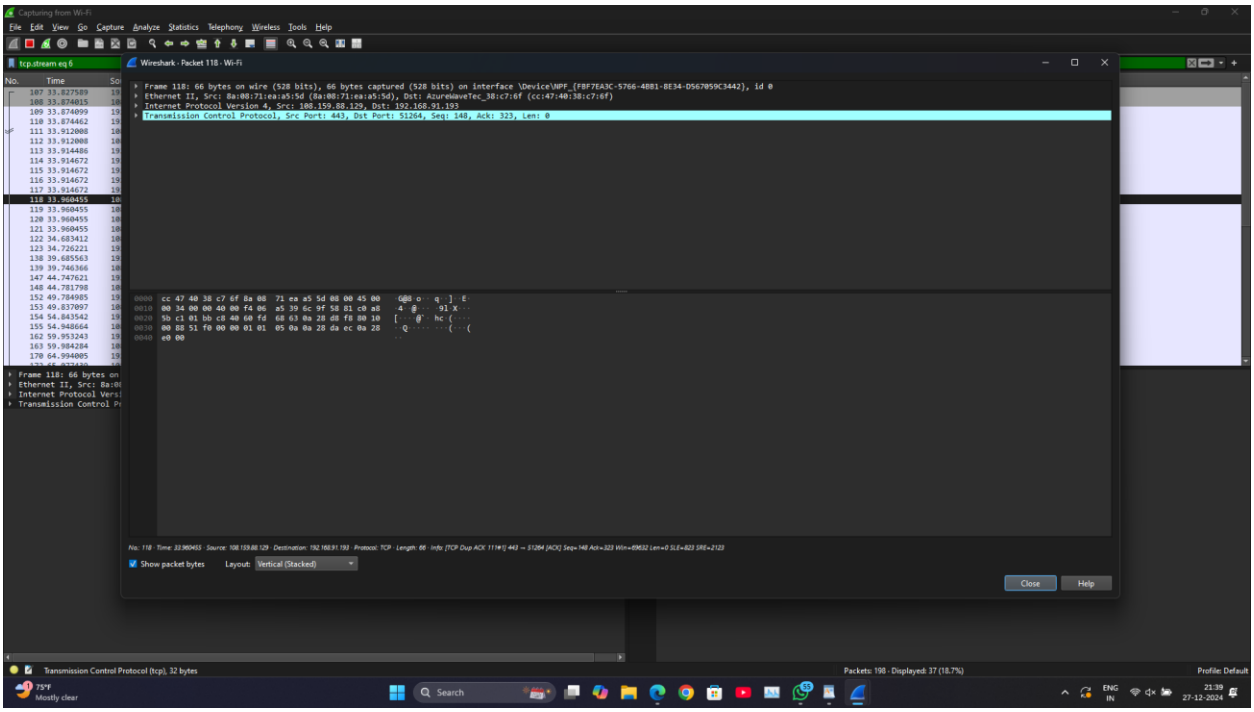
Once you understand the normal traffic patterns, you can start looking for unusual behavior that might indicate a security threat. Here's what to watch for:

Unusual IP Addresses

What to watch for: If you see traffic from unknown or suspicious IP addresses, especially ones from foreign countries or ranges not

used by your organization or home network, it might indicate unauthorized access attempts.

How to spot it: Filter by IP address using ip. addr == X.X.X.X to see all communication with a specific IP.



Monitor Live Traffic

Observe the packets displayed in real time, with each packet listed by details such as time, source, destination, protocol, and info. Click on any packet to see more detailed information in the lower pane, showing layer-by-layer breakdowns like Ethernet, IP, and TCP headers.

Network security is important because it keeps sensitive data safe from cyber attack and ensures the network is usable and trustworthy. Successful network security strategies employ multiple security solutions to protect users and organizations from malware and cyber attack, like distributed denial of service. A network is composed of interconnected devices, such as computers, servers and wireless networks. Many of these devices are susceptible to potential attackers. Network security involves the use of a variety of software and hardware tools on a network or as software as a service.

Security becomes more important as networks grow more complex and enterprises rely more on their networks and data to conduct business.

Network security is critical because it prevents cybercriminals from gaining access to valuable data and sensitive information. When hackers get hold of such data, they can cause a variety of problems, including identity theft, stolen assets and reputational harm.