-ATHARVA KATKAR

TABLE OF CONTENTS

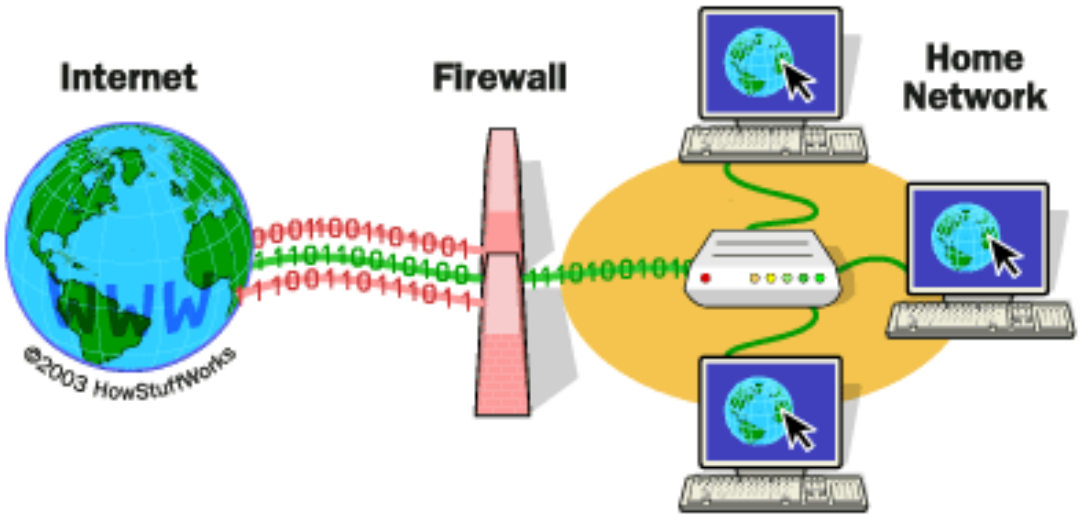
TABLE OF CONTENTS

8. **Firewall Evasion Defence**
   8.1 How to Defend Against Firewall Evasion
   8.2 Common Firewall Evasion Techniques
9. **IDS Evasion Defence**
   9.1 How to Defend Against IDS Evasion
   9.2 IDS Evasion Techniques

FIREWALL IDS / IPS

What Is a Firewall ?

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules. Its main purpose is to block unauthorized access to or from a private network while allowing legitimate communication to pass through.



➢ **Types of Firewalls**

1. Packet-Filtering Firewall

- Checks packets against predefined rules such as IP address, port number, and protocol.
- It is basic and fast but provides limited inspection of traffic.

2. Stateful Inspection Firewall

- Monitors and tracks active connections.
- Makes filtering decisions based on the state of the traffic.
- More secure than packet-filtering firewalls.

3. Application-Level Gateway (Proxy Firewall)

- Filters traffic at the application layer (for example, HTTP and FTP).
- Inspects the content of traffic, providing deep and detailed security.

4. Next-Generation Firewall (NGFW)

- Combines traditional firewall capabilities with advanced security features such as:
    - Deep packet inspection
    - Intrusion prevention
    - Application awareness
    - Malware protection

5. Software Firewall

- Installed on individual devices (for example, Windows Defender Firewall).
- Protects only the device on which it is installed.

6. Hardware Firewall

- A physical device placed between the internal network and the internet.
- Commonly used in organizations and business environments.

Why Firewalls Are Important

- Prevent unauthorized access to networks
- Protect systems from malware and cyberattacks
- Enforce organizational security policies
- Log and audit network activity for monitoring and analysis

INTRUSION DETECTION SYSTEM (IDS)

What Is an Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security tool that monitors and analyses network or system activities to detect unauthorized access, malicious behaviour, or violations of security policies.

Uses / Objectives of IDS

1. Monitors network or system traffic for suspicious activities.
2. Detects potential intrusions and security breaches.
3. Alerts administrators about detected threats.
4. Identifies malware, exploits, and attack patterns.
5. Helps in the early detection of cyberattacks.
6. Assists in forensic analysis after a security incident.
7. Enforces organizational security policies.
8. Complements firewalls and other security tools.
9. Tracks user activity to detect insider threats.

How IDS Works (Step-by-Step)

1. Traffic / Activity occurs
2. IDS captures data
3. IDS analyses behaviour
4. Match with rules or patterns
5. Alert is generated

➢ Types of IDS:

1. Network-Based Intrusion Detection System (NIDS)

Definition

A Network-Based Intrusion Detection System (NIDS) monitors network traffic across a specific network segment to detect suspicious or malicious activities.

Key Points

- Placed at strategic points in the network, such as near gateways or the DMZ.
- Analyses all incoming and outgoing network traffic.
- Most effective for detecting large-scale or external attacks.

Examples

- Snort
- Suricata

Use Cases

- Detecting port scans, Denial-of-Service (DoS) attacks, and malware traffic.
- Monitoring real-time data flow within a network environment

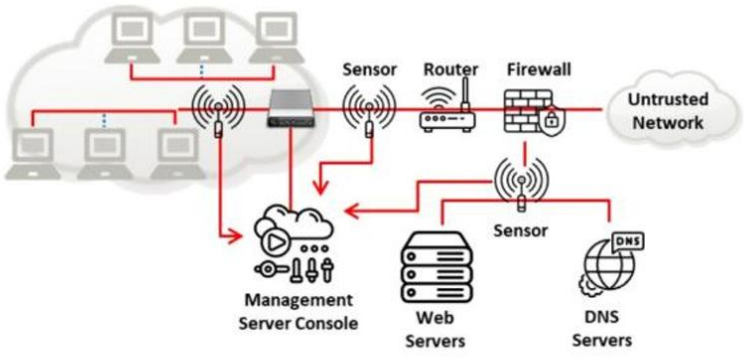


Fig-:Network-Based IDS

2. Host-Based Intrusion Detection System (HIDS)

Definition

A Host-Based Intrusion Detection System (HIDS) is a security solution that monitors the internal behaviour and activities of a specific host or endpoint to detect suspicious or malicious actions.

Key Points

- Installed directly on individual systems such as servers and workstations.
- Analyses system logs, file integrity, configuration changes, and user behaviour.
- Most effective for detecting insider threats and local system compromises.

Examples

- OSSEC, Tripwire

Use Cases

- Detecting unauthorized file modifications and suspicious login attempts.
- Protecting critical servers and endpoints from local exploits and attacks.

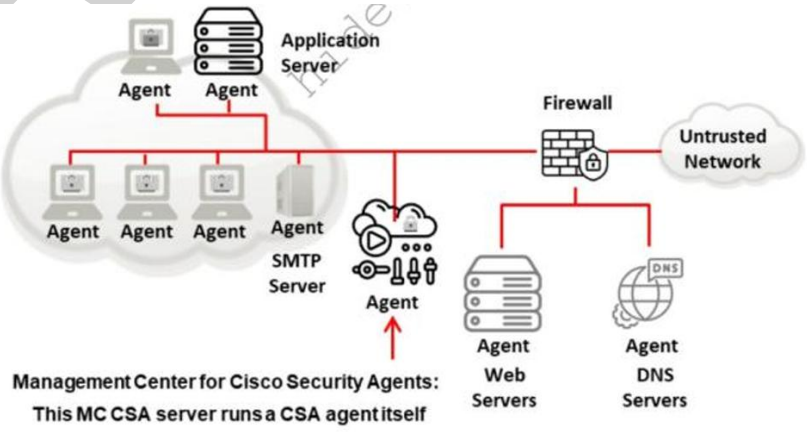


Fig- Host-Based IDS

➢ How an IDS Detects an Intrusion?

An Intrusion Detection System (IDS) detects intrusions using one or more of the following detection techniques:

1. Signature-Based Detection

- Compares network traffic or system activity against a database of known attack patterns called signatures.
- Detects attacks by matching activity with predefined signatures.

Example:

- Identifies a known malware hash or a specific exploit packet.

Strength:

- Highly accurate for detecting known threats.

Weakness:

- Cannot detect new, unknown, or zero-day attacks.

2. Anomaly-Based Detection

- Establishes a baseline of normal behaviour for a system or network.
- Flags any activity that deviates significantly from this normal behaviour.

Example:

- A sudden spike in outbound network traffic from a server at midnight.

Strength:

- Capable of detecting unknown or zero-day attacks.

Weakness:

May generate false positives due to unusual but legitimate activity.

3. Protocol Anomaly Detection (PAD)

- A specialized form of anomaly-based intrusion detection.
- Identifies intrusions by detecting deviations from normal protocol behaviour as defined by protocol standards such as TCP, HTTP, and DNS.

Example:

- Detecting malformed packets or abnormal protocol usage that violates standard protocol rules.

➢ Types of IDS Alerts

IDS alerts are categorized based on how accurately the Intrusion Detection System identifies malicious activity.

1. True Positive (TP)

- An attack is present, and the IDS successfully detects it.
- This represents a correct and accurate detection.

Example:

- An actual SQL injection attack occurs, and the IDS raises an alert.

2. True Negative (TN)

- No attack is present, and the IDS does not raise any alert.
- This indicates correct system behaviour.

Example:

- Normal user traffic occurs, and the IDS remains silent.

3. False Positive (FP)

- No attack is present, but the IDS raises an alert.
- This is an incorrect detection and may lead to unnecessary investigation.

Example:

- A regular user uploads a file, and the IDS mistakenly flags it as malware.

4. False Negative (FN)

- An attack is present, but the IDS fails to detect it.
- This is dangerous because the attack goes unnoticed.

Example:

- A new type of ransomware enters the network, but the IDS does not generate an alert.

INTRUSION PREVENTION SYSTEM (IPS)

An Intrusion Prevention System (IPS) is a network security solution that sits in-line (directly in the traffic path) between network devices and continuously monitors network traffic. When suspicious or malicious activity is detected, the IPS can automatically take preventive action to stop the threat.

Actions performed by an IPS include:

- Dropping malicious packets
- Blocking traffic from a specific IP address
- Resetting network connections
- Alerting system or network administrators

➢ **How an IPS Works**

1. Traffic Inspection
    - Analyses network traffic using Deep Packet Inspection (DPI).
2. Signature Matching
    - Compares traffic patterns with known attack signatures such as viruses and exploits.
3. Behaviour Analysis
    - Detects abnormal behaviour, such as excessive requests from a single IP address.
4. Prevention
    - Automatically blocks or stops attacks before they can succeed.

Types of Intrusion Prevention Systems:

1. Network-Based IPS (NIPS)

- Location: Deployed at key points in the network, usually behind a firewall.
- Purpose: Monitors all traffic flowing between network hosts.
- Detection Scope: Protects the entire network.

Examples:

- Cisco Firepower
- Suricata
- Snort (IPS mode)

Best For:

- Detecting and blocking threats that spread across the network.

2. Host-Based IPS (HIPS)

- Location: Installed on individual systems such as servers, desktops, and laptops.
- Purpose: Monitors system calls, logs, application behavior, and file access.
- Detection Scope: Protects only the local system on which it is installed.

Examples:

- OSSEC (with HIPS modules)
- Symantec Endpoint Protection

Best For:

- Detecting local exploits such as privilege escalation and unauthorized file modifications.

3. Wireless IPS (WIPS)

- Location: Monitors wireless network traffic and infrastructure.
- Purpose: Detects and blocks rogue devices, unauthorized access points, and wireless attacks (e.g., deauthentication attacks).

Examples:

- Aruba WIPS
- Cisco Meraki AirMarshal

Best For:

- Securing wireless environments such as corporate Wi-Fi networks and public access areas.

4. Network Behavior Analysis (NBA) IPS

- Location: Typically integrated into advanced IPS or security appliances.
- Purpose: Monitors network traffic to identify unusual behavior such as large data transfers or Distributed Denial-of-Service (DDoS) attacks.
- Detection Method: Uses behavior modeling and anomaly detection techniques.

Examples:

- Darktrace
- Cisco Stealthwatch

Best For:

- Identifying zero-day attacks, insider threats, and large-scale network attacks.

HONEYPOT

What is a Honeypot?

A honeypot is a cybersecurity mechanism that is deliberately designed to attract attackers. It simulates a vulnerable system, application, or network service so that attackers interact with it. This allows defenders to monitor, detect, and analyse malicious activity without putting real systems at risk.

Main Goals of a Honeypot

1. Detection – Detect unauthorized access and malicious activity.
2. Diversion – Distract attackers from real targets.
3. Analysis – Study attacker behavior, tools, and techniques.
4. Prevention – Improve security defenses based on collected insights.

How a Honeypot Works

1. It mimics a legitimate target such as a web server, database, or IoT device.
2. It is placed in a controlled and isolated environment, separate from real systems.
3. When an attacker interacts with it (scanning, exploitation, etc.), all actions are logged and recorded.
4. The security team analyzes this data for investigation and threat intelligence.

Types of Honeypots

1. Based on Level of Interaction

- Low-Interaction Honeypots – Simulate limited services with minimal risk.
- Medium-Interaction Honeypots – Provide more interaction without a full operating system.
- High-Interaction Honeypots – Fully emulate real systems for in-depth attacker engagement.

2. Based on Purpose

- Research Honeypots – Used to study attacker behavior and collect threat intelligence.
- Production Honeypots – Deployed in live networks to detect and deflect attacks.

3. Based on Location

- External Honeypots – Placed outside the firewall to capture external attackers.
- Internal Honeypots – Placed inside the network to detect insider threats or lateral movement.

4. Based on Technology

- Malware Honeypots – Designed to capture and analyze malware.
- Spam Honeypots – Mimic open email relays to attract spam messages.
- Database Honeypots – Simulate vulnerable databases to detect SQL injection and data exfiltration attempts.
- Web Application Honeypots – Mimic websites or CMS platforms to detect web-based attacks.
- Industrial Control System (ICS) Honeypots – Simulate SCADA/ICS environments to detect threats targeting critical infrastructure.

Honeynet

Honeynet – A network of multiple interconnected honeypots designed for broader attack simulation and detailed analysis.

SNORT

What is SNORT?

SNORT is an open-source Network Intrusion Detection System (NIDS) and Intrusion Prevention System (IPS) developed by Martin Roesch. It is used to monitor network traffic in real time, detect malicious activity, and generate alerts when suspicious behavior is found.SNORT analyzes network packets and compares them against a database of predefined rules and signatures to identify attacks such as malware, denial-of-service (DoS), port scans, buffer overflows, and other threats.

Features of SNORT

- Real-time traffic analysis
- Packet logging and inspection
- Signature-based detection
- Protocol analysis
- Custom rule creation
- Can work as IDS or IPS
- Lightweight and fast
- Free and open-source

Main Functions of SNORT

1. **Packet Sniffing** – Captures and displays network packets.
2. **Packet Logging** – Logs packets to disk for later analysis.
3. **Intrusion Detection** – Detects attacks using rules and signatures.
4. **Intrusion Prevention** – Blocks malicious traffic when used in inline mode.

How SNORT Works

1. SNORT captures network traffic using a network interface card (NIC).
2. Captured packets are decoded into readable format.
3. Preprocessors normalize and prepare traffic for analysis.
4. The detection engine compares traffic with predefined rules.
5. If a rule matches, an alert is generated or action is taken.
6. Logs and alerts are stored for security analysis.

Download Link – https://www.snort.org/downloads

- After installing snort , go to the snort location and open etc folder.

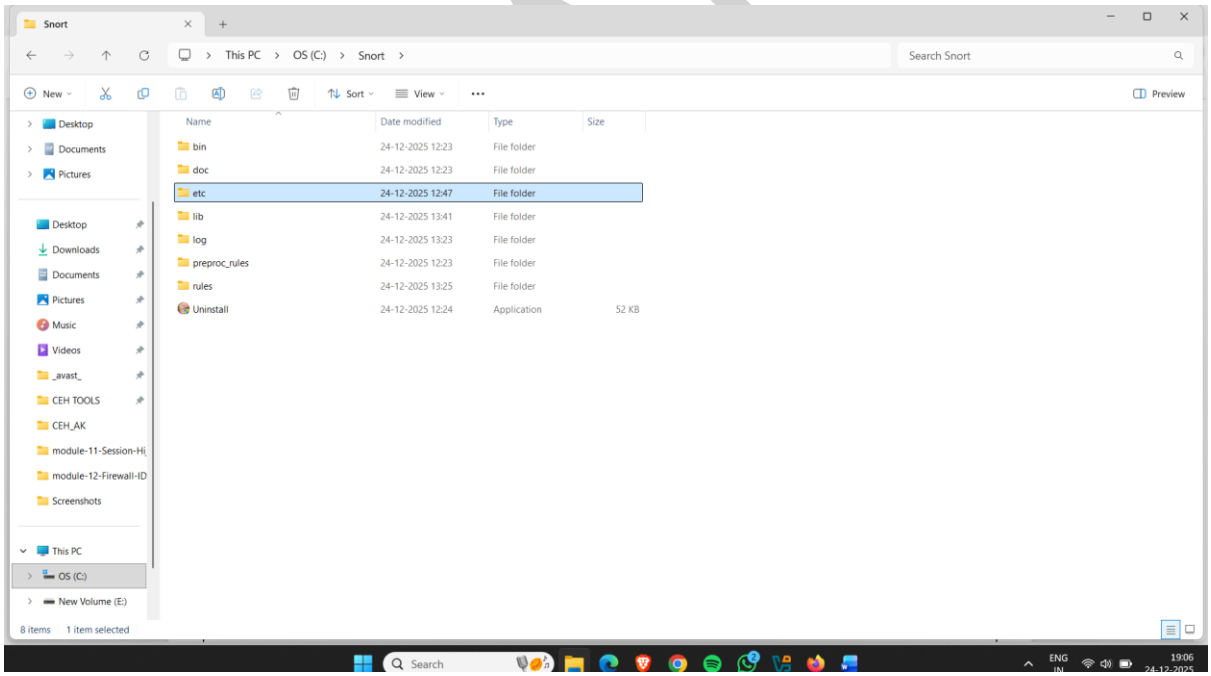


Figure 1

- Copy snort.exe file and paste it again on same location.

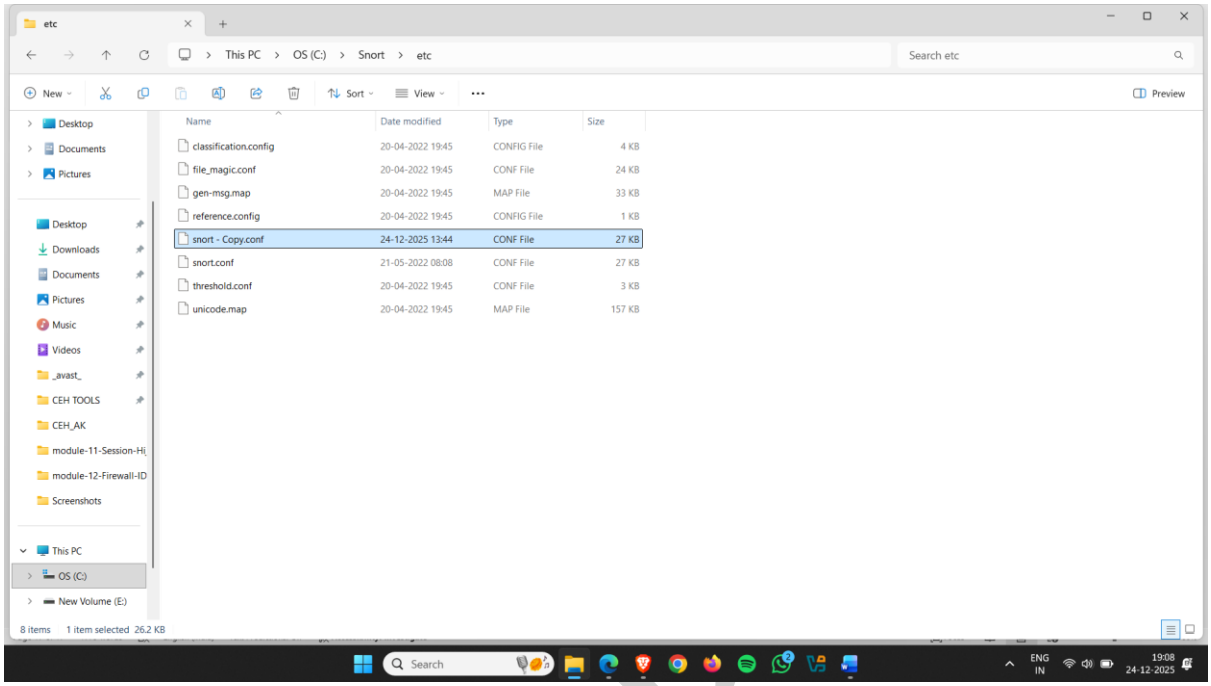


Figure 2

- Now , open copied file in Notepad++

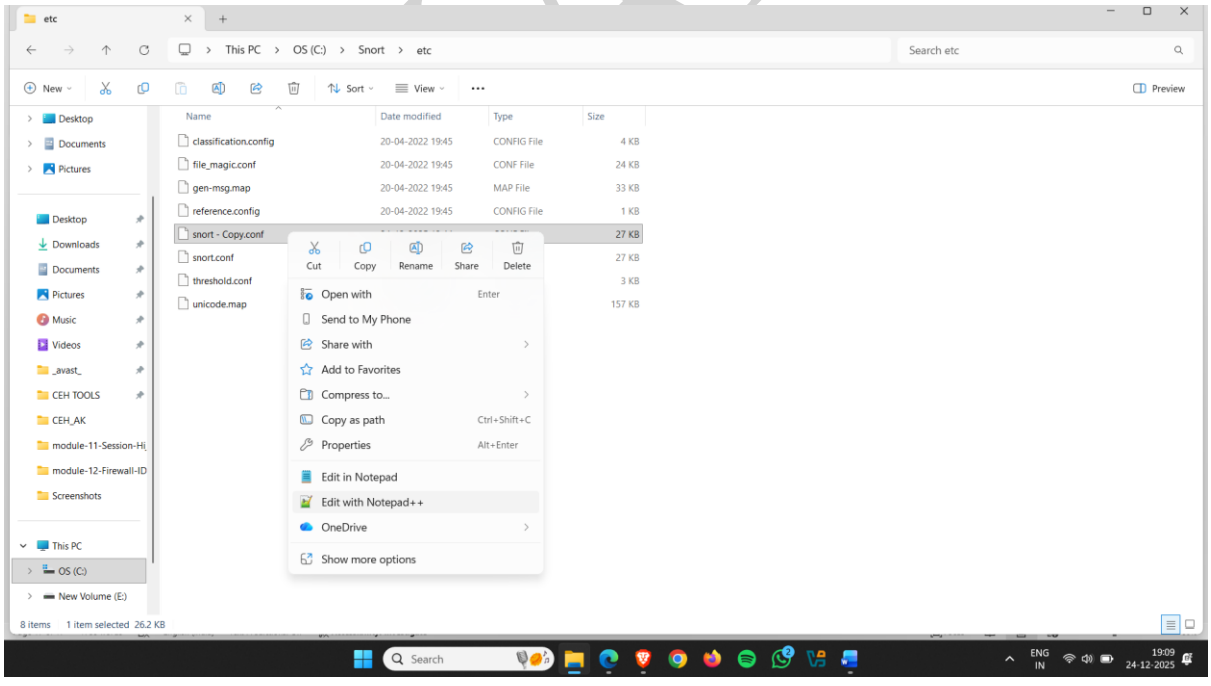


Figure 3

- Go to the line number 45
- Replace any word to ip address

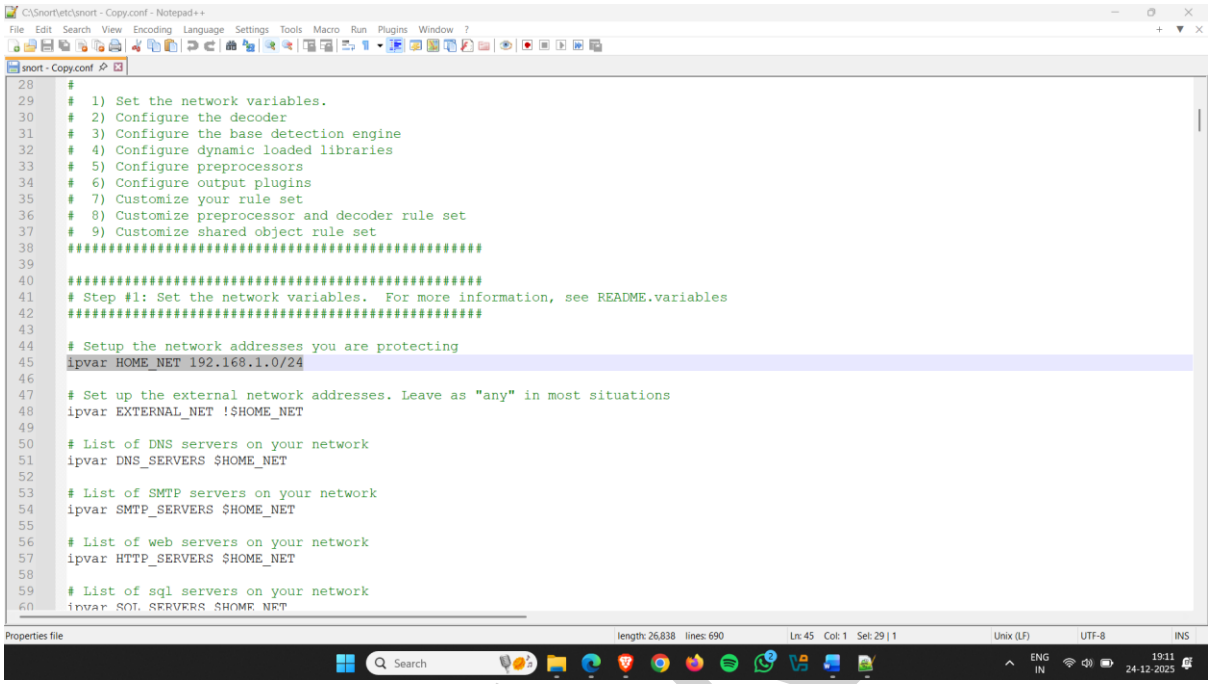


Figure 4

- Go to the line number 48
- Replace Any to the !$HOME_NET

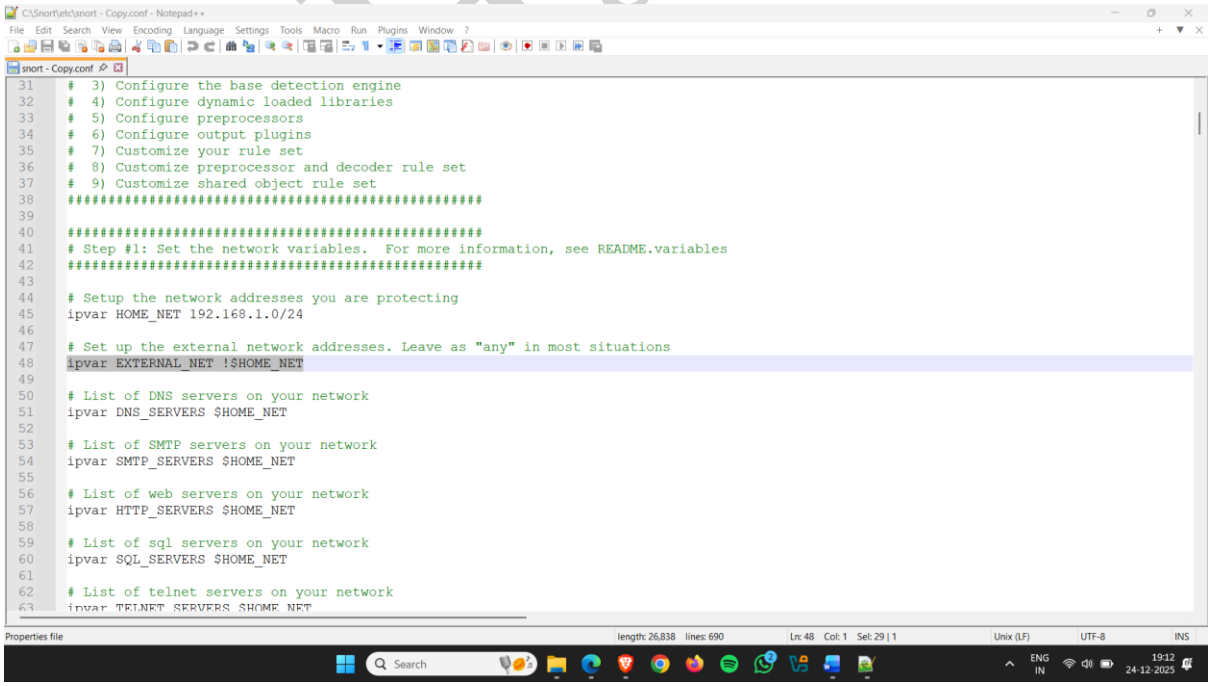


Figure 5

- Go to the line number 104
- Set rules folder location (C:\\Snort\rules)

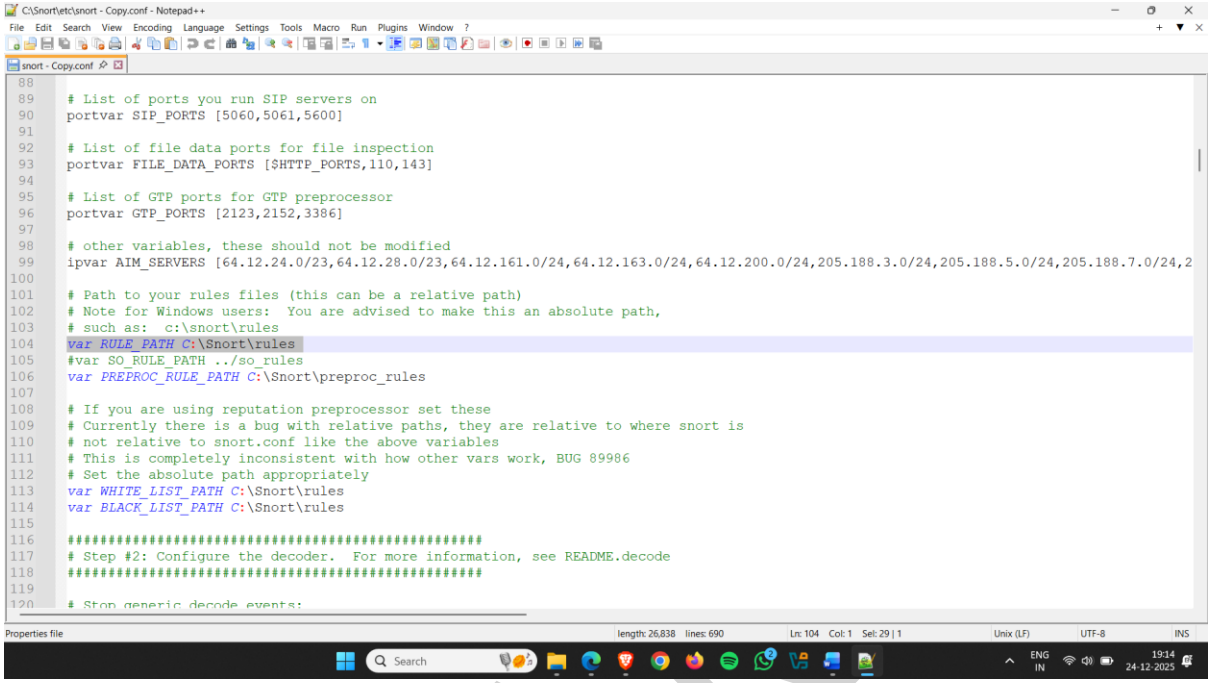


Figure 6

- Go to the line number 105
- Add # on the front of the line number 105

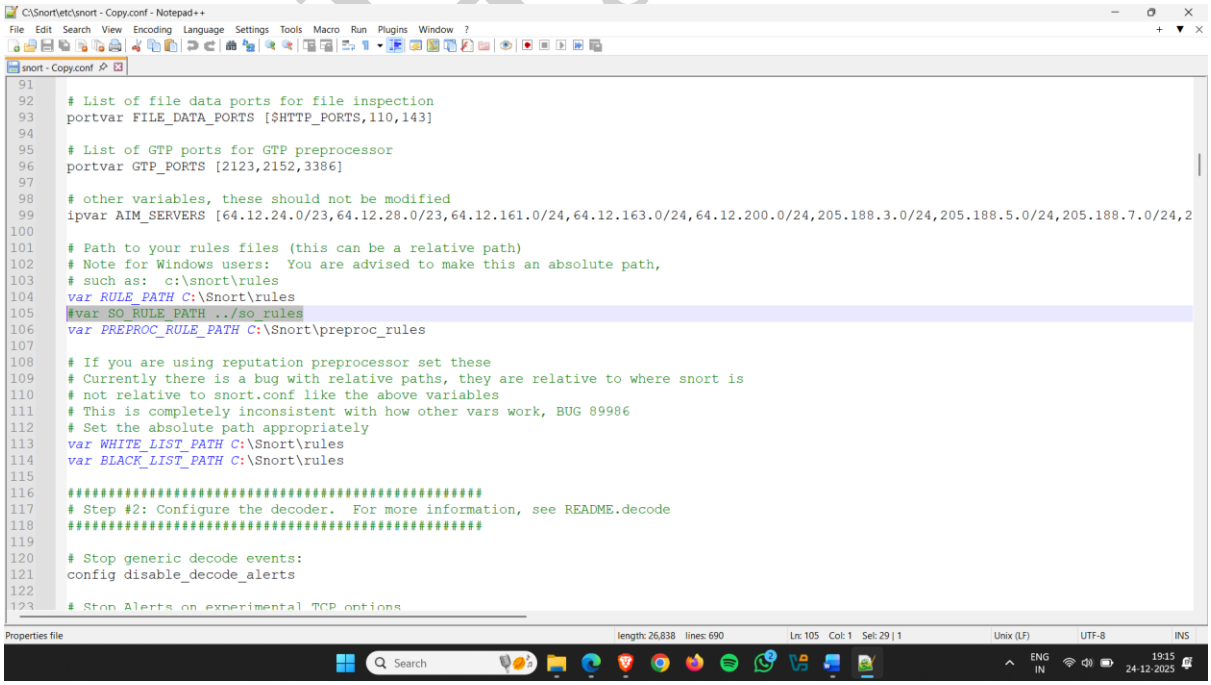


Figure 7

- Go to the line number 106
- Set preproc_rules (C:\Snort\preproc_rules)

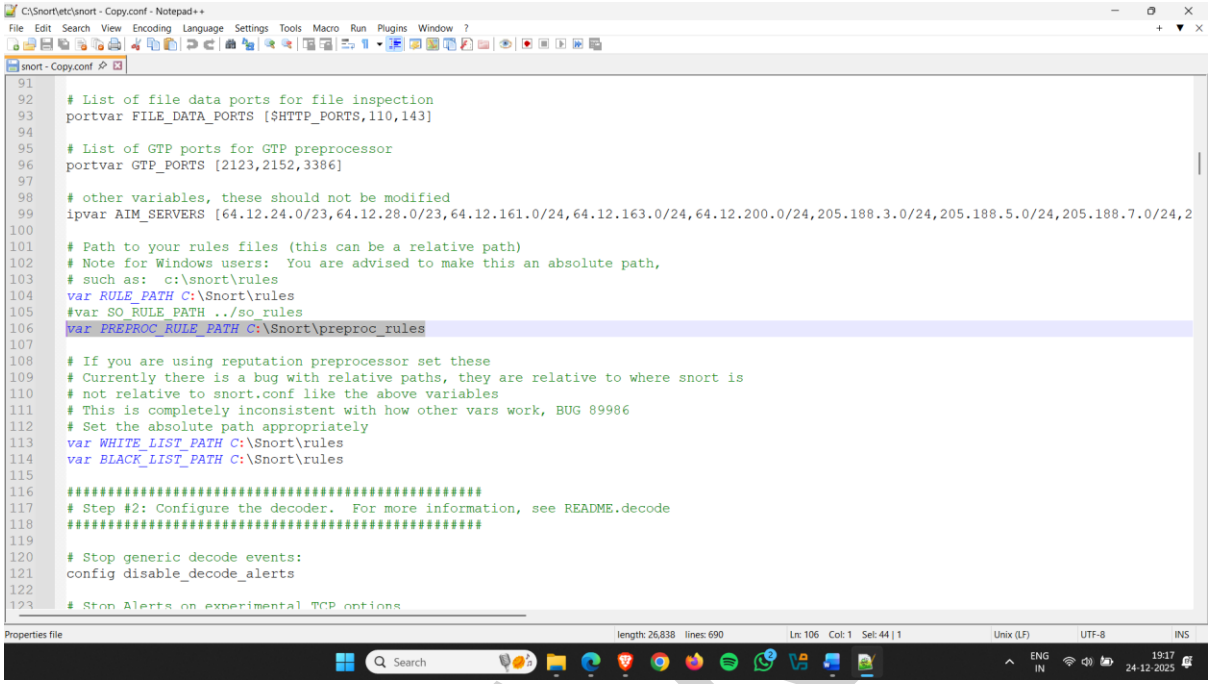


Figure 8

- Go to the line number 113 and 114
- add rules file path/location (C:\\Snort\rules)

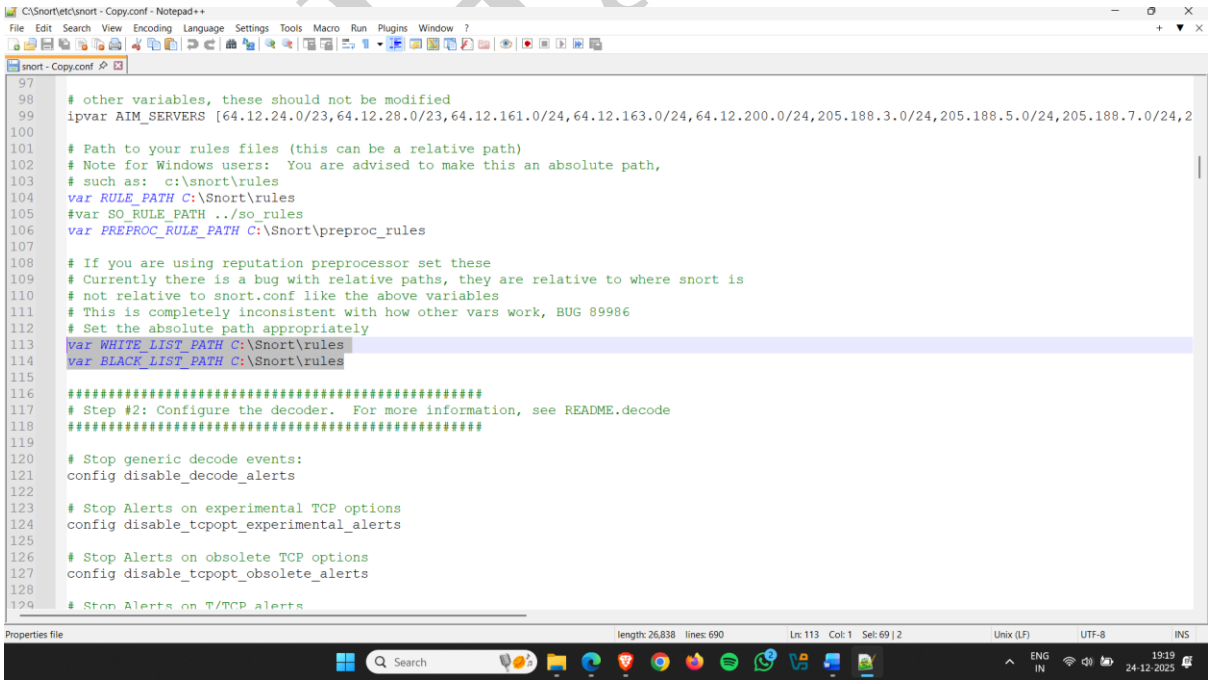


Figure 9

- Go to the line number 186
- Remove hash

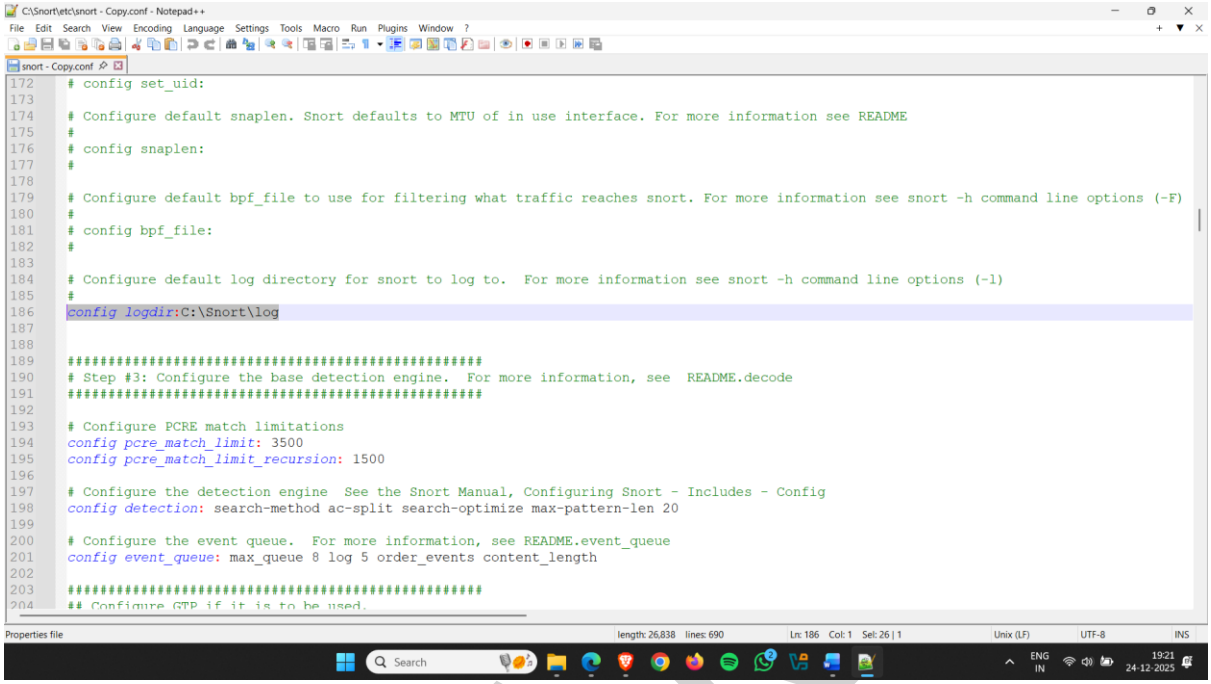


Figure 10

- Go to the line number 247
- Set snort_dynamicpreprocessor file path/location -: c:\Snort\lib\snort_dynamicpreprocessor

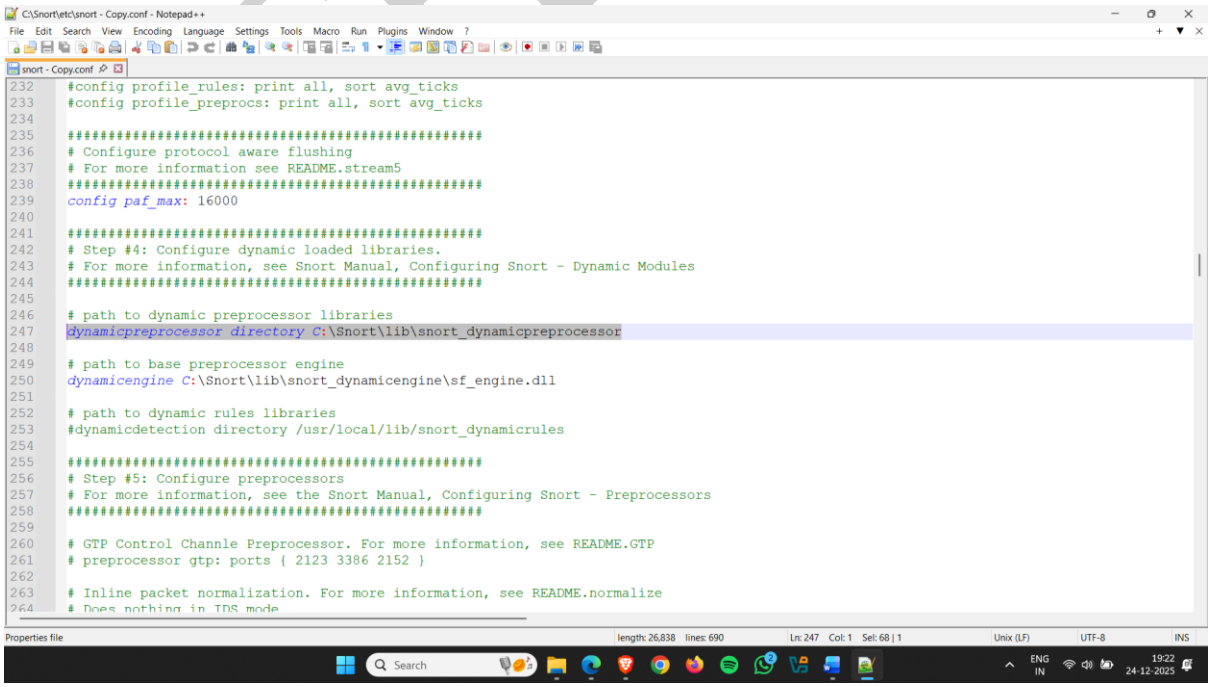


Figure 11

- Go to the line number number 250
- Set sf_engine.dll file location -: c:\Snort\lib\snort_dynamicengine/sf_engine.dll

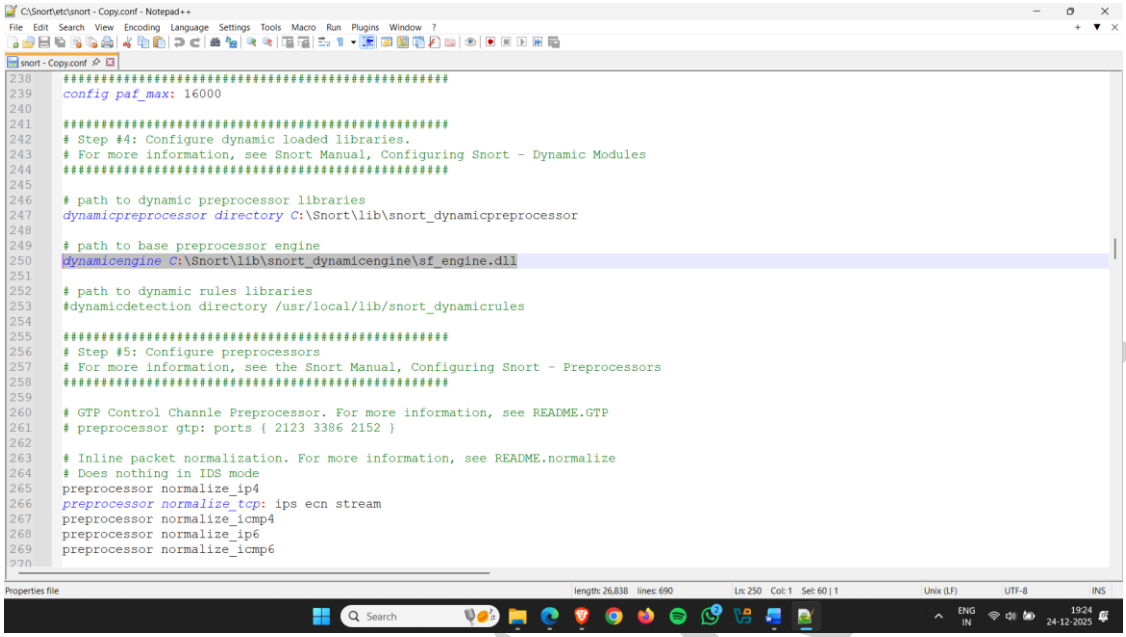


Figure 12

- Go to the line number 511 and 512
- **Note-:** before changing on the line number 511 and 512 firstly go to the snort >>rules folder and there is file in folder named, blacklist.rules copy file and paste in same folder and rename copy file to the whitelist.rules.

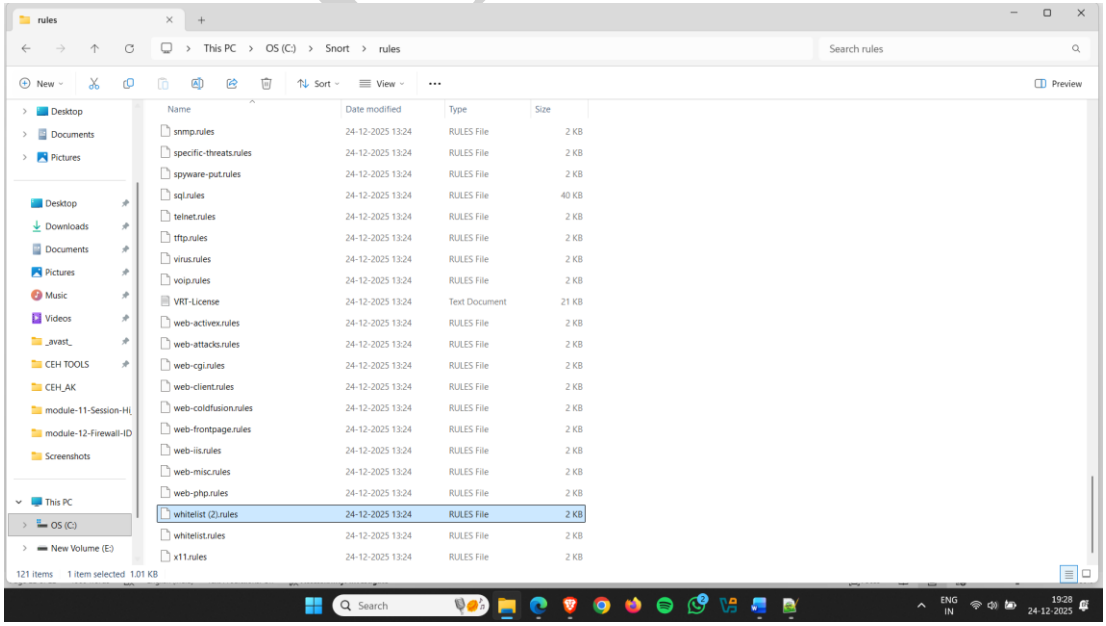


Figure 13

- Go to the line number 511 and 512
  - ➢ Replace white_list.rules to whitelist.rules
  - ➢ Replace black_list.rules to blacklist.rules

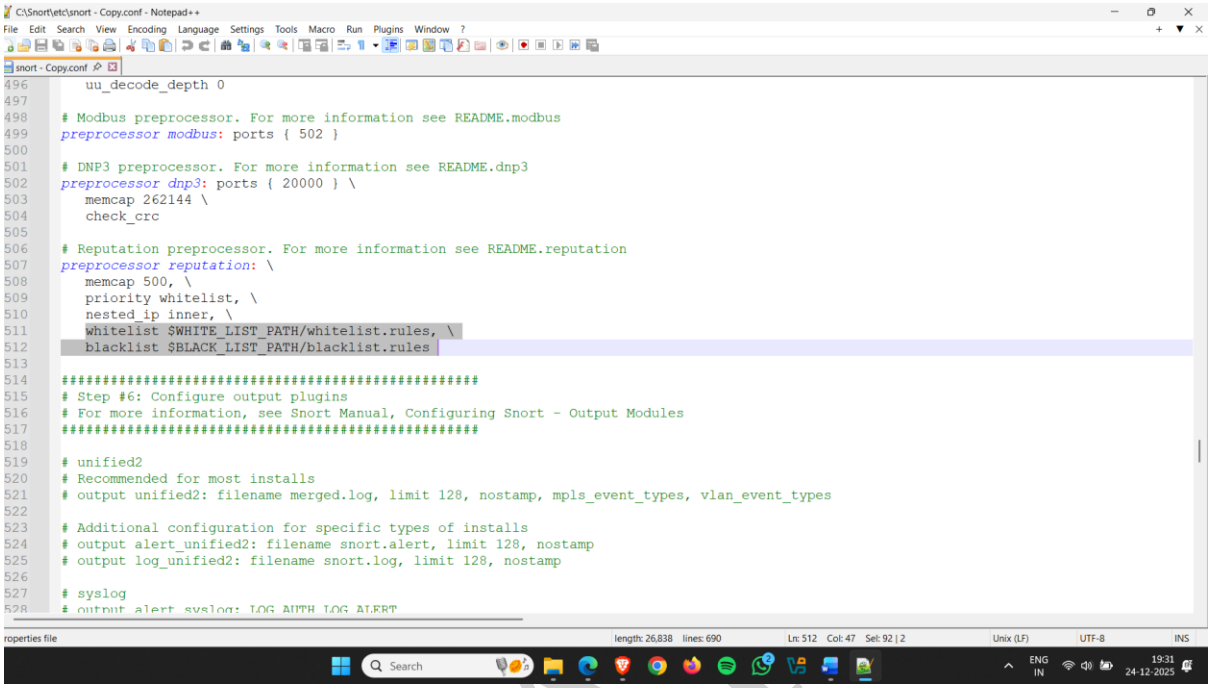


Figure 14

- Go to the line number 546
- Replace "/" to "\" 546 upto 651
- Press ctrl+f

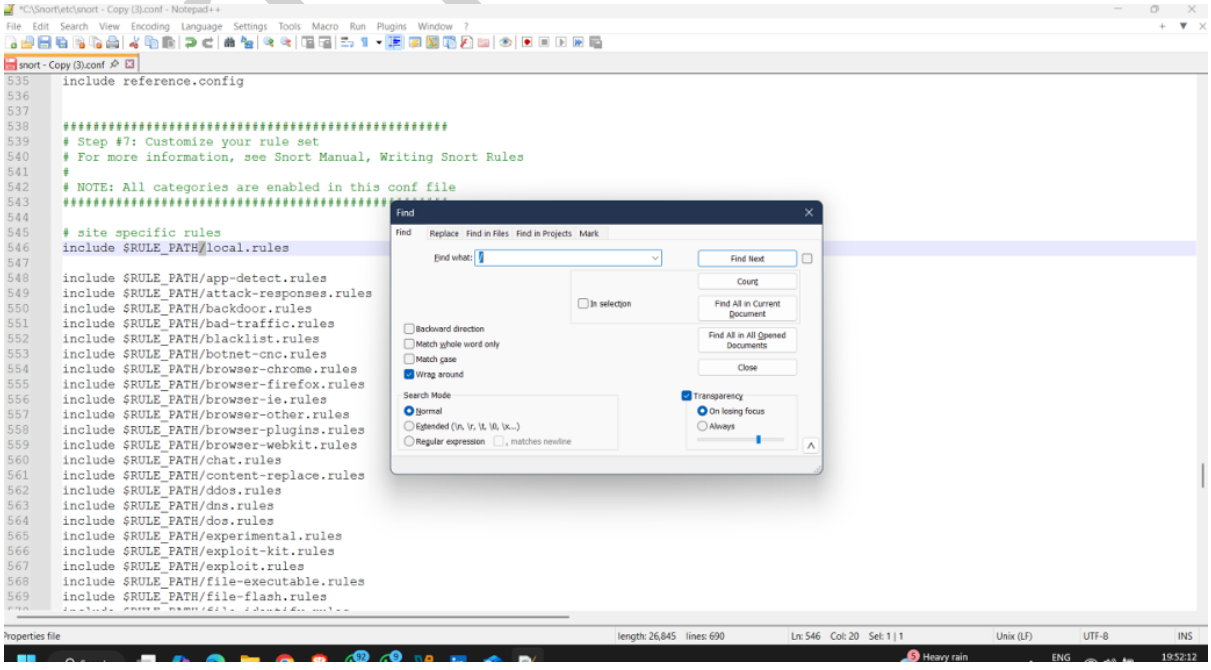


Figure 15

- Add “/” in first box
- Add “\” in second column & click on replace

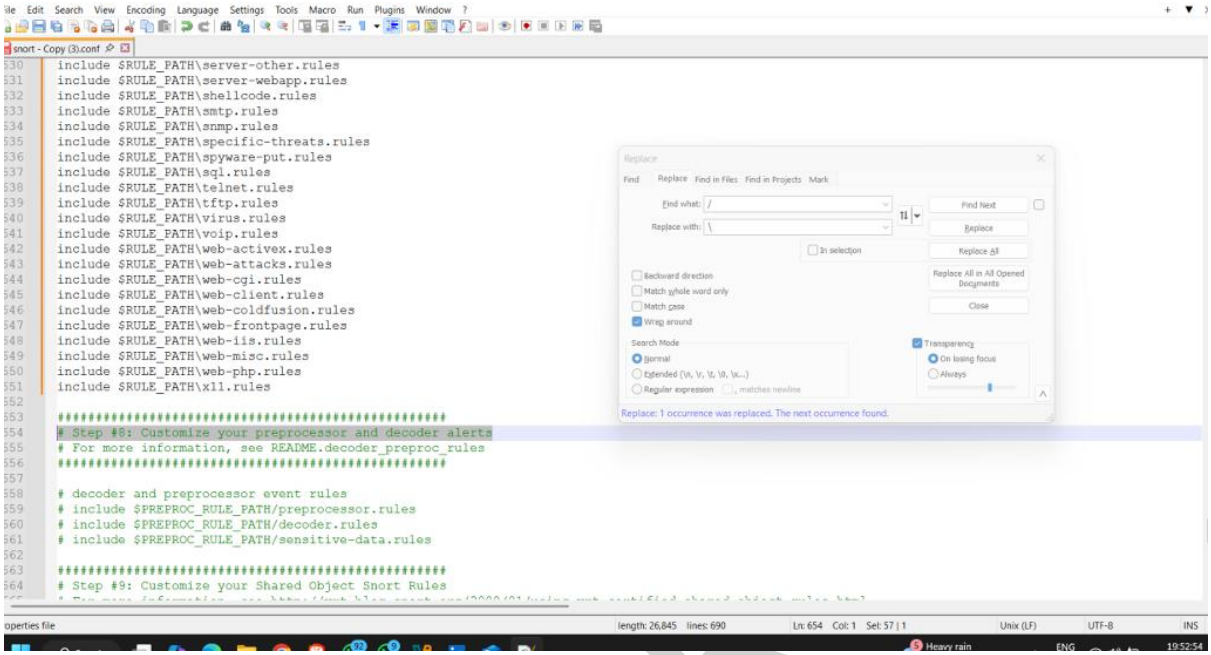


Figure 16

- All the slash are being replaced.

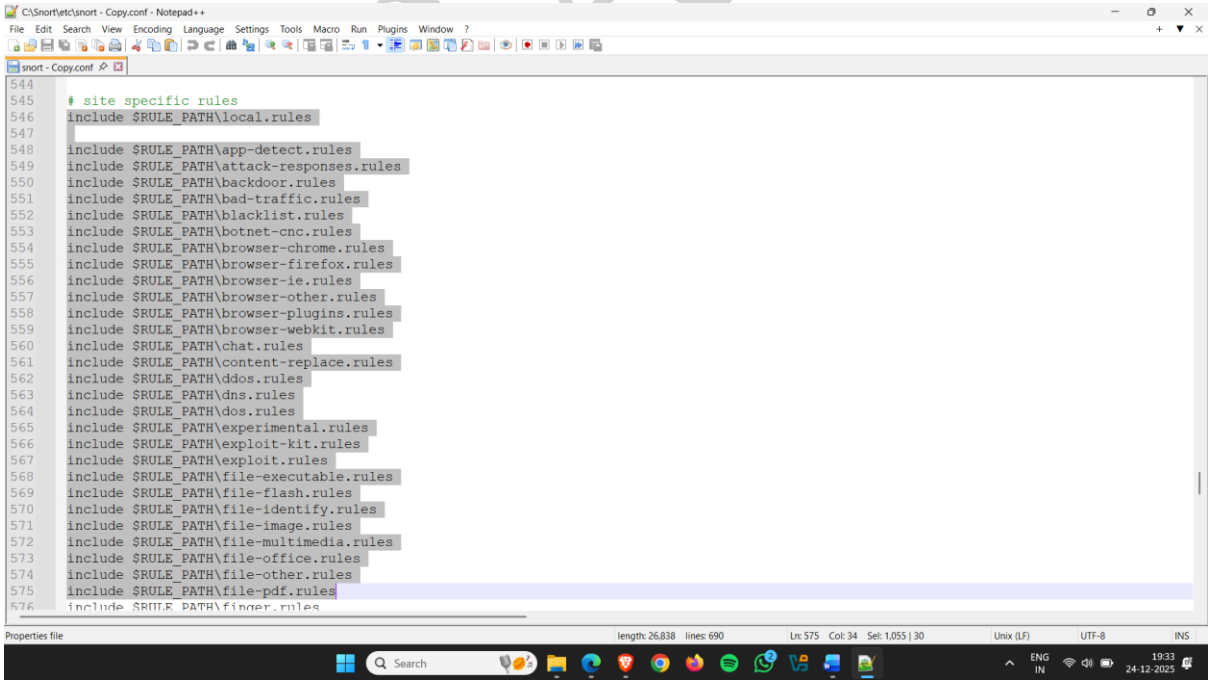


Figure 17

- Open CMD & do run as administrator

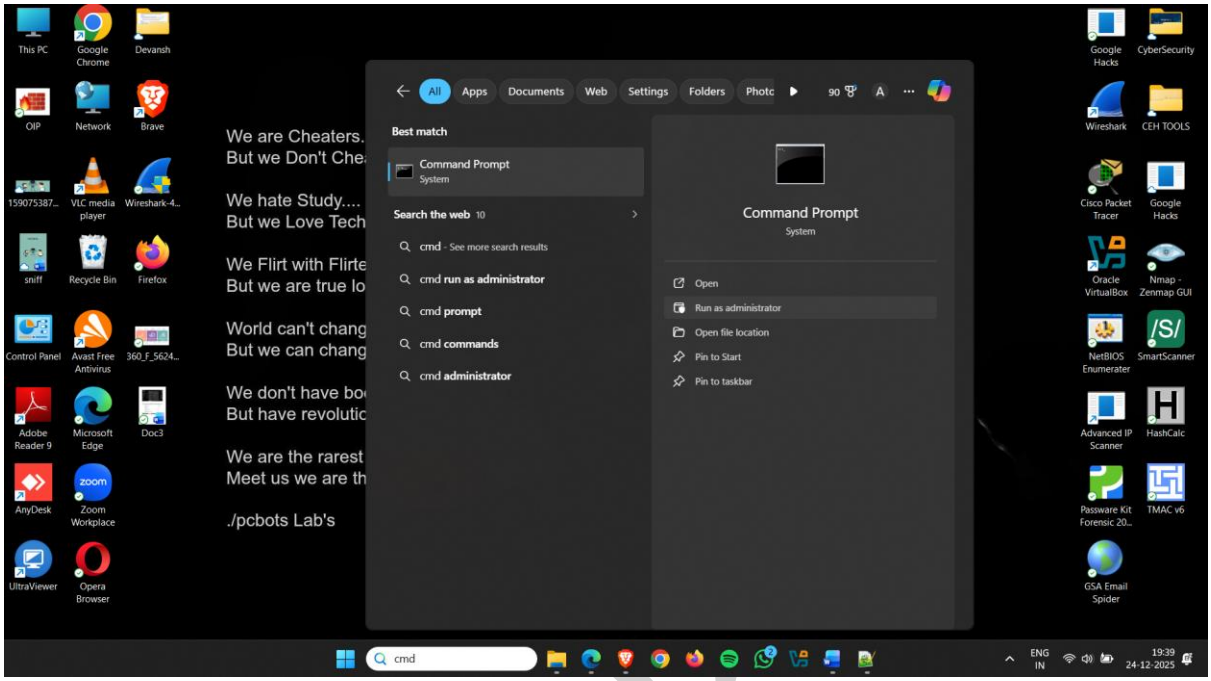


Figure 18

- Go to the Snort folder

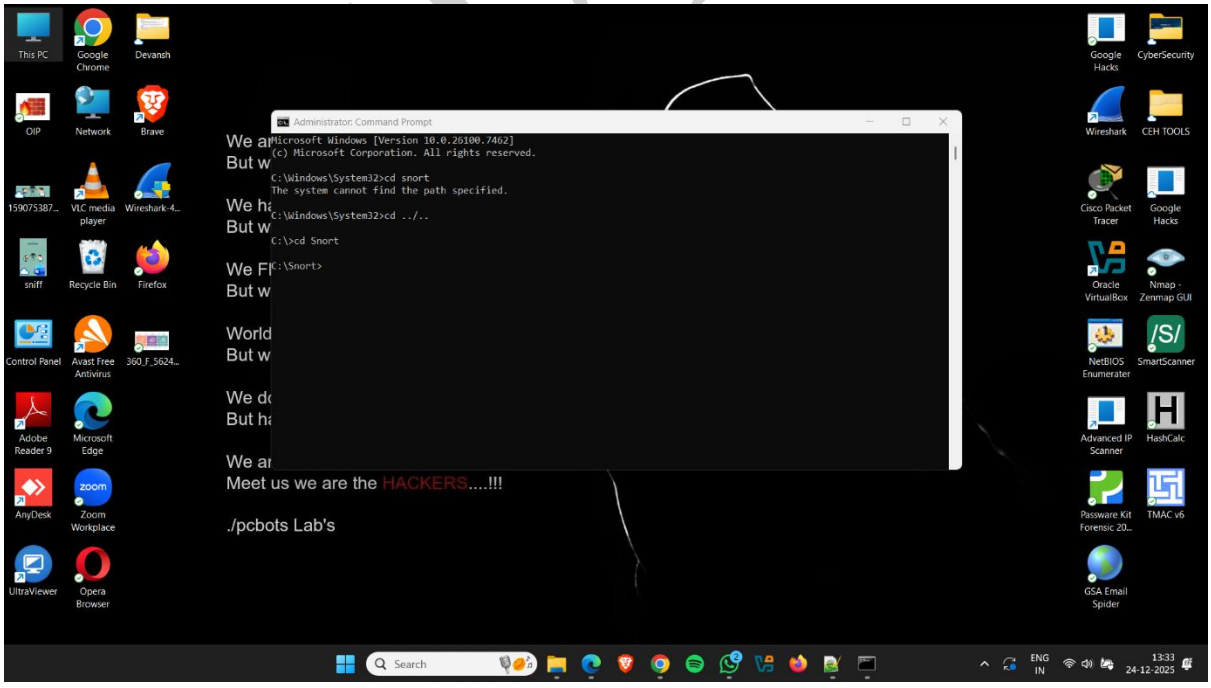


Figure 19

- Go to the Snort\bin Folder

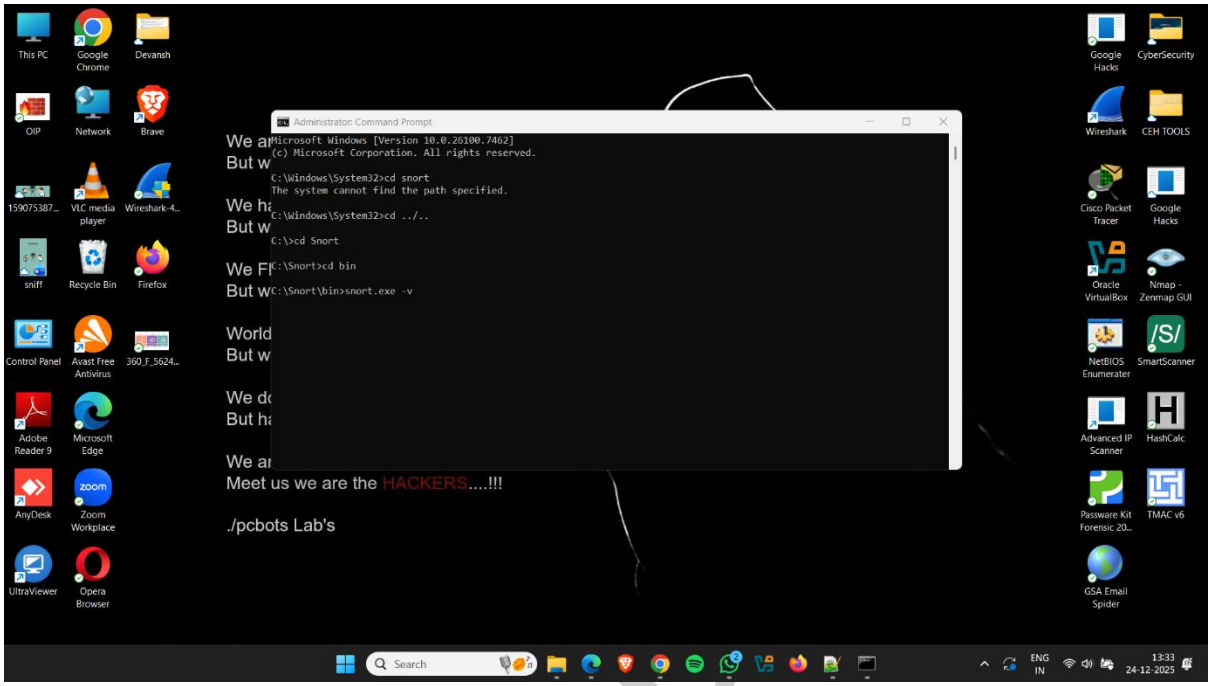


Figure 20

- Run file snort.exe -v (v for version)

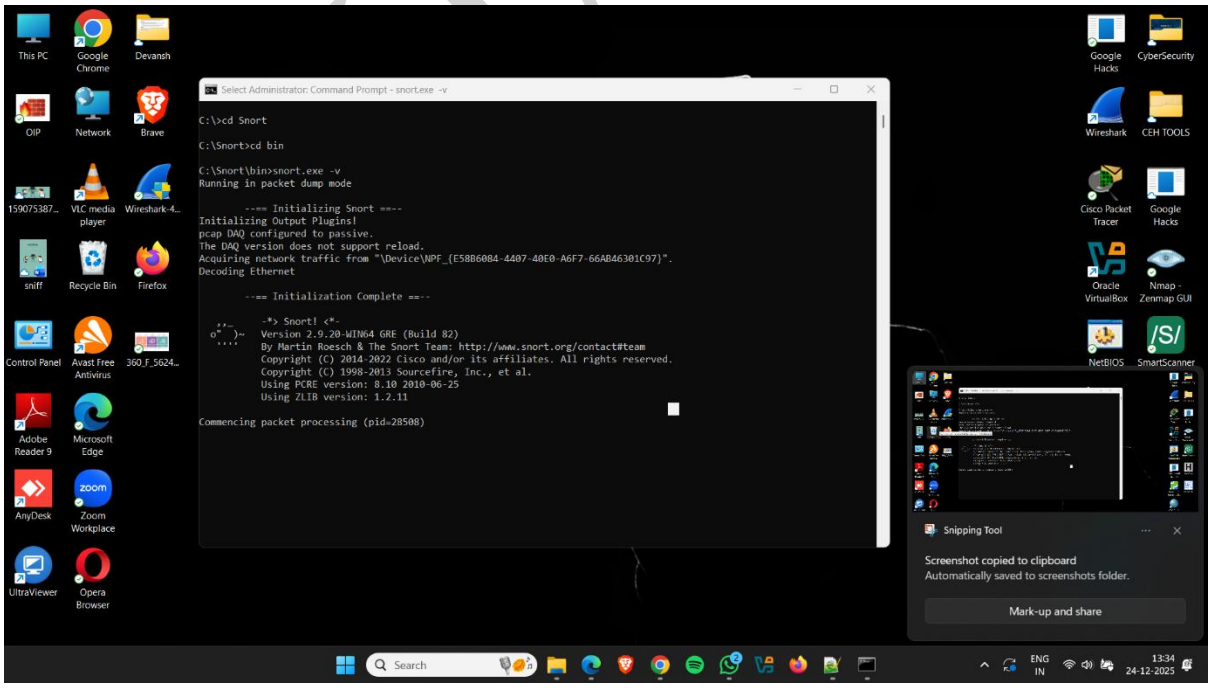


Figure 21

- Use next command for finding network interface (snort.exe –W)

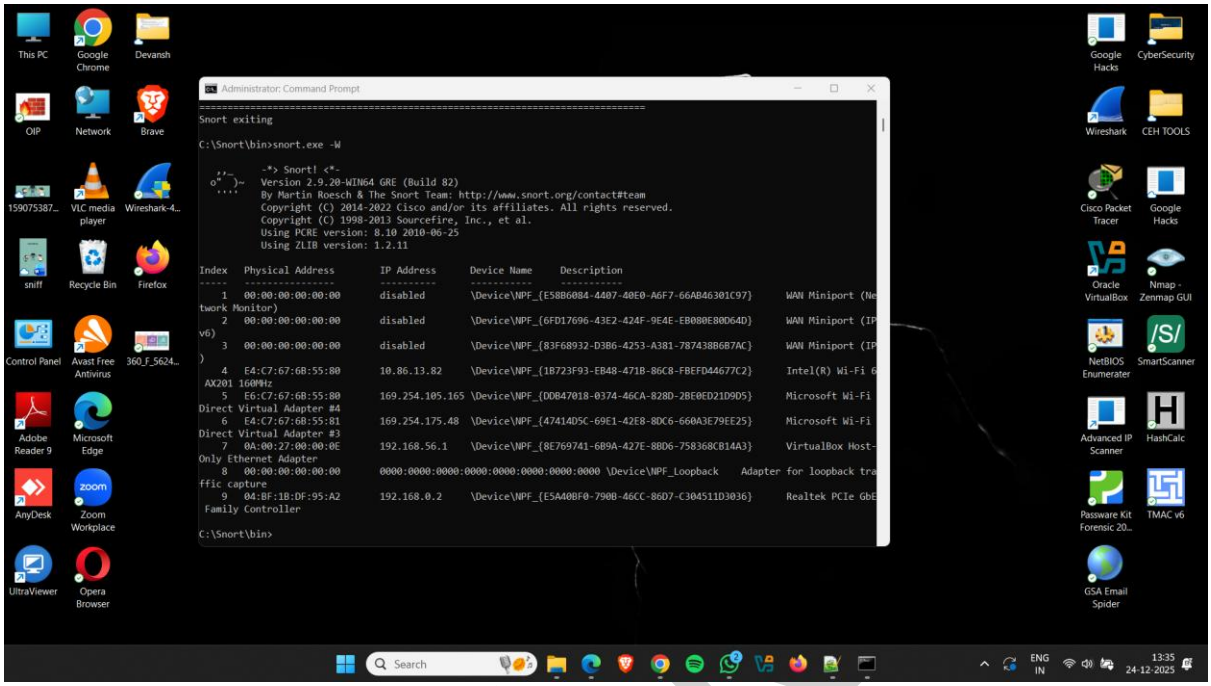


Figure 22

- Command for configuration testing -: snort.exe -i 4 -c “c:\Snort\etc\file name “ -T

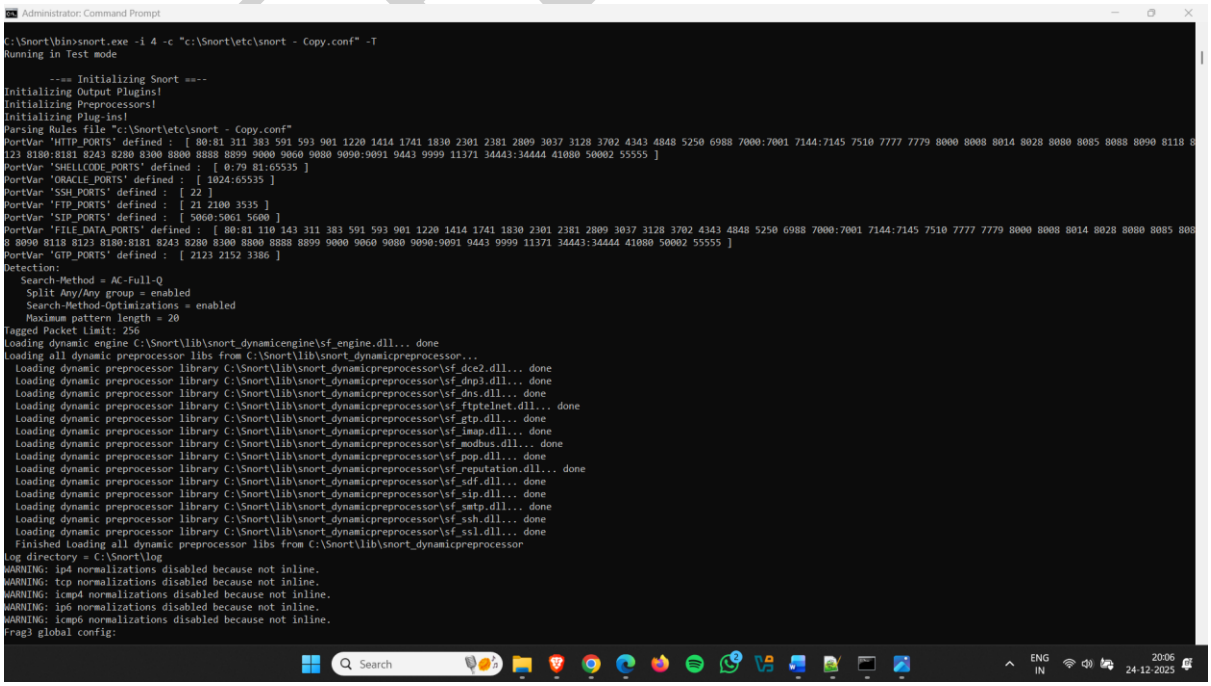


Figure 23

- Snort successfully validated the configuration!

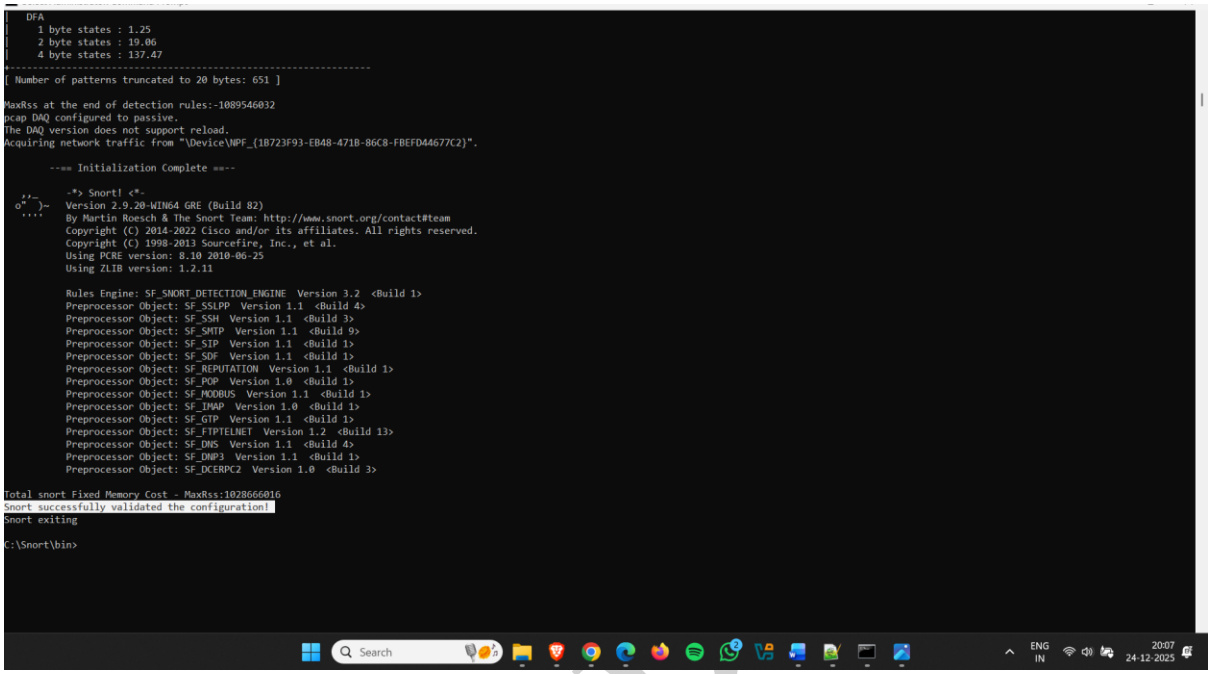


Figure 24

- Command to start snort
  snort.exe -i 4 -c"c:\Snort\etc\file name " -A console

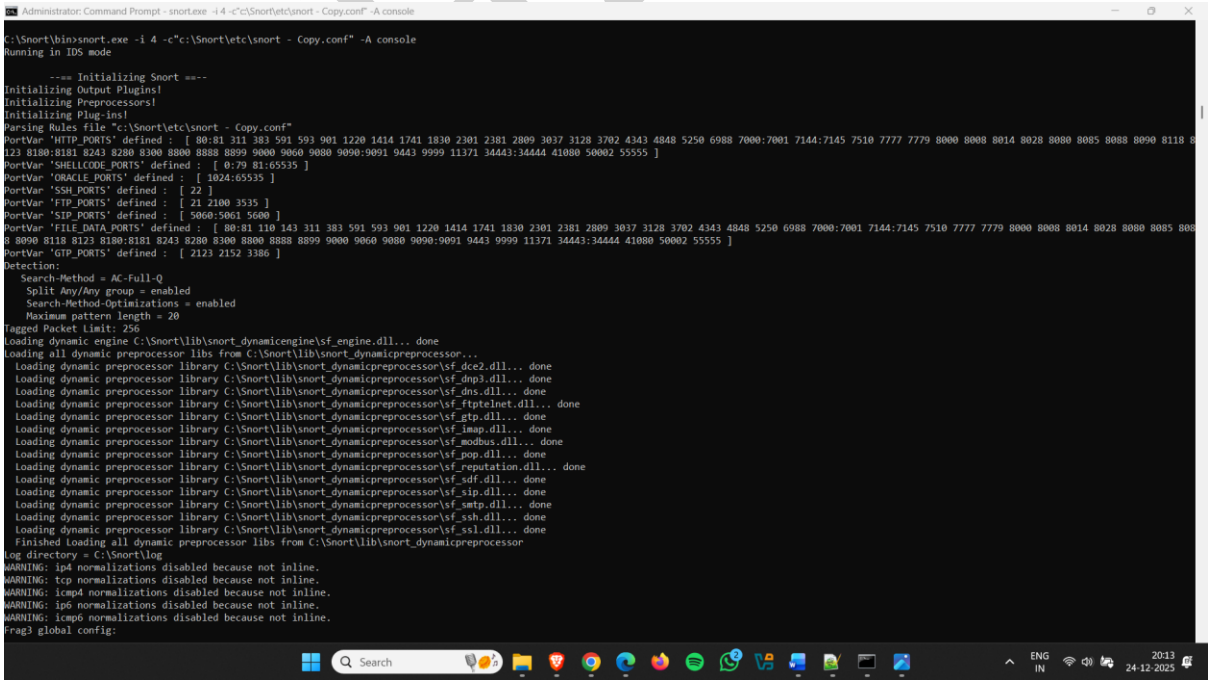


Figure 25

- Started capturing network traffic

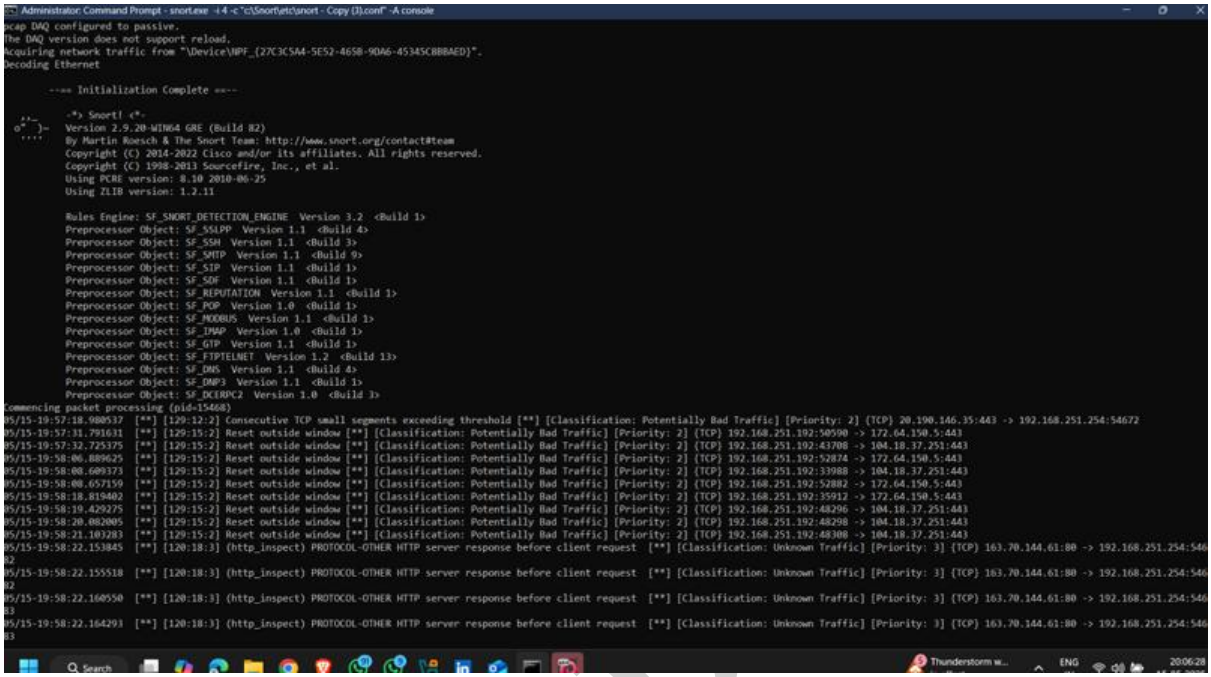


Figure 26

Windows Firewall Configuration

Windows Firewall (now known as Windows Defender Firewall) is a built-in security feature in Microsoft Windows operating systems. It helps protect a computer by monitoring and filtering incoming and outgoing network traffic based on predefined security rules.

Purpose of Windows Firewall

The primary purpose of Windows Firewall is to prevent unauthorized access to or from a private network by acting as a protective barrier between the computer and external threats such as hackers, malware, and unauthorized applications.

Key Features of Windows Firewall

1. Inbound and Outbound Filtering

- Blocks or allows network traffic based on security rules.
- **Inbound traffic:** Data coming into the computer.
- **Outbound traffic:** Data leaving the computer.

2. Predefined Security Rules

- Automatically configures security rules for commonly used applications and system services.
- Reduces the need for manual configuration.

3. Application Control

- Prompts the user when an unknown or unauthorized application attempts to access the network.
- Allows users to permit or block applications as needed.

4. Network Profiles

Windows Firewall allows different security settings based on the network type:

- **Private Network:** Used for home or trusted networks.
- **Public Network:** Used for unsecured networks such as public Wi-Fi.
- **Domain Network:** Used in corporate or organizational environments.

5. Integration with Windows Security Center

- Can be easily managed through:
  - Control Panel
  - Windows Security Settings
- Provides centralized security management.

6. Logging and Monitoring

- Maintains logs of blocked packets and connection attempts.
- Helps administrators monitor suspicious activity and troubleshoot network issues.

(INBOUND RULES)

- Click on Windows Button and search Firewall and open.

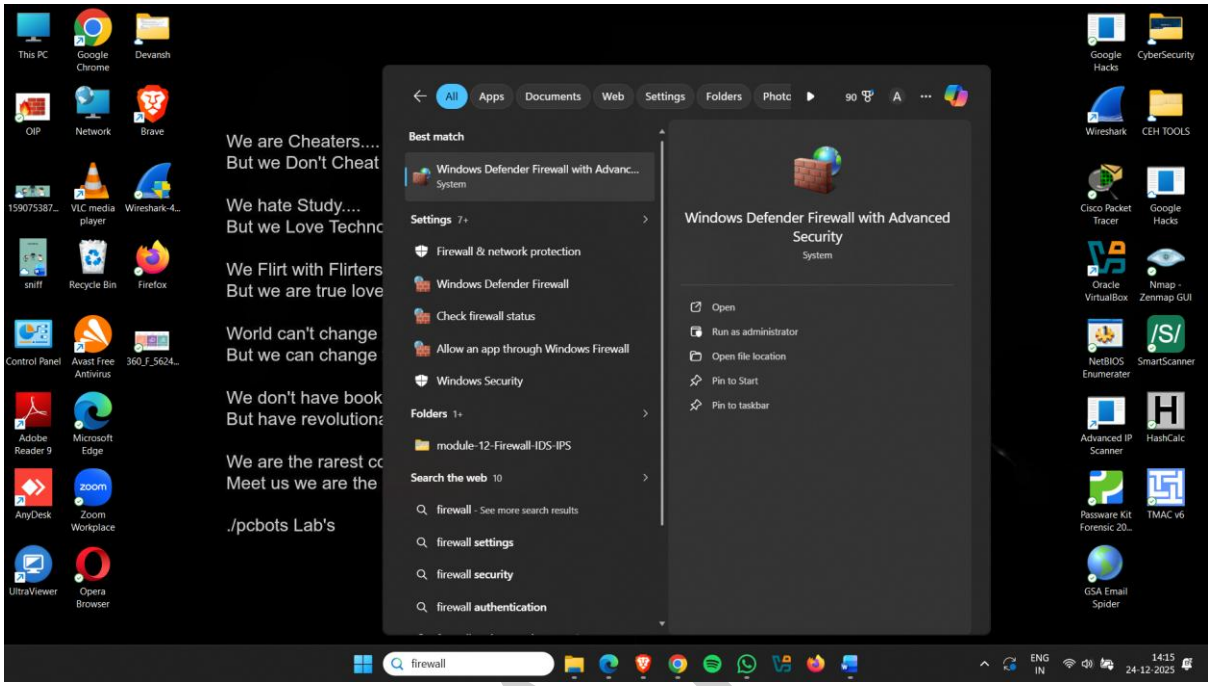


Figure 27

- There is option inbound rules – it means setting rules for incoming network.

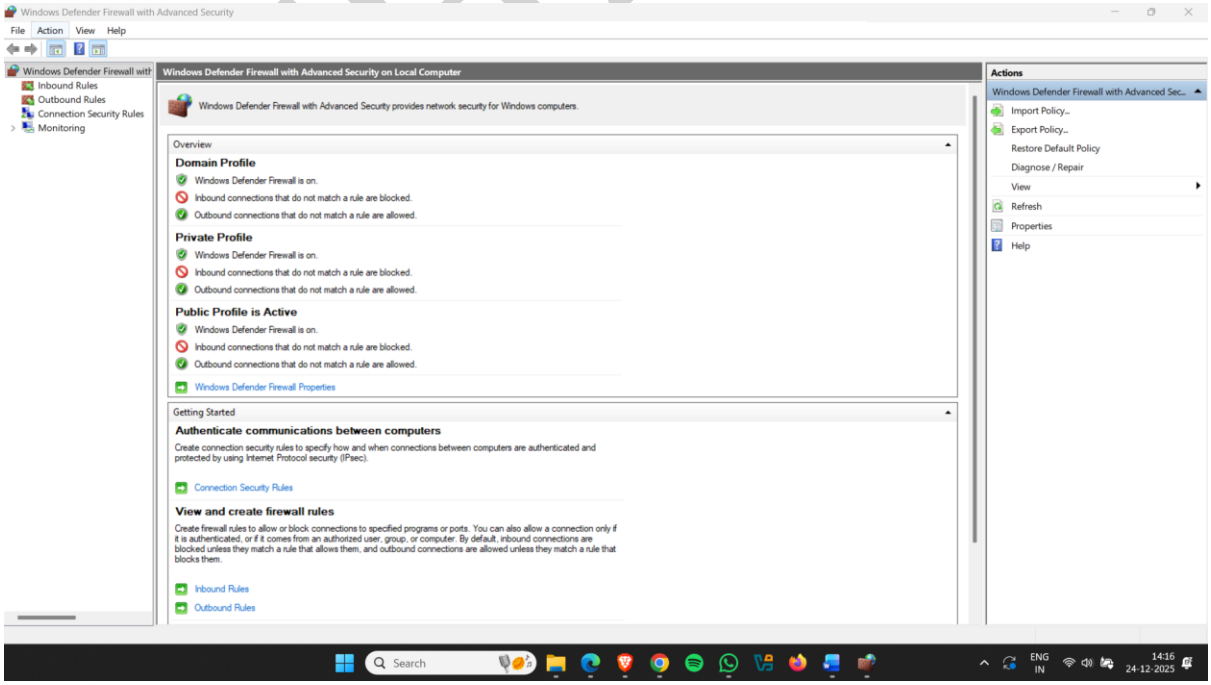


Figure 28

- Click on Inbound rules then click on new rule

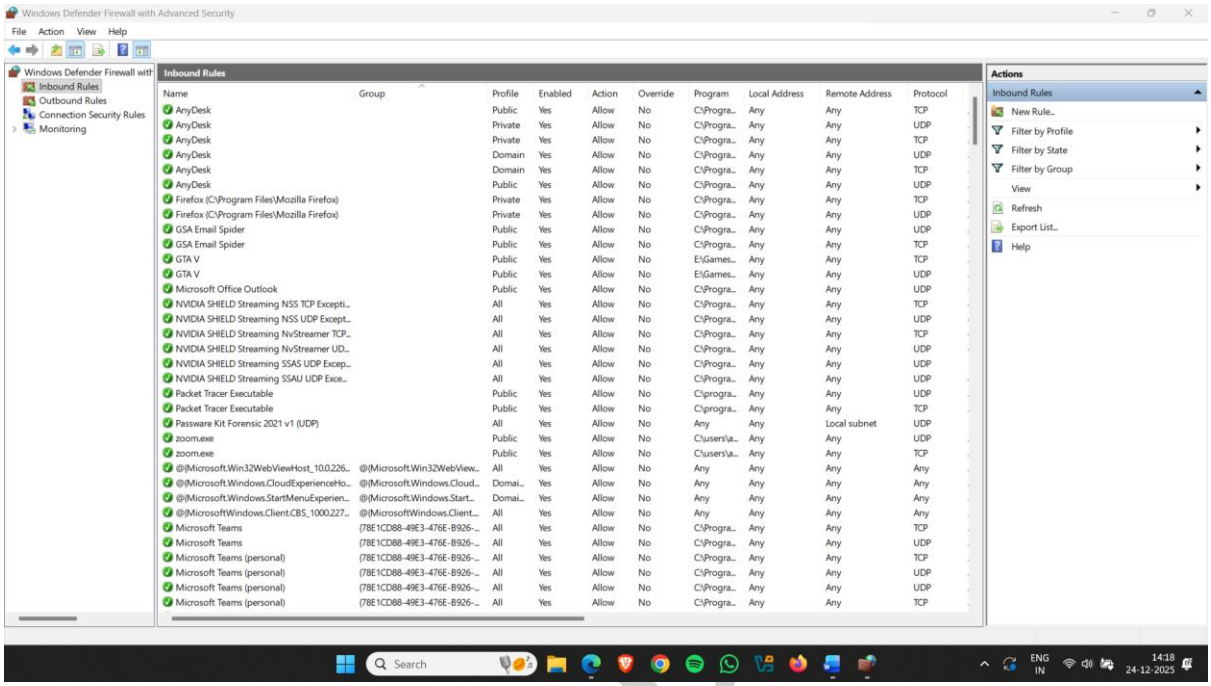


Figure 29

- Select the option that you want to set configuration like particular port or program , and then click on next.

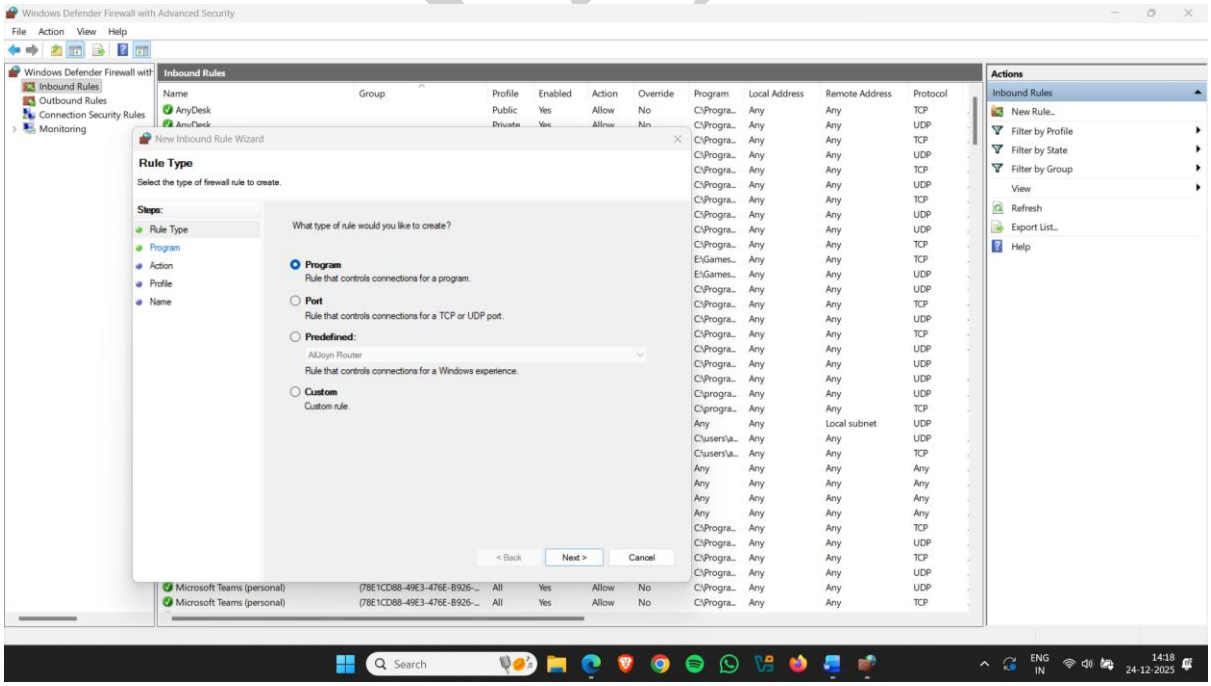


Figure 30

- Then set a path of program
  Select a file and click on open

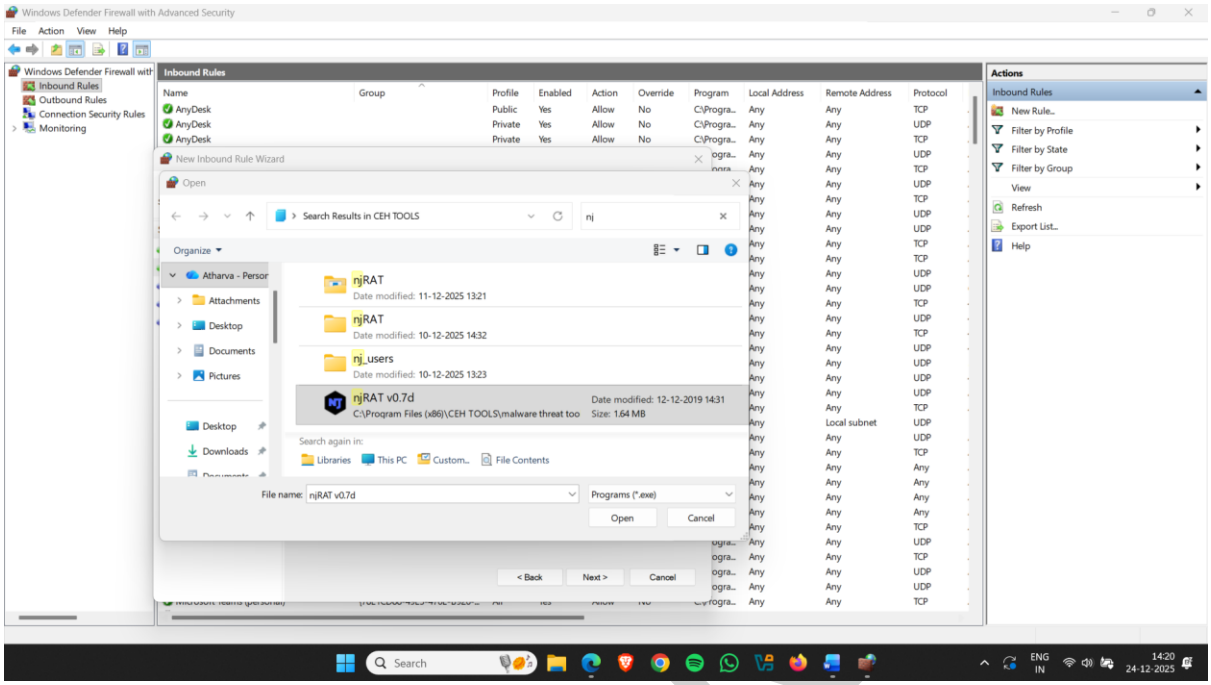


Figure 31

- Click on next

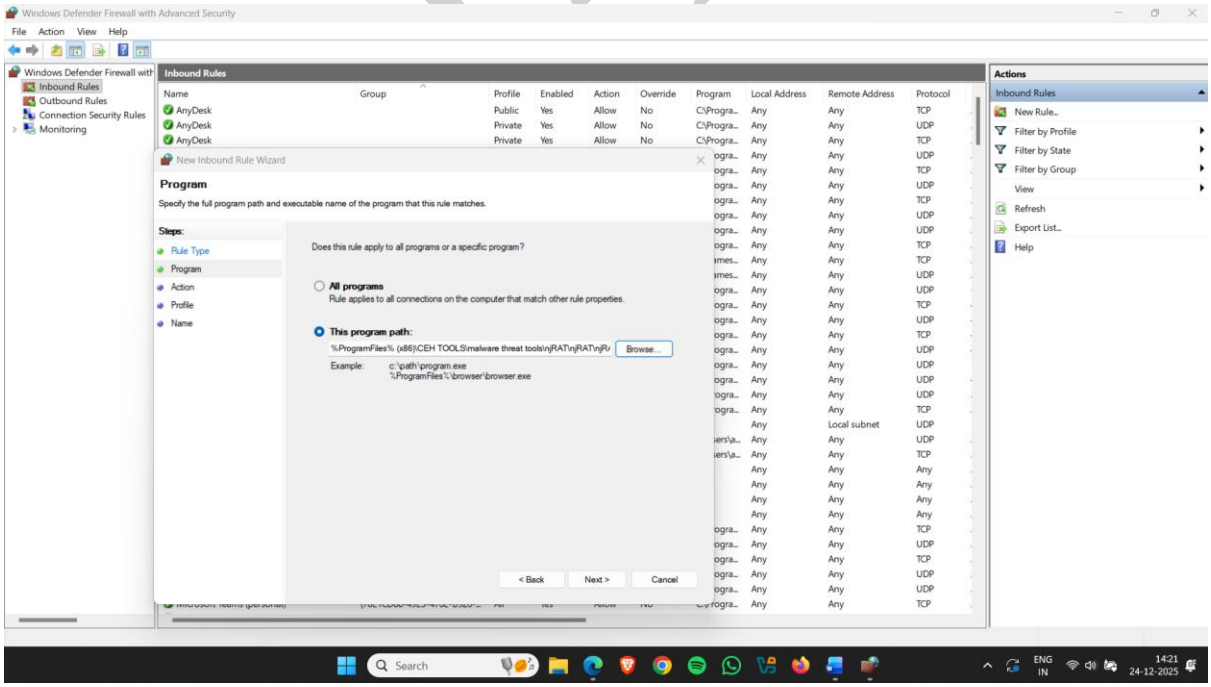


Figure 32

- **Connection Action Options**

There are three available options to control how incoming connections are handled:

---

1. Allow the Connection

Description:
Allows all matching incoming traffic, whether the connection is secured or not.

Security:

- No restriction on authentication or encryption
- Unsecured traffic is also permitted

Use When:

- You trust the application, port, or IP address

---

2. Allow the Connection if It Is Secure

Description:
Allows only those connections that are authenticated using **IPsec (Internet Protocol Security)**.

Requires:

- Proper configuration of IPsec policies
- IPsec must be enabled and correctly set up

Security:

- Ensures encrypted and authenticated communication
- Blocks unsecured connections

Use When:

- Protecting sensitive systems or confidential data

Note:

- The **Customize** button remains greyed out unless IPsec is configured

---

3. Block the Connection

Description:
Completely denies the connection, regardless of whether it is secure or unsecured.

Security:

- Strictest security setting
- No traffic is allowed

Use When:

- You want to prevent any communication through specific ports, programs, or IP addresses

---

- Select an option & then click on next

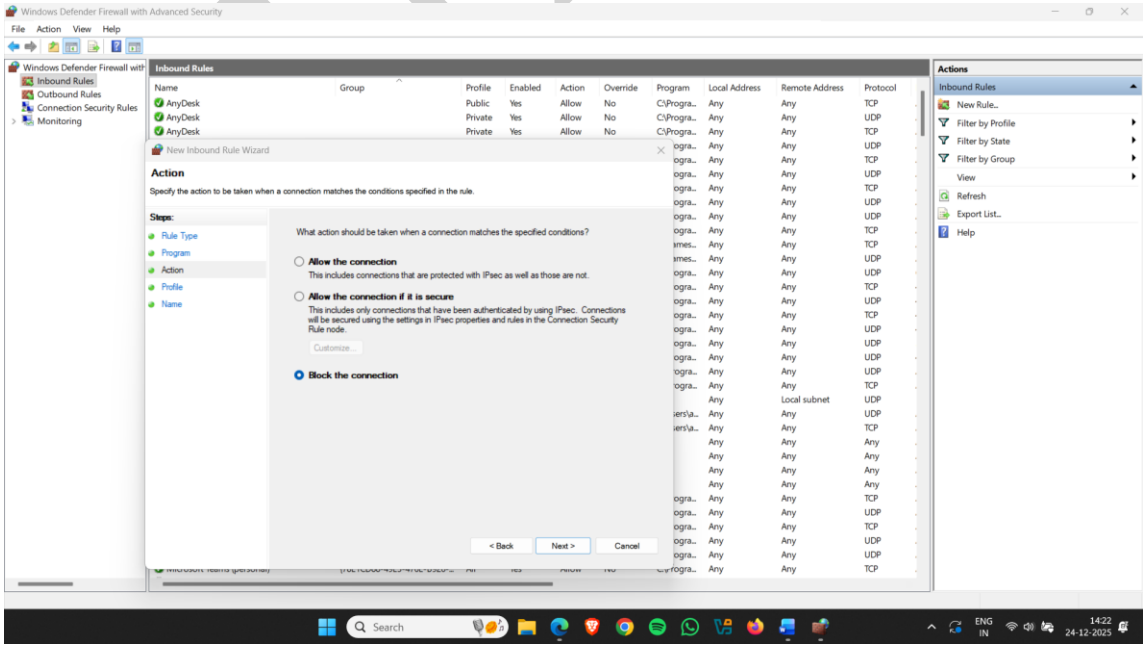


Figure 33

- **Network Profile Options**

Again, three network profile options appear. These determine **when the firewall rule will be applied** based on the type of network the system is connected to.

---

1. Domain

Applies When:

- The system is connected to a corporate or organizational network
- The computer is joined to a **domain** (e.g., office or enterprise environment using **Active Directory**)

Use Case:

- Apply this rule when you want it to work only in secure, managed networks
- Suitable for enterprise-level security policies

---

2. Private

Applies When:

- The computer is connected to a trusted private network
- Examples include home Wi-Fi or a small office network

Use Case:

- Enable this rule when you are at home or on a network you trust
- Allows flexibility while maintaining security

---

3. Public

Applies When:

- The system is connected to a public network
- Examples include cafés, airports, hotels, or other open networks

Use Case:

- Apply the rule when using public networks
- Extra caution is required because public networks are less secure

---

- Select an option & then click on next

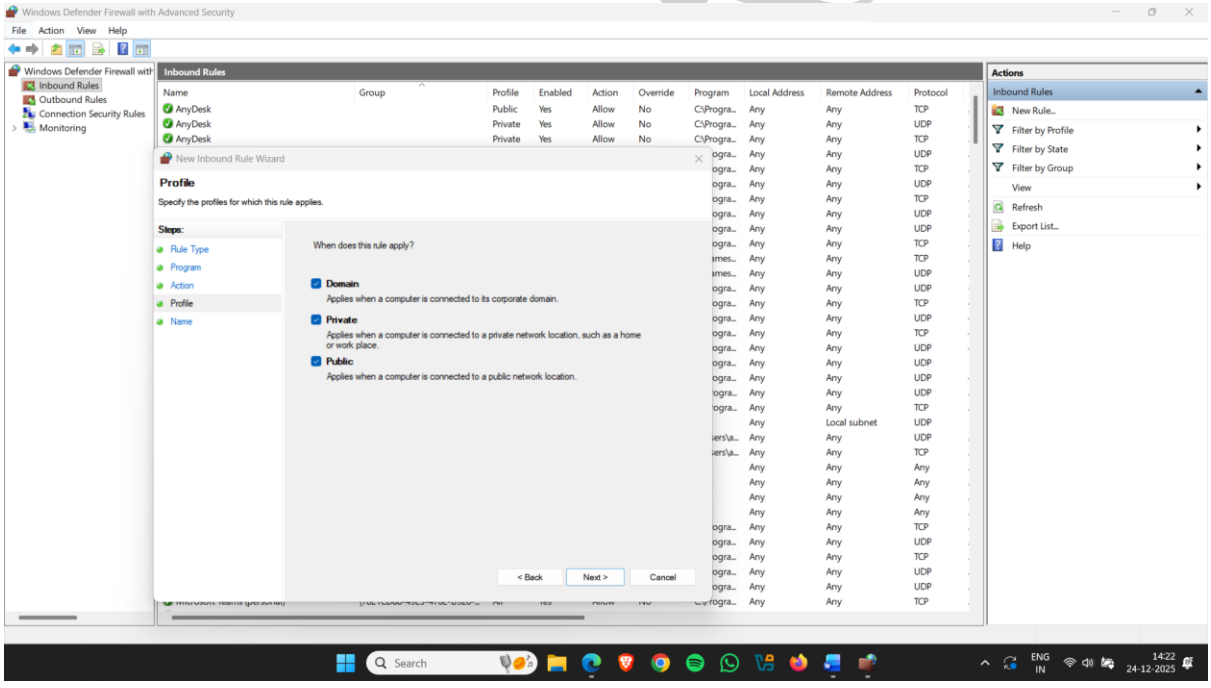


Figure 34

- Set any name and click on finish

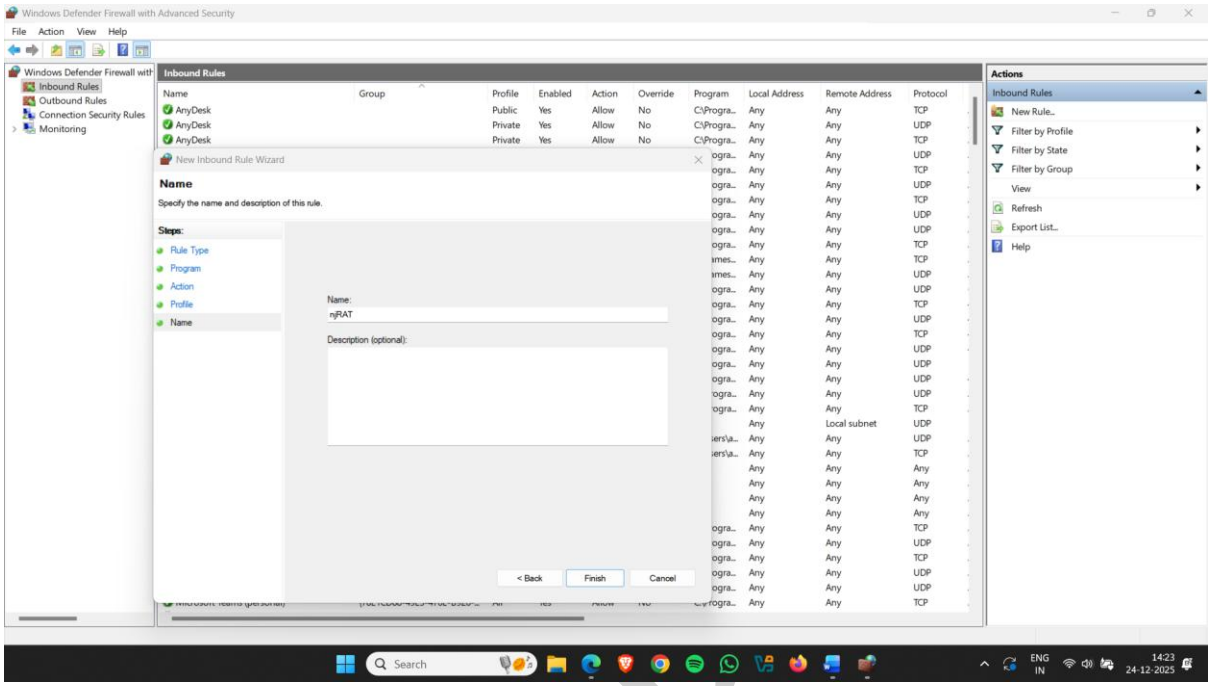


Figure 35

- Configuration has been set for inbound rules

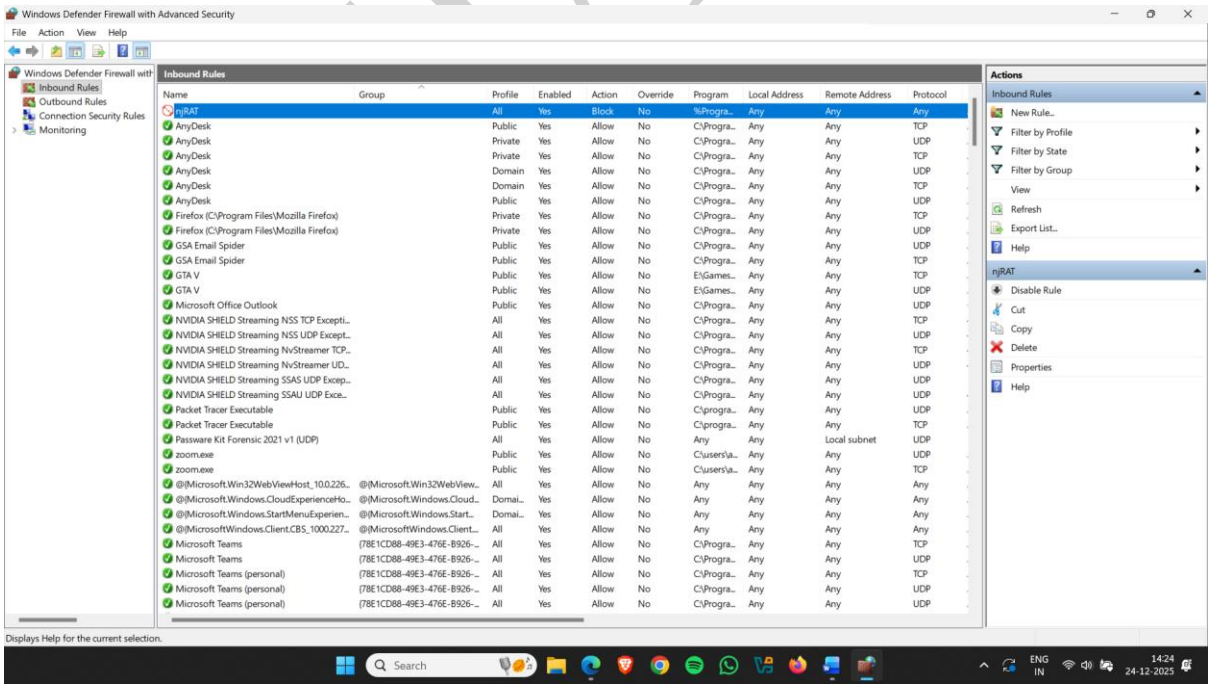


Figure 36

(OUTBOUND RULES)

- Click on Windows Button and search Firewall and open it

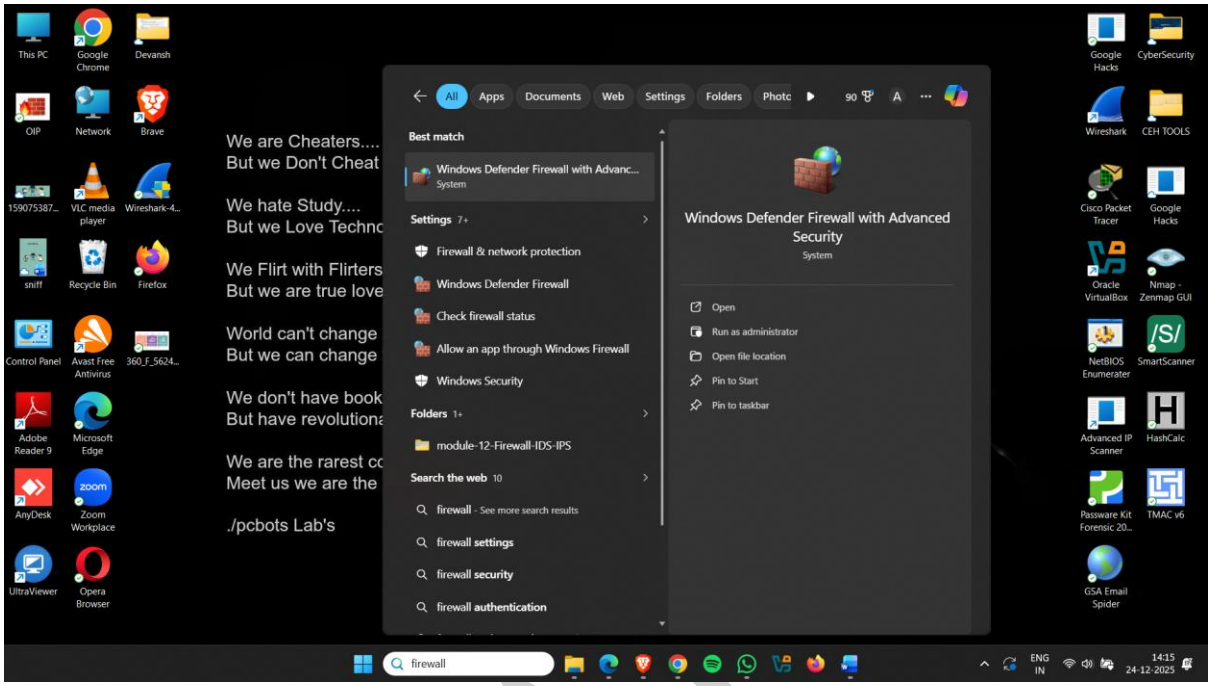


Figure 37

- There is option outbound rules – it means set rules for outgoing network

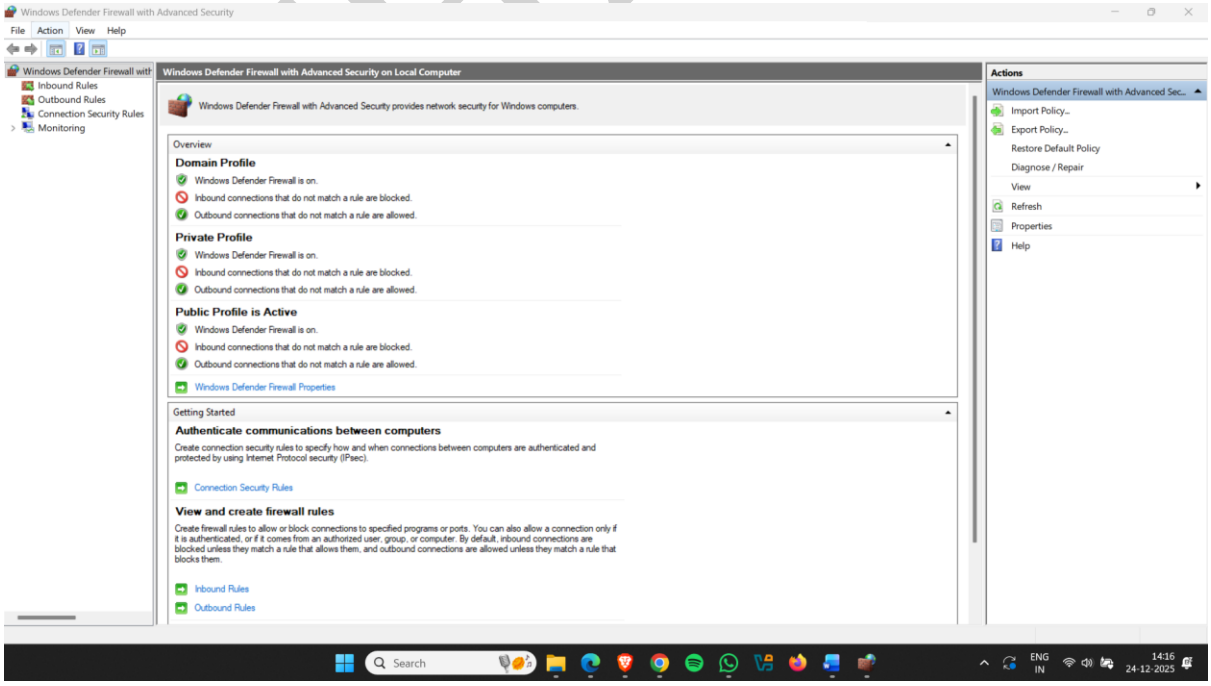


Figure 38

- Click on Outbound rules

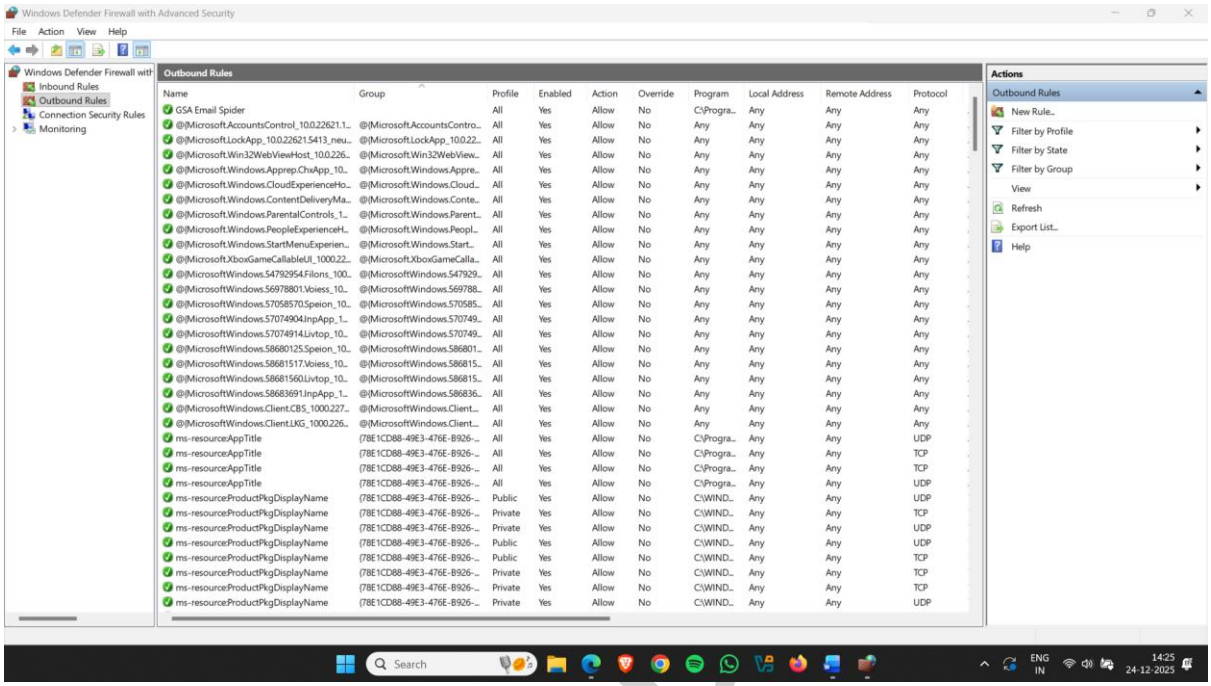


Figure 39

- Then click on New Rule
- New Pop Up appear with Three Options ,click
- on that you want to set a rule, and click on next.

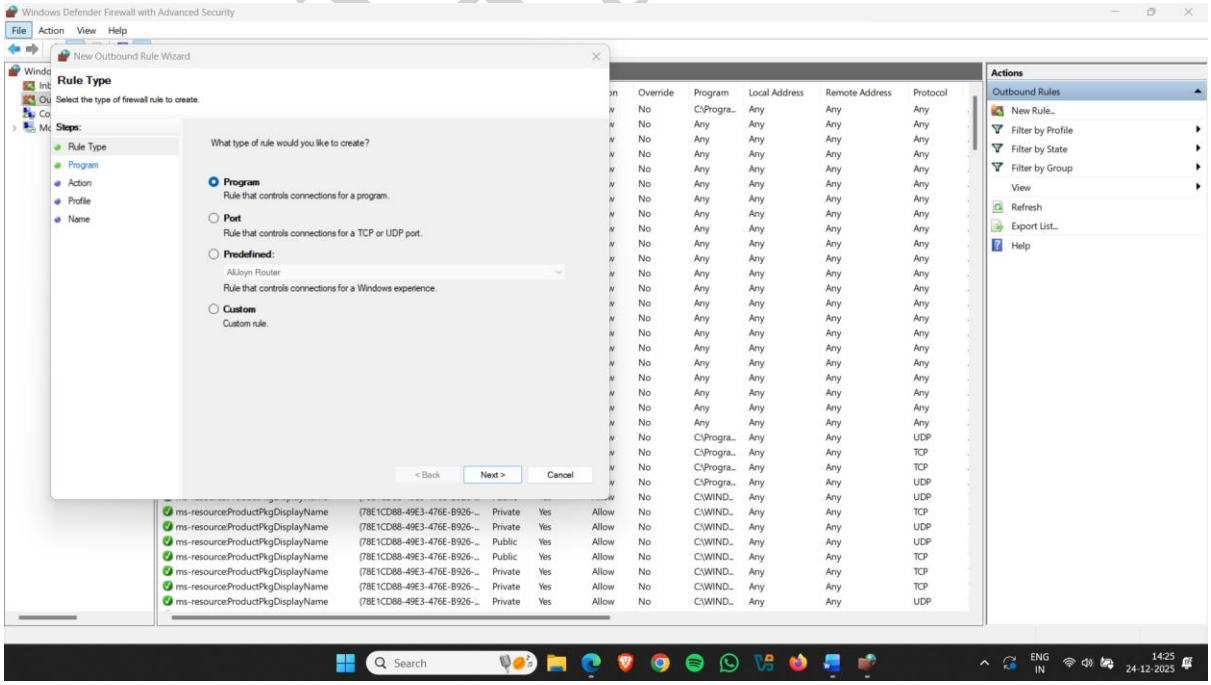


Figure 40

- Then set a path of program
  Select a file and click on open

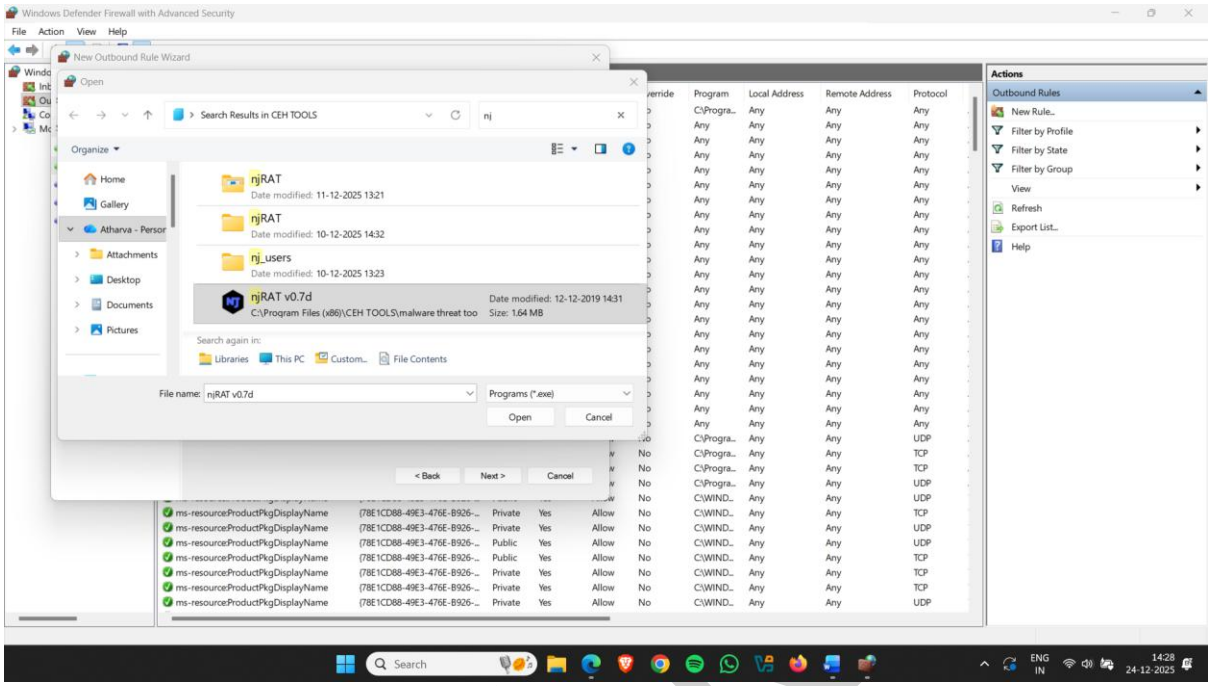


Figure 41

- Now ,set the path by clicking on Browse

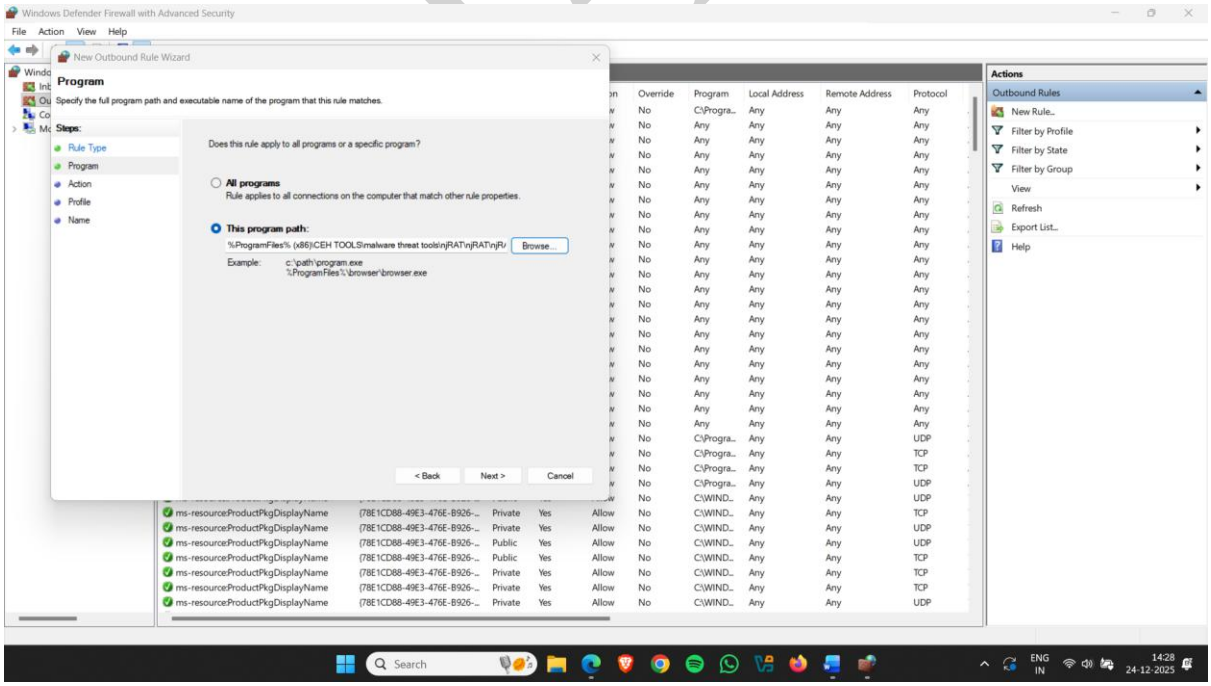


Figure 42

When configuring a firewall rule, three connection action options are available:

- **Allow the Connection**

Description:
This option allows all matching incoming traffic, regardless of whether the connection is secured or not.

Security Level:

Not restricted to authenticated or encrypted connections.

Allows both secure and non-secure traffic.

Use When:

You trust the application, service, or traffic source.

You want to permit communication without enforcing additional security measures.

- **Allow the Connection if it is Secure**

Description:
This option allows only those connections that are authenticated and secured using **IPsec (Internet Protocol Security)**.

Requirements:

Proper configuration of IPsec policies is required.

Security Level:

Provides encrypted and authenticated communication.

More secure than allowing all connections.

Use When:

You want to protect sensitive systems or data transfers.

Only trusted and verified devices should be allowed to connect.

- **Block the Connection**

Description:
This option completely denies the connection, whether it is secure or not.

Security Level:

Strictest security setting.

Prevents all matched traffic.

Use When:

You want to stop all communication on specific ports, programs, or IP addresses.

The traffic is untrusted or potentially harmful.

- Select an option & then click on next

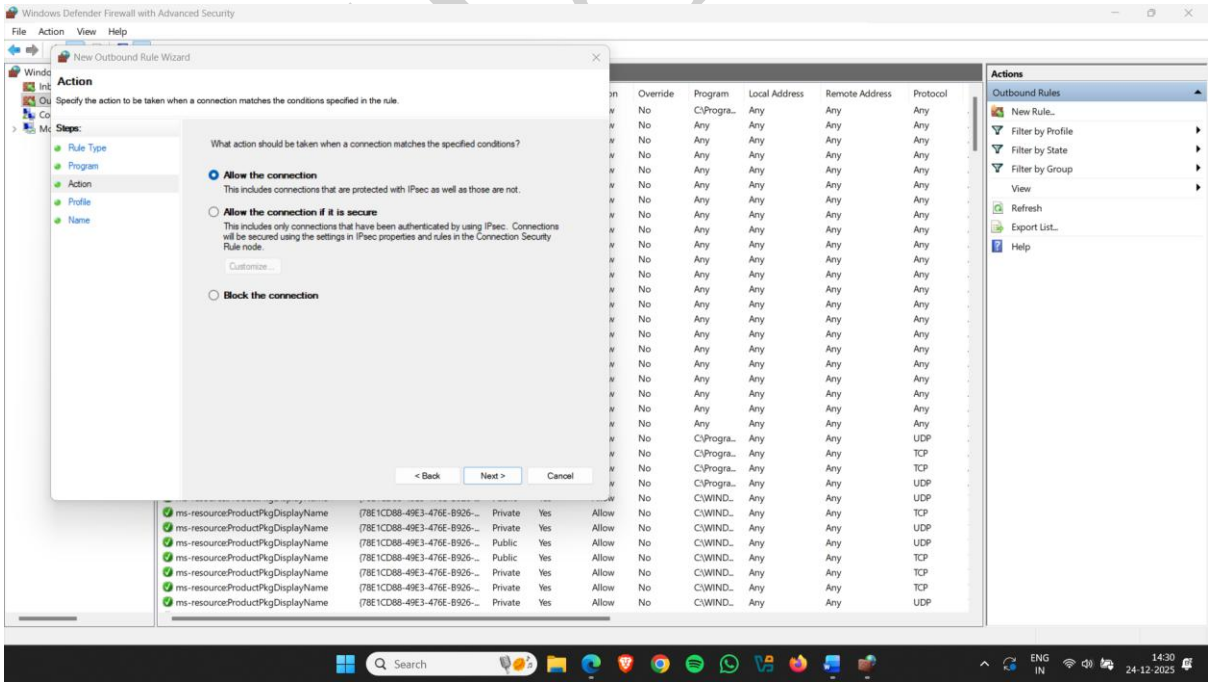


Figure 43

- Click on NEXT

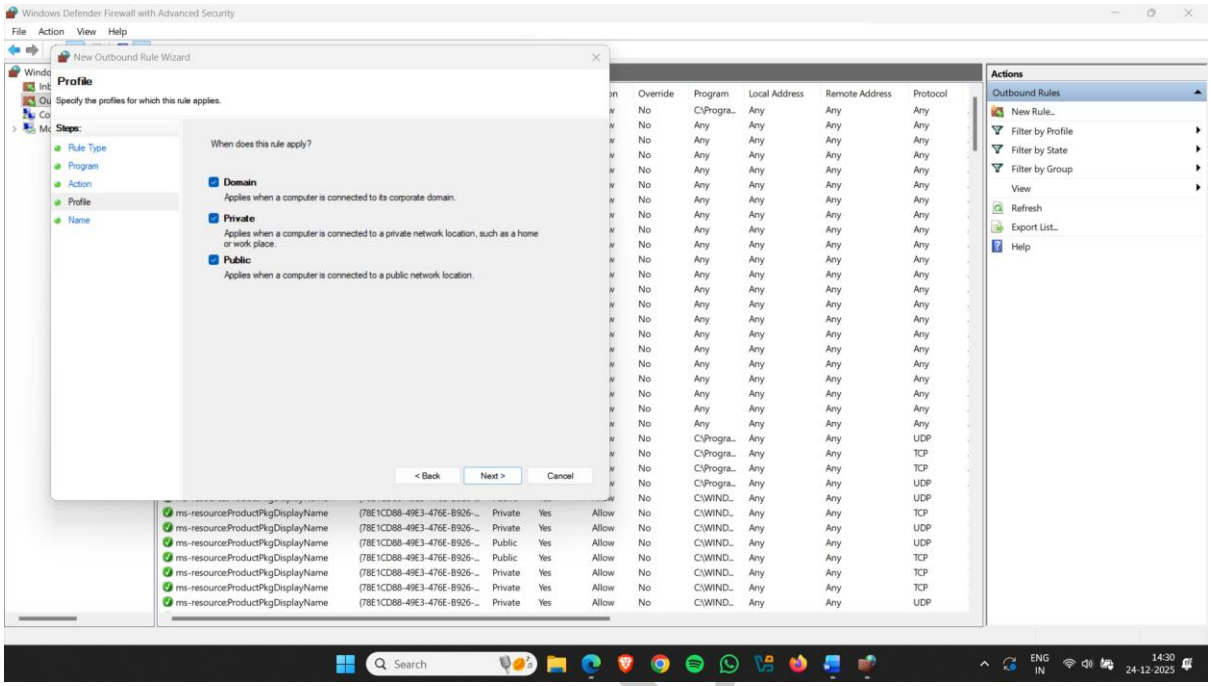


Figure 44

- Set the name of the Rule and description and click on next

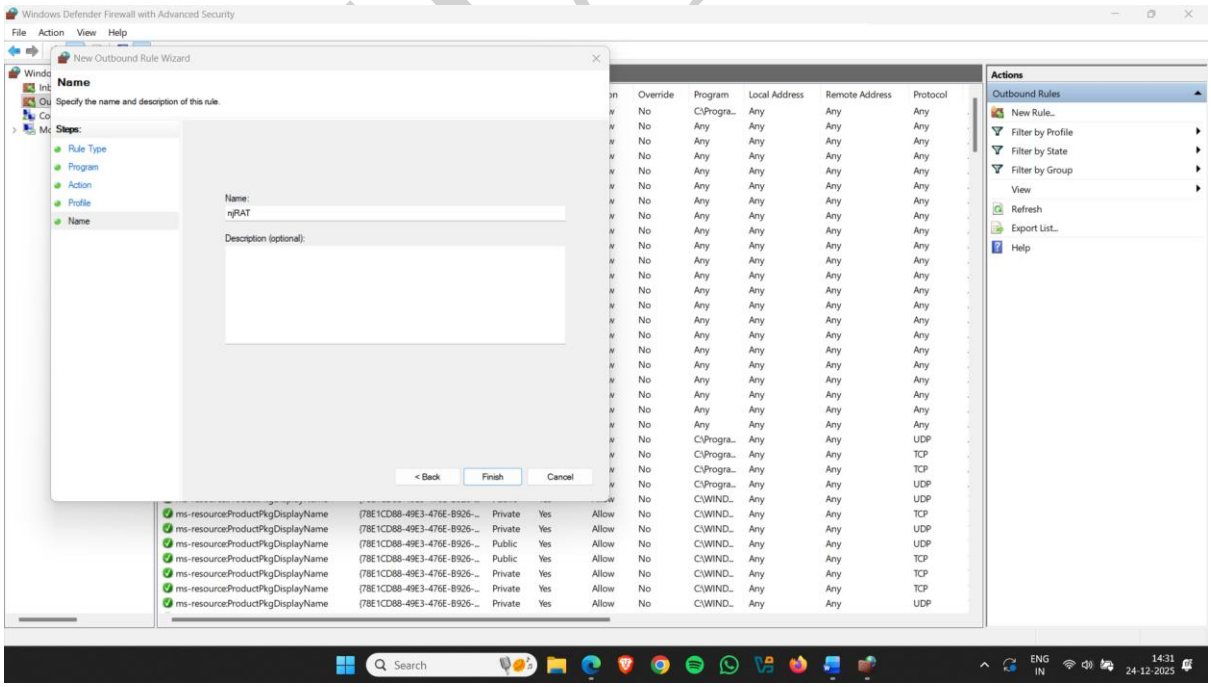


Figure 45

- Rule set successfully

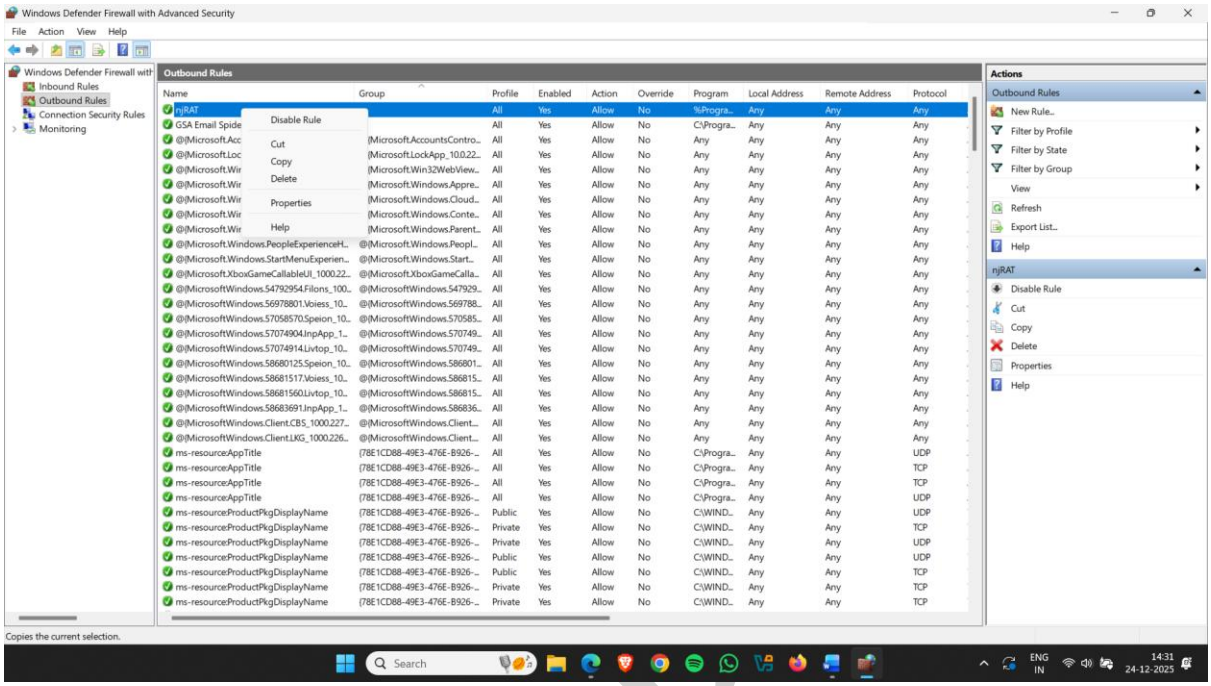


Figure 46

EXTRA ACTIVITY

Zone Alarm Firewall

ZoneAlarm Firewall is a third-party software firewall for Windows developed by Check Point Software Technologies. It provides an additional layer of security beyond the default Windows Defender Firewall, making it especially useful for users who want greater control over network activities.

Key Features of ZoneAlarm Firewall

1. Two-Way Firewall

- Monitors both incoming and outgoing network traffic.
- Blocks unauthorized inbound and outbound connections.

---

2. Stealth Mode

- Makes the PC invisible to hackers on the internet.
- Hides open ports from external scans and attacks.

---

3. Application Control

- Alerts users when applications attempt to access the internet.
- Allows or blocks internet access on a per-application basis.

---

4. Real-Time Monitoring

- Continuously tracks all network activity.
- Displays which programs are currently using the internet.

---

5. DefenseNet™

- A cloud-based security feature.
- Uses community feedback and intelligence to automatically configure trusted applications.

---

6. Identity Protection *(Optional – Pro Version)*

- Alerts users if personal or sensitive data is at risk.
- Includes credit monitoring features (available for U.S.-based users).

How to use it:

- After Installation , Open the application
- Now click on firewall

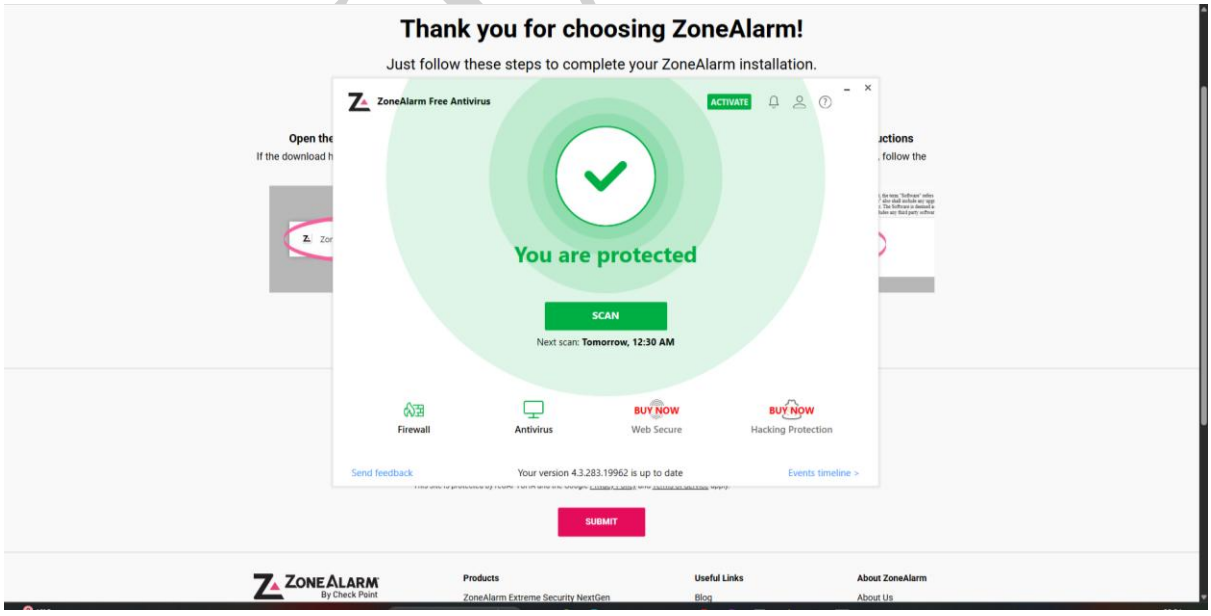


Figure 47

- Click on Application Permissions

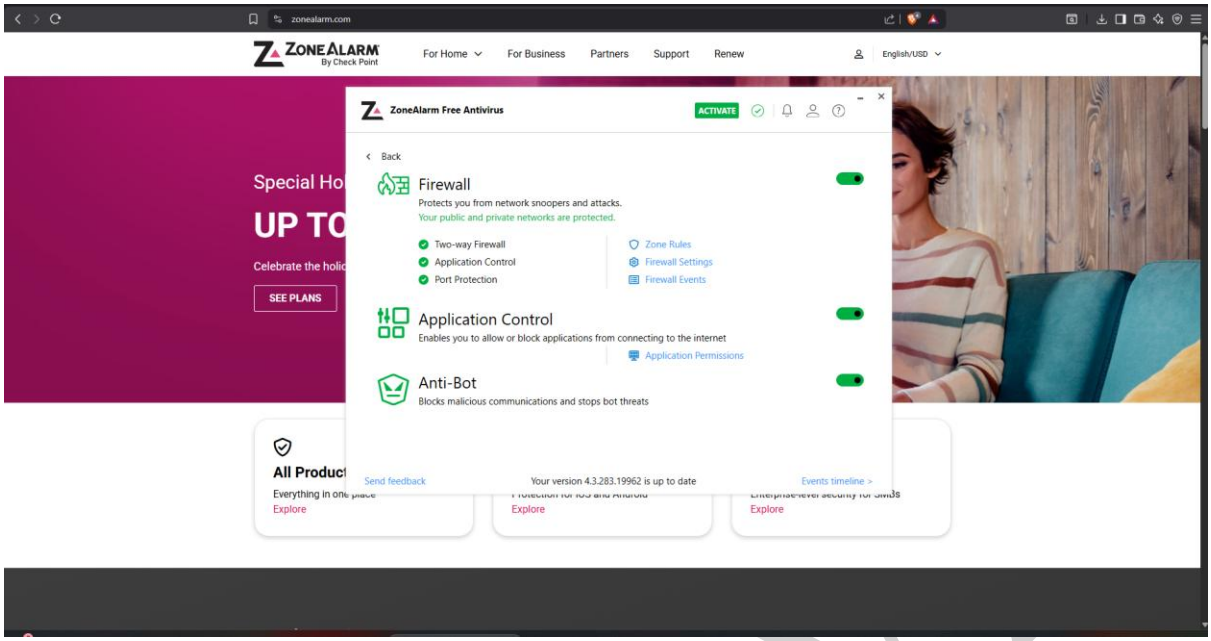


Figure 48

- Select the program that you want set a rule

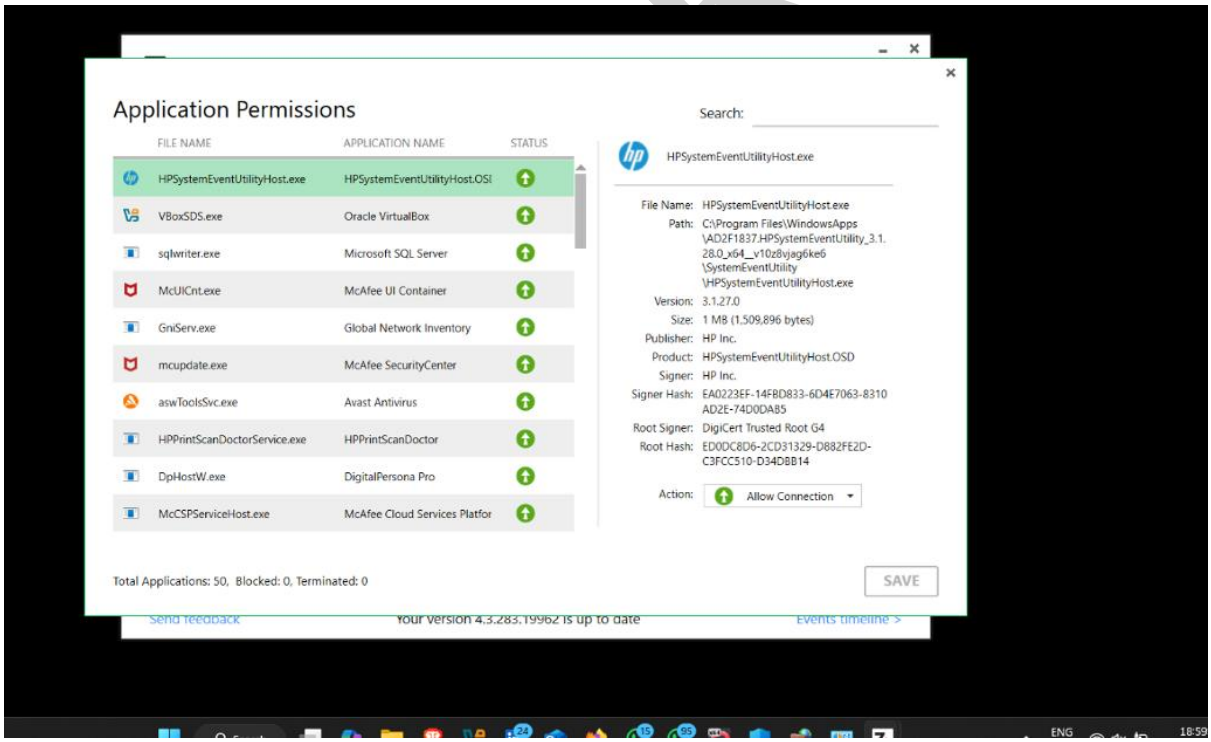


Figure 49

- Now , you can allow connection , Block Connection and Terminate Process

1. Allow Connection

Description:

- Permits the selected application or service to access the internet.
- The firewall allows all related network communication.

Use When:

- The application is trusted and requires internet access.

---

2. Block Connection

Description:

- Prevents the selected application or service from accessing the internet.
- All network communication for the application is denied.

Use When:

- The application is untrusted or should not communicate over the network.

---

3. Terminate Process

Description:

- Immediately stops the selected process if it is currently running.
- Prevents further network or system activity by the process.

Use When:

- The process is suspicious, unresponsive, or consuming excessive resources.

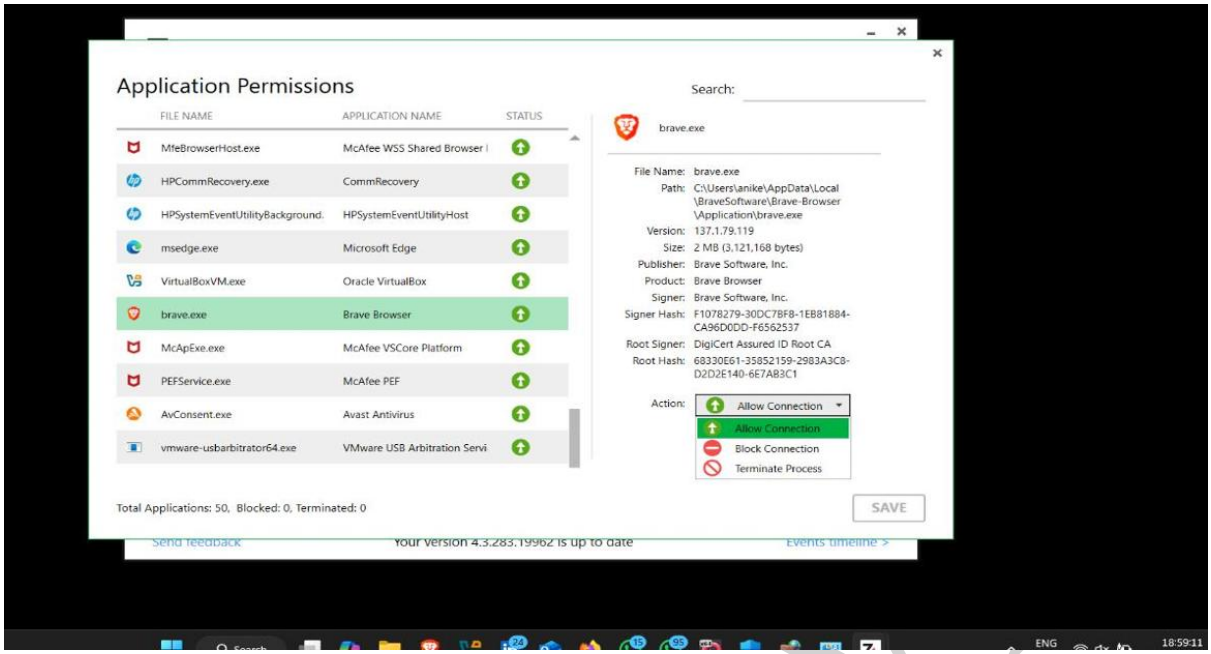


Figure 50

- Select an option & then click on save

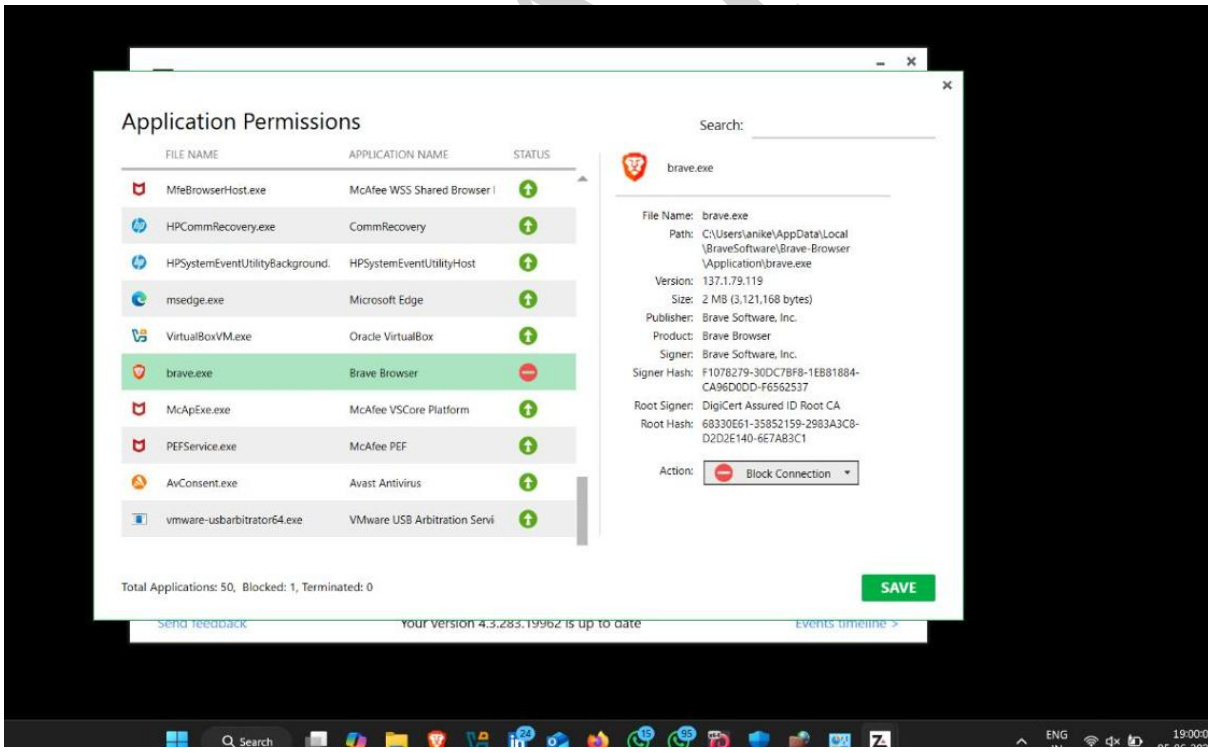


Figure 51

- Now click on Firewall Events that show the event logs that they capture during monitoring and capturing

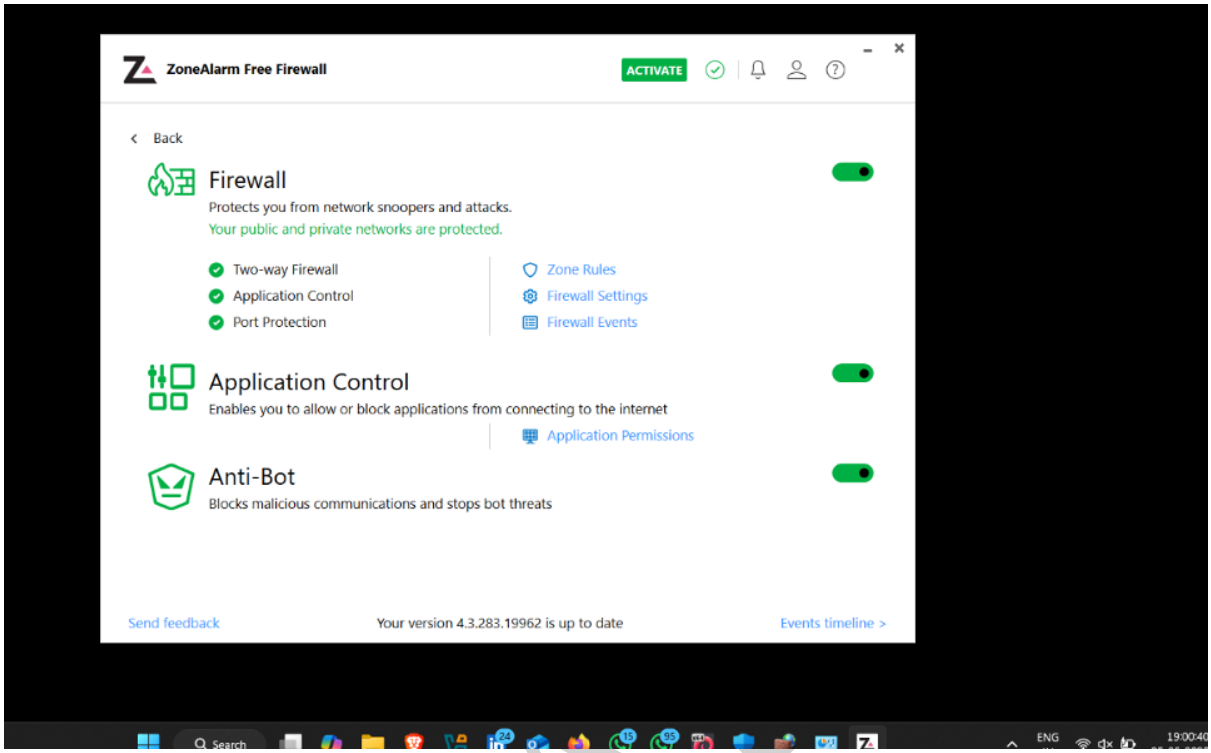


Figure 52

- It show all the event

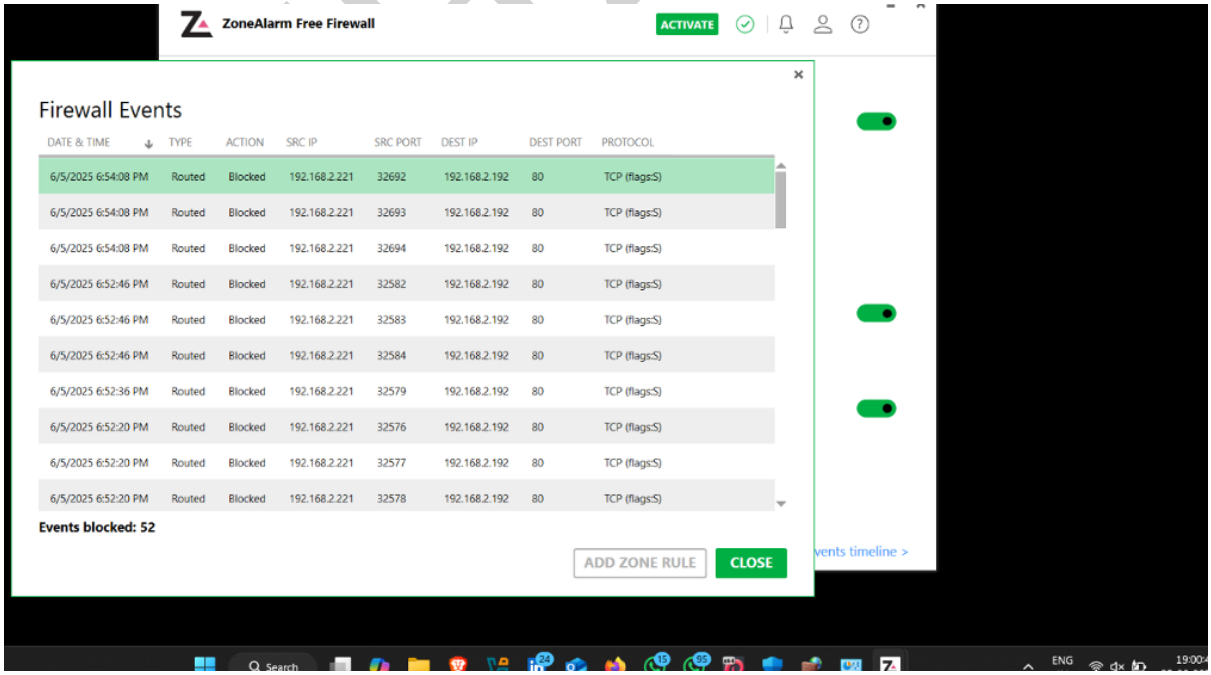


Figure 53

How to Defend Against Firewall Evasion

Defending against firewall evasion requires a combination of advanced firewall capabilities, strict traffic validation, continuous monitoring, and layered security controls. The following best practices help prevent attackers from bypassing firewall protections.

---

1. Implement Stateful Inspection Firewalls

- Use firewalls that track the full state of active network connections.
- Stateful firewalls can identify and reject out-of-state or unexpected packets.

2. Enable Strict Packet Filtering and Validation

- Validate protocol compliance for all incoming and outgoing traffic.
- Drop malformed, unexpected, or suspicious packets immediately.

3. Use Deep Packet Inspection (DPI)

- Inspect packet payloads in addition to packet headers.
- Detect tunneling techniques and malicious payloads hidden inside allowed protocols.

4. Block IP Spoofing

- Enable **Reverse Path Forwarding (RPF)** or **Unicast RPF** on routers and firewalls.
- Reject packets with source IP addresses that do not match legitimate routing paths.

5. Disallow Source Routing

- Block IP packets that have source routing options enabled.
- Most modern firewalls provide configuration options to reject such packets.

6. Reassemble Fragments for Inspection

- Ensure the firewall can fully reassemble fragmented IP packets before inspection.
- Prevent attackers from hiding malicious data within packet fragments.

7. Inspect and Control Encrypted Traffic

- Use SSL/TLS inspection or secure proxy servers to decrypt and analyze HTTPS traffic.
- Detect malware or command-and-control traffic concealed inside encrypted channels.

8. Implement Strict Port and Protocol Controls

- Explicitly allow only required ports and protocols.
- Block unused, unnecessary, or risky services.

9. Regularly Update Firewall Firmware and Rules

- Keep firewall software and firmware updated to fix known evasion vulnerabilities.
- Regularly review, audit, and fine-tune firewall rules.

10. Use an Intrusion Prevention System (IPS) Alongside the Firewall

- Deploy an IPS to detect and block sophisticated or evasive attack signatures.
- Adds an additional layer of real-time traffic inspection.

11. Monitor Logs and Traffic Patterns

- Continuously monitor firewall logs for abnormal or suspicious activity.
- Identify patterns that may indicate firewall evasion attempts.

12. Employ Network Segmentation and Zero Trust

- Divide the network into segments to limit lateral movement.
- Apply **Zero Trust principles**, where no traffic is trusted by default.

13. Implement Rate Limiting and Traffic Shaping

- Restrict excessive traffic bursts and scanning behavior.
- Helps block slow, stealthy, or low-rate evasion techniques.

14. Use Anti-Spoofing Filters at the Network Edge

- Configure edge routers and switches to drop spoofed packets.
- Reduces malicious traffic before it reaches the firewall.

Common Firewall Evasion Techniques Used by Attackers

1. IP Spoofing

- Attackers fake the source IP address of packets to make them appear as if they are coming from a trusted host.

2. Port Spoofing and Port Changing

- Malicious traffic is sent through non-standard or commonly allowed ports to bypass blocked or monitored ports.

3. Fragmentation Attacks

- Malicious packets are split into smaller fragments to evade firewall inspection and reassembly mechanisms.

4. Protocol Anomalies and Violations

- Attackers send malformed or unexpected packets to confuse firewall protocol analysis and inspection engines.

5. Tunneling and Encapsulation

- Malicious traffic is hidden inside permitted protocols such as:
  - HTTP tunneling
  - DNS tunneling
  - VPN encapsulation

6. Use of Encrypted Traffic

- Attackers use SSL/TLS encryption so the firewall cannot inspect packet contents effectively.

7. Source Routing

- Manipulation of IP header fields to control packet routing and potentially bypass firewall filtering rules.

8. Session Hijacking and TCP Sequence Prediction

- Attackers manipulate TCP session parameters to bypass stateful firewall inspection mechanisms.

9. Fragment Overlaps and Reassembly Confusion

- Exploiting weaknesses in how firewalls reassemble fragmented packets to avoid detection.

10. Malicious Payload in Allowed Traffic

- Malware is concealed within legitimate-looking traffic such as HTTPS or DNS communications.

How to Defend Against IDS Evasion

Intrusion Detection System (IDS) evasion refers to techniques used by attackers to bypass detection mechanisms by manipulating network traffic patterns, packet structure, or payload content. Understanding these evasion techniques helps security professionals strengthen IDS effectiveness.

---

1. Use a Combination of Detection Methods

- Combine **signature-based IDS** with **anomaly-based IDS**.
- Anomaly-based IDS can detect unusual traffic behavior even when attackers attempt signature evasion.

2. Enable Full Packet Reassembly

- Configure the IDS to fully reassemble fragmented IP packets and TCP streams before analysis.
- Prevent evasion techniques such as fragmentation and overlapping packets.

3. Regularly Update IDS Signatures

- Frequently update IDS rules and signatures to cover the latest exploits and evasion techniques.
- Use vendor updates and threat intelligence feeds.

4. Use Deep Packet Inspection (DPI)

- Inspect packet payloads in detail rather than only headers.
- Decode encoded or obfuscated payloads before analysis to reveal hidden attacks.

5. Implement SSL/TLS Inspection

- Use SSL/TLS decryption capabilities or proxy solutions to inspect encrypted traffic.

- Helps identify malicious content hidden inside encrypted sessions.

6. Behavioral and Contextual Analysis

- Correlate IDS alerts with logs from firewalls, endpoints, and other security systems.
- Use contextual information such as user behavior, time of day, and historical traffic patterns to detect evasion.

7. Deploy Multi-Layered Security

- Integrate IDS with:
  - Intrusion Prevention Systems (IPS)
  - Firewalls
  - Endpoint protection solutions
  - Network segmentation
- A **defense-in-depth** strategy significantly reduces the success of evasion attempts.

8. Tune IDS Rules to Reduce False Negatives

- Customize IDS rules based on the specific network environment.
- Modify or remove ineffective rules while balancing false positives.

9. Monitor Traffic Patterns

- Watch for unusual traffic timing, burst patterns, or inconsistent data flows.
- Use **Network Behavior Anomaly Detection (NBAD)** tools.

10. Log and Audit Everything

- Maintain detailed logs of IDS alerts, network flows, and system events.
- Enables detection and analysis of stealthy or long-term attacks.

11. Use Honeypots and Deception Techniques

- Deploy honeypots to attract attackers and observe evasive behavior.
- Helps in identifying new or unknown evasion techniques.

12. Train Security Personnel

- Keep SOC analysts and network administrators updated on IDS evasion tactics.
- Train teams to recognize suspicious activity that may bypass IDS controls.

Common IDS Evasion Techniques Used by Attackers

1. Fragmentation

- Breaking malicious payloads into small IP fragments so the IDS cannot properly reassemble or detect the complete attack.

2. Packet Overlapping

- Sending overlapping TCP/IP packets with conflicting data to confuse IDS packet reassembly and analysis.

3. Protocol Anomalies

- Using unusual, malformed, or non-standard packets that the IDS may fail to parse correctly.

4. Polymorphic Shellcode

- Continuously changing malware code structure or encryption methods to evade signature-based detection.

5. Payload Encoding

- Encoding attack payloads using formats such as:
  - Base64 encoding
  - URL encoding
  - Unicode encoding
- This helps hide known attack patterns from IDS signatures.

6. Traffic Timing and Rate Manipulation

- Sending packets very slowly or in irregular bursts to avoid threshold-based or anomaly-based detection.

7. Use of Encrypted Traffic

- Using SSL/TLS encryption or VPN tunnels so the IDS cannot inspect the payload contents.

8. Evasion of Signature Matching

- Exploiting zero-day vulnerabilities or using modified attack variants not covered by existing IDS signatures.

9. Avoiding Known Ports

- Transmitting malicious traffic through uncommon or commonly allowed ports to bypass IDS monitoring rules.

10. Session Splicing

- Splitting an attack across multiple sessions or connections to prevent the IDS from detecting a complete attack sequence.

How to Defend Against IPS Evasion

Intrusion Prevention System (IPS) evasion refers to techniques used by attackers to bypass inline security controls by manipulating packet structure, traffic behavior, or payload content. Understanding these techniques helps in strengthening IPS detection and prevention mechanisms.

---

1. Implement Stateful Inspection Firewalls

- Use firewalls that track the full state of active network connections.
- Stateful firewalls can identify and reject out-of-state or unexpected packets.

2. Enable Strict Packet Filtering and Validation

- Validate protocol compliance for all incoming and outgoing traffic.
- Drop malformed, unexpected, or suspicious packets immediately.

3. Use Deep Packet Inspection (DPI)

- Inspect packet payloads in addition to packet headers.
- Detect tunneling techniques and malicious payloads hidden inside allowed protocols.

4. Block IP Spoofing

- Enable **Reverse Path Forwarding (RPF)** or **Unicast RPF** on routers and firewalls.
- Reject packets with source IP addresses that do not match legitimate routing paths.

5. Disallow Source Routing

- Block IP packets that have source routing options enabled.
- Most modern firewalls provide configuration options to reject such packets.

6. Reassemble Fragments for Inspection

- Ensure the firewall can fully reassemble fragmented IP packets before inspection.
- Prevent attackers from hiding malicious data within packet fragments.

7. Inspect and Control Encrypted Traffic

- Use SSL/TLS inspection or secure proxy servers to decrypt and analyze HTTPS traffic.
- Detect malware or command-and-control traffic concealed inside encrypted channels.

8. Implement Strict Port and Protocol Controls

- Explicitly allow only required ports and protocols.
- Block unused, unnecessary, or risky services.

9. Regularly Update Firewall Firmware and Rules

- Keep firewall software and firmware updated to fix known evasion vulnerabilities.
- Regularly review, audit, and fine-tune firewall rules.

10. Use an Intrusion Prevention System (IPS) Alongside the Firewall

- Deploy an IPS to detect and block sophisticated or evasive attack signatures.
- Adds an additional layer of real-time traffic inspection.

11. Monitor Logs and Traffic Patterns

- Continuously monitor firewall logs for abnormal or suspicious activity.
- Identify patterns that may indicate firewall evasion attempts.

12. Employ Network Segmentation and Zero Trust

- Divide the network into segments to limit lateral movement.
- Apply **Zero Trust principles**, where no traffic is trusted by default.

13. Implement Rate Limiting and Traffic Shaping

- Restrict excessive traffic bursts and scanning behavior.
- Helps block slow, stealthy, or low-rate evasion techniques.

14. Use Anti-Spoofing Filters at the Network Edge

- Configure edge routers and switches to drop spoofed packets.
- Reduces malicious traffic before it reaches the firewall

Common IPS Evasion Techniques Used by Attackers

1. Packet Fragmentation

- Splitting the attack payload into very small fragments to avoid detection during packet inspection and reassembly.

2. TCP Stream Manipulation

- Manipulating TCP packets by altering:
    - Sequence numbers
    - Overlapping segments
    - Out-of-order packets
- This confuses the IPS during stream reassembly.

3. Protocol Violations and Anomalies

- Sending malformed packets or using unusual protocol behaviour's to evade signature-based or protocol-aware inspection.

4. Encoding and Obfuscation

- Encoding payloads using techniques such as Base64 or Unicode.
- Using polymorphic malware to bypass signature-based detection.

5. Traffic Timing Evasion

- Sending attacks slowly over time (low-and-slow attacks) to avoid triggering threshold-based IPS rules.

6. Use of Encrypted Traffic

- Encrypting attack payloads inside SSL/TLS sessions so the IPS cannot inspect contents without decryption capabilities.

7. Tunneling and Encapsulation

- Wrapping malicious traffic inside allowed protocols such as:
    - HTTP/DNS/SSH tunnels

8. Payload Padding and NOP Sleds

- Adding no-operation (NOP) instructions or junk bytes to disrupt signature matching.

9. Attack Variants and Zero-Day Exploits

- Using unknown, new, or slightly modified exploits that are not yet included in IPS signature databases.

10. Session Splicing

- Splitting an attack across multiple TCP sessions or connections to avoid full detection.