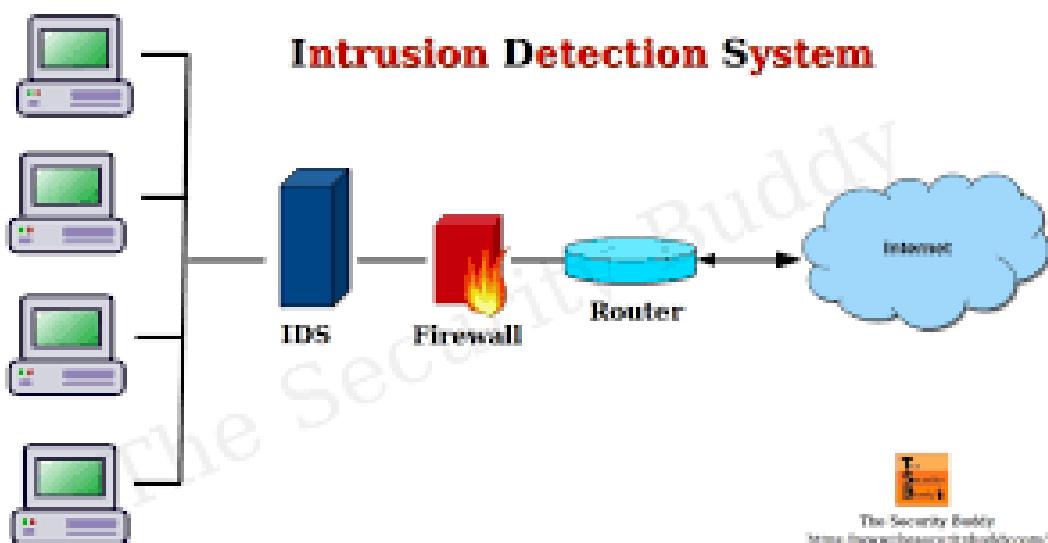


Module 12

Evading IDS, Firewalls & Honeypots

IDS:



An Intrusion Detection System (IDS) is a security tool that monitors network traffic and systems for malicious activity or policy violations. It essentially acts as an early warning system, detecting potential threats and reporting them to security personnel.

Here's a more detailed explanation:

How an IDS Works:

1. 1. Monitoring:

IDSs constantly monitor network traffic (for network-based IDSs) or system logs (for host-based IDSs).

2. 2. Threat Detection:

They analyze this traffic or logs, comparing it against a set of predefined rules (signature-based) or learning models (anomaly-based) to identify suspicious patterns.

3. 3. Reporting:

When a potential threat is detected, the IDS sends an alert to security teams, allowing them to investigate and respond.

Types of IDSs:

- **Network Intrusion Detection System (NIDS):** Monitors network traffic for suspicious activity.
- **Host Intrusion Detection System (HIDS):** Monitors logs and activity on a specific computer or server.
- **Signature-based IDS:** Detects known threats by comparing traffic against a database of known attack signatures.
- **Anomaly-based IDS:** Detects unknown threats by identifying deviations from normal behavior.
- **Hybrid IDS:** Combines both signature and anomaly-based detection techniques.

Example Diagram:

[Image: ids ips on an enterprise network diagram]

In this diagram:

- **Network:** Represents the network being protected.
- **Firewall:** Provides a first line of defense, controlling traffic flow based on rules.
- **IDS:** Monitors network traffic for suspicious activity and reports it.
- **IPS:** (Not shown in the simplified diagram but often used in conjunction with IDS) can block malicious traffic in real-time.
- **Server/Workstations:** Represent the resources being protected.

Key Points:

- IDSs are a crucial part of a comprehensive security strategy.
- They help to detect and prevent intrusion attempts before they cause damage.
- There are various types of IDSs, each with its own strengths and weaknesses.

- Proper implementation and configuration are essential for maximizing the effectiveness of an IDS.

IPS :

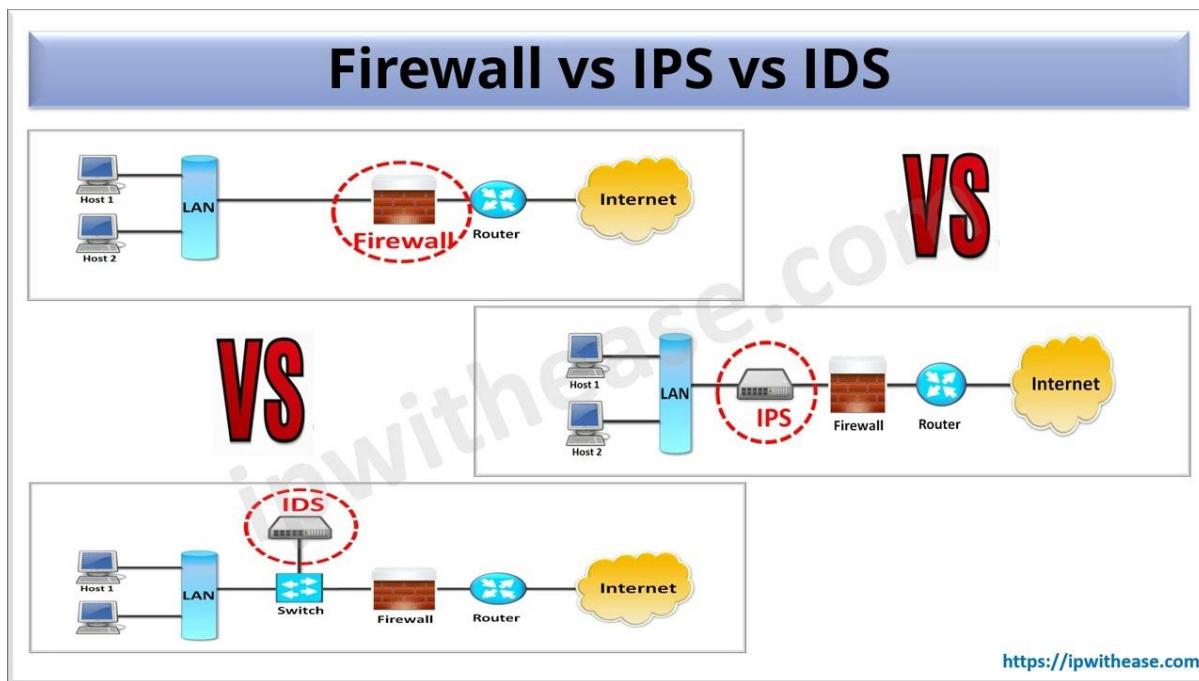
In cybersecurity, IPS stands for **Intrusion Prevention System**. It's a network security tool that monitors network traffic for malicious activity and takes automated actions to prevent it, including blocking or dropping malicious traffic, according to Fortinet. Unlike Intrusion Detection Systems (IDS) which only detect and alert about potential threats, IPS actively takes steps to mitigate the threat. [1, 2, 3, 4]

Here's a more detailed explanation:

- **What it does:** IPS systems continuously monitor network traffic, looking for patterns or characteristics that indicate a potential attack or intrusion. [2, 3]
- **Active protection:** When a suspicious activity is detected, the IPS system takes immediate action to prevent the attack from succeeding, such as blocking the malicious traffic or shutting down a compromised process. [2, 3, 5, 6, 7]
- **Types of IPS:**
 - **Network-based IPS (NIPS):** Deployed at the network level to protect all systems on the network. [8]
 - **Host-based IPS (HIPS):** Installed on individual endpoints (like computers) to monitor traffic to and from that specific host. [8]
- **How it works:**
 - **Signature-based:** IPS systems use predefined signatures or rules to identify known attack patterns. [2, 4]
 - **Behavior-based:** They also analyze network traffic behavior to detect unusual or suspicious activity that might indicate an intrusion. [2, 4]
- **Benefits:**
 - **Improved security:** IPS systems help prevent unauthorized access and protect against a variety of attacks. [2, 3]
 - **Reduced risk:** By actively blocking threats, IPS systems reduce the risk of successful attacks and data breaches. [2, 3]
 - **Real-time protection:** IPS systems provide real-time protection by responding to threats as they occur. [2, 3]

- **Relationship to other security tools:**
 - **Firewalls:** IPS systems can work in conjunction with firewalls to provide a layered security approach. [9]
 - **Intrusion Detection Systems (IDS):** IDS systems detect and alert about potential threats, while IPS systems take action to prevent them. [3, 10]

Difference between IDS and IPS :



🔍 IDS (Intrusion Detection System):

- **Purpose:** Detect and alert on suspicious activities or policy violations.
- **Placement:** Monitors network traffic and analyzes it against a database of known threats.
- **Action:** Generates alerts for administrators but does not block or prevent the attack.
- **Type:** Passive monitoring system.
- **Example Use:** Identifying port scanning attempts, malware infections, or suspicious user behavior.

🔒 IPS (Intrusion Prevention System):

- **Purpose:** Detect and **prevent** threats in real-time.

Name : kunal Jawale

- **Placement:** Inline with the network traffic, allowing it to actively control data flow.
 - **Action:** Blocks, drops, or re-routes malicious traffic based on defined rules.
 - **Type:** Active monitoring and prevention system.
 - **Example Use:** Automatically blocking an SQL injection attempt or preventing access from blacklisted IP addresses.
-

Key Differences:

Aspect	IDS	IPS
Action	Detects and alerts	Detects and blocks
Mode	Passive	Active
Placement	Outside the flow of traffic	Inline with traffic
Response Time	Post-event (after detection)	Real-time (during attack)
Network Impact	Minimal latency	Slight latency due to inspection

Would you like me to explain how IDS and IPS can be integrated together in modern network security?

4o

You said:

yes

ChatGPT said:

Integrating IDS and IPS in Modern Network Security:

In modern network architectures, **IDS (Intrusion Detection System)** and **IPS (Intrusion Prevention System)** are often integrated to create a **layered defense strategy**. This integration maximizes security by combining the strengths of detection and prevention.



Integration Models:

1. Unified Threat Management (UTM):

- A single appliance that includes both IDS and IPS along with firewalls, anti-virus, and VPN capabilities.
- Simplifies management and reduces hardware costs.

2. Next-Generation Firewalls (NGFW):

- Modern firewalls often come with built-in IDS/IPS capabilities.
- They allow for deep packet inspection, application awareness, and real-time blocking of threats.

3. Hybrid Deployment:

- IDS and IPS can be deployed separately but configured to work together.
 - IDS monitors traffic and forwards suspicious activities to IPS for real-time prevention.
-

⚙️ How They Work Together:

1. Detection First (IDS):

- The IDS analyzes network traffic and flags suspicious activities.
- Alerts are sent to security teams and IPS for analysis.

2. Prevention Next (IPS):

- If the flagged activity matches known attack patterns or violates policies, the IPS takes immediate action.
- Actions include dropping packets, resetting connections, or blocking IP addresses.

3. Feedback Loop:

- IDS logs and analysis are fed back into IPS to improve its threat database.
 - Machine learning can be applied to adapt to new threats in real-time.
-

🔍 Example Scenario:

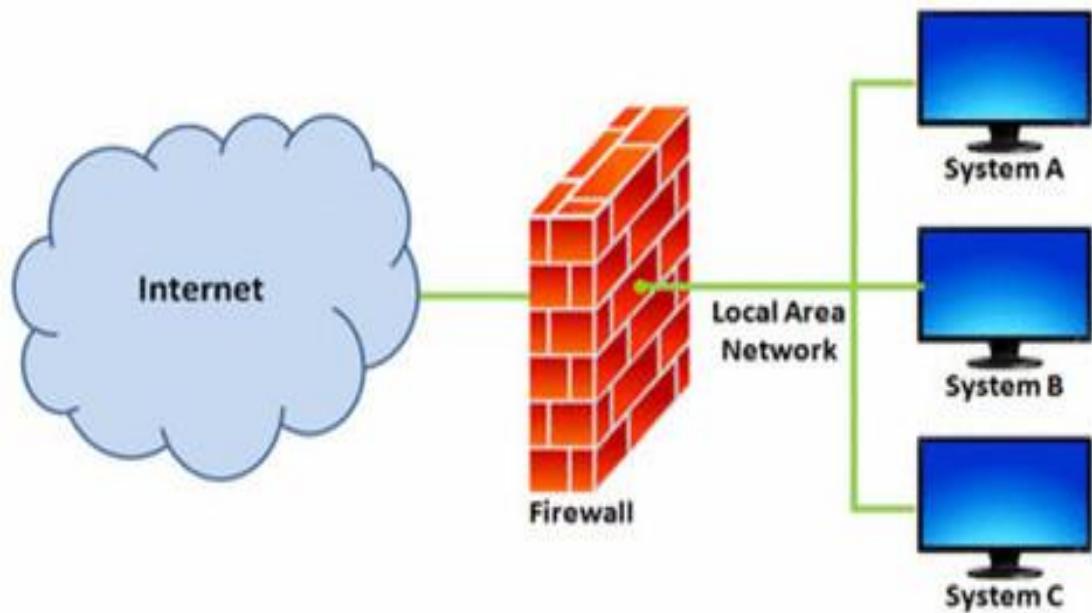
Imagine a **DDoS attack** on a company's web server:

1. The **IDS** detects unusual traffic spikes and identifies the potential attack.
2. The **IPS** receives the alert and begins filtering out malicious IP addresses.

3. Legitimate traffic continues while malicious packets are dropped, ensuring uptime and security.

Aspect	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Function	Monitors and detects suspicious activities	Detects and actively prevents suspicious activities
Mode	Passive (listens and analyzes traffic)	Active (in-line with traffic, can drop or block traffic)
Action Taken	Alerts administrators of threats	Blocks or mitigates threats in real-time
Placement	Outside of the main traffic path	Inline with the traffic flow
Response Time	After the event (post-analysis)	Immediate (real-time prevention)
Impact on Traffic	No impact; only monitors	Can introduce slight latency due to inspection
Security Approach	Detection-based	Prevention-based
Network Visibility	High visibility but no control over traffic	Full visibility and control over traffic
Example Threats	Port scanning, brute force attacks, reconnaissance	SQL injection, DDoS attacks, malware propagation
Alert Handling	Sends alerts for manual intervention	Automatically responds to threats
False Positives	Generates alerts even for benign activities	Can block legitimate traffic if not configured properly

Firewalls :



Firewalls in Context:

In the context of , firewalls are critical components for establishing the perimeter defense of a network. They are designed to **monitor, filter, and control incoming and outgoing network traffic** based on predefined security rules.

🔍 What is a Firewall?

- A **firewall** is a network security device—software or hardware—that acts as a barrier between a trusted internal network and untrusted external networks (like the internet).
 - It **inspects packets** of data against a set of security policies and decides whether to **allow, block, or log** the traffic.
 - Firewalls are the **first line of defense** in protecting sensitive information from cyber threats.
-

🌐 Types of Firewalls :

1. Packet Filtering Firewall

- Works at the **Network Layer (Layer 3)** of the OSI model.
- Filters traffic based on source/destination IP addresses, ports, and protocols.

- Fast but limited in detecting complex threats.

2. Stateful Inspection Firewall

- Operates at the **Transport Layer (Layer 4)**.
- Monitors the **state of active connections** and makes decisions based on the context of the traffic.
- More secure than packet filtering, as it understands the flow of traffic.

3. Proxy Firewall (Application-Level Gateway)

- Works at the **Application Layer (Layer 7)**.
- Intercepts all traffic between the user and the internet, acting as a middleman.
- Provides deep inspection of packets but is slower due to high processing.

4. Next-Generation Firewall (NGFW)

- Combines traditional firewall capabilities with **IDS/IPS**, application awareness, and deep packet inspection.
- Operates across **multiple OSI layers**.
- Offers protection against modern threats like malware, encrypted traffic, and application-layer attacks.

5. Web Application Firewall (WAF)

- Specifically protects **web applications** from threats like **SQL Injection, XSS, and CSRF**.
- Focuses on HTTP/HTTPS traffic and secures applications hosted on websites.

💡 How Firewalls Work:

1. Rule-Based Filtering:

- Admins define rules (allow, deny, log) based on IP, port, or application.

2. Network Address Translation (NAT):

- Hides internal IP addresses from external entities for privacy and security.

3. Virtual Private Network (VPN) Support:

- Some firewalls can manage VPN connections to secure remote access.

4. Logging and Alerts:

- Firewalls generate logs for traffic, helping in auditing and incident response.

5. Traffic Segmentation:

- Divides network traffic into trusted and untrusted zones, enhancing security.
-



Importance of Firewalls :

- Understanding firewalls is crucial for:
 - **Penetration Testing:** Identifying and bypassing firewall rules.
 - **Scanning and Enumeration:** Learning how firewalls respond to different types of scans.
 - **Attack Mitigation:** Knowing how to harden firewall configurations against common attacks.
 - **Defense Strategies:** Configuring rules to prevent exploits and malware propagation.
-

Task1 : Detect Intrusions using Snort

Snort : An Open-Source Intrusion Detection and Prevention System (IDS/IPS)



What is Snort?

- Snort is an **open-source network intrusion detection and prevention system (IDS/IPS)** developed by **Sourcefire**, which is now a part of **Cisco Systems**.
 - It can **monitor network traffic** in real-time and analyze it against predefined attack patterns and behaviors.
 - Snort is capable of:
 - **Traffic analysis**
 - **Packet logging**
 - **Real-time alerting**
 - **Detection of probes or attacks** (e.g., port scans, buffer overflows, malware, DoS attacks)
-



Snort Operating Modes:

1. Sniffer Mode:

- Captures and displays network packets in real-time.
- Example command: snort -v
- Useful for basic packet inspection.

2. Packet Logger Mode:

- Saves packets to disk for detailed analysis.
- Example command: snort -dev -l /log_directory
- Allows offline inspection of packet logs.

3. Network Intrusion Detection System (NIDS) Mode:

- Analyzes network traffic in real-time and matches it against a database of attack signatures.
- Example command: snort -c /etc/snort/snort.conf -i eth0
- Generates alerts when suspicious activity is detected.

4. Inline Mode (IPS Mode):

- Functions as an Intrusion Prevention System (IPS).
- It can **drop, reject, or modify packets** in real-time.
- Requires additional setup with iptables or PF_RING.



Snort Rule Structure:

Snort uses **rules** to detect suspicious activities. A rule has two parts:

1. **Rule Header:** Defines action, protocol, source IP, source port, destination IP, and destination port.
2. **Rule Options:** Defines what to look for, such as payload content, flags, and message alerts.

Example Rule:

```
alert tcp any any -> 192.168.1.0/24 80 (msg:"Potential XSS Attack";  
content:<script>; nocase; sid:1000001; rev:1;)
```

- **Action:** alert
- **Protocol:** tcp
- **Source:** any IP, any port
- **Destination:** IP range 192.168.1.0/24, port 80
- **Options:**
 - msg: Alert message
 - content: Searches for the string <script>

- nocase: Case-insensitive search
 - sid: Unique Snort ID
 - rev: Rule revision number
-

Key Features of Snort:

1. **Real-Time Analysis:**
 - Monitors live traffic and detects suspicious behavior instantly.
 2. **Signature-Based Detection:**
 - Uses predefined attack signatures to identify known threats.
 3. **Protocol Analysis:**
 - Inspects the behavior of network protocols to spot anomalies.
 4. **Content Matching:**
 - Searches packet payloads for specific strings or byte patterns.
 5. **Flexible Deployment:**
 - Can be configured as a **NIDS, IPS, or packet logger**.
 6. **Community Support and Regular Updates:**
 - Large community and regular rule updates from the **Snort community and Cisco Talos**.
-

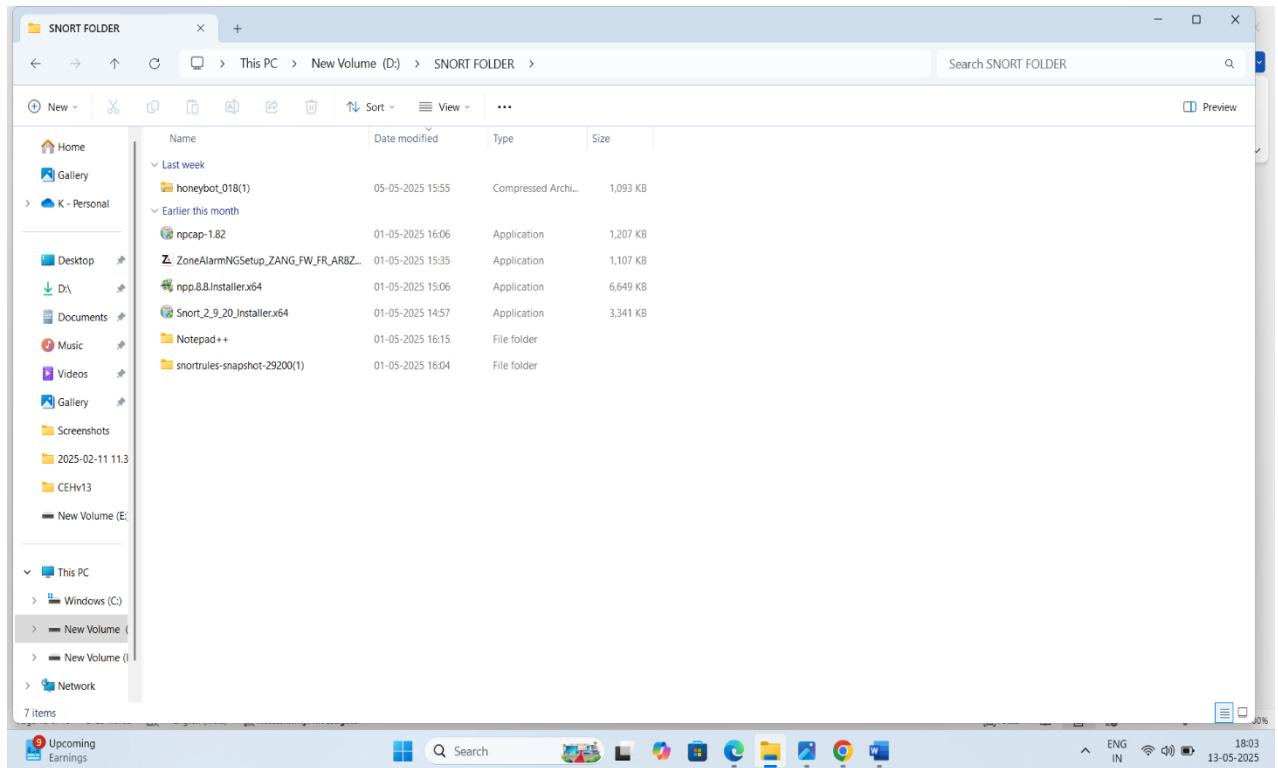
Why Snort is Important for CEH:

- Understanding Snort is critical for **penetration testing** and **network security assessments**.
 - Ethical hackers use Snort to:
 - **Detect vulnerabilities** in real time.
 - **Simulate attacks** and observe IDS responses.
 - **Analyze firewall evasion techniques**.
 - **Log attack patterns** for post-event analysis.
-

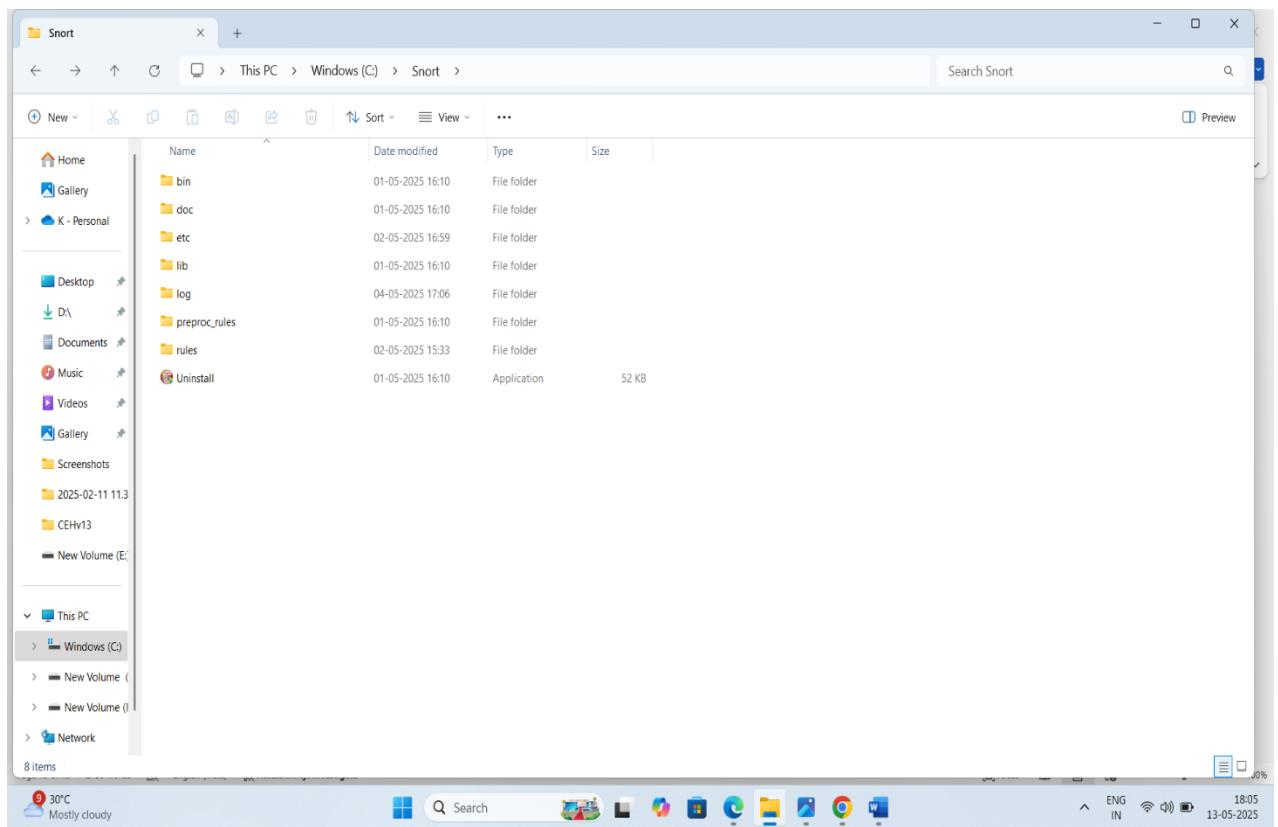
Steps of configuration of snort :

1. Download snort and notepad ++ using any browser
2. Download snort rules and crate a folder and give a name snort

Name : kunal Jawale

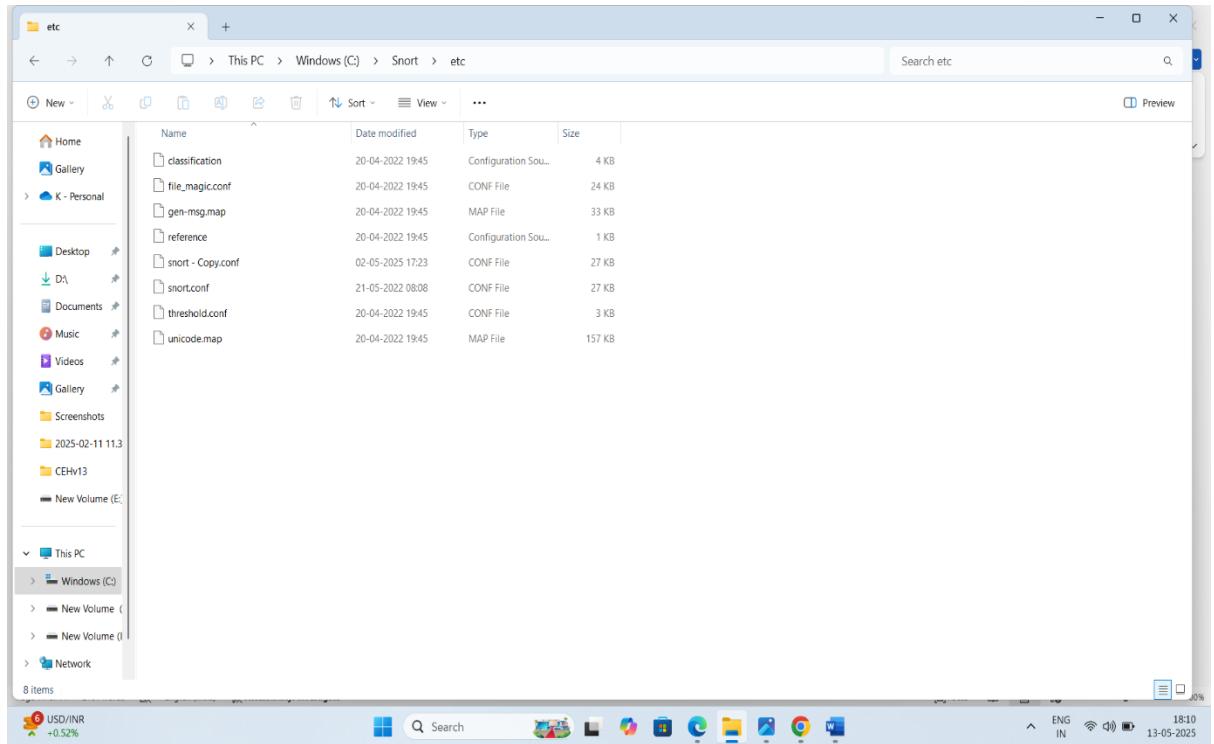


3. Copy the rules and preproc_rules and paste in C: drive snort folder in rules and preproc rules destination



Name : kunal Jawale

4. Click on etc folder in snort
5. After opening etc folder copy paste the snort.conf in same destination like this :



6. After the copy paste open with the snort-copy.conf with notepad ++

```
# Per Rule latency configuration
#config ppm: max-rule-time 200, \
#    threshold 3, \
#    suspend-expensive-rules, \
#    suspend-timeout 20, \
#    rule-log alert

#####
# Configure Perf Profiling for debugging
# For more information see README.PerfProfiling
#####

#config profile_rules: print all, sort avg_ticks
#config profile_procs: print all, sort avg_ticks

#####
# Configure protocol aware flushing
# For more information see README.stream5
#####

config paf_max: 16000

#####
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
#####

# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
#dynamicdetection directory /usr/local/lib/snort_dynamicrules

#####
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
#####

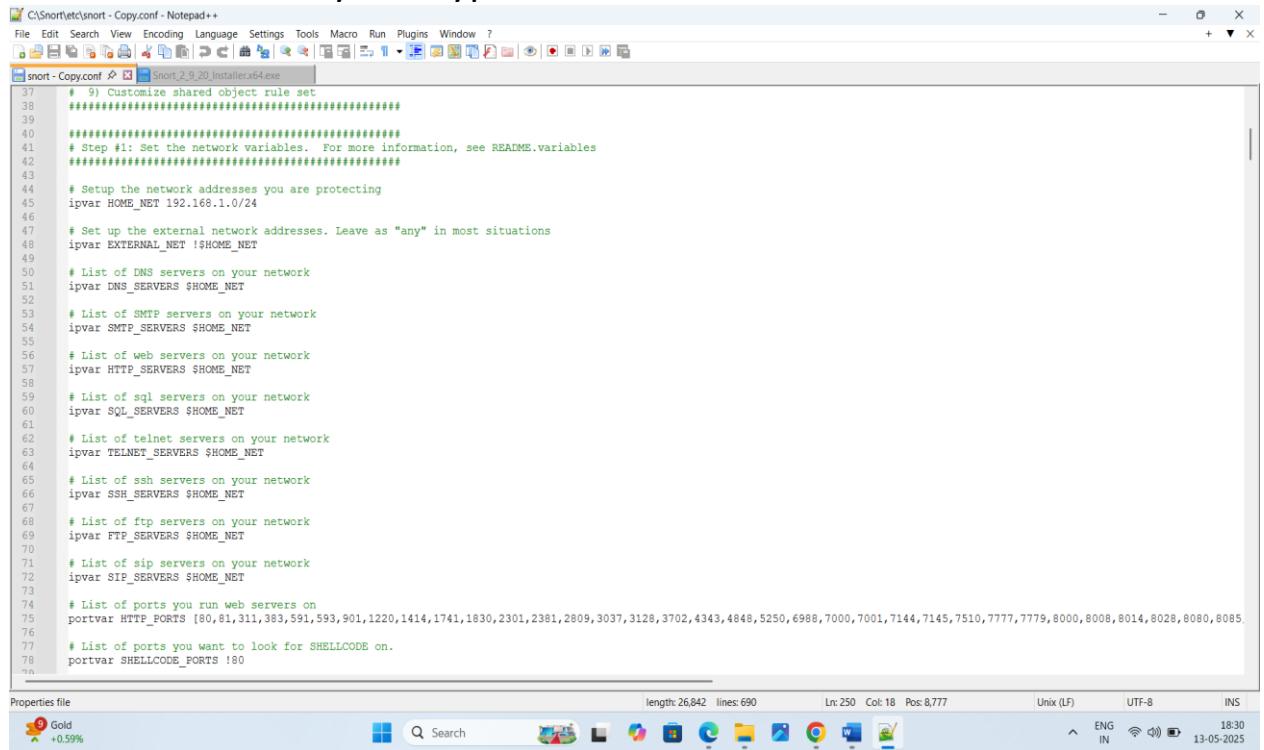
# GTP Control Channel Preprocessor. For more information, see README.GTP
#
```

Name : kunal Jawale

7. Make some few changes in steps

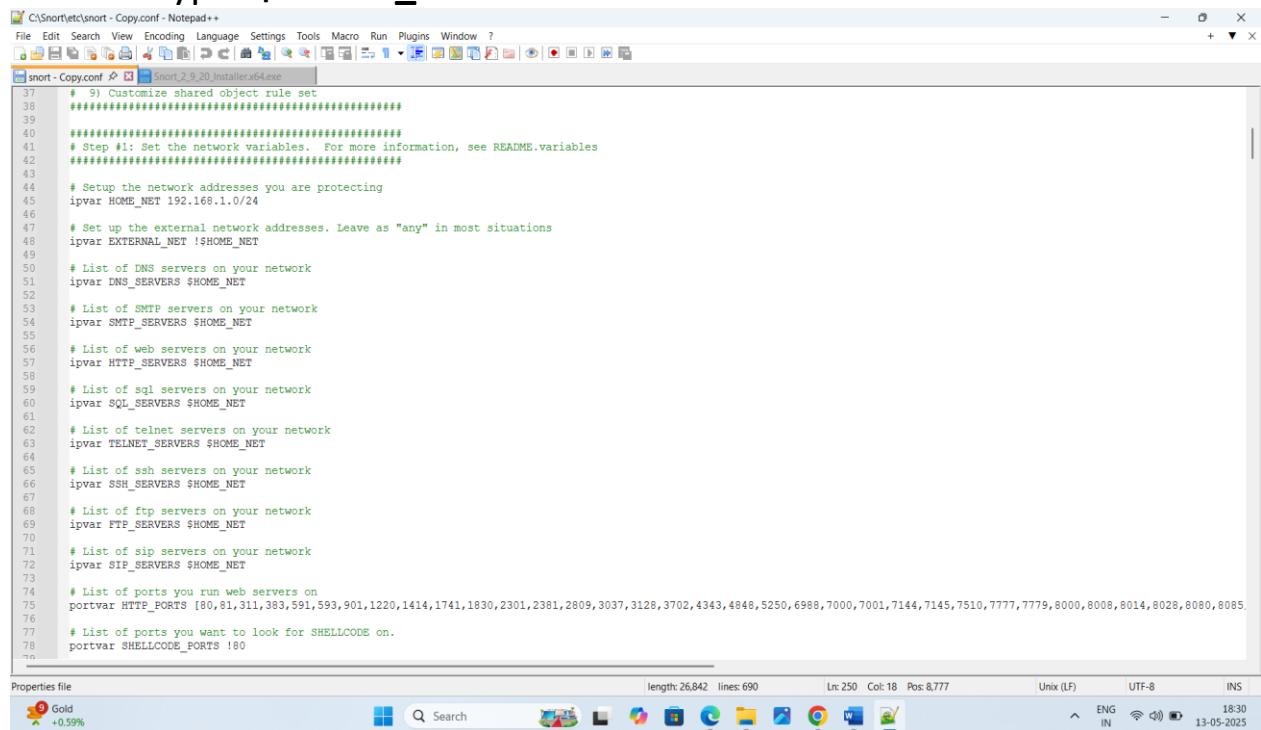
Step 1

45 line :remove any and type IP like 192.168.1.0/24



```
C:\Snort\etc\snort - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort - Copy.conf > Snort_2.9.20_installer\x64.exe
31 # 9) Customize shared object rule set
32 #####
33
34 #####
35 # Step #1: Set the network variables. For more information, see README.variables
36 #####
37
38 # Setup the network addresses you are protecting
39 ipvar HOME_NET 192.168.1.0/24
40
41 # Set up the external network addresses. Leave as "any" in most situations
42 ipvar EXTERNAL_NET !$HOME_NET
43
44 # List of DNS servers on your network
45 ipvar DNS_SERVERS $HOME_NET
46
47 # List of SMTP servers on your network
48 ipvar SMTP_SERVERS $HOME_NET
49
50 # List of web servers on your network
51 ipvar HTTP_SERVERS $HOME_NET
52
53 # List of sql servers on your network
54 ipvar SQL_SERVERS $HOME_NET
55
56 # List of telnet servers on your network
57 ipvar TELNET_SERVERS $HOME_NET
58
59 # List of ssh servers on your network
60 ipvar SSH_SERVERS $HOME_NET
61
62 # List of ftp servers on your network
63 ipvar FTP_SERVERS $HOME_NET
64
65 # List of sip servers on your network
66 ipvar SIP_SERVERS $HOME_NET
67
68 # List of ports you run web servers on
69 portvar HTTP_PORTS [80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000,8008,8014,8028,8080,8085,
70
71 # List of ports you want to look for SHELLCODE on.
72 portvar SHELLCODE_PORTS !80
73
74
75
76
77
78
79
79
Properties file length: 26,842 lines: 690 Ln: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS
Gold +0.59% 18:30 IN 13-05-2025
```

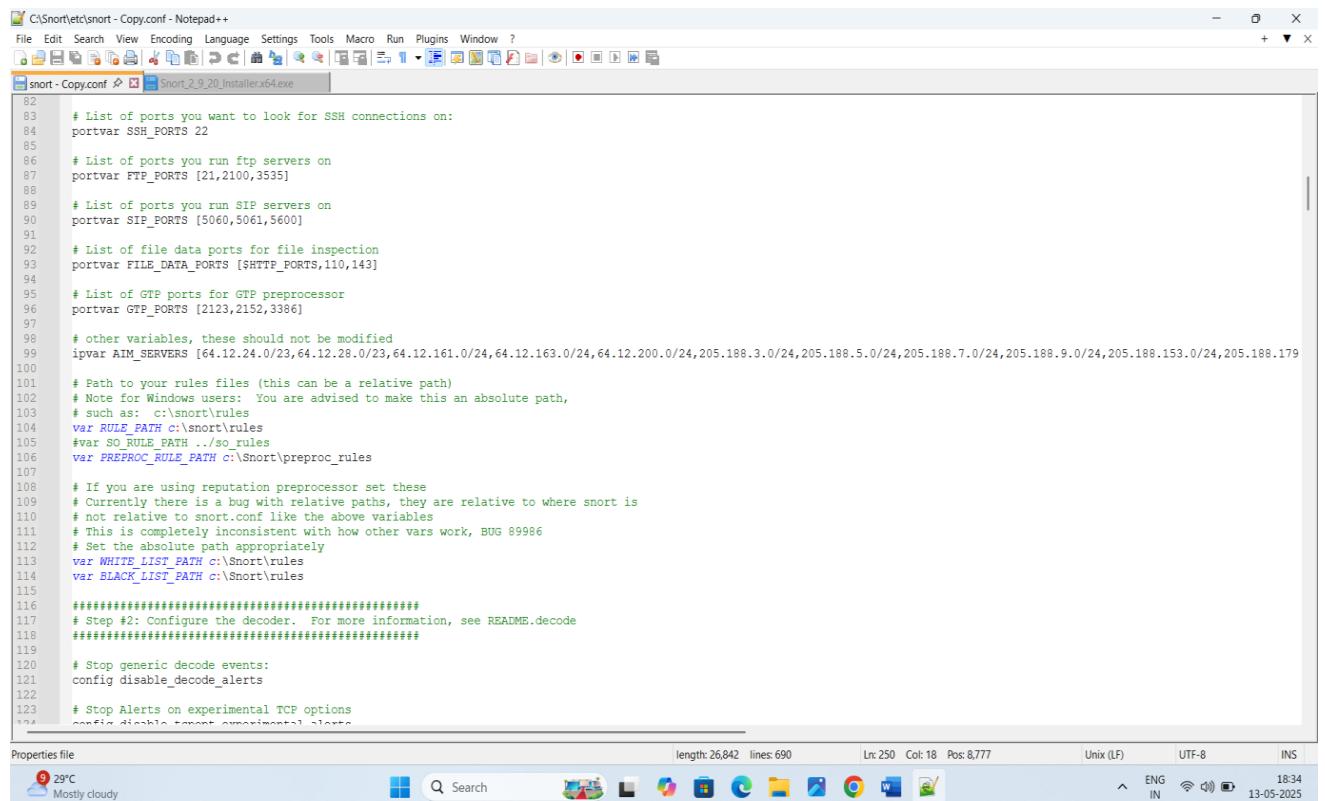
48 line : type !\$ Home_NET



```
C:\Snort\etc\snort - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort - Copy.conf > Snort_2.9.20_installer\x64.exe
37 # 9) Customize shared object rule set
38 #####
39
40 #####
41 # Step #1: Set the network variables. For more information, see README.variables
42 #####
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 192.168.1.0/24
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET !$HOME_NET
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS $HOME_NET
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of ssh servers on your network
66 ipvar SSH_SERVERS $HOME_NET
67
68 # List of ftp servers on your network
69 ipvar FTP_SERVERS $HOME_NET
70
71 # List of sip servers on your network
72 ipvar SIP_SERVERS $HOME_NET
73
74 # List of ports you run web servers on
75 portvar HTTP_PORTS [80,81,311,383,591,593,901,1220,1414,1741,1830,2301,2381,2809,3037,3128,3702,4343,4848,5250,6988,7000,7001,7144,7145,7510,7777,7779,8000,8008,8014,8028,8080,8085,
76
77 # List of ports you want to look for SHELLCODE on.
78 portvar SHELLCODE_PORTS !80
79
79
Properties file length: 26,842 lines: 690 Ln: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS
Gold +0.59% 18:30 IN 13-05-2025
```

104 line : remove rules and type C:\snort\rules

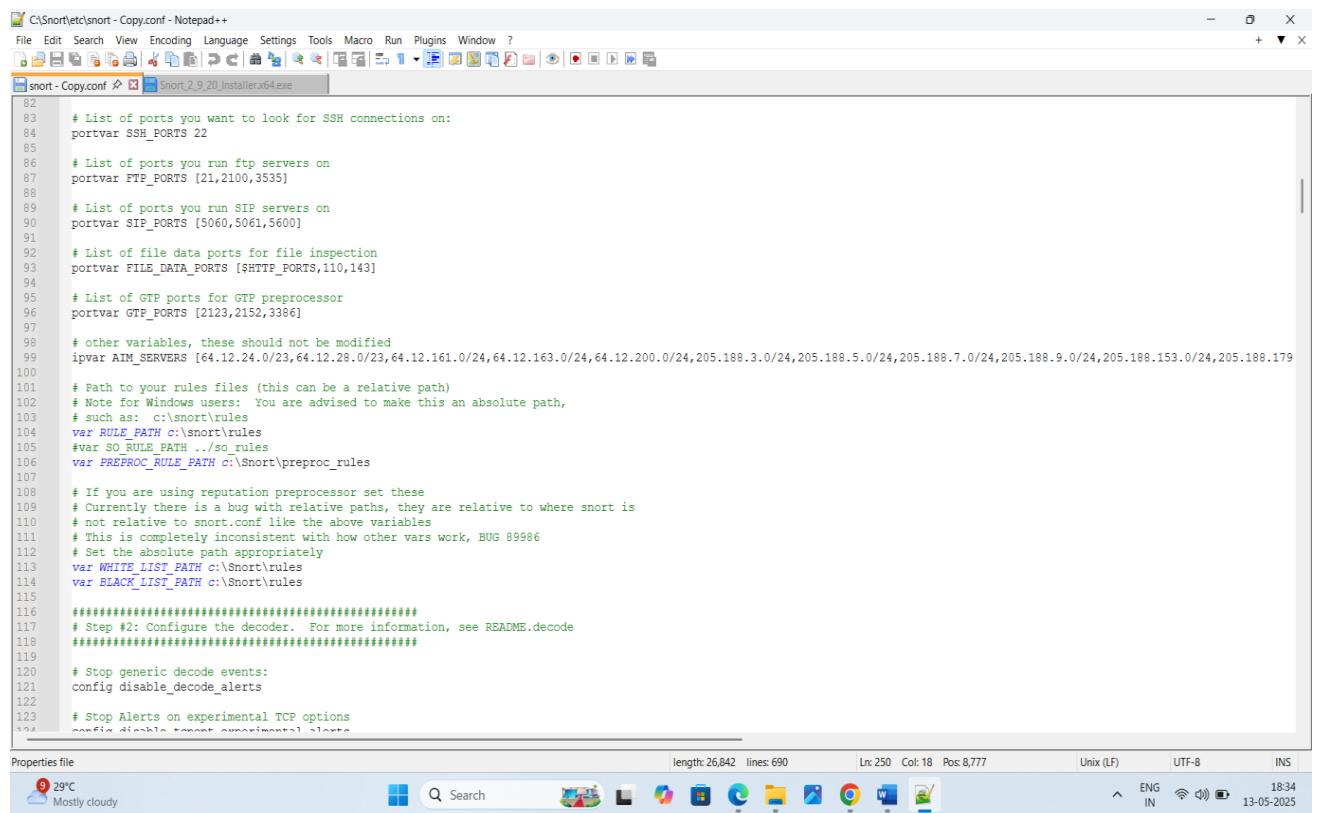
Name : kunal Jawale



The screenshot shows a Notepad+ window with the title "C:\Snort\etc\snort - Copy.conf - Notepad+". The file contains a Snort configuration script. Line 105 is highlighted with a red rectangle. The status bar at the bottom right shows "length: 26,842 lines: 690 Lr: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS". The taskbar at the bottom includes icons for File Explorer, Task View, Start, Taskbar settings, and several pinned applications.

```
82
83     # List of ports you want to look for SSH connections on:
84     portvar SSH_PORTS 22
85
86     # List of ports you run ftp servers on
87     portvar FTP_PORTS [21,2100,3535]
88
89     # List of ports you run SIP servers on
90     portvar SIP_PORTS [5060,5061,5600]
91
92     # List of file data ports for file inspection
93     portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95     # List of GTP ports for GTP preprocessor
96     portvar GTP_PORTS [2123,2152,3386]
97
98     # other variables, these should not be modified
99     ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179
100
101    # Path to your rules files (this can be a relative path)
102    # Note for Windows users: You are advised to make this an absolute path,
103    # such as: c:\snort\rules
104    var RULE_PATH c:\snort\rules
105    #var SO_RULE_PATH ..\so_rules
106    var PREPROC_RULE_PATH c:\snort\preproc_rules
107
108    # If you are using reputation preprocessor set these
109    # Currently there is a bug with relative paths, they are relative to where snort is
110    # not relative to snort.conf like the above variables
111    # This is completely inconsistent with how other vars work, BUG 89986
112    # Set the absolute path appropriately
113    var WHITE_LIST_PATH c:\Snort\rules
114    var BLACK_LIST_PATH c:\Snort\rules
115
116    ##### Step #2: Configure the decoder. For more information, see README.decode
117    # Step #2: Configure the decoder. For more information, see README.decode
118    #####
119
120    # Stop generic decode events:
121    config disable_decode_alerts
122
123    # Stop Alerts on experimental TCP options
124    config disable_expert_experimental_alerts
```

Line 105 : add # in front of the line like this



The screenshot shows a Notepad+ window with the title "C:\Snort\etc\snort - Copy.conf - Notepad+". The file content is identical to the previous screenshot, but line 105 has been modified. The status bar at the bottom right shows "length: 26,842 lines: 690 Lr: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS". The taskbar at the bottom includes icons for File Explorer, Task View, Start, Taskbar settings, and several pinned applications.

```
82
83     # List of ports you want to look for SSH connections on:
84     portvar SSH_PORTS 22
85
86     # List of ports you run ftp servers on
87     portvar FTP_PORTS [21,2100,3535]
88
89     # List of ports you run SIP servers on
90     portvar SIP_PORTS [5060,5061,5600]
91
92     # List of file data ports for file inspection
93     portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95     # List of GTP ports for GTP preprocessor
96     portvar GTP_PORTS [2123,2152,3386]
97
98     # other variables, these should not be modified
99     ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179
100
101    # Path to your rules files (this can be a relative path)
102    # Note for Windows users: You are advised to make this an absolute path,
103    # such as: c:\snort\rules
104    var RULE_PATH c:\snort\rules
105    #var SO_RULE_PATH ..\so_rules
106    var PREPROC_RULE_PATH c:\snort\preproc_rules
107
108    # If you are using reputation preprocessor set these
109    # Currently there is a bug with relative paths, they are relative to where snort is
110    # not relative to snort.conf like the above variables
111    # This is completely inconsistent with how other vars work, BUG 89986
112    # Set the absolute path appropriately
113    var WHITE_LIST_PATH c:\Snort\rules
114    var BLACK_LIST_PATH c:\Snort\rules
115
116    ##### Step #2: Configure the decoder. For more information, see README.decode
117    # Step #2: Configure the decoder. For more information, see README.decode
118    #####
119
120    # Stop generic decode events:
121    config disable_decode_alerts
122
123    # Stop Alerts on experimental TCP options
124    config disable_expert_experimental_alerts
```

106 line: type C:\snort\preproc_rules

Name : kunal Jawale

The screenshot shows a Notepad++ window with the file 'snort - Copy.conf' open. The code in the file is a Snort configuration script. It includes definitions for various ports (SSH_PORTS, FTP_PORTS, SIP_PORTS, FILE_DATA_PORTS, GTP_PORTS) and variables (RULE_PATH, SO_RULE_PATH, PREFPROC_RULE_PATH). It also contains sections for rule paths, decoder configuration, and alert suppression. The status bar at the bottom provides file statistics and system information.

```
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [SHTF_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH c:\snort\rules
105 var SO_RULE_PATH .../so_rules
106 var PREFPROC_RULE_PATH c:\snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH c:\snort\rules
114 var BLACK_LIST_PATH c:\snort\rules
115
116 ##### Step #2: Configure the decoder. For more information, see README.decode
117 ##### Step #2: Configure the decoder. For more information, see README.decode
118
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_expert_experimental_alerts
```

Properties file length: 26,842 lines: 690 Ln: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS

29°C Mostly cloudy Search ^ ENG IN 18:34 13-05-2025

Line 113 : type C:\snort\rules

Line 114 : C:\snort\rules

The screenshot shows a Notepad++ window with the file 'snort - Copy.conf' open. The code is identical to the previous screenshot, except for two lines that have been modified:

- Line 113: The original value 'c:\snort\rules' has been replaced by 'C:\snort\rules'.
- Line 114: The original value 'c:\snort\rules' has been replaced by 'C:\snort\rules'.

The status bar at the bottom provides file statistics and system information.

```
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [SHTF_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\snort\rules
105 var SO_RULE_PATH .../so_rules
106 var PREFPROC_RULE_PATH C:\snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 # Currently there is a bug with relative paths, they are relative to where snort is
110 # not relative to snort.conf like the above variables
111 # This is completely inconsistent with how other vars work, BUG 89986
112 # Set the absolute path appropriately
113 var WHITE_LIST_PATH C:\snort\rules
114 var BLACK_LIST_PATH C:\snort\rules
115
116 ##### Step #2: Configure the decoder. For more information, see README.decode
117 ##### Step #2: Configure the decoder. For more information, see README.decode
118
119
120 # Stop generic decode events:
121 config disable_decode_alerts
122
123 # Stop Alerts on experimental TCP options
124 config disable_expert_experimental_alerts
```

Properties file length: 26,842 lines: 690 Ln: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS

29°C Mostly cloudy Search ^ ENG IN 18:34 13-05-2025

Name : kunal Jawale

Step 2 : configure decoder

186 line : remove # from front of the line and add C:\snort\rules

```
C:\Snort\etc\snort - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort - Copy.conf Snort_2.9.20_Installer64.exe
166 # <var> ::= arbitrary <name><value passed to DAQ
167 # <dir> ::= path as to where to look for DAQ module so's
168
169 # Configure specific UID and GID to run snort as after dropping privs. For more information see snort -h command line options
170 #
171 # config set_gid:
172 # config set_uid:
173
174 # Configure default snaplen. Snort defaults to MTU of in use interface. For more information see README
175 #
176 # config snaplen:
177 #
178
179 # Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
180 #
181 # config bpf_file:
182 #
183
184 # Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
185 #
186 config logdir:c:\Snort\log
187
188 #####
189 # Step #3: Configure the base detection engine. For more information, see README.decode
190 #####
191
192 # Configure PCRE match limitations
193 config pcre_match_limit: 3500
194 config pcre_match_limit_recursion: 1500
195
196 # Configure the detection engine See the Snort Manual, Configuring Snort - Includes - Config
197 config detection: search-method ac-split search-optimize max-pattern-len 20
198
199 # Configure the event queue. For more information, see README.event_queue
200 config event_queue: max_queue 8 log 5 order_events content_length
201
202 #####
203 ## Configure GTP if it is to be used.
204 ## For more information, see README.GTP
205 #####
206
207 # config enable_gtp
208
209
Properties file length: 26,842 lines: 690 Ln: 250 Col: 18 Pos: 8,777 Unix (LF) UTF-8 INS
29°C Mostly cloudy Search 18:40 ENG IN 13-05-2025
```

Step 3 : same as it is

Step 4 :

247 line : "dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor/

250 line : dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll

253 line : add # in front of the line

```
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

Step 5 : configure processor

In etc folder make some few changes like copy blacklists rules rename with whiterules and paste In same directory

Line 511 : whitelist \$WHITE_LIST_PATH/whitelist.rules, \

Name : kunal Jawale

Line 512: blacklist \$BLACK_LIST_PATH/blacklist.rules

C:\Snort\etc\snort - Copy.conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

snort - Copy.conf > Snort_2.9.20_installer.x64.exe

```
487     bitenc_decode_depth 0 \
488     uu_decode_depth 0
489
490 # POP preprocessor. For more information see README.pop
491 preprocessor pop: \
492     ports { 110 } \
493     b64_decode_depth 0 \
494     qp_decode_depth 0 \
495     bitenc_decode_depth 0 \
496     uu_decode_depth 0
497
498 # Modbus preprocessor. For more information see README.modbus
499 preprocessor modbus: ports { 502 }
500
501 # DNP3 preprocessor. For more information see README.dnp3
502 preprocessor dnp3: ports { 20000 } \
503     memcap 262144 \
504     check_crc
505
506 # Reputation preprocessor. For more information see README.reputation
507 preprocessor reputation: \
508     memcap 500, \
509     priority whitelist, \
510     nested_ip inner, \
511     whitelist $WHITE_LIST_PATH/whitelist.rules, \
512     blacklist $BLACK_LIST_PATH/blacklist.rules
513
514 ##### Step #6: Configure output plugins
515 # Step #6: Configure output plugins
516 # For more information, see Snort Manual, Configuring Snort - Output Modules
517 #####
518
519 # unified2
520 # Recommended for most installs
521 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
522
523 # Additional configuration for specific types of installs
524 # output alert_unified2: filename snort.alert, limit 128, nostamp
525 # output log_unified2: filename snort.log, limit 128, nostamp
526
527 # syslog
528 # output alert_syslog: LOG_AUTH LOG_ALERT
```

Properties file

length: 26,842 lines: 690 Ln: 512 Col: 47 Pos: 20,609 Unix (LF) UTF-8 IN

29°C Mostly cloudy

Search

18:51 13-05-2025

Step 6 : configure output plugins

Same as it is

Step 7 :

From 546 line to 662 line remove / and add \ this

Properties file

29°C Mostly cloudy

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

snort - Copy.conf Notepad++

snort - Copy.conf C:\Snort\etc\snort - Copy.conf - Notepad++

```
544
545 # site specific rules
546
547 include $RULE_PATH\local.rules
548
549 include $RULE_PATH\app-detect.rules
550 include $RULE_PATH\attack-recon.rules
551 include $RULE_PATH\http-traffic.rules
552 include $RULE_PATH\blacklist.rules
553 include $RULE_PATH\botnet.rules
554 include $RULE_PATH\browser-chrome.rules
555 include $RULE_PATH\browser-firefox.rules
556 include $RULE_PATH\browser-ie.rules
557 include $RULE_PATH\browser-plugins.rules
558 include $RULE_PATH\browser-webkit.rules
559 include $RULE_PATH\chat.rules
560 include $RULE_PATH\client-side-place.rules
561 include $RULE_PATH\dos.rules
562 include $RULE_PATH\dns.rules
563 include $RULE_PATH\file-arc.rules
564 include $RULE_PATH\file-evil.rules
565 include $RULE_PATH\file-exploit-kit.rules
566 include $RULE_PATH\file-exploit.rules
567 include $RULE_PATH\file-fingerprint.rules
568 include $RULE_PATH\file-flash.rules
569 include $RULE_PATH\file-identify.rules
570 include $RULE_PATH\file-image.rules
571 include $RULE_PATH\file-malware.rules
572 include $RULE_PATH\file-office.rules
573 include $RULE_PATH\file-other.rules
574 include $RULE_PATH\file-p2p.rules
575 include $RULE_PATH\file-pcap.rules
576 include $RULE_PATH\file-finger.rules
577 include $RULE_PATH\http.rules
578 include $RULE_PATH\http-info.rules
579 include $RULE_PATH\http-amp.rules
580 include $RULE_PATH\imap.rules
581 include $RULE_PATH\indicator-compromise.rules
582 include $RULE_PATH\indicator-obfuscation.rules
583 include $RULE_PATH\malware-shellcode.rules
584 include $RULE_PATH\info.rules
585 include $RULE_PATH\malware-backdoor.rules
586
587
```

Name : kunal Jawale

Step 8

Remove # from line

659,660 and 661

C:\Snort\etc\snort - Copy.conf - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

snort - Copy.conf snort_2.9.20_installerx64.exe

```
631 include $RULE_PATH\server-webapp.rules
632 include $RULE_PATH\shellcode.rules
633 include $RULE_PATH\smtp.rules
634 include $RULE_PATH\snmp.rules
635 include $RULE_PATH\specific-threats.rules
636 include $RULE_PATH\spyware-put.rules
637 include $RULE_PATH\sql.rules
638 include $RULE_PATH\telnet.rules
639 include $RULE_PATH\tftp.rules
640 include $RULE_PATH\virus.rules
641 include $RULE_PATH\voip.rules
642 include $RULE_PATH\web-activex.rules
643 include $RULE_PATH\web-attacks.rules
644 include $RULE_PATH\web-cgi.rules
645 include $RULE_PATH\web-client.rules
646 include $RULE_PATH\web-coldfusion.rules
647 include $RULE_PATH\web-frontpage.rules
648 include $RULE_PATH\web-iis.rules
649 include $RULE_PATH\web-misc.rules
650 include $RULE_PATH\web-php.rules
651 include $RULE_PATH\xml.rules
652
653 #####
654 # Step #8: Customize your preprocessor and decoder alerts
655 # For more information, see README.decoder_preproc_rules
656 #####
657
658 # decoder and preprocessor event rules
659 include $PREPROC_RULE_PATH\preprocessor.rules
660 include $PREPROC_RULE_PATH\decoder.rules
661 include $PREPROC_RULE_PATH\sensitive-data.rules
662
663 #####
664 # Step #9: Customize your Shared Object Snort Rules
665 # For more information, see http://vrt-blog.snort.org/2009/01/using-vrt-certified-shared-object-rules.html
666 #####
667
668 # dynamic library rules
669 # include $SO_RULE_PATH\bad-traffic.rules
670 # include $SO_RULE_PATH\chat.rules
671 # include $SO_RULE_PATH\dos.rules
672 # include $SO_RULE_PATH\exploit.rules
673 # include $SO_RULE_PATH\icmp.rules
```

Here we done the configuration of snort

8. Now open the CMD and go to snort directory using cd snort

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following text:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd ..
C:\Windows>cd snort
C:\Snort>
```

The desktop background is visible behind the window, showing a dark blue gradient. At the bottom of the screen, the taskbar displays the Start button, a search bar with the word "Search", and icons for various pinned applications including File Explorer, Edge, and File History. On the far right of the taskbar, there are system status icons for battery level (8%), temperature (27°C), cloudiness (Mostly cloudy), signal strength, and network connection. The date and time (13-05-2025) are also shown. The system tray at the bottom right includes icons for volume, brightness, and power.

Name : kunal Jawale

9. Go in snort/ bin directory

```
C:\Administrator: Command Prompt
Volume Serial Number is 749E-50E7

Directory of C:\Snort

01-05-2025 16:10 <DIR> .
01-05-2025 16:10 <DIR> bin
01-05-2025 16:10 <DIR> doc
02-05-2025 16:59 <DIR> etc
01-05-2025 16:10 <DIR> lib
04-05-2025 17:06 <DIR> log
01-05-2025 16:10 <DIR> preproc_rules
02-05-2025 15:33 <DIR> rules
01-05-2025 16:10 52,666 Uninstall.exe
1 File(s) 52,666 bytes
8 Dir(s) 132,889,739,264 bytes free

C:\Snort>cd bin

C:\Snort\bin>dir
Volume in drive C is Windows
Volume Serial Number is 749E-50E7

Directory of C:\Snort\bin

01-05-2025 16:10 <DIR> .
01-05-2025 16:10 <DIR> ..
20-04-2022 19:45 54,784 npptools.dll
20-04-2022 19:45 274,489 ntwdllib.dll
20-04-2022 19:45 36,948 Packet.dll
20-04-2022 19:45 94,208 pcre.dll
24-05-2022 10:21 1,559,552 snort.exe
20-04-2022 19:45 53,326 WanPacket.dll
20-04-2022 19:45 208,974 wpcap.dll
20-04-2022 19:45 73,728 zlib1.dll
8 File(s) 2,356,009 bytes
2 Dir(s) 132,888,068,096 bytes free

C:\Snort\bin>snort -V

,,_ -> Snort! <*-
o" )~ Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

C:\Snort\bin>
```

10. After coming the directory type

Snort -V to check version

```
C:\Administrator: Command Prompt
Volume Serial Number is 749E-50E7

Directory of C:\Snort

01-05-2025 16:10 <DIR> .
01-05-2025 16:10 <DIR> ..
20-04-2022 19:45 54,784 npptools.dll
20-04-2022 19:45 274,489 ntwdllib.dll
20-04-2022 19:45 36,948 Packet.dll
20-04-2022 19:45 94,208 pcre.dll
24-05-2022 10:21 1,559,552 snort.exe
20-04-2022 19:45 53,326 WanPacket.dll
20-04-2022 19:45 208,974 wpcap.dll
20-04-2022 19:45 73,728 zlib1.dll
8 File(s) 2,356,009 bytes
2 Dir(s) 132,888,068,096 bytes free

C:\Snort\bin>snort -V

,,_ -> Snort! <*-
o" )~ Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

C:\Snort\bin>snort -W

Index Physical Address IP Address Device Name Description
----- -----
1 00:00:00:00:00:00 disabled \Device\NPF_{5D5C4D9-A8B8-4B08-B5D2-81FB146A9C5} WAN Miniport (IPv6)
2 00:00:00:00:00:00 disabled \Device\NPF_{F9EB7BE-5199-4FD8-BD00-1BFDB1641259} WAN Miniport (IP)
3 00:00:00:00:00:00 disabled \Device\NPF_{8E8A4C5D-BFDD-4301-B659-6E2A358ACB00} WAN Miniport (Network Monitor)
4 CC-47:40:CA:88:EF 169.254.162.174 \Device\NPF_{3C0154CF-0001-4A46-A8B8-9483D812767C} Bluetooth Device (Personal Area Network)
5 CC-47:40:CA:88:EF 192.168.1.75.150 \Device\NPF_{E255EE51-0A23-41E6-AF72-F94DC0386F58} Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
6 00:50:56:00:00:08 192.168.248.1 \Device\NPF_{D60CF23D-E71A-4F4E-9018-D1FFEA0E2026} VMware Virtual Ethernet Adapter for VMnet8
7 00:50:56:00:00:01 192.168.126.1 \Device\NPF_{BD00A5A0-C38E-4BF9-955E-ASCFC900C36E} VMware Virtual Ethernet Adapter for VMnet1
8 C2:47:40:CA:88:EE 169.254.176.222 \Device\NPF_{A81A15B8-3242-4B51-A4CA-2E5F2531AF81} Microsoft Wi-Fi Direct Virtual Adapter #3
9 CE:47:40:CA:88:EE 169.254.70.219 \Device\NPF_{9FD364FB-FFF4-4BE8-8970-6CC40C75C61} Microsoft Wi-Fi Direct Virtual Adapter
10 00:00:00:00:00:00 0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture

C:\Snort\bin>
```

Name : kunal Jawale

11. Snort -w to check interface

```
C:\> Administrator: Command Prompt
01-05-2025 16:10 <DIR> .
01-05-2025 16:10 <DIR> ..
20-04-2022 19:45 54,784 npptools.dll
20-04-2022 19:45 274,489 ntwdblib.dll
20-04-2022 19:45 36,948 Packet.dll
20-04-2022 19:45 94,208 pcre.dll
24-05-2022 10:21 1,559,552 snort.exe
20-04-2022 19:45 53,326 WanPacket.dll
20-04-2022 19:45 208,974 wpcap.dll
20-04-2022 19:45 73,728 zlib1.dll
8 File(s) 2,356,009 bytes
2 Dir(s) 132,888,068,096 bytes free

C:\>Snort\bin>snort -V
```
-*> Snort! <*-

o")~ Version 2.9.20-WIN64 GRE (Build 82)

... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team

Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.

Copyright (C) 1998-2013 Sourcefire, Inc., et al.

Using PCRE version: 8.10 2010-06-25

Using ZLIB version: 1.2.11

C:\>Snort\bin>snort -W
```
-*> Snort! <*-  

o" )~ Version 2.9.20-WIN64 GRE (Build 82)  

... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  

Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.  

Copyright (C) 1998-2013 Sourcefire, Inc., et al.  

Using PCRE version: 8.10 2010-06-25  

Using ZLIB version: 1.2.11

Index Physical Address IP Address Device Name Description
-----  

1 00:00:00:00:00:00 disabled \Device\NPF_{5DF5CA09-A888-4B08-B5D2-81FB146AB9C5} WAN Miniport (IPv6)
2 00:00:00:00:00:00 disabled \Device\NPF_{F9E87BEE-5199-4FD8-BD00-1BF01641259} WAN Miniport (IP)
3 00:00:00:00:00:00 disabled \Device\NPF_{8EA84C5D-BFD0-4301-B659-6E2A35BAC8D8} WAN Miniport (Network Monitor)
4 CC:47:40:CA:88:EF 169.254.162.174 \Device\NPF_{3C815ACF-00D1-4446-ABBB-9483D812767C} Bluetooth Device (Personal Area Network)
5 CC:47:40:CA:88:EE 192.168.175.150 \Device\NPF_{E255E551-0423-4256-AF72-F94DX8286F58} Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
6 00:50:56:00:00:08 192.168.248.1 \Device\NPF_{D606FA30-E71A-4F4E-9018-D41FE40E2026} VMware Virtual Ethernet Adapter for VMnet8
7 00:50:56:00:00:01 192.168.126.1 \Device\NPF_{B000A5A0-C38E-4BFF-955E-A5CCF980DC36E} VMware Virtual Ethernet Adapter for VMnet1
8 C2:47:40:CA:88:EE 169.254.176.222 \Device\NPF_{A81A15B8-3242-4B51-A4CA-2E5F2531AF81} Microsoft Wi-Fi Direct Virtual Adapter #3
9 CE:47:40:CA:88:EE 169.254.70.219 \Device\NPF_{F0364FB-FFFF-4B8E-8970-6C40C735C61} Microsoft Wi-Fi Direct Virtual Adapter
10 00:00:00:00:00:00 0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback Adapter for loopback traffic capture

C:\>Snort\bin>
```

27°C Mostly cloudy ENG IN 19:05 13-05-2025

12. snort -i 2 -c c:\Snort\etc\snort.conf -T this is for testing snort configuration

```
C:\> Administrator: Command Prompt
Used Memory : 0
No of Allocs : 0
No of Frees : 0
IMAP Config
Used Memory : 1379
No of Allocs : 3
No of Frees : 48
Total memory used : 1379

Heap Statistics of imap:
Total Statistics:
Memory in use: 1379 bytes
No of allocs: 3
No of frees: 48
Config Statistics:
Memory in use: 1379 bytes
No of allocs: 3
No of frees: 48
=====
Memory Statistics for File at:Tue May 13 19:08:31 2025
Total buffers allocated: 0
Total buffers freed: 0
Total buffers released: 0
Total file mempool: 0
Total allocated file mempool: 0
Total freed file mempool: 0
Total released file mempool: 0

Heap Statistics of file:
Total Statistics:
Memory in use: 280 bytes
No of allocs: 6
No of frees: 1
Session Statistics:
Memory in use: 0 bytes
No of allocs: 1
No of frees: 1
Mempool Statistics:
Memory in use: 280 bytes
No of allocs: 5
No of frees: 0
=====

Snort exiting
C:\>Snort\bin>
C:\>Snort\bin>
C:\>Snort\bin>snort.exe -i5 -c "c:\snort\etc\snort - Copy.conf" -T
```

27°C Mostly cloudy ENG IN 19:08 13-05-2025

Name : kunal Jawale

13. snort -i 2 -c c:\Snort\etc\snort.conf -A console monitoring mode

```
Administrator: Command Prompt
[ State Density      : 68.3%
  Patterns          : 10772
  Match States      : 11666
  Memory (MB)       : 162.28
    Patterns        : 1.26
    Match Lists     : 2.85
  DFA
    1 byte states   : 1.25
    2 byte states   : 19.06
    4 byte states   : 137.47
  -----
  [ Number of patterns truncated to 20 bytes: 651 ]
MaxRSS at the end of detection rules:301347120
pcap DAQ configured to passive.
The DAO version does not support reload.
Acquiring network traffic from "Device\NPf_{E255EE51-0A23-43E6-AF72-F94DC0386F58}".

    === Initialization Complete ===

o`--> Snort! <-
    Version 2.9.20-WIN64 GRE (Build 82)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2010-06-25
    Using ZLIB version: 1.2.11

    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2.0 <Build 1>
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>
    Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
    Preprocessor Object: SF_STP Version 1.1 <Build 1>
    Preprocessor Object: SF_SDP Version 1.1 <Build 1>
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
    Preprocessor Object: SF_POP Version 1.0 <Build 1>
    Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>

Total snort Fixed Memory Cost - MaxRSS:874394272
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>snort.exe -i5 -c "c:\snort\etc\snort - Copy.conf" -A
27°C Mostly cloudy Search ENG IN 19:09 13-05-2025
```

```
Administrator: Command Prompt
Total snort Fixed Memory Cost - MaxRSS:874394272
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>snort.exe -i5 -c "c:\snort\etc\snort - Copy.conf" -A
snort.exe: option requires an argument -- A
o`--> Snort! <-
    Version 2.9.20-WIN64 GRE (Build 82)
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
    Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.
    Using PCRE version: 8.10 2010-06-25
    Using ZLIB version: 1.2.11

USAGE: snort.exe [-options] <filter options>
snort.exe /SERVICE /INSTALL [-options] <filter options>
snort.exe /SERVICE /UNINSTALL
snort.exe /SERVICE /SHOW

Options:
  -A      Set alert mode: fast, full, console, test or none (alert file alerts only)
  -b      Log packets in tcpdump format (much faster)
  -B <mask> Obfuscates IP addresses in alerts and packet dumps using CIDR mask
  -c <rules> Use Rules file <rules>
  -C      Print out payloads with character data only (no hex)
  -d      Dump the Application layer
  -e      Display the second layer header info
  -E      Log alert messages to NT Eventlog. (Win32 only)
  -f      Turn off flush() calls after binary log writes
  -F <bpf> Create binary log files from file <bpf>
  -G <oxid> Log Identifier (to uniquely id events for multiple snorts)
  -h <hn>  Set home network = <hn>
            (for use with -l or -B, does NOT change $HOME_NET in IDS mode)
  -H      Make hash tables deterministic.
  -i <if> Listen on interface <if>
  -I      Add Interface name to alert output
  -k <mode> Checksum mode (all,noip,notcp,noudp,noicmp,none)
  -K <mode> Logging mode (pcap[default],ascii,none)
  -l <ld>  Log to directory <ld>
  -L <file> Log to this tcpdump file
  -n <cnt> Exit after receiving <cnt> packets
  -N      Turn off logging (alerts still work)
  -O      Obfuscate the logged IP addresses
  -P      Disable promiscuous mode sniffing
  -P <snap> Set explicit snapshot of packet (default: 1514)
  -q      Quiet. Don't show banner and status report
  -r <tff> Read and process tcpdump file <tff>
  -R <id>  Include 'id' in snort_intf<id>.pid file name

File Edit View
CCNA.txt CCNA.txt references.b CCNA.txt ms office de Snc + - x
File c:\Snort\bin
snort -V to check version
snort -W to check Interface
snort -i 2 -c c:\Snort\etc\snort.conf -T this is for testing snort configuration
snort -i 2 -c c:\Snort\etc\snort.conf -A console monitoring mode

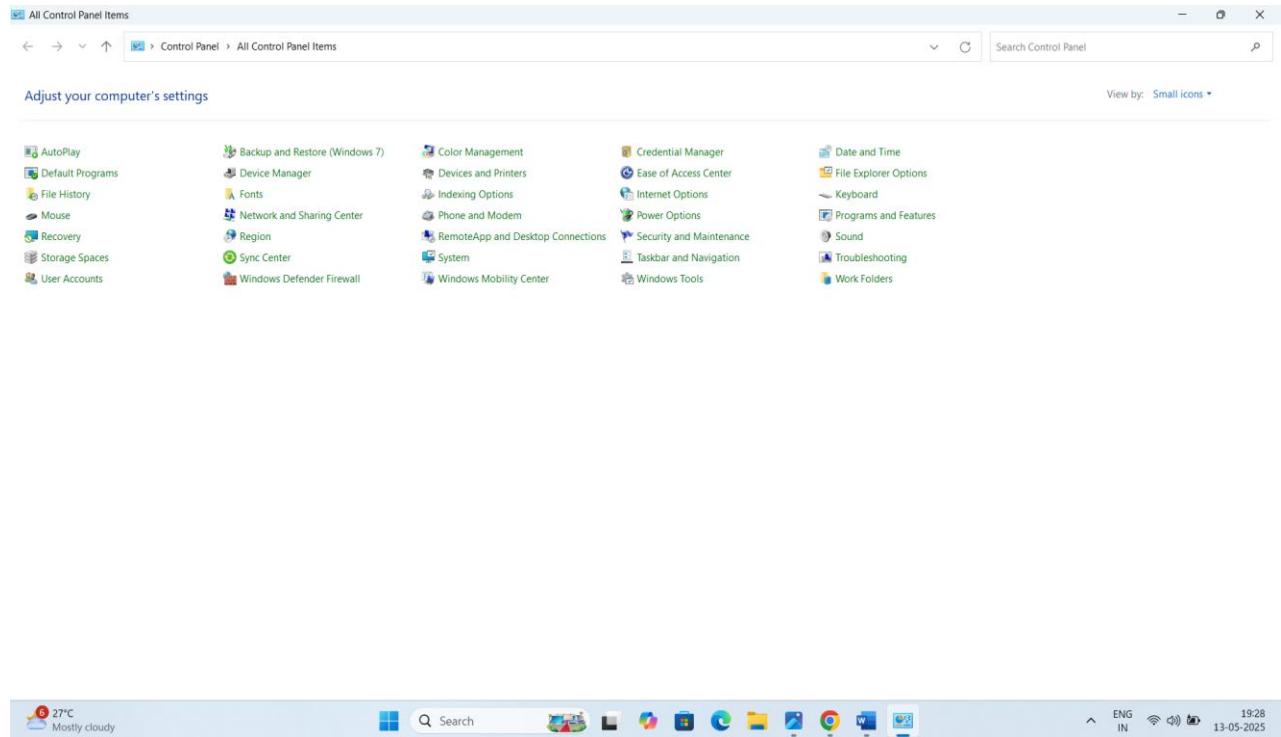
Ln 1, Col 1 433 characters 100% Windows (CRLF) UTF-8
27°C Mostly cloudy Search ENG IN 19:09 13-05-2025
```

Start snort successfully

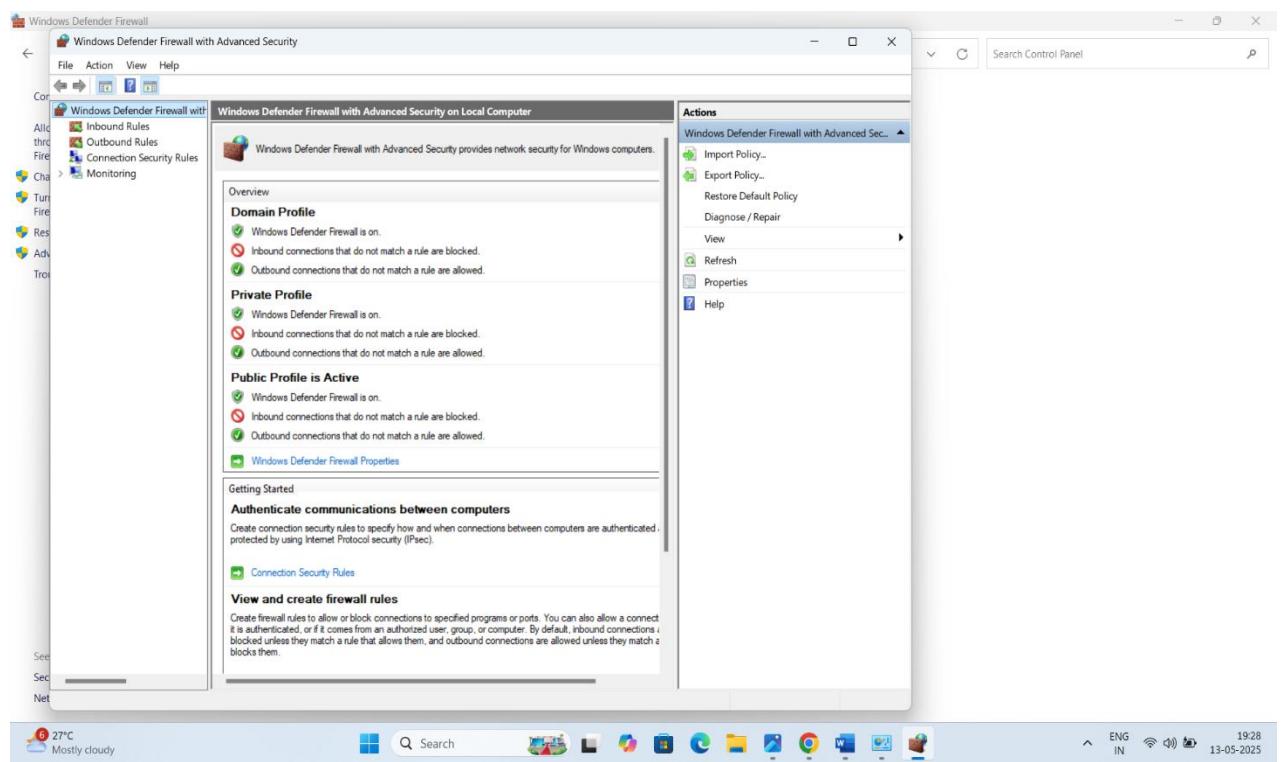
Name : kunal Jawale

Firewall : Windows Defender firewall

Step 1 : open windows firewall using control panel

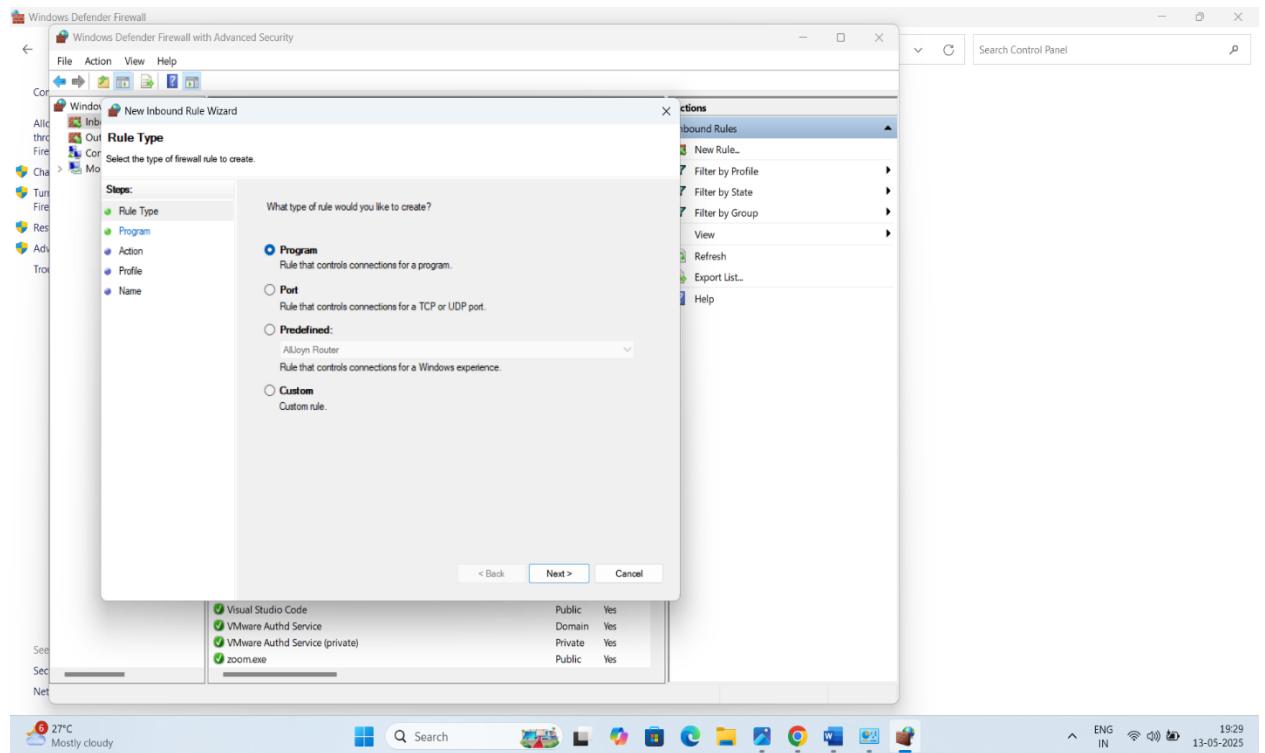


Step 2 : go to advance setting



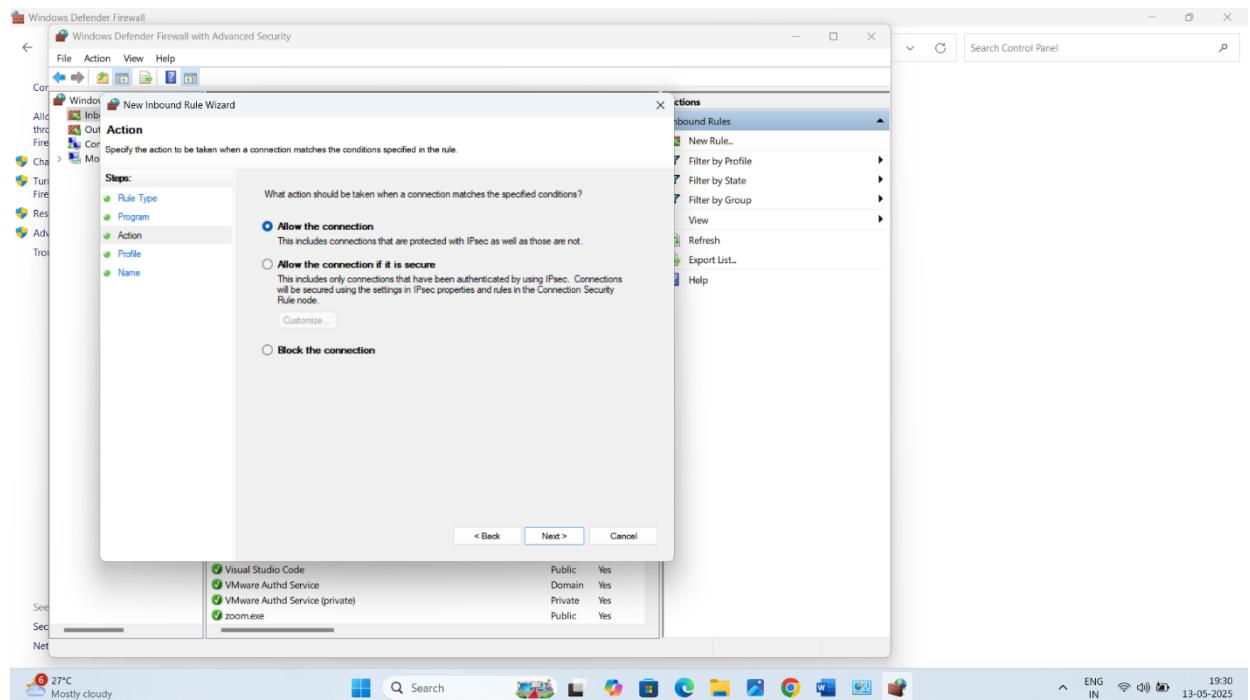
Name : kunal Jawale

Step 3 :click on inbound rules and select program and click on next



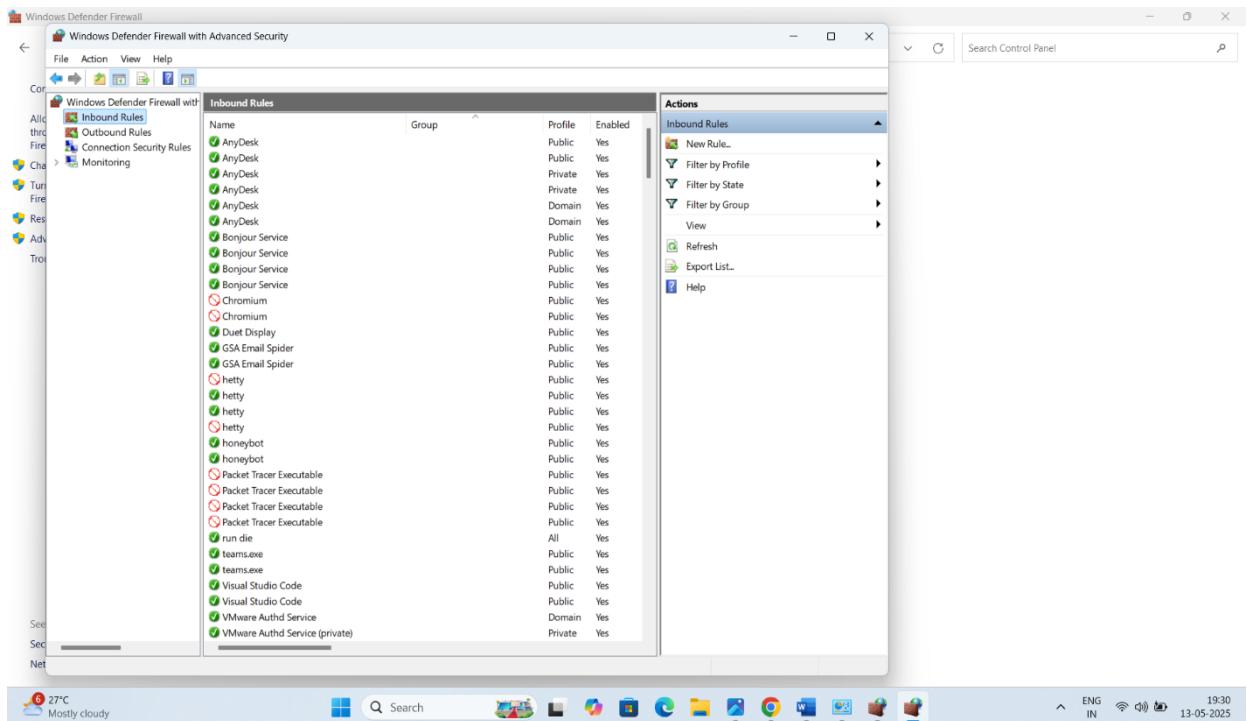
Step 4 : give a file path which you want and hit next

Step 5 : after giving a file path take a action what you want block or allow



Name : kunal Jawale

Here we see a rule create



Done.

In this process same we use for set outbound rules

If you want to change port rules go for ports

➤ ZoneAlarm

ZoneAlarm: Firewall and Antivirus Software Suite

⌚ What is ZoneAlarm?

- **ZoneAlarm** is a security software suite developed by **Check Point Software Technologies**.
- It primarily functions as a **personal firewall**, but it also includes:
 - **Antivirus protection**
 - **Anti-phishing**
 - **Anti-spyware**

- **Ransomware protection**
- **Web security**

ZoneAlarm is designed to **protect personal computers and small networks** from cyber threats, unauthorized access, and malicious software.



Key Features of ZoneAlarm:

1. Firewall Protection:

- Monitors incoming and outgoing network traffic.
- Uses a **Two-Way Firewall**:
 - **Inbound Protection**: Prevents unauthorized access to your computer.
 - **Outbound Protection**: Stops malware from sending data out to attackers.

2. Stealth Mode:

- Makes your PC invisible to hackers by blocking pings and port scans.
- Prevents network discovery and reduces attack vectors.

3. Application Control:

- Monitors applications trying to access the internet.
- Prompts the user to **allow or deny** connections.
- Prevents **zero-day attacks** by controlling untrusted software.

4. Advanced Firewall (OSFirewall):

- Monitors not just the network but also system behaviors.
- Detects suspicious changes to your OS, registry, and critical files.

5. Real-Time Antivirus & Anti-Spyware:

- Scans and removes viruses, spyware, Trojans, and worms.
- Updates automatically with new threat signatures.

6. Anti-Phishing and Web Security:

- Blocks malicious websites and phishing attempts.
- Prevents access to fake websites that steal personal information.

7. Identity Protection Services:

- Monitors your personal information and alerts you if it is exposed.
- Includes features for credit monitoring and fraud alerting.

8. Ransomware Protection:

- Real-time protection against ransomware attacks.
- Monitors suspicious encryption behavior and stops it before damage occurs.

How ZoneAlarm Works:

1. Traffic Monitoring:

- Monitors all network traffic entering and leaving your computer.

2. Behavior Analysis:

- Observes software behavior and detects suspicious activities.

3. Blocking Threats:

- Blocks unauthorized attempts to access your device.
- Alerts you when unknown applications attempt to connect to the network.

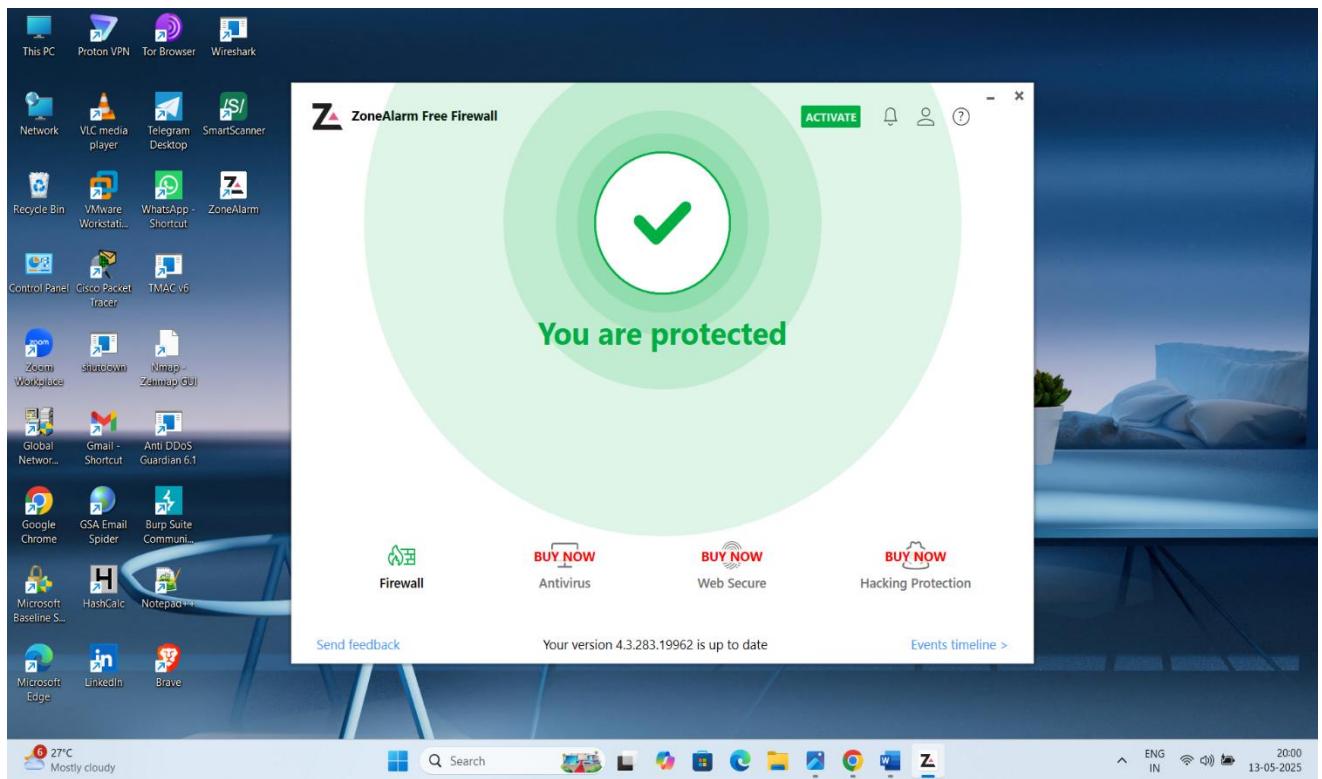
4. Sandboxing Technology:

- Isolates suspicious applications to prevent them from causing harm.
-

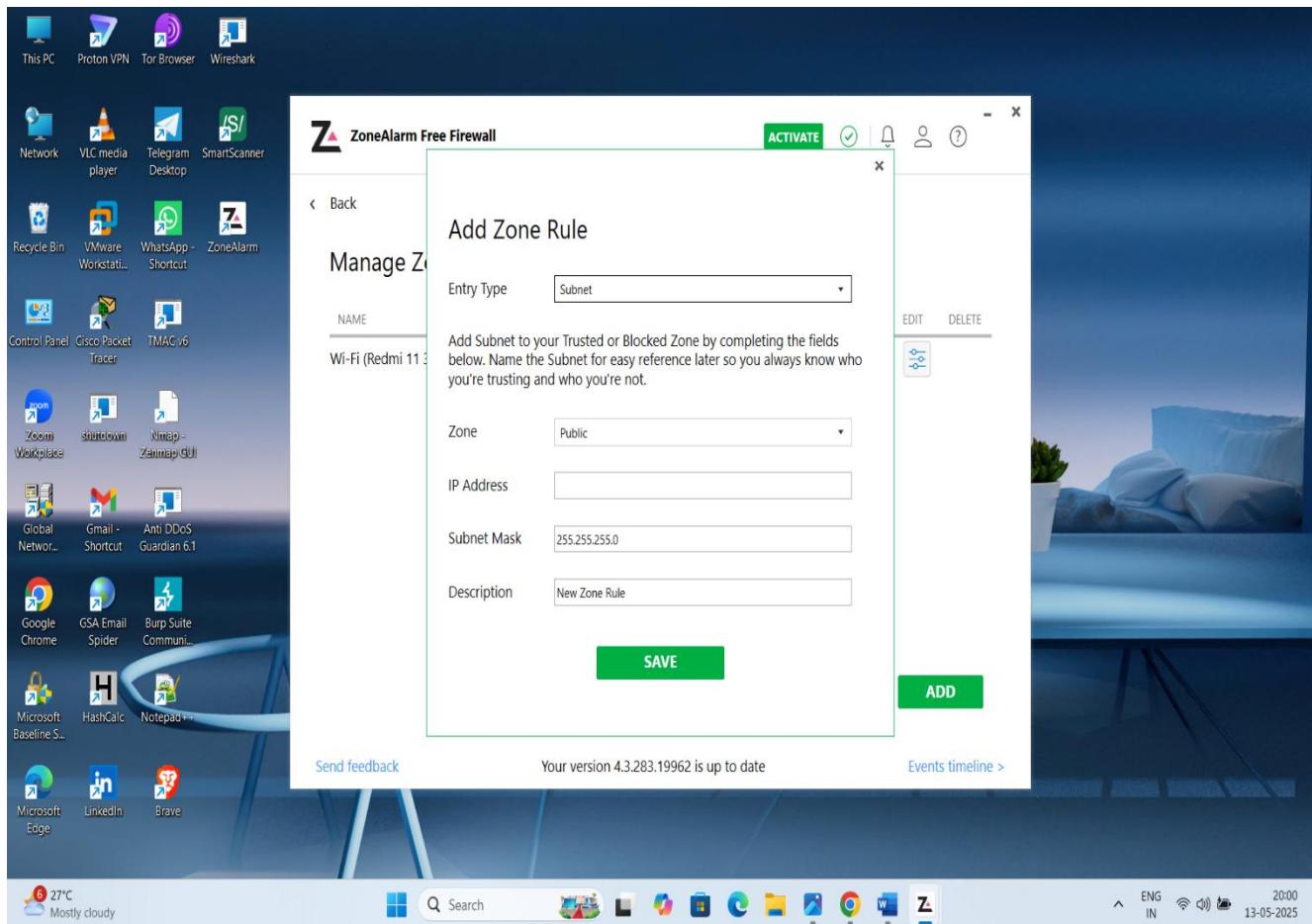
Why ZoneAlarm is Important for CEH (Certified Ethical Hacker):

- Ethical hackers need to understand how **personal firewalls** like ZoneAlarm:
 - Detect and block scanning attempts.
 - Respond to penetration testing.
 - Handle **Trojan attempts** and **port scanning**.
 - Secure end-user devices, which are often the **weakest link** in security.
 - **Penetration Testers** often explore ways to bypass such firewalls during security assessments.
-

Name : kunal Jawale



Make a new rules for system go for rules like this



Honeybot: A Honeypot for Network Security

🔍 What is Honeybot?

- Honeybot is a **honeypot application** designed to simulate a vulnerable system on a network.
 - It acts as a **decoy** to attract attackers, allowing security professionals to:
 - Monitor attack methods
 - Gather intelligence on intrusions
 - Study hacking techniques without risking actual systems
 - **Purpose:** To trap, log, and analyze unauthorized activities, providing insights into attacker behavior and vulnerabilities.
-

💡 Key Features of Honeybot:

1. Port Emulation:

- Honeybot can emulate **open ports** (e.g., FTP, HTTP, Telnet) to simulate real services.
- Attackers think they are connecting to actual services, but all activities are being monitored.

2. Traffic Logging:

- Logs every connection attempt, including IP addresses, timestamps, and commands sent.
- Useful for forensic analysis and understanding attack patterns.

3. Deception Techniques:

- Mimics known vulnerabilities, encouraging attackers to interact with the honeypot.
- Provides fake responses to make the attacker believe they are making progress.

4. Attack Analysis:

- Collects detailed information about intrusion attempts, including:
 - Exploit techniques
 - Malware dropped
 - Commands executed

5. Minimal Impact:

- Operates independently and is isolated from critical systems to prevent real damage.

- Designed to **observe, not respond**, minimizing the risk of escalation.

6. Easy Deployment:

- Lightweight and easy to set up on Windows-based systems.
 - Can be configured to mimic various server types and protocols.
-

💡 How Honeybot Works:

1. Setup and Configuration:

- Honeybot is configured with specific IP addresses and ports that appear vulnerable.

2. Simulating Services:

- It mimics common protocols like HTTP, FTP, SMTP, and others to attract malicious traffic.

3. Logging and Monitoring:

- All connection attempts are logged for analysis:
 - Source IP address
 - Destination port
 - Time and date of access
 - Commands executed

4. Data Analysis:

- Security teams analyze logs to identify:
 - New attack vectors
 - Scanning patterns
 - Potential vulnerabilities

5. Detection of Attack Tools:

- If an attacker deploys malware or scanning tools, Honeybot captures the activity without risk to real systems.
-

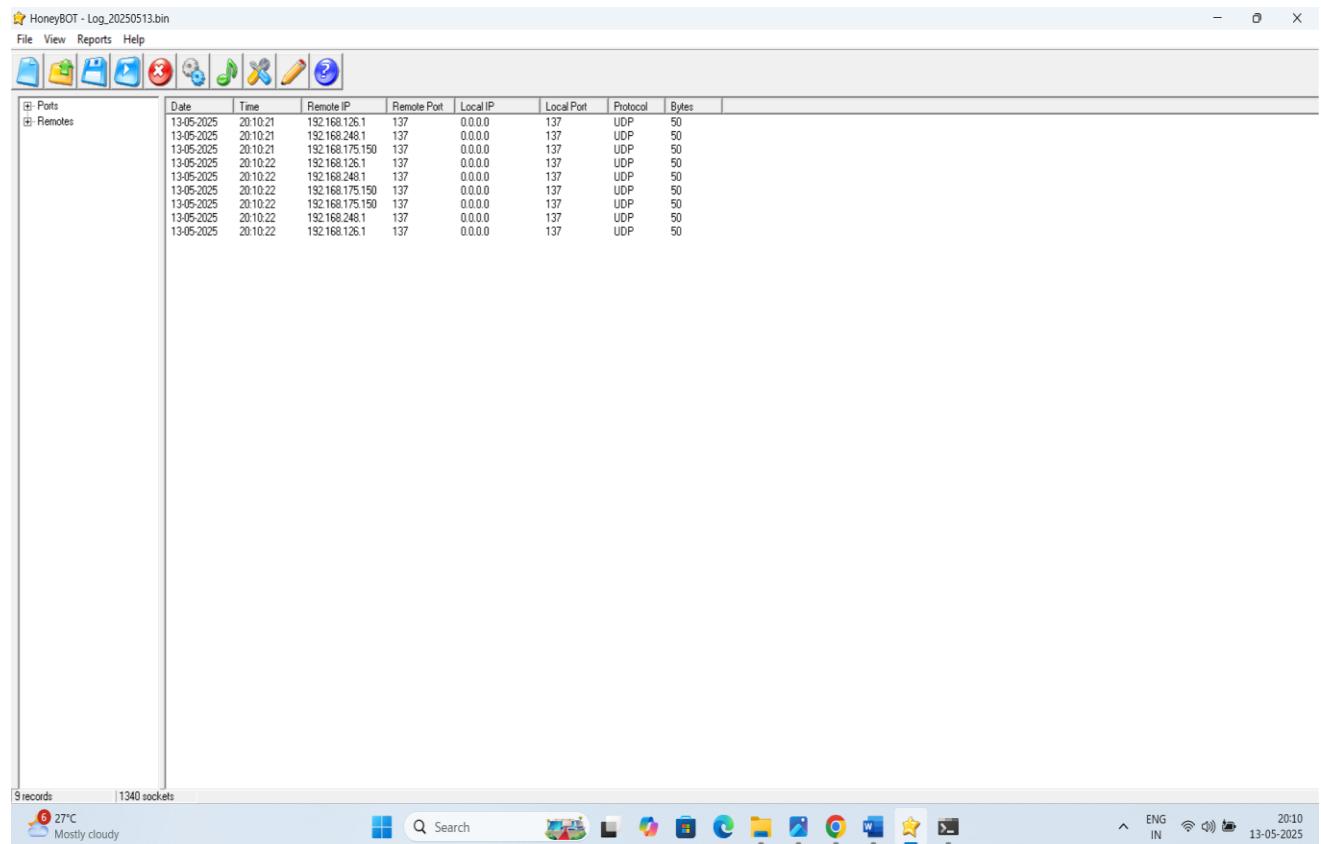
💡 Why Honeybot is Important for CEH (Certified Ethical Hacker):

- **Honeypots** like Honeybot are important tools for:
 - **Understanding attack behaviors:** Learning how hackers probe and exploit networks.
 - **Early Threat Detection:** Identifying malicious intent before it reaches real systems.

Name : kunal Jawale

- **Forensic Analysis:** Studying attack vectors and methods for improving defenses.
 - **Learning Exploit Techniques:** Ethical hackers can observe real-world attack strategies safely.
-

Screenshot of honeypot :



The screenshot shows the HoneyBOT software interface. At the top, there's a menu bar with 'File', 'View', 'Reports', and 'Help'. Below the menu is a toolbar with various icons. The main area is a table displaying network log data. The columns are labeled: Date, Time, Remote IP, Remote Port, Local IP, Local Port, Protocol, and Bytes. The data shows several entries from May 13, 2010, at different times, with remote IPs like 192.168.126.1 and 192.168.248.1, and local ports mostly set to 137. The protocol is UDP and bytes transferred are 50. At the bottom of the table, it says '9 records | 1340 sockets'. The status bar at the bottom shows the date as 13-05-2025, the time as 20:10, the weather as '27°C Mostly cloudy', and system information like 'ENG IN' and signal strength.

	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Ports	13-05-2025	20:10:21	192.168.126.1	137	0.0.0.0	137	UDP	50
Remotes	13-05-2025	20:10:21	192.168.248.1	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:21	192.168.175.150	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.126.1	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.248.1	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.175.150	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.175.150	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.248.1	137	0.0.0.0	137	UDP	50
	13-05-2025	20:10:22	192.168.126.1	137	0.0.0.0	137	UDP	50

Name : kunal Jawale