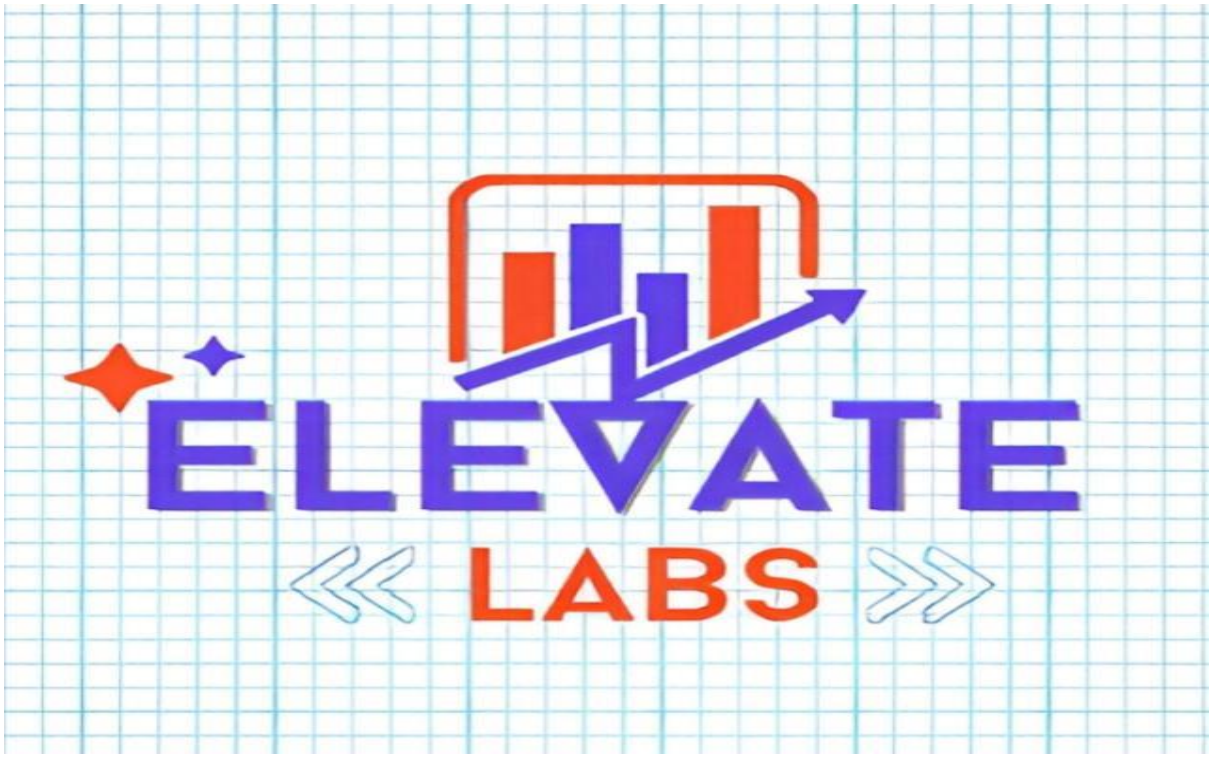
Task 3: Networking Basics for Cyber Security



Name: - Ch Rohit Kumar

University: - Aditya University

Gmail: - rohitkumarrrr20@gmail.com

1.Learn firewall concepts.

What is a Firewall?

A **firewall** is a **security device or software** that monitors and controls **incoming and outgoing network traffic** based on predefined rules.

👉 Think of it as a **security guard** between your computer/network and the internet.

Purpose of a Firewall

- Prevent **unauthorized access**
- Protect systems from **malware & attacks**
- Control **network traffic**
- Enforce **security policies**

How a Firewall Works

- Inspects network packets
- Checks **source IP, destination IP, port number, protocol**
- **Allows or blocks** traffic based on rules

□ Types of Firewalls

1□Packet Filtering Firewall

- Checks packets individually
- Uses rules based on IP, port, protocol
- Fast but **less secure**

Example: Basic router firewall

2□Stateful Inspection Firewall

- Tracks **active connections**
- Makes decisions based on connection state
- More secure than packet filtering

3□Proxy Firewall (Application-Level)

- Acts as an **intermediary**
- Inspects application data (HTTP, FTP)
- Slower but very secure

4️⃣ Next-Generation Firewall (NGFW)

- Includes:
    - Deep Packet Inspection (DPI)
    - Intrusion Prevention System (IPS)
    - Application awareness
- Used in **modern enterprises**

Firewall Based on Deployment

🔹 Network-based Firewall

- Protects entire network
- Installed at network perimeter
- Example: Cisco ASA, FortiGate

🔹 Host-based Firewall

- Installed on individual systems
  Example: Windows Defender Firewall, iptables

Firewall Rules

Rules define what traffic is:

- **Allowed**
- **Denied**

Rules are based on:

- IP address
- Port number
- Protocol (TCP/UDP/ICMP)
- Direction (Inbound/Outbound)

Common Firewall Policies

- **Allow all, deny some**
- **Deny all, allow some** (Most secure)

Examples of Firewall Usage

- Blocking malicious IPs

- Allowing only HTTP/HTTPS traffic
- Preventing unauthorized SSH access
- Protecting servers from attacks

Limitations of Firewalls

- Cannot stop **social engineering**
- Cannot protect against insider threats
- Needs proper configuration

Real-World Examples

- Windows Firewall
- Linux iptables / UFW
- pfSense
- Palo Alto Firewall

2.Configure rules.

What are Firewall Rules?

Firewall rules are **instructions** that tell the firewall **which traffic to allow or block**.

Each rule is checked when a packet enters or leaves the network.

Components of a Firewall Rule

A firewall rule is based on:

- **Source IP address** – where traffic comes from
- **Destination IP address** – where traffic goes
- **Port number** – service being accessed (e.g., 80, 443, 22)
- **Protocol** – TCP, UDP, ICMP
- **Direction** – Inbound or Outbound
- **Action** – Allow or Deny

Types of Firewall Rules

1. Inbound Rules

- Control **incoming traffic**
- Protect the system from external threats

Example:
Allow HTTP (port 80) traffic to a web server

2️⃣ Outbound Rules

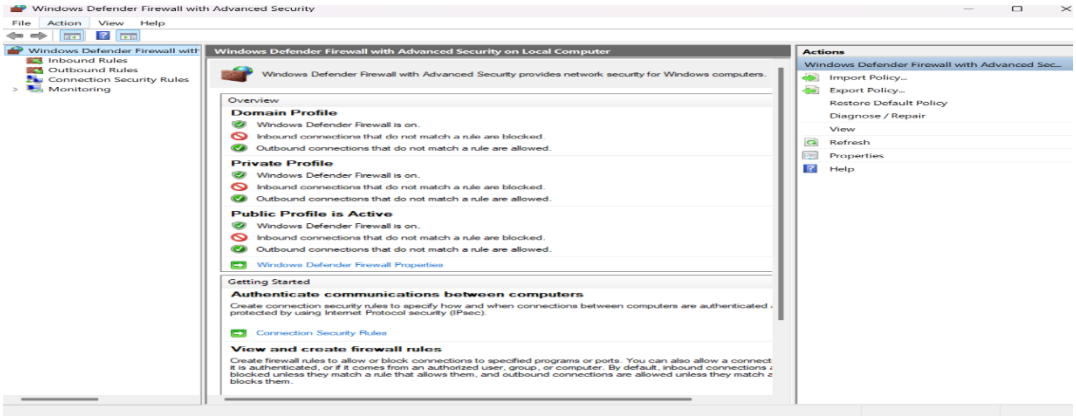
- Control **outgoing traffic**
- Prevent data leaks or malware communication

Example:
Block outbound FTP traffic

➢ Steps to Configure Firewall Rules

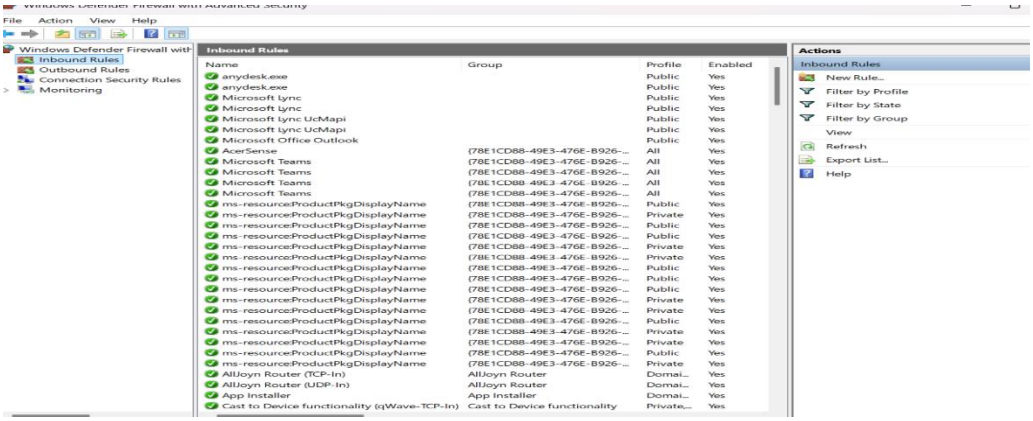
Step 1: Open Firewall

- Press **Win + R**
- Type wf.msc
- Press **Enter**



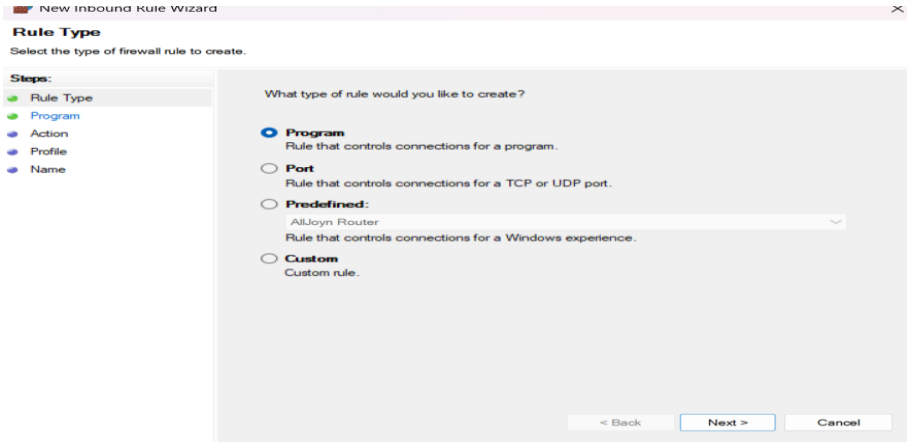
🔷 Step 2: Choose Rule Type

- Click **Inbound Rules** (for incoming traffic)
- OR **Outbound Rules** (for outgoing traffic)



🔷 Step 3: Create New Rule

- Click **New Rule**
- Select **Port**
- Click **Next**



🔹 Step 4: Configure Port

- Choose **TCP** or **UDP**
- Enter port number (e.g., 80, 22)
- Click **Next**

🔹 Step 5: Action

- Select:
  - ✅ Allow the connection
  - ❌ Block the connection
- Click **Next**

🔹 Step 6: Profile

- Domain
- Private
- Public

(Usually select all)

🔹 Step 7: Name the Rule

- Example: Block SSH
- Click **Finish**

✅ Rule applied successfully

3.Allow/deny ports.

What does Allow / Deny Ports mean?

Allowing or denying ports means **controlling access to network services** by permitting or blocking specific **port numbers** used by applications.

Example:

- Port **80** → HTTP (Web)
- Port **22** → SSH
- Port **443** → HTTPS

Why Allow or Deny Ports?

- Reduce attack surface
- Block unnecessary services
- Prevent unauthorized access
- Improve system security

How to Allow / Deny Ports (Practical)

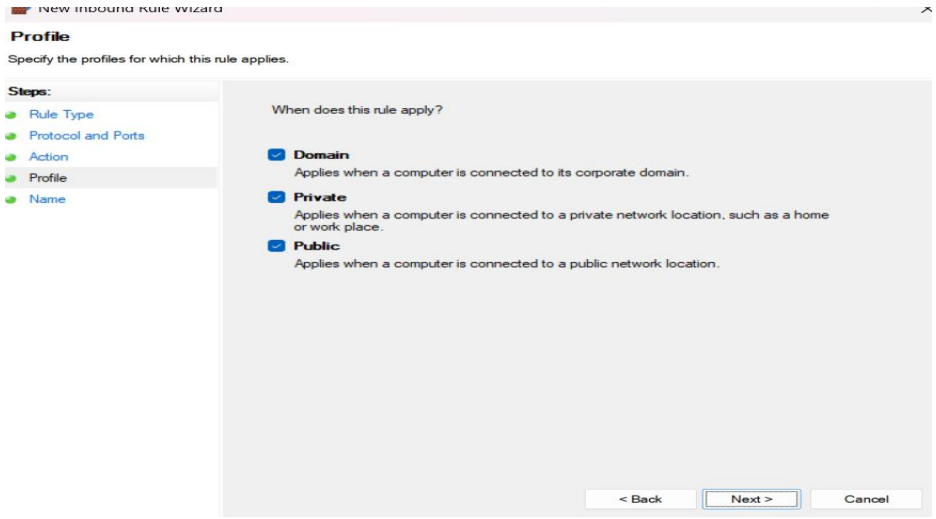
1️⃣Windows Firewall

✅ Allow a Port

1. Open **Run → wf.msc**
2. Click **Inbound Rules**
3. Click **New Rule**
4. Select **Port**
5. Choose **TCP/UDP**
6. Enter port number (e.g., 80)
7. Select **Allow the connection**
8. Apply profiles
9. Name rule → Finish

❌ Deny (Block) a Port

- Follow same steps
- Choose **Block the connection**
- Example: Block port 21



4.Test connectivity.

What is Connectivity Testing?

Connectivity testing is the process of **verifying whether a system can communicate with another system or service** after configuring firewall rules.

It confirms whether traffic is **allowed or blocked as intended**.

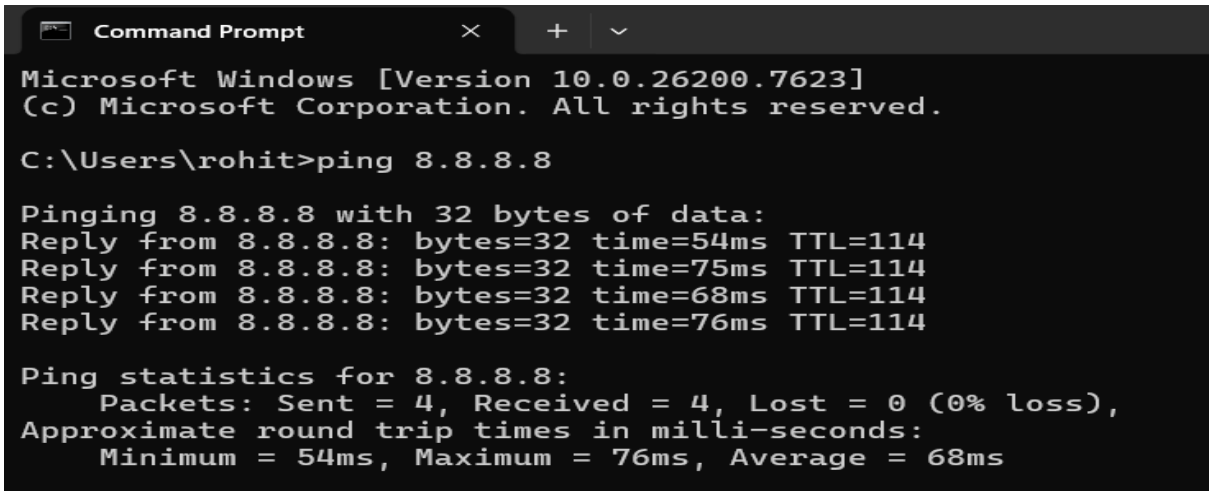
Why Test Connectivity?

- Ensure firewall rules work correctly
- Confirm allowed ports are accessible
- Detect misconfigurations
- Avoid service downtime

1️⃣ Test Network Reachability (PING)

🔹 **Steps**

1. Press **Win + R**
2. Type cmd → Enter
3. Run:
   ping 8.8.8.8



🔹 **Result**

- ✓ Reply received → Network reachable
- ✗ Request timed out → ICMP blocked or host unreachable

📌 Note: Ping uses **ICMP**, not TCP ports.

2️⃣ Test Open / Blocked Ports (TELNET)

🔹 **Enable Telnet Client**

1. Control Panel → Programs
2. Turn Windows features on or off
3. Check **Telnet Client**
4. OK

🔹 **Test Port**

telnet 192.168.1.10 80

🔹 **Result**

- ✓ Blank screen → Port allowed
- ✗ Could not open connection → Port blocked

3️⃣ Test Ports using PowerShell (Recommended)

🔹 **Command**

Test-NetConnection 192.168.1.10 -Port 443

🔹 **Result**

- TcpTestSucceeded : True → Port allowed
- TcpTestSucceeded : False → Port blocked

Best tool for Windows firewall testing.

4️⃣ Test Web Connectivity (Browser)

🔹 **Steps**

- Open browser
- Visit:
  - http://localhost (Port 80)
  - https://localhost (Port 443)

🔹 **Result**

- Page loads → Allowed
- Error → Blocked or service not running

5️⃣ Check Firewall Logs (Windows)

🔹 **Steps**

1. Open **wf.msc**
2. Click **Windows Defender Firewall Properties**
3. Enable **Logging**
4. Check log file:
   C:\Windows\System32\LogFiles\Firewall\pfirewall.log

5.Observe logs.

What are Firewall Logs?

Firewall logs are records that show:

- **Allowed connections**
- **Blocked connections**
- **Source & destination IPs**
- **Ports and protocols used**

Logs help verify firewall behavior and troubleshoot issues.

Why Observe Firewall Logs?

- **Confirm blocked/allowed traffic**
- **Detect suspicious activity**
- **Troubleshoot connectivity problems**

- **Audit security events**

How to Observe Firewall Logs in Windows

1️⃣ Enable Firewall Logging

🔹 Steps

1. **Press Win + R**
2. **Type wf.msc → Enter**
3. **Click Windows Defender Firewall with Advanced Security**
4. **Right-click → Properties**
5. **For each profile (Domain / Private / Public):**
    - **Logging → Customize**
    - **Set Log dropped packets → Yes**
    - **Set Log successful connections → Yes**
6. **Click OK**

6.Block malicious IP.

What is Blocking a Malicious IP?

Blocking a malicious IP means **preventing all network traffic** from a known attacker or suspicious source from accessing your system.

This helps stop:

- Brute-force attacks
- Port scanning
- Malware communication
- Unauthorized access

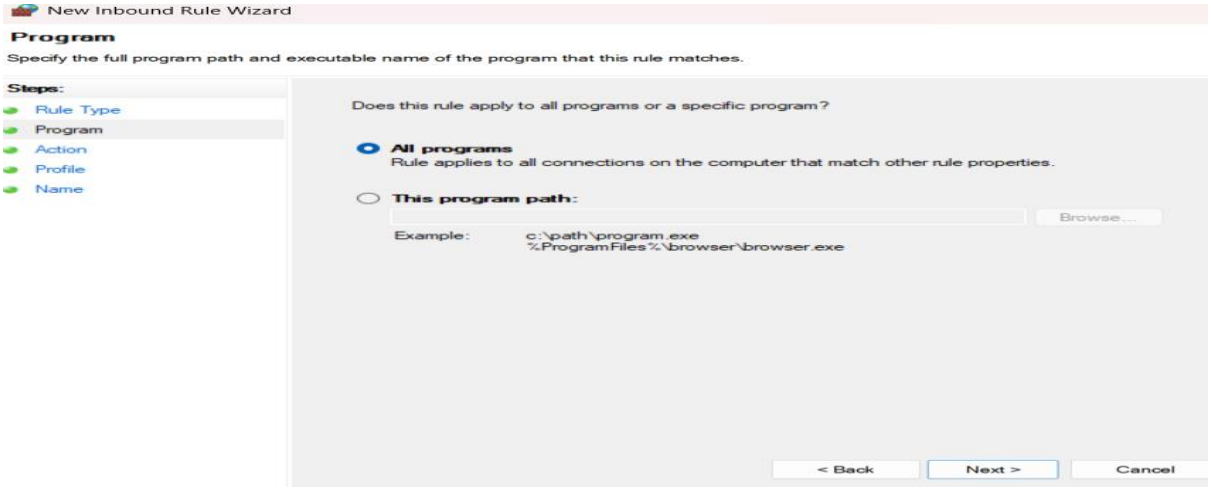
Method 1: Block IP using Windows Firewall (GUI)

🔹 Step-by-Step

1. Press **Win + R**
2. Type wf.msc → Enter
3. Click **Inbound Rules**
4. Click **New Rule**

◈ Rule Configuration

1. Rule Type → **Custom**
2. Program → **All programs**
3. Protocol and Ports → **Any**



4. Scope →
    - Remote IP addresses → **These IP addresses**
    - Click **Add**
    - Enter malicious IP (example: 203.0.113.45)
5. Action → **Block the connection**
6. Profile → Domain / Private / Public (select all)
7. Name → Block Malicious IP
8. Finish

✅ IP blocked successfully

7.Document rules.

What does "Document Rules" mean?

Documenting firewall rules means **recording all firewall configurations** in a clear and organized manner so they can be:

- Reviewed later
- Audited
- Troubleshot
- Recreated if needed

🎯 Why Document Firewall Rules?

- Avoid misconfiguration
- Track security changes
- Support audits & compliance
- Help team members understand rules
- Easy recovery after system failure

📄 What to Include in Firewall Documentation

🔹 Essential Details

- Rule name
- Rule type (Inbound / Outbound)
- Action (Allow / Block)
- Protocol (TCP / UDP / ICMP)
- Port number(s)
- Source IP
- Destination IP
- Profile (Domain / Private / Public)
- Purpose of the rule
- Date created
- Created by (admin name)

8.Explain impact.

What Does "Impact" Mean?

Impact refers to the **effect that firewall rules have on network security, system accessibility, and overall IT operations**.

Essentially: *how allowing or blocking traffic changes system/network behavior*.

Key Impacts of Firewall Rules

1️⃣Security Impact

- Blocks unauthorized access → prevents hacking attempts
- Stops malware from communicating → reduces infection risk
- Restricts sensitive services to trusted IPs → protects critical resources

2️⃣Network Accessibility

- Allowed ports enable required services (HTTP, HTTPS, SSH)
- Blocked ports prevent unnecessary or insecure traffic
- Misconfigured rules can **accidentally block legitimate traffic** → downtime

3️⃣ Performance Impact

- Simple rules: minimal effect
- Complex rules or logging all traffic → slight latency
- Efficient rule organization improves network performance

4️⃣ Compliance & Audit Impact

- Proper rules help meet **security policies & regulations** (ISO, GDPR)
- Documented rules → easier audits and incident investigations

5️⃣ Operational Impact

- Well-defined rules → smoother system operations
- Poorly configured rules → service disruption, lost connectivity

Conclusion

Firewalls protect networks by **controlling traffic** using rules.

1. **Learn Concepts** – Understand firewall types and purpose.
2. **Configure Rules** – Define allow/deny rules by IP, port, protocol.
3. **Allow/Deny Ports** – Permit required ports (80, 443) and block unused/insecure ports (21, 23).
4. **Test Connectivity** – Verify rules using ping, telnet, PowerShell, or browser.
5. **Observe Logs** – Monitor allowed and blocked traffic for security and troubleshooting.
6. **Block Malicious IPs** – Prevent attacks by denying traffic from suspicious sources.
7. **Document Rules** – Keep records of rules for auditing and recovery.
8. **Explain Impact** – Rules affect security, access, performance, and compliance.