Module 12

Firewall,IDS,IPS, Honeypots

23.12.2025

Name : Mugdha Makarand Govilkar

Instructor : Satish Singh

1 . Firewall :

1.1 What is firewall ?

1.2 Types of firewall ?

1.3 Importance of firewall ?

1.4 Working of firewall ?

2 . IDS

2.1 What is IDS ?

2.2 Types of IDS ?

2.3 Importance of IDS ?

2.4 Working of IDS ?

3 . IPS

3.1 What is IPS ?

3.2 Types of IPS ?

3.3 Importance of IPS ?

3.4 Working of IPS ?

4 . Honeypot

4.1 What is honeypot ?

4.2 Types of honeypot ?

4.3 Importance of honeypot ?

4.4 Working of honeypot ?

5 . Tools :

1 . Snort

2 . Zone alarm

3 . Honeybot

4 . Wireshark

1 . Firewall :

1.1 What is firewall ?

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules, allowing trusted traffic and blocking unauthorized access.

1.2 Types of firewall ?

1 . Packet Filtering Firewall – Filters packets based on IP address, port number, and protocol.

2 . Stateful Inspection Firewall – Tracks active connections and allows only valid traffic.

3 . Proxy Firewall (Application-level) – Acts as an intermediary between user and server.

4 . Next-Generation Firewall (NGFW) – Includes deep packet inspection, IDS/IPS, and application control.

5 . Software Firewall: A firewall program installed on a system to protect a single device.

6 . Hardware Firewall: A physical security device that protects an entire network from unauthorized access.

1.3 Importance of firewall ?

1 . Protects the network from unauthorized access.

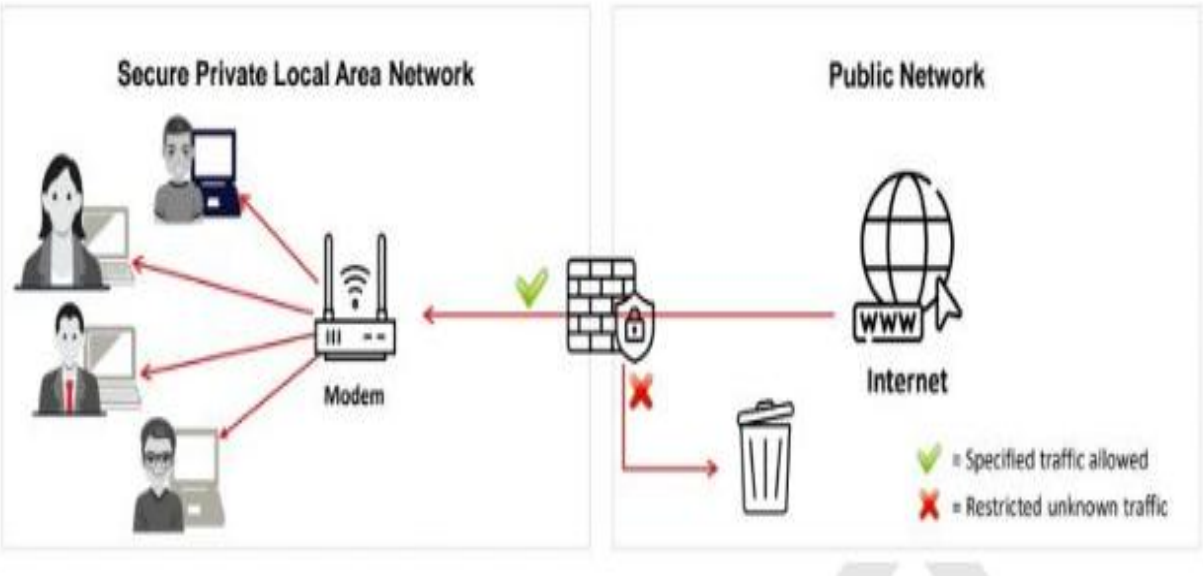
2 . Prevents malware and cyber attacks.

3 . Controls incoming and outgoing traffic.

4 . Safeguards sensitive data from theft.

5 . Improves overall network security.

1.4 Working of firewall ?



2 . IDS

2.1 What is IDS ?

IDS (Intrusion Detection System) is a security system that monitors network or system activity to detect suspicious or malicious actions.

2.2 Types of IDS ?

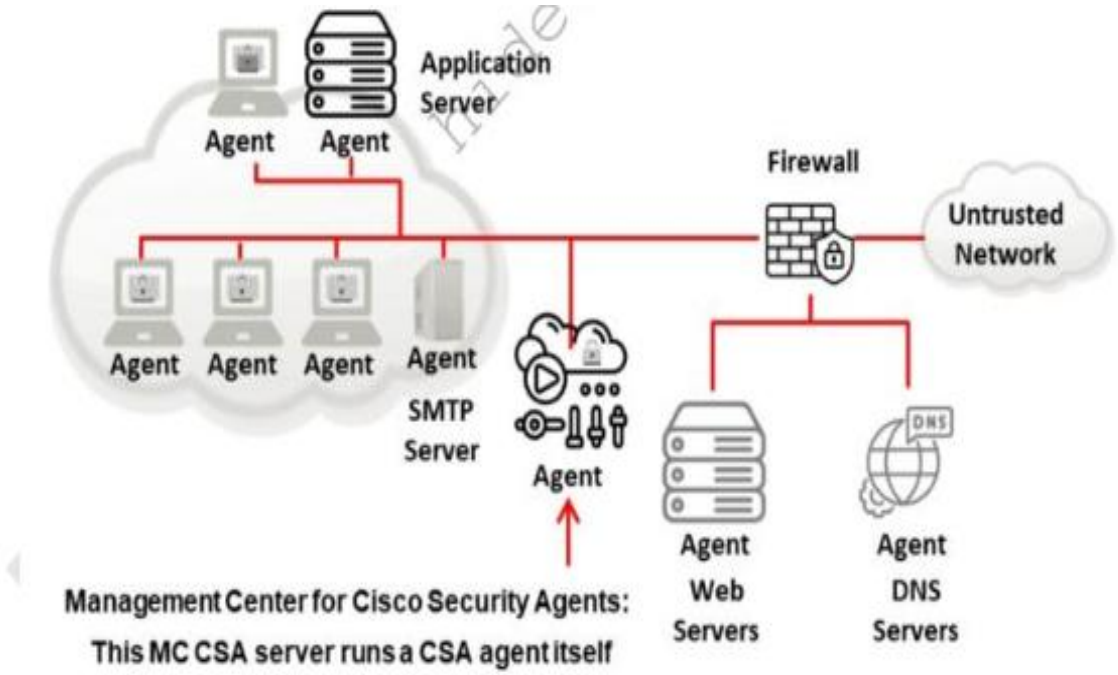
1 . NIDS (Network-based IDS):
Monitors network traffic to detect suspicious activity. Works on network segments, e.g., Snort.

2 . HIDS (Host-based IDS):
Monitors a single system's logs, files, and applications. Detects attacks on that host, e.g., OSSEC.

2.3 Importance of IDS ?

IDS detects attacks early, monitors networks and systems, protects data, aids incident response, and helps identify new threats while supporting compliance.

2.4 Working of IDS ?



3 . IPS

3.1 What is IPS ?

An IPS sits in-line (directly in the traffic path) between network devices and monitors traffic continuously. When it detects suspicious activity, it can automatically take action to stop the threat.

3.2 Types of IPS ?

1 . NIPS (Network-based IPS):
Monitors and prevents malicious activity on the network. Blocks attacks like DoS, malware, or unauthorized access.

2 . HIPS (Host-based IPS):
Installed on individual systems to prevent attacks on that host. Monitors system logs, files, and applications.

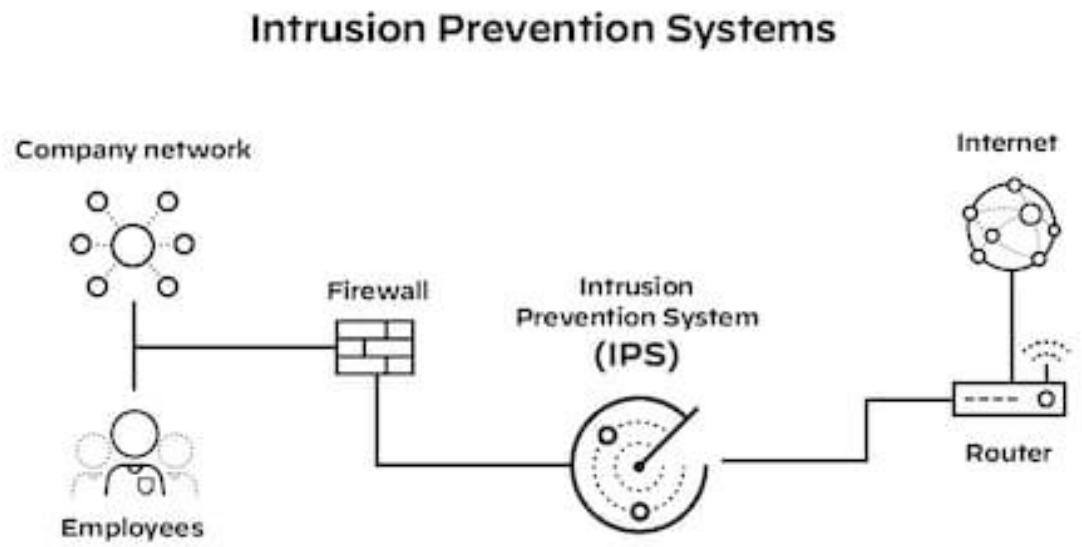
3 . Wireless IPS (WIPS):
Protects wireless networks by detecting and blocking rogue access points and wireless attacks.

4 . Network Behavior Analysis (NBA) IPS:
Detects unusual traffic patterns or anomalies in the network. Useful for detecting unknown attacks like zero-day exploits.

3.3 Importance of IPS ?

An Intrusion Prevention System (IPS) is important because it actively blocks malicious traffic and attacks, protecting networks, systems, and sensitive data. It strengthens security by preventing breaches, supporting compliance, and providing logs for analysis, while also detecting both known and unknown threats to keep the organization safe.

3.4 Working of IPS ?



4 . Honeypot

4.1 What is 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 — allowing defenders to monitor, detect, and analyze malicious activity without risking real systems.

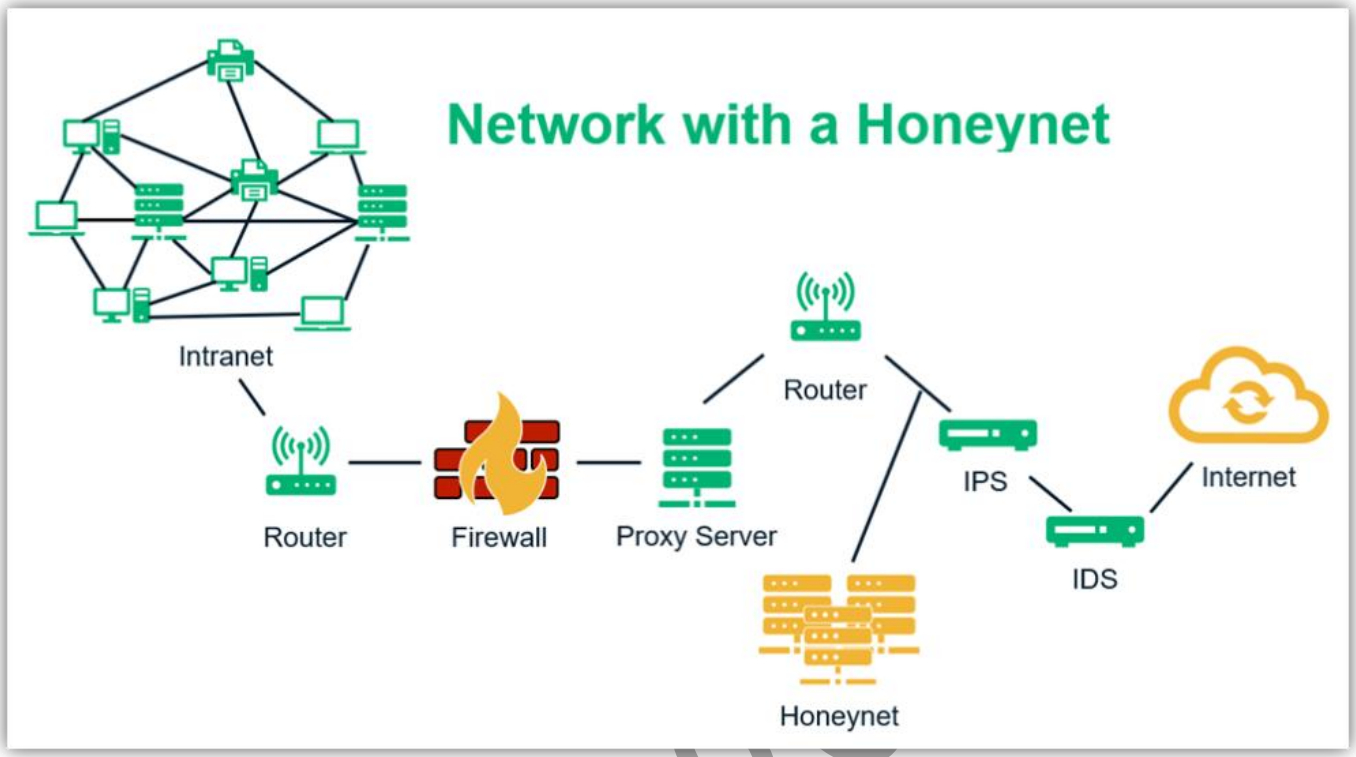
4.2 Types of honeypot ?

1. **Low-interaction honeypot: Simulates limited services to attract attackers; easy and safe but gives less information.**
2. **High-interaction honeypot: Real system that fully interacts with attackers; provides detailed data but is risky.**
3. **Production honeypot: Used in organizations to detect and divert attacks from real systems.**
4. **Research honeypot: Used by researchers to study attacker behavior and attack techniques.**

4.3 Importance of honeypot ?

A honeypot is important because it attracts attackers away from real systems and helps detect intrusions early. It allows organizations to study attacker behavior, understand new attack techniques, improve security defenses, and reduce the risk to critical systems.

4.4 Working of honeypot ?



4 . Tools :

1 . Snort :

1.1 What is snort ?

Snort is an open-source network intrusion detection system (NIDS) and intrusion prevention system (IPS) developed by Cisco Systems. It's one of the most widely used tools for real-time traffic analysis and packet logging on IP networks.

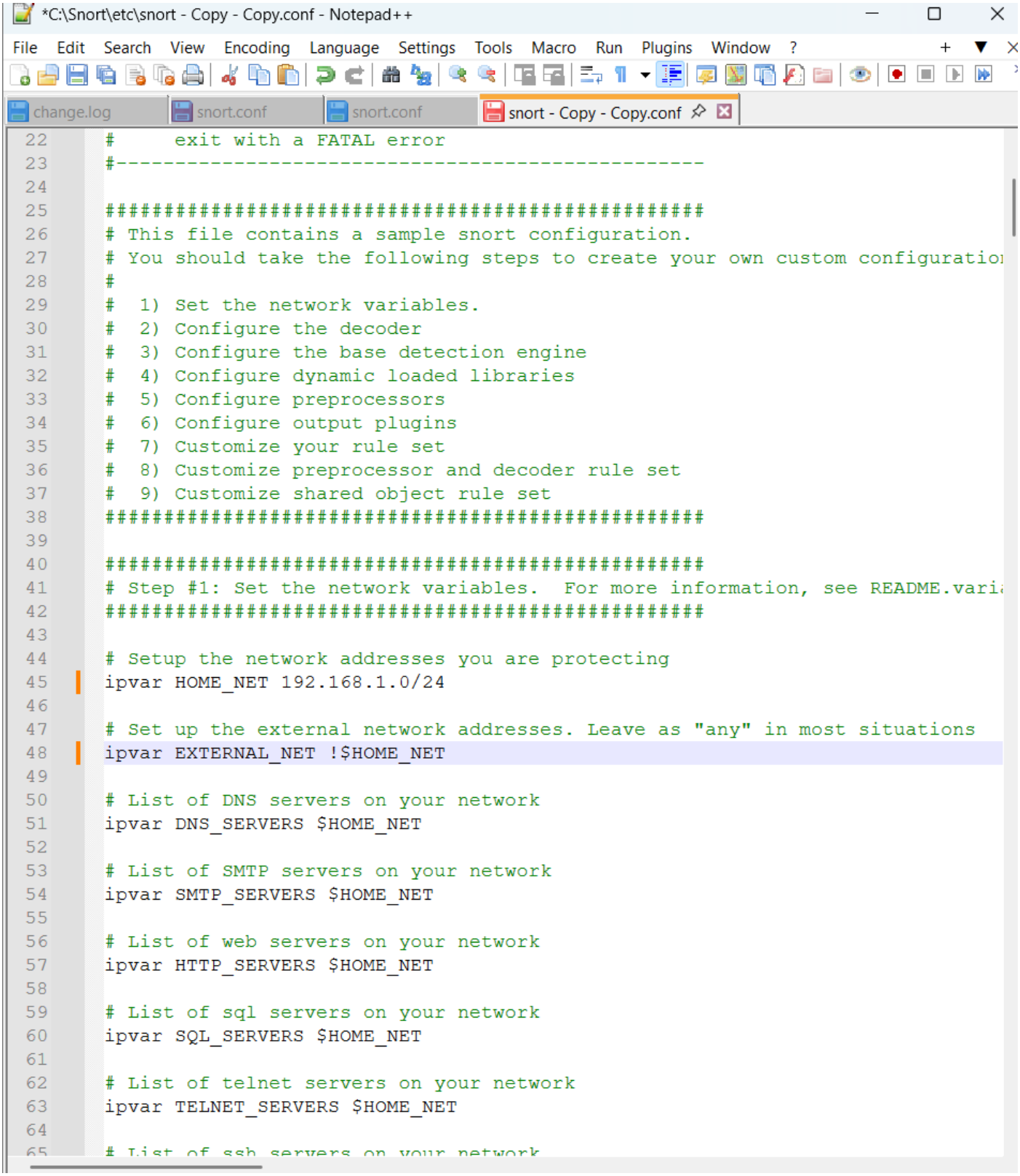
1.2 Uses/Objectives of Snort :

- **Detects network intrusions in real-time.**
- **Performs deep packet inspection (DPI).**
- **Monitors traffic for suspicious behavior.**
- **Logs packets for later analysis.**
- **Prevents attacks when used in IPS mode.**
- **Detects port scans and probes.**
- **Identifies malware and exploit attempts.**
- **Enforces security policies on networks.**
- **Supports custom rule creation for threat detection.**
- **Assists in forensic and incident response analysis.**

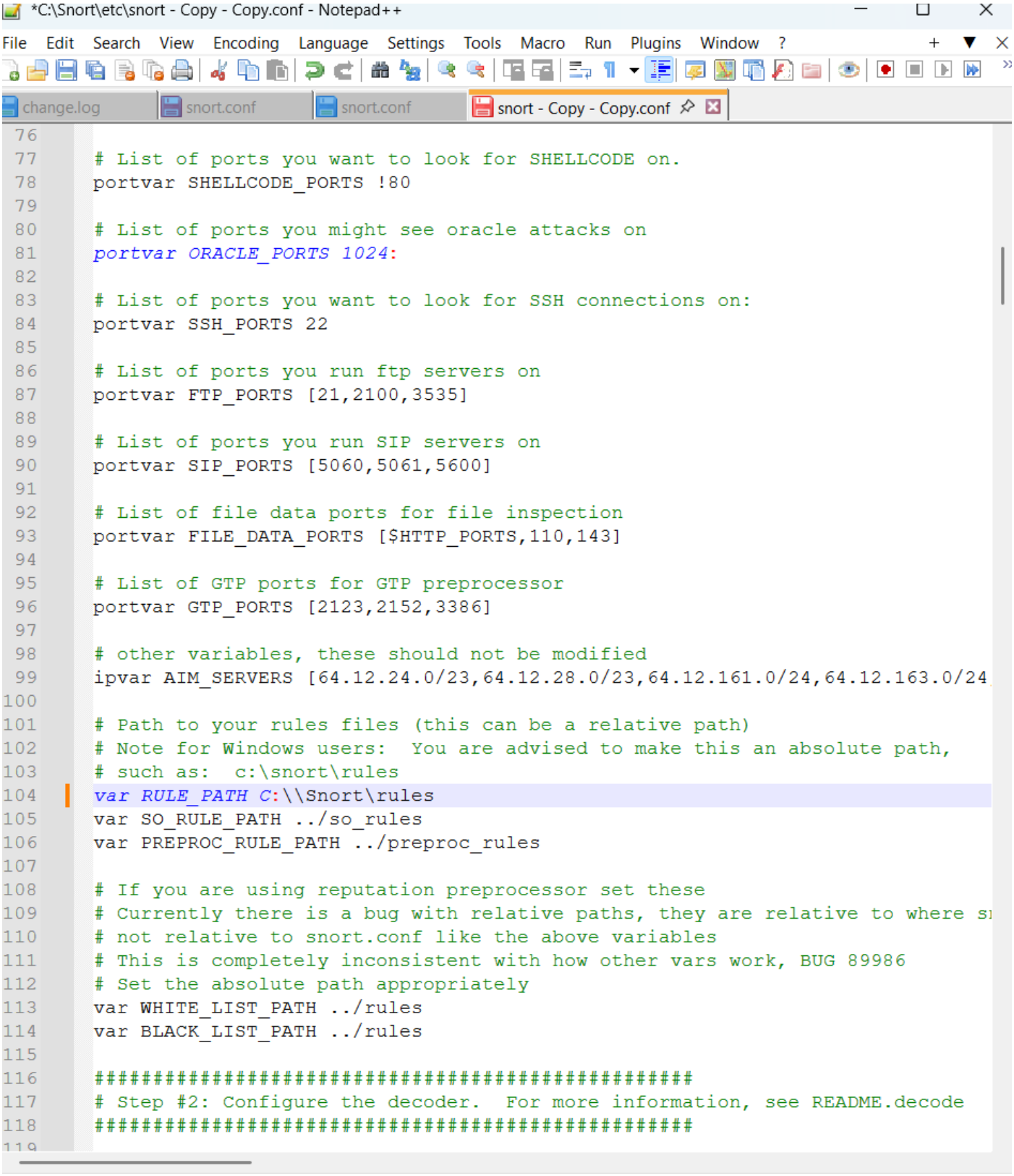
change.log | snort.conf | snort.conf | snort - Copy - Copy.conf

```
#      exit with a FATAL error
#--------------------------------------------------

##################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuratio
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
##################################################

##################################################
# Step #1: Set the network variables.  For more information, see README.vari
##################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
```

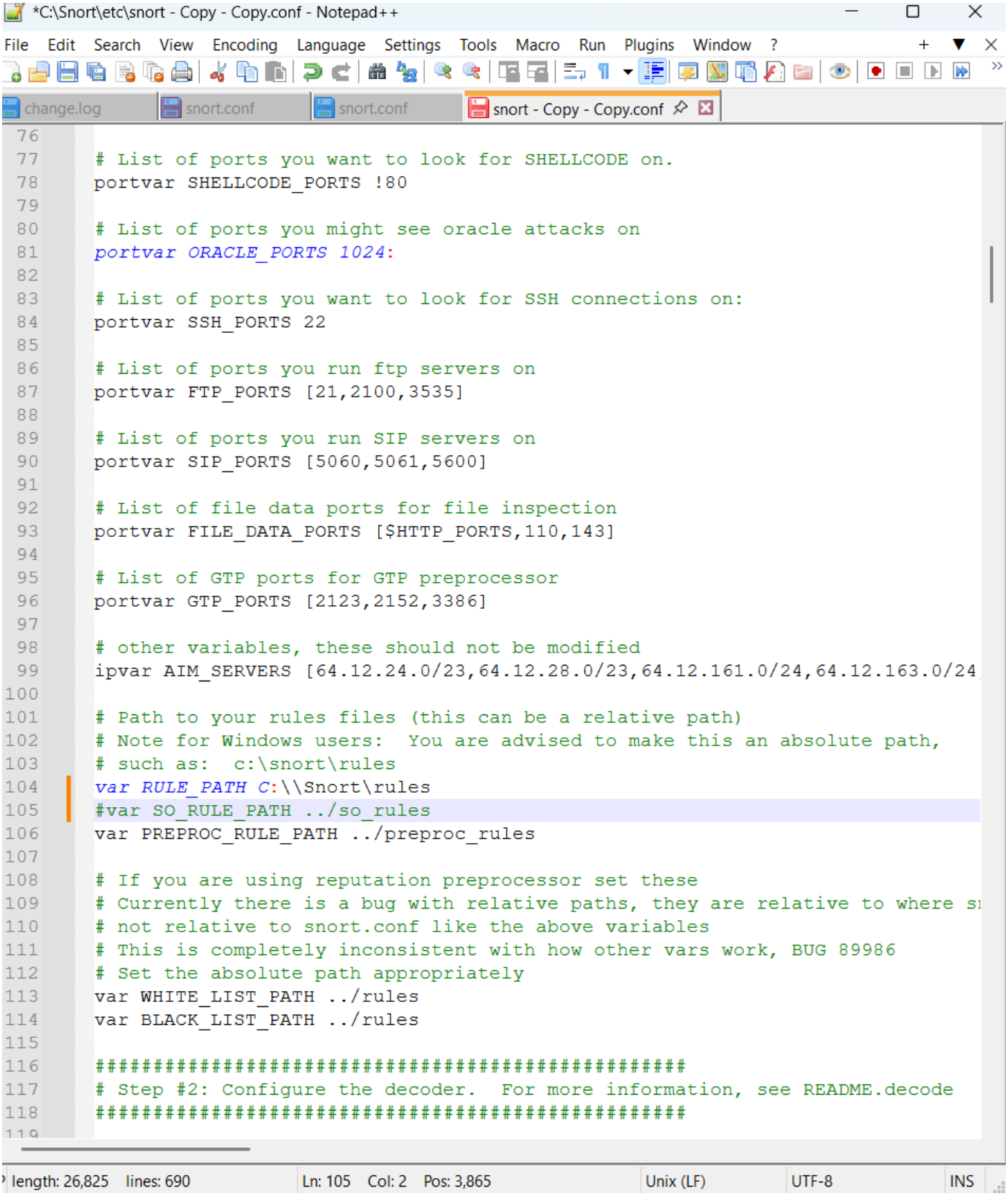
1.1


*C:\Snort\etc\snort - Copy - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
22 # exit with a FATAL error
23 #--
24
25 ##
26 # This file contains a sample snort configuration.
27 # You should take the following steps to create your own custom configuratio
28 #
29 # 1) Set the network variables.
30 # 2) Configure the decoder
31 # 3) Configure the base detection engine
32 # 4) Configure dynamic loaded libraries
33 # 5) Configure preprocessors
34 # 6) Configure output plugins
35 # 7) Customize your rule set
36 # 8) Customize preprocessor and decoder rule set
37 # 9) Customize shared object rule set
38 ##
39
40 ##
41 # Step #1: Set the network variables. For more information, see README.varia
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

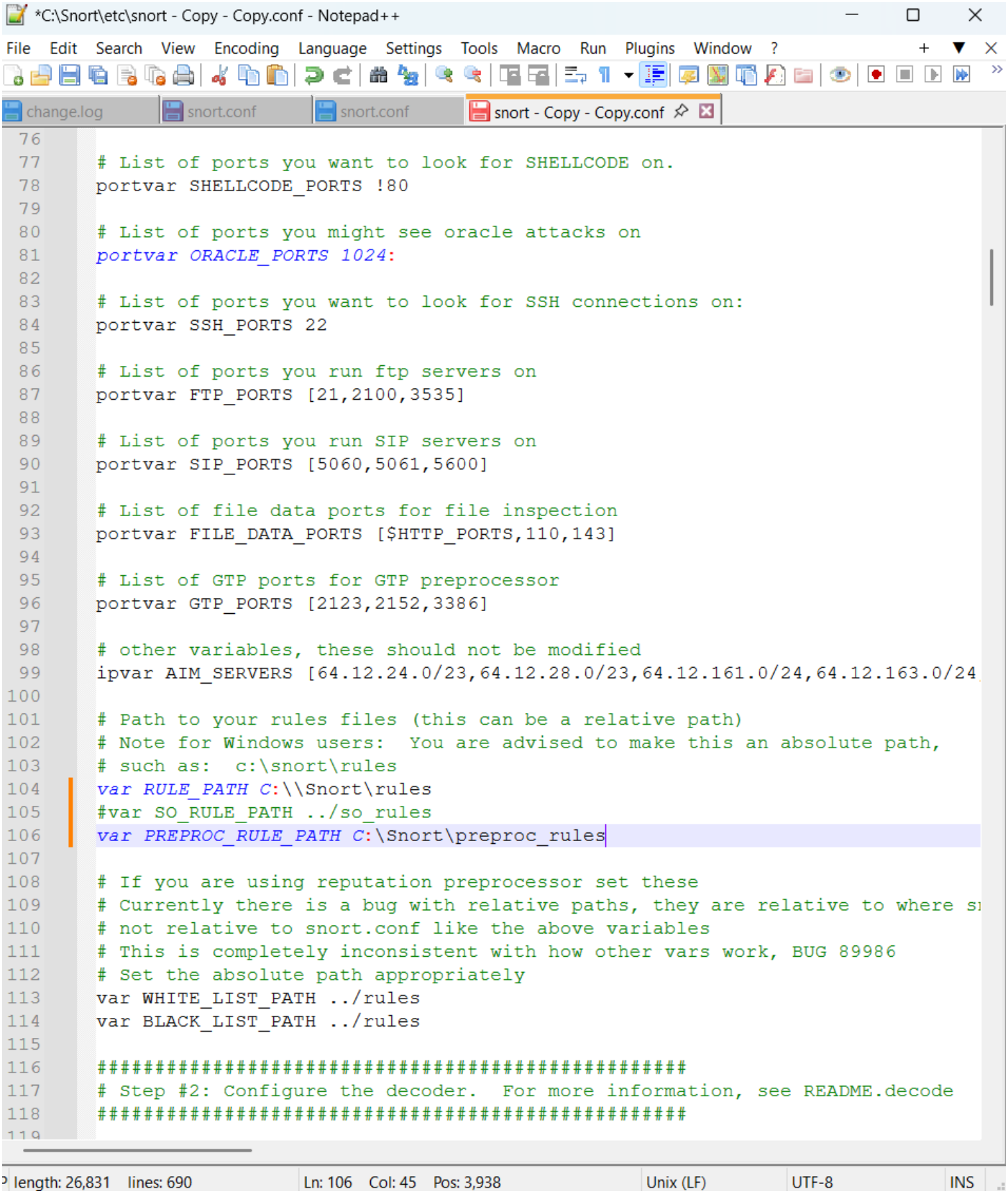
1.2


*C:\Snort\etc\snort - Copy - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
List of ports you want to look for SHELLCODE on.
portvar SHELLCODE_PORTS !80
List of ports you might see oracle attacks on
portvar ORACLE_PORTS 1024:
List of ports you want to look for SSH connections on:
portvar SSH_PORTS 22
List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]
List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]
List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]
other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24
Path to your rules files (this can be a relative path)
Note for Windows users: You are advised to make this an absolute path,
such as: c:\snort\rules
var RULE_PATH C:\\Snort\rules
var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH ../preproc_rules
If you are using reputation preprocessor set these
Currently there is a bug with relative paths, they are relative to where s
not relative to snort.conf like the above variables
This is completely inconsistent with how other vars work, BUG 89986
Set the absolute path appropriately
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules
##
Step #2: Configure the decoder. For more information, see README.decode
##

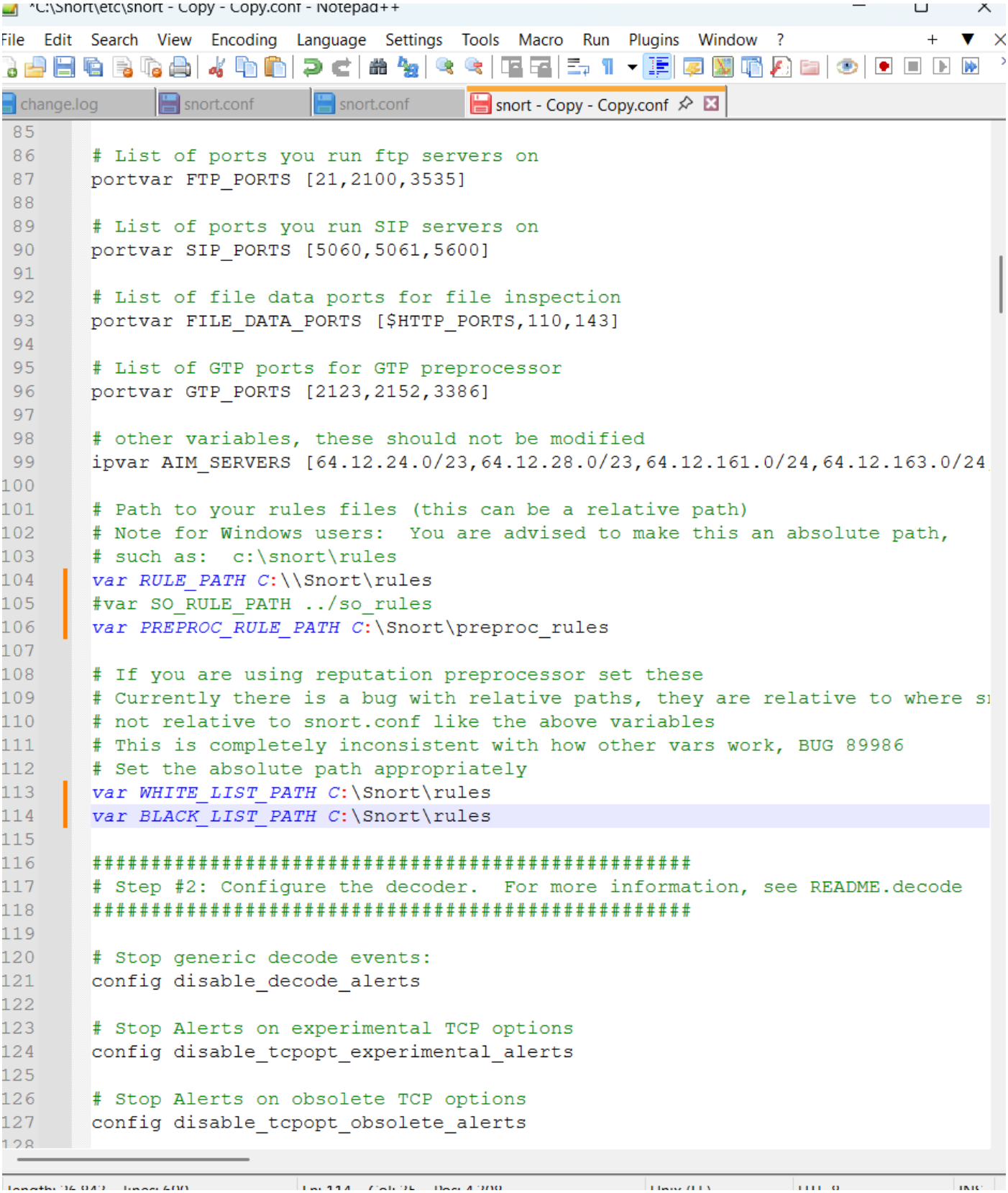
1.3


*C:\Snort\etc\snort - Copy - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
76
77 # List of ports you want to look for SHELLCODE on.
78 portvar SHELLCODE_PORTS !80
79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024:
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
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 ../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 s
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 ../rules
114 var BLACK_LIST_PATH ../rules
115
116 ##
117 # Step #2: Configure the decoder. For more information, see README.decode
118 ##
length: 26,825 lines: 690
Ln: 105 Col: 2 Pos: 3,865
Unix (LF)
UTF-8
INS

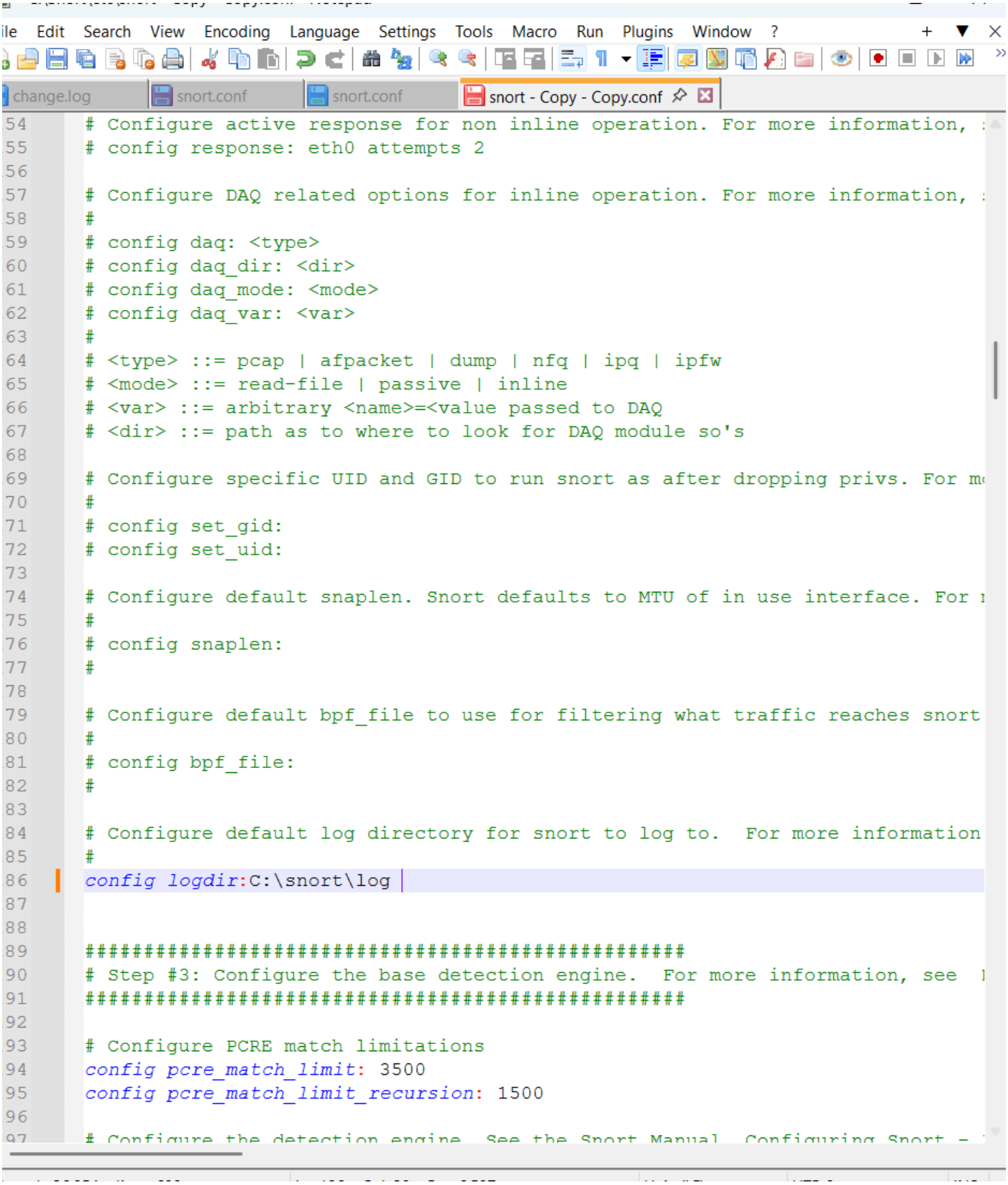
1.4


*C:\Snort\etc\snort - Copy - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
76
77 # List of ports you want to look for SHELLCODE on.
78 portvar SHELLCODE_PORTS !80
79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024:
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
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 s
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 ../rules
114 var BLACK_LIST_PATH ../rules
115
116 ##
117 # Step #2: Configure the decoder. For more information, see README.decode
118 ##
length: 26,831 lines: 690
Ln: 106 Col: 45 Pos: 3,938
Unix (LF)
UTF-8
INS

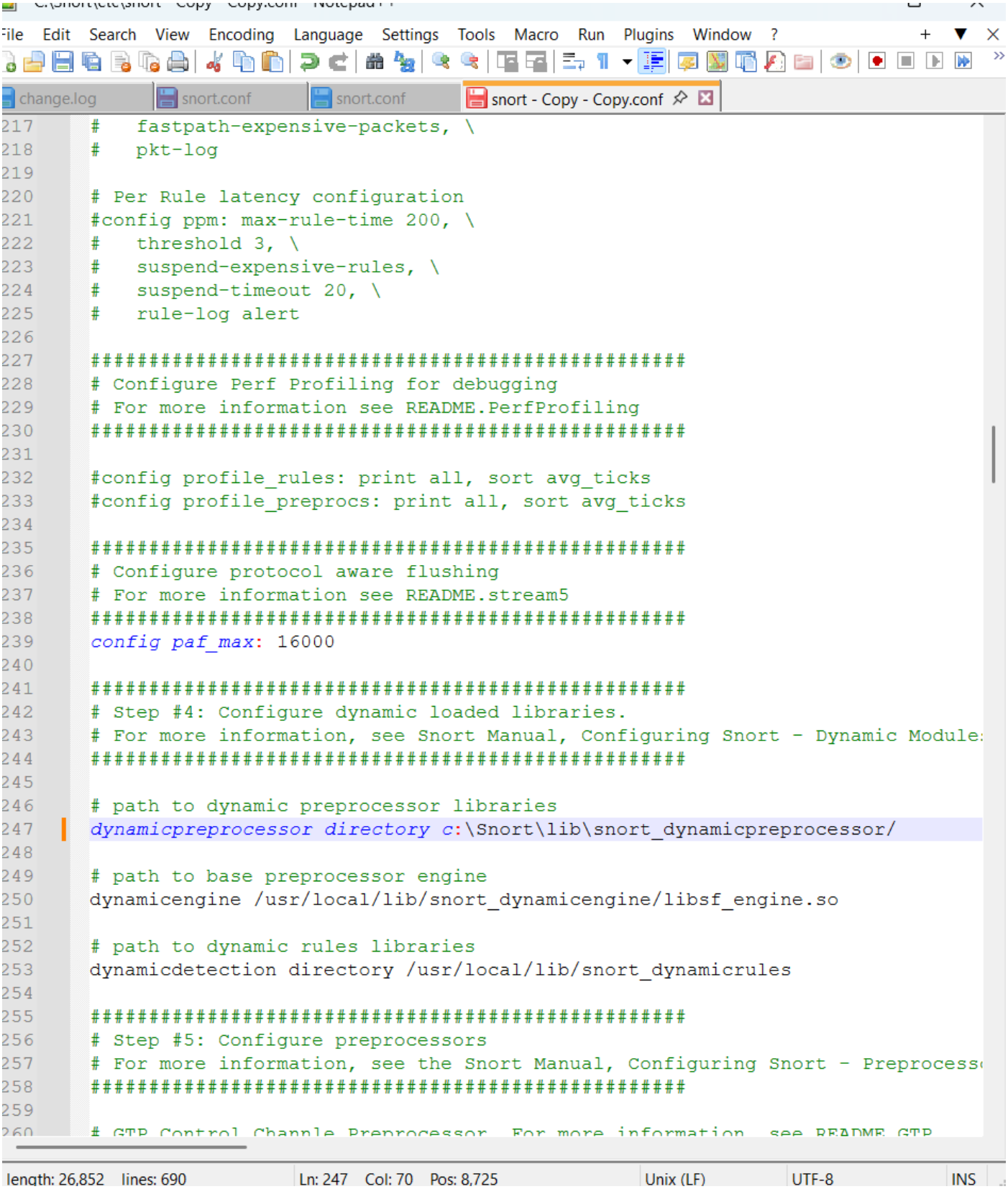
1.5


*C:\Snort\etc\snort - Copy - Copy.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
List of ports you run ftp servers on
portvar FTP_PORTS [21,2100,3535]
List of ports you run SIP servers on
portvar SIP_PORTS [5060,5061,5600]
List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]
other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24
Path to your rules files (this can be a relative path)
Note for Windows users: You are advised to make this an absolute path,
such as: c:\snort\rules
var RULE_PATH C:\\Snort\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
If you are using reputation preprocessor set these
Currently there is a bug with relative paths, they are relative to where s
not relative to snort.conf like the above variables
This is completely inconsistent with how other vars work, BUG 89986
Set the absolute path appropriately
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
##
Step #2: Configure the decoder. For more information, see README.decode
##
Stop generic decode events:
config disable_decode_alerts
Stop Alerts on experimental TCP options
config disable_tcpopt_experimental_alerts
Stop Alerts on obsolete TCP options
config disable_tcpopt_obsolete_alerts

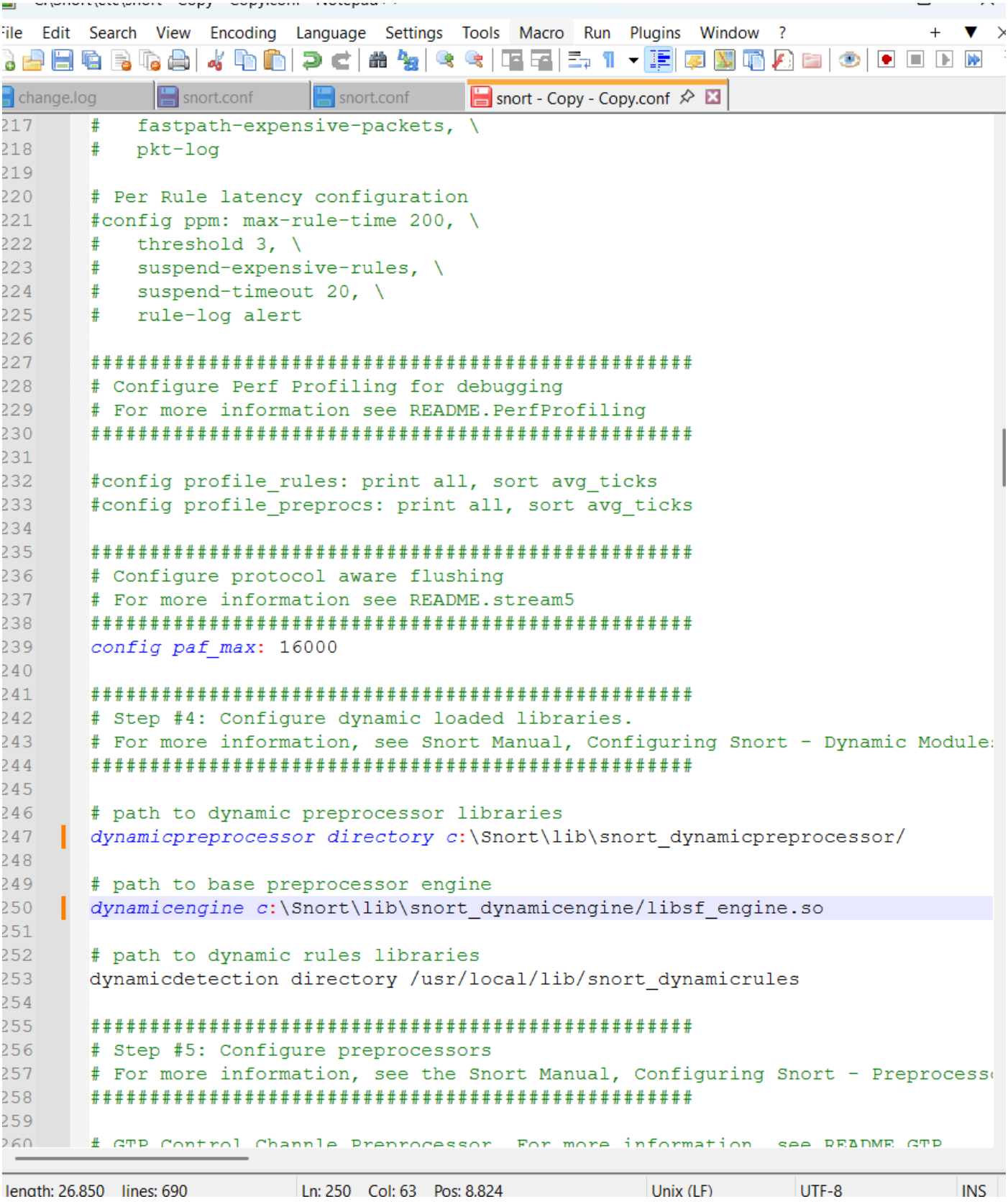
1.6


ile Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
54 # Configure active response for non inline operation. For more information,
55 # config response: eth0 attempts 2
56
57 # Configure DAQ related options for inline operation. For more information,
58 #
59 # config daq: <type>
60 # config daq_dir: <dir>
61 # config daq_mode: <mode>
62 # config daq_var: <var>
63 #
64 # <type> ::= pcap | afpacket | dump | nfq | ipq | ipfw
65 # <mode> ::= read-file | passive | inline
66 # <var> ::= arbitrary <name>=<value passed to DAQ
67 # <dir> ::= path as to where to look for DAQ module so's
68
69 # Configure specific UID and GID to run snort as after dropping privs. For m
70 #
71 # config set_gid:
72 # config set_uid:
73
74 # Configure default snaplen. Snort defaults to MTU of in use interface. For
75 #
76 # config snaplen:
77 #
78
79 # Configure default bpf_file to use for filtering what traffic reaches snort
80 #
81 # config bpf_file:
82 #
83
84 # Configure default log directory for snort to log to. For more information
85 #
86 config logdir:C:\snort\log
87
88
89 ##
90 # Step #3: Configure the base detection engine. For more information, see
91 ##
92
93 # Configure PCRE match limitations
94 config pcre_match_limit: 3500
95 config pcre_match_limit_recursion: 1500
96
97 # Configure the detection engine See the Snort Manual Configuring Snort -

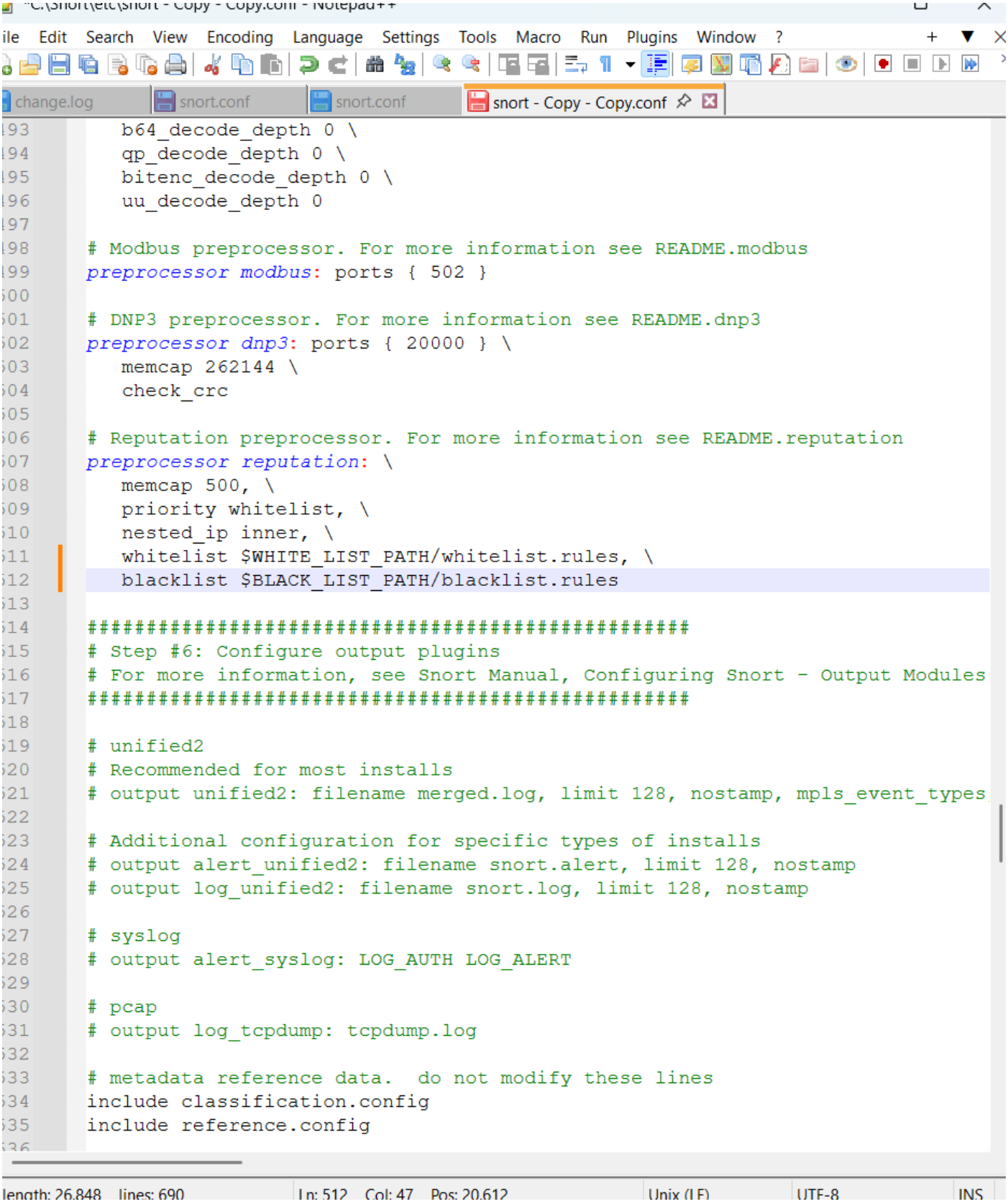
1.7


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
217 # fastpath-expensive-packets, \
218 # pkt-log
219
220 # Per Rule latency configuration
221 #config ppm: max-rule-time 200, \
222 # threshold 3, \
223 # suspend-expensive-rules, \
224 # suspend-timeout 20, \
225 # rule-log alert
226
227 ##
228 # Configure Perf Profiling for debugging
229 # For more information see README.PerfProfiling
230 ##
231
232 #config profile_rules: print all, sort avg_ticks
233 #config profile_preprocs: print all, sort avg_ticks
234
235 ##
236 # Configure protocol aware flushing
237 # For more information see README.stream5
238 ##
239 config paf_max: 16000
240
241 ##
242 # Step #4: Configure dynamic loaded libraries.
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Module
244 ##
245
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor/
248
249 # path to base preprocessor engine
250 dynamicengine /usr/local/lib/snort_dynamicengine/libsf_engine.so
251
252 # path to dynamic rules libraries
253 dynamicdetection directory /usr/local/lib/snort_dynamicrules
254
255 ##
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocess
258 ##
259
260 # GTP Control Channle Preprocessor. For more information, see README.GTP
length: 26,852 lines: 690
Ln: 247 Col: 70 Pos: 8,725
Unix (LF)
UTF-8
INS

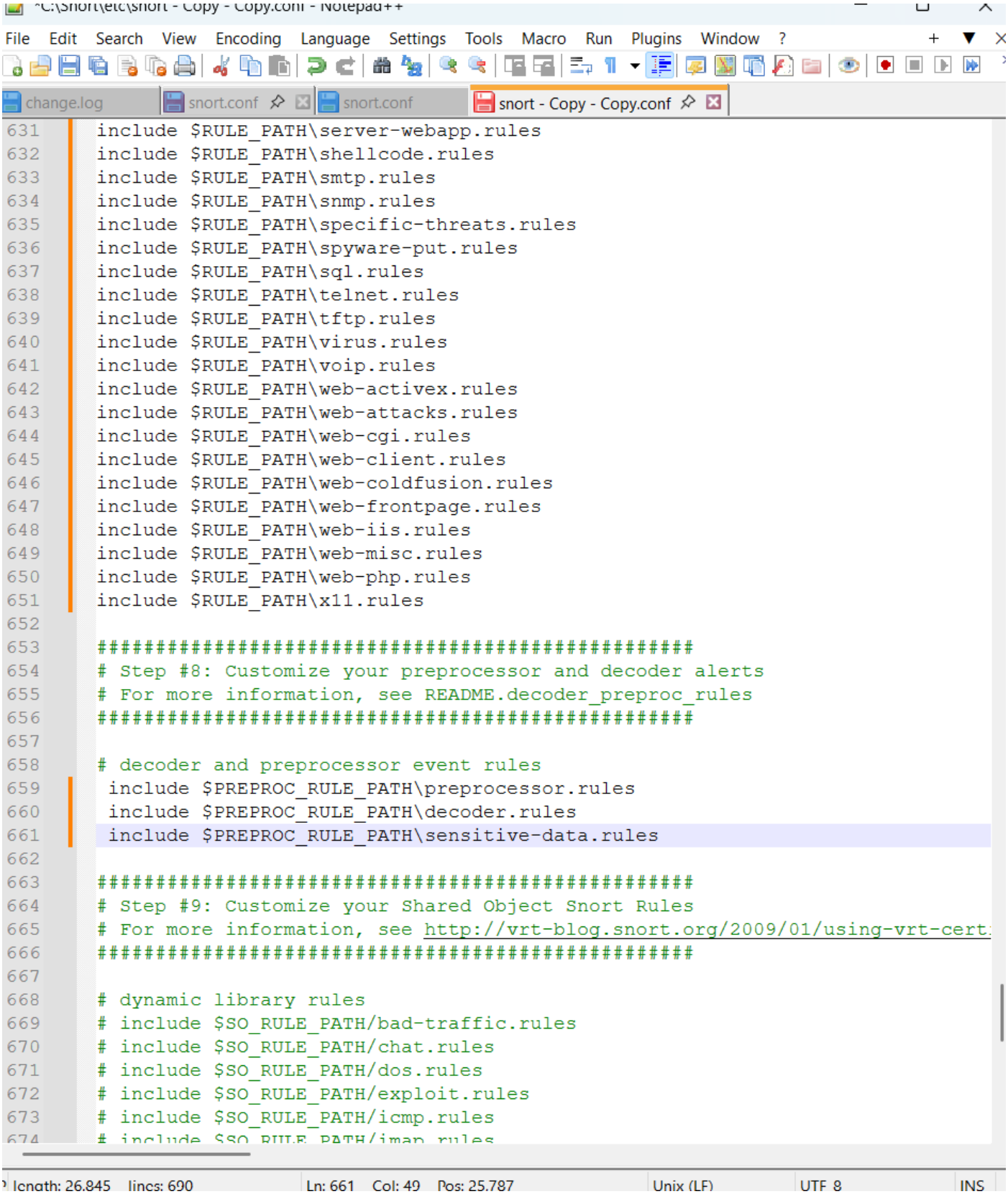
1.8


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
fastpath-expensive-packets, \
pkt-log
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_preprocs: 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 Module
path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor/
path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine/libsf_engine.so
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 - Preprocess
length: 26,850 lines: 690
Ln: 250 Col: 63 Pos: 8,824
Unix (LF)
UTF-8
INS

1.9


ile Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
b64_decode_depth 0 \
qp_decode_depth 0 \
bitenc_decode_depth 0 \
uu_decode_depth 0
Modbus preprocessor. For more information see README.modbus
preprocessor modbus: ports { 502 }
DNP3 preprocessor. For more information see README.dnp3
preprocessor dnp3: ports { 20000 } \
memcap 262144 \
check_crc
Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
memcap 500, \
priority whitelist, \
nested_ip inner, \
whitelist $WHITE_LIST_PATH/whitelist.rules, \
blacklist $BLACK_LIST_PATH/blacklist.rules
##
Step #6: Configure output plugins
For more information, see Snort Manual, Configuring Snort - Output Modules
##
unified2
Recommended for most installs
output unified2: filename merged.log, limit 128, nostamp, mpls_event_types
Additional configuration for specific types of installs
output alert_unified2: filename snort.alert, limit 128, nostamp
output log_unified2: filename snort.log, limit 128, nostamp
syslog
output alert_syslog: LOG_AUTH LOG_ALERT
pcap
output log_tcpdump: tcpdump.log
metadata reference data. do not modify these lines
include classification.config
include reference.config
length: 26,848 lines: 690
Ln: 512 Col: 47 Pos: 20,612
Unix (LF)
UTF-8
INS

2.1


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log
snort.conf
snort.conf
snort - Copy - Copy.conf
include $RULE_PATH\server-webapp.rules
include $RULE_PATH\shellcode.rules
include $RULE_PATH\smtp.rules
include $RULE_PATH\snmp.rules
include $RULE_PATH\specific-threats.rules
include $RULE_PATH\spyware-put.rules
include $RULE_PATH\sql.rules
include $RULE_PATH\telnet.rules
include $RULE_PATH\tftp.rules
include $RULE_PATH\virus.rules
include $RULE_PATH\voip.rules
include $RULE_PATH\web-activex.rules
include $RULE_PATH\web-attacks.rules
include $RULE_PATH\web-cgi.rules
include $RULE_PATH\web-client.rules
include $RULE_PATH\web-coldfusion.rules
include $RULE_PATH\web-frontpage.rules
include $RULE_PATH\web-iis.rules
include $RULE_PATH\web-misc.rules
include $RULE_PATH\web-php.rules
include $RULE_PATH\x11.rules
Step #8: Customize your preprocessor and decoder alerts
For more information, see README.decoder_preproc_rules
decoder and preprocessor event rules
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
include $PREPROC_RULE_PATH\sensitive-data.rules
Step #9: Customize your Shared Object Snort Rules
dynamic library rules
include $SO_RULE_PATH/bad-traffic.rules
include $SO_RULE_PATH/chat.rules
include $SO_RULE_PATH/dos.rules
include $SO_RULE_PATH/exploit.rules
include $SO_RULE_PATH/icmp.rules
Ln: 661 Col: 49 Pos: 25,787
Unix (LF)
UTF-8
INS

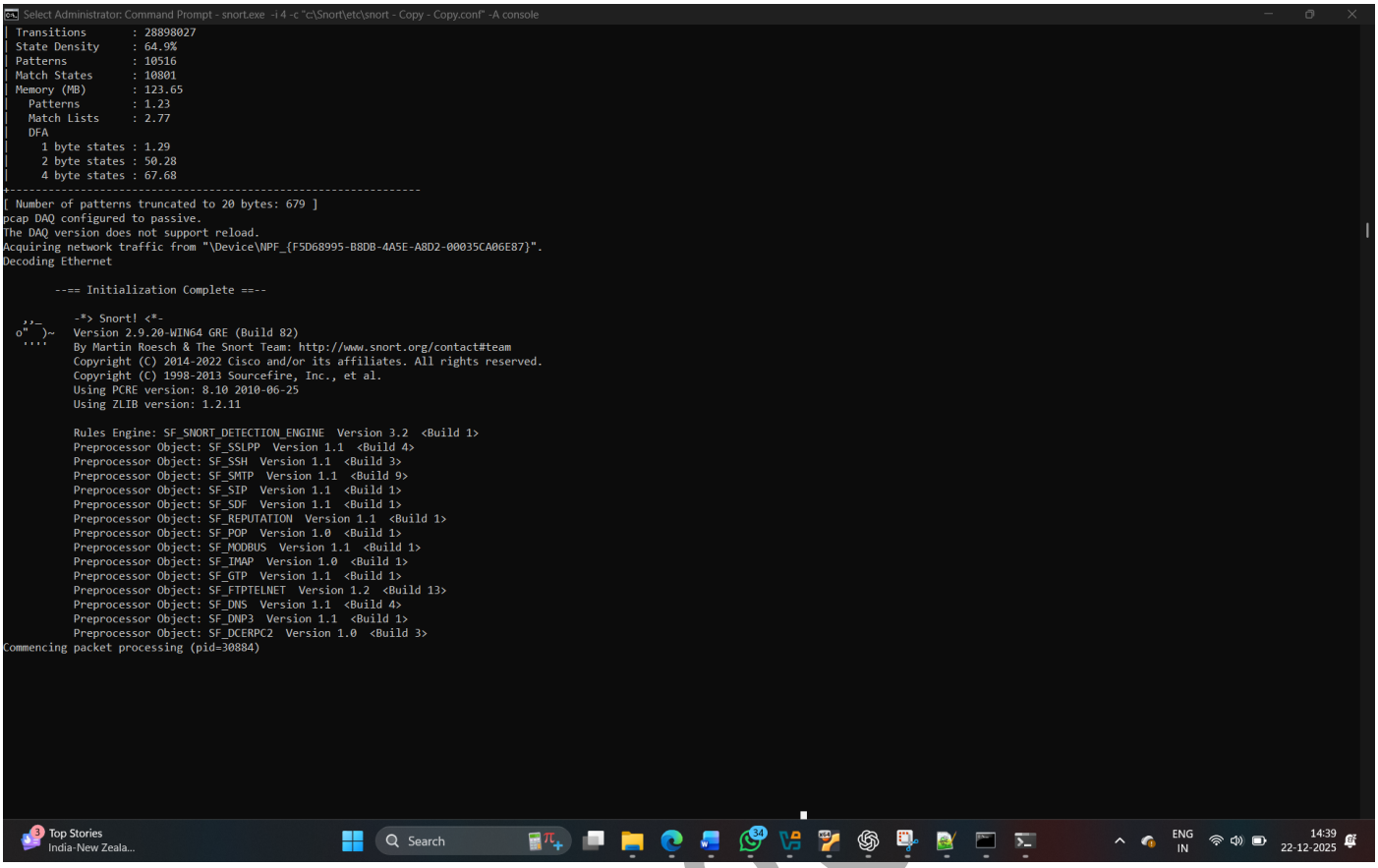
2.2

```
Microsoft Windows [Version 10.0.26200.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd Snort
The system cannot find the path specified.

C:\Windows\System32>cd snort
The system cannot find the path specified.

C:\Windows\System32>cd ..

C:\Windows>cd Snort
The system cannot find the path specified.

C:\Windows>cd snort
The system cannot find the path specified.

C:\Windows>cd ..

C:\>cd Snort

C:\Snort>cd bin

C:\Snort\bin>snort.exe -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.exe -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_{722D86F2-B129-4A27-AC90-9A3D56E77789}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{5C03AC1B-6CF7-4E1F-9F10-D5D7D04F61E3}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{C2EFDD92-20D5-4CC1-8057-92793C0EB16E}      WAN Miniport (IP)
    4   70:15:FB:7B:41:0B       169.254.203.254 \Device\NPF_{F5D68995-B8DB-4A5E-A8D2-00035CA06E87}      Bluetooth Device (Personal Area Network)
    5   70:15:FB:7B:41:07       192.168.1.70    \Device\NPF_{9A011CFF-3923-4559-BADD-F1C0868364E3}      Intel(R) Wi-Fi 6E AX211 160MHz
    6   72:15:FB:7B:41:07       169.254.223.70  \Device\NPF_{80F598CE-DCAB-4ECC-871C-785986AB261B}      Microsoft Wi-Fi Direct Virtual Adapter #2
    7   70:15:FB:7B:41:08       169.254.170.249 \Device\NPF_{C7EECEFF-C27C-4078-AF0C-DE20B6A93BD5}      Microsoft Wi-Fi Direct Virtual Adapter
    8   0A:00:27:00:00:05       192.168.212.1   \Device\NPF_{1CA6F718-5199-4ABE-85CA-E3DD174E4C53}      VirtualBox Host-Only Ethernet Adapter #2
    9   0A:00:27:00:00:03       192.168.56.1    \Device\NPF_{1034D2B1-FFD4-43C1-9DCA-2D1A600FFB5C}      VirtualBox Host-Only Ethernet Adapter
```

2.3

```
Select Administrator: Command Prompt - snort.exe  -i 4 -c "c:\Snort\etc\snort - Copy - Copy.conf" -A console
|     2 byte states : 50.28
|     4 byte states : 67.68
+-------------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 679 ]

MaxRss at the end of detection rules:1679100496
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{9A011CFF-3923-4559-BADD-F1C0868364E3}".

        --== Initialization Complete ==--

   ,,_     -*> 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  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:-1441385824
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>snort.exe -i 4 -c"c:\Snort\etc\file name " -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\file name "
ERROR: c:\Snort\etc\file name (0) Unable to open rules file "c:\Snort\etc\file name ": No such file or directory.

Fatal Error, Quitting..

C:\Snort\bin>snort.exe -i 4 -c "c:\Snort\etc\file name " -A console
Running in IDS mode
```


2.4


Select Administrator: Command Prompt - snort.exe -i 4 -c "c:\Snort\etc\snort - Copy - Copy.conf" -A console
| Transitions : 28898027
| State Density : 64.9%
| Patterns : 10516
| Match States : 10801
| Memory (MB) : 123.65
| Patterns : 1.23
| Match Lists : 2.77
| DFA
| 1 byte states : 1.29
| 2 byte states : 50.28
| 4 byte states : 67.68
+---
[Number of patterns truncated to 20 bytes: 679]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F5D68995-B8DB-4A5E-A8D2-00035CA06E87}".
Decoding Ethernet
--== Initialization Complete ==--
-*> 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 <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_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF 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>
Commencing packet processing (pid=30884)
Top Stories
India-New Zeala...
Search
ENG
IN
14:39
22-12-2025

2.5

2.ZoneAlarm :

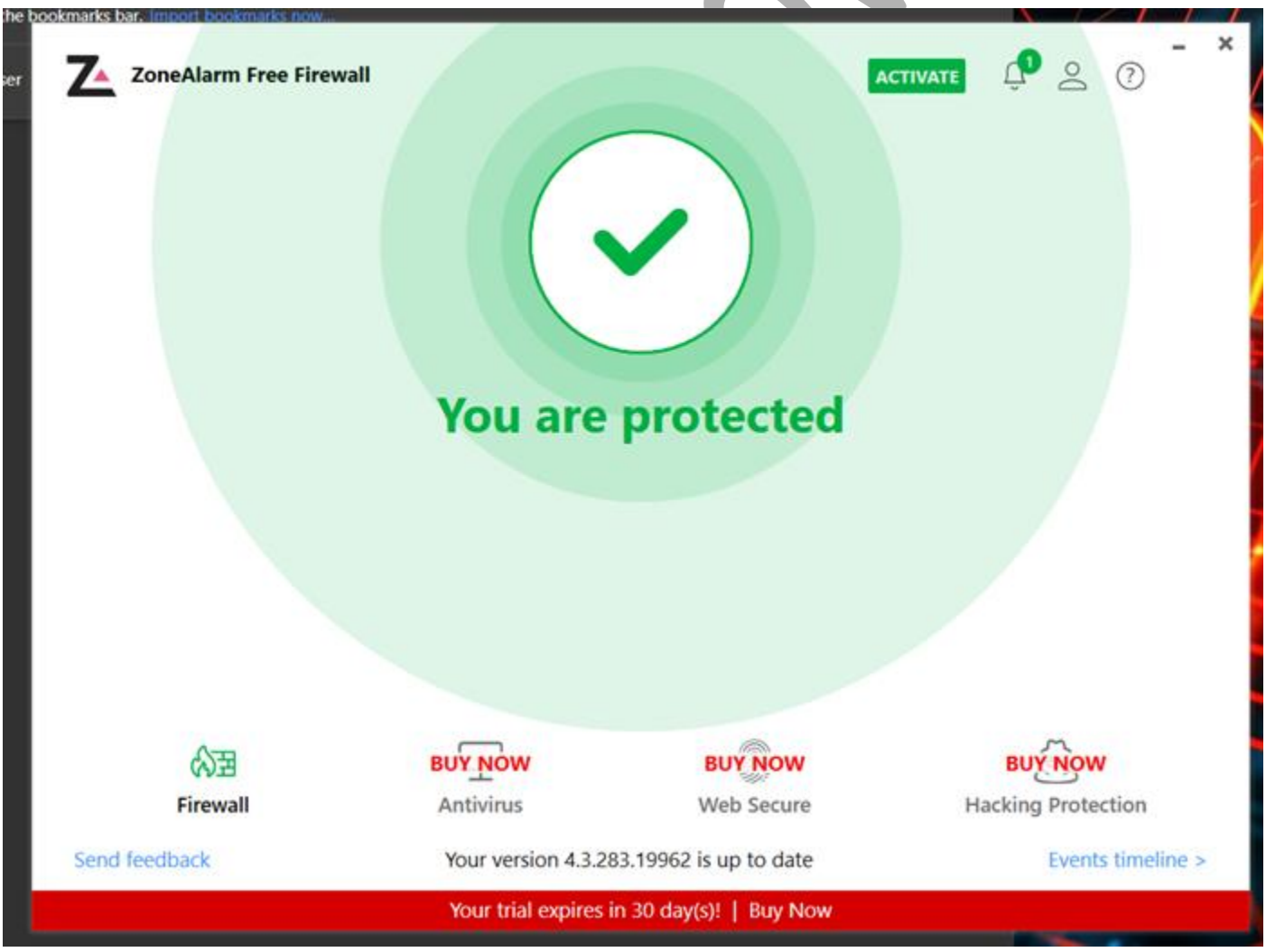
ZoneAlarm Firewall is a third-party software firewall for Windows developed by Check Point Software Technologies. It provides an extra layer of protection beyond the default Windows Defender Firewall, especially useful for users who want more detailed control over network activities.

Steps :

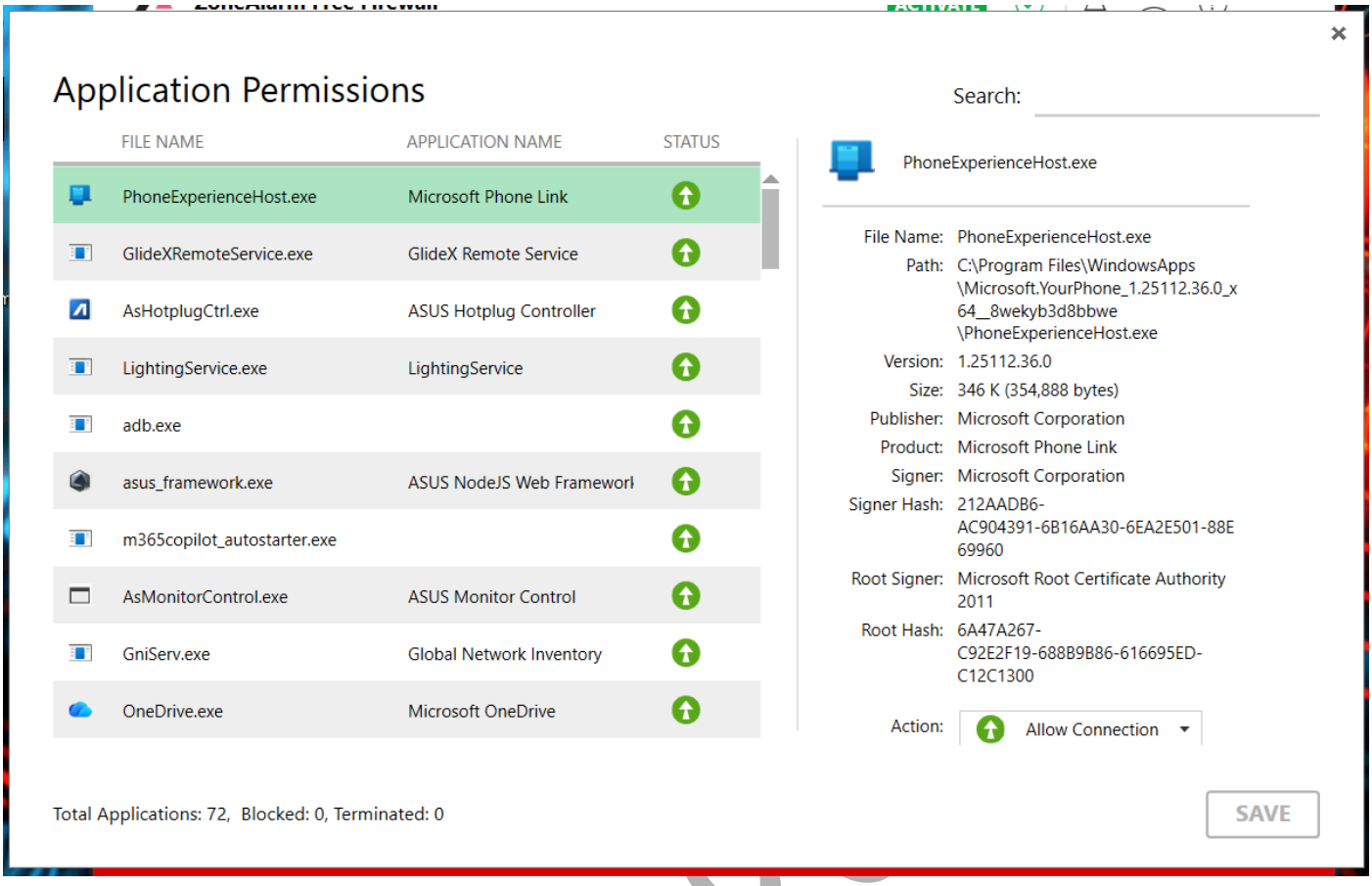
1 . After Installation , Open the application

2 . Now click on firewall

3 . Click on Application Permissions



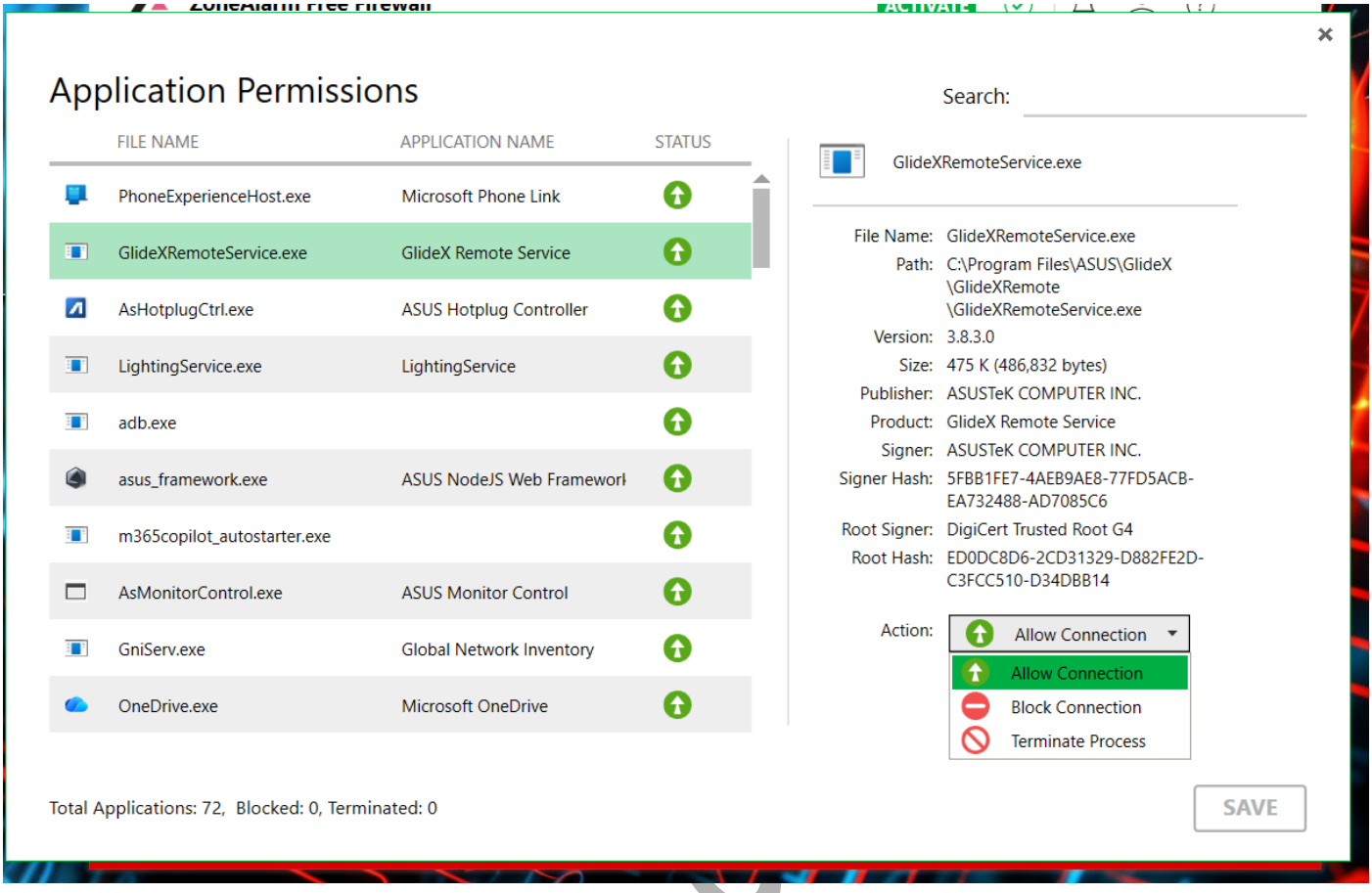
1.1



1.2

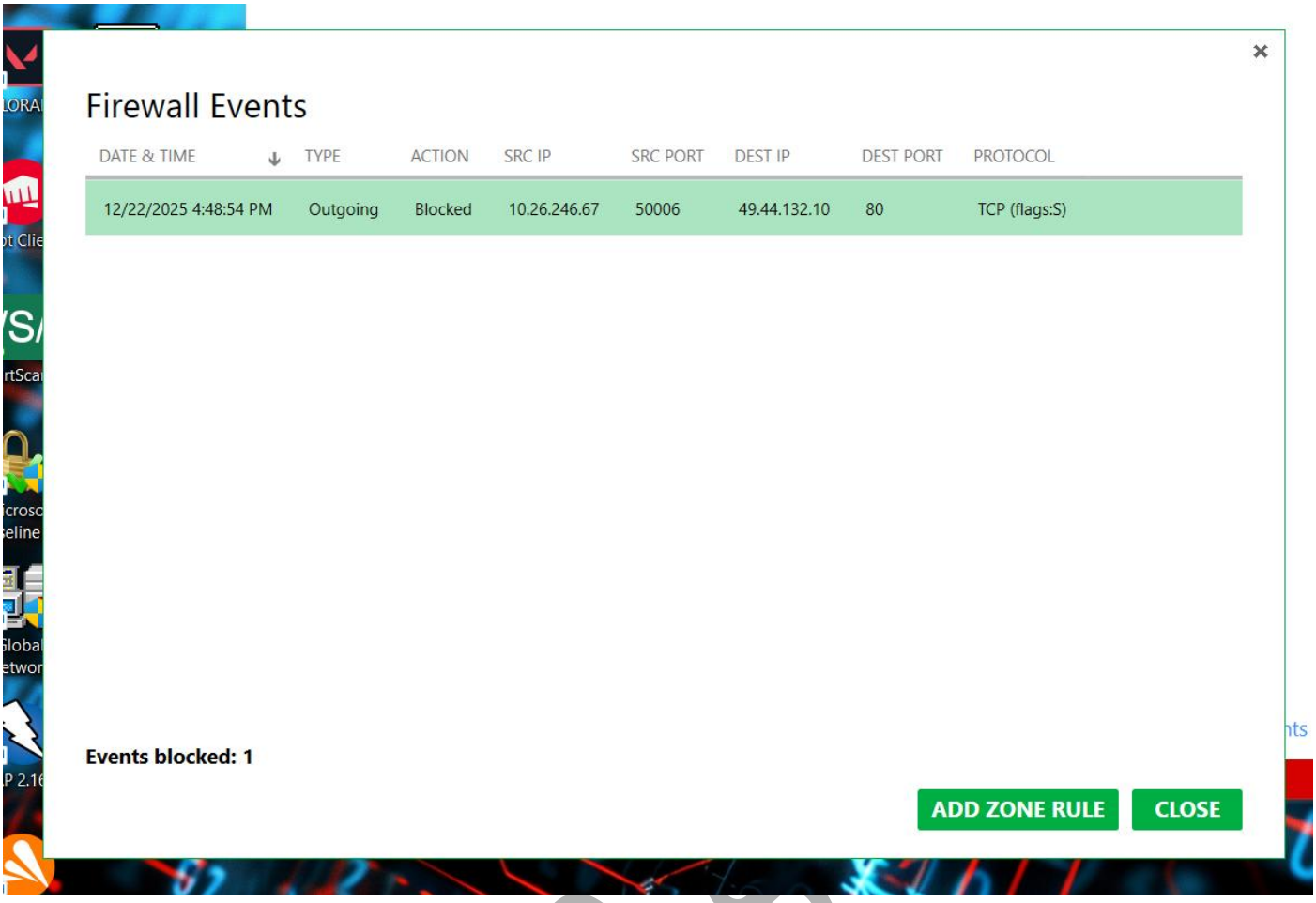
4 . Now , you can allow connection , Block Connection and Terminate Process Action Dropdown: • Allow Connection (Selected) – The firewall allows to access the internet. • Block Connection – Prevents from accessing the internet. • Terminate Process – Stops the process if it is running.

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



1.3

6 . It show all the event


Firewall Events
DATE & TIME
TYPE
ACTION
SRC IP
SRC PORT
DEST IP
DEST PORT
PROTOCOL
12/22/2025 4:48:54 PM
Outgoing
Blocked
10.26.246.67
50006
49.44.132.10
80
TCP (flags:S)
Events blocked: 1
ADD ZONE RULE
CLOSE

1.4

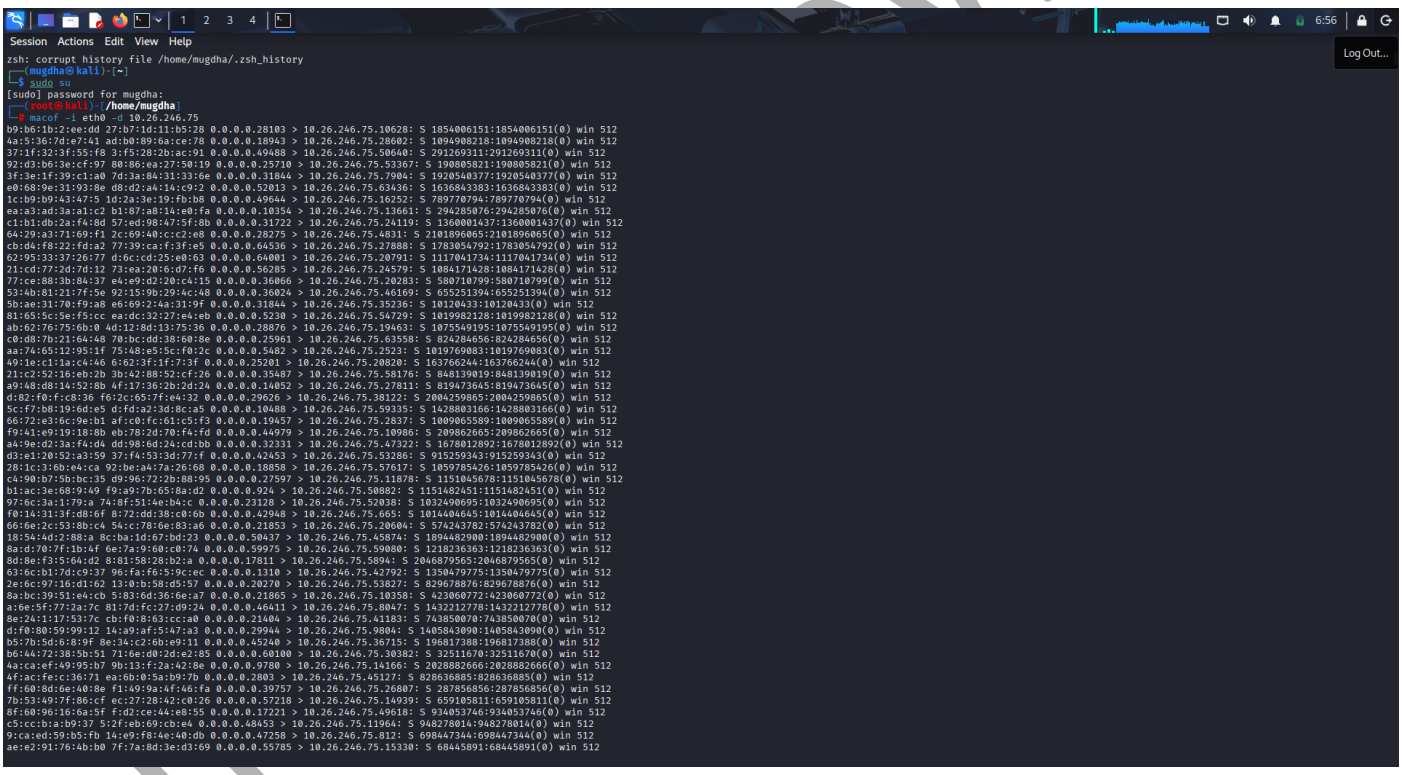
3 . Wireshark :

Wireshark is a free and open-source network protocol analyzer used to capture and inspect packets in real time across networks. It's used for network troubleshooting, security analysis, and protocol development.

Steps :

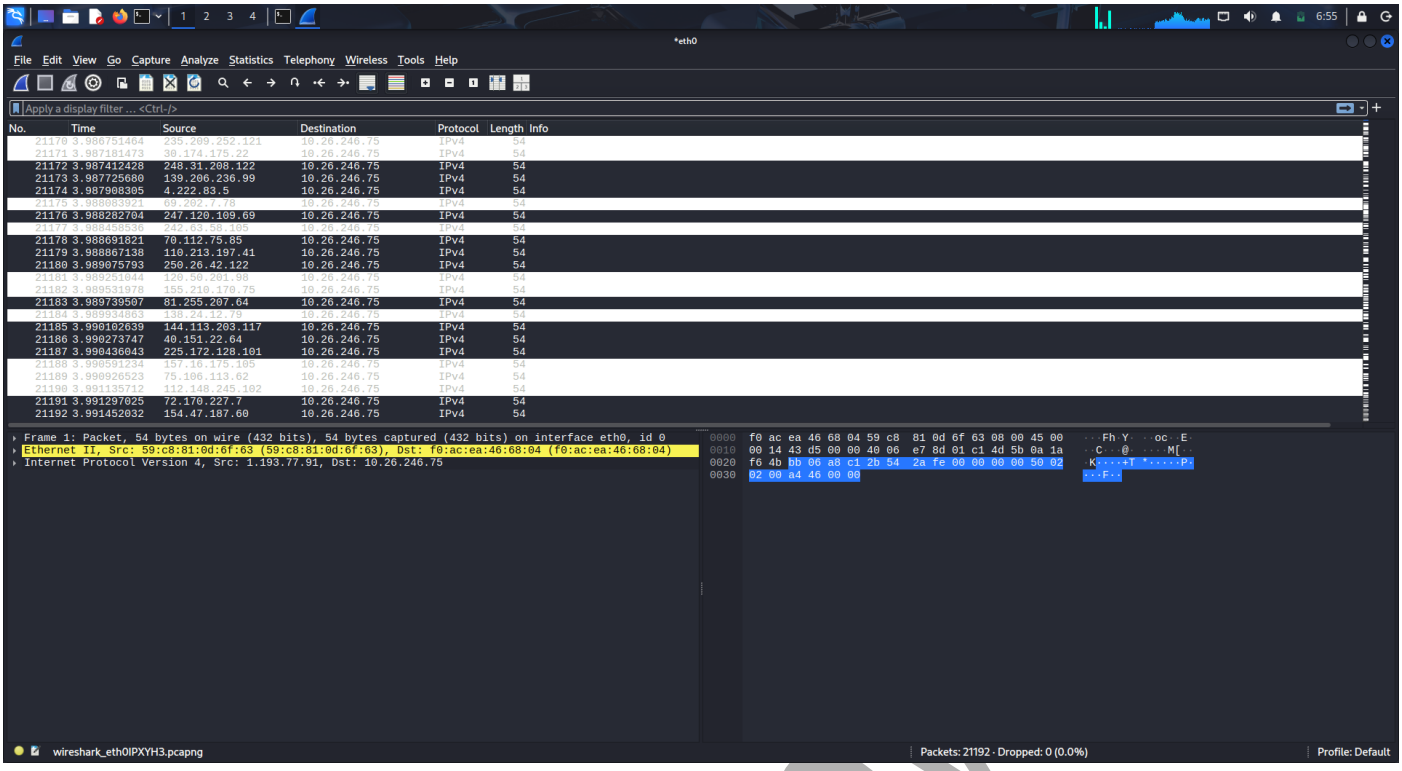
1 . Open Kali linux for Attack on Target • Attack on target

Attack Started



1.1

2 . Now Back to the Victim machine and open Wireshark



1.2

4 . honeybot :

HoneyBOT is a Windows-based honeypot software used for cybersecurity monitoring and intrusion detection. It simulates a vulnerable system or services to attract malicious attackers, allowing security professionals to monitor, detect, and analyze attack behavior in a controlled environment.

Steps :

1 . Attacker Setup: The Kali Linux machine uses hping3 to generate a high volume of UDP packets.

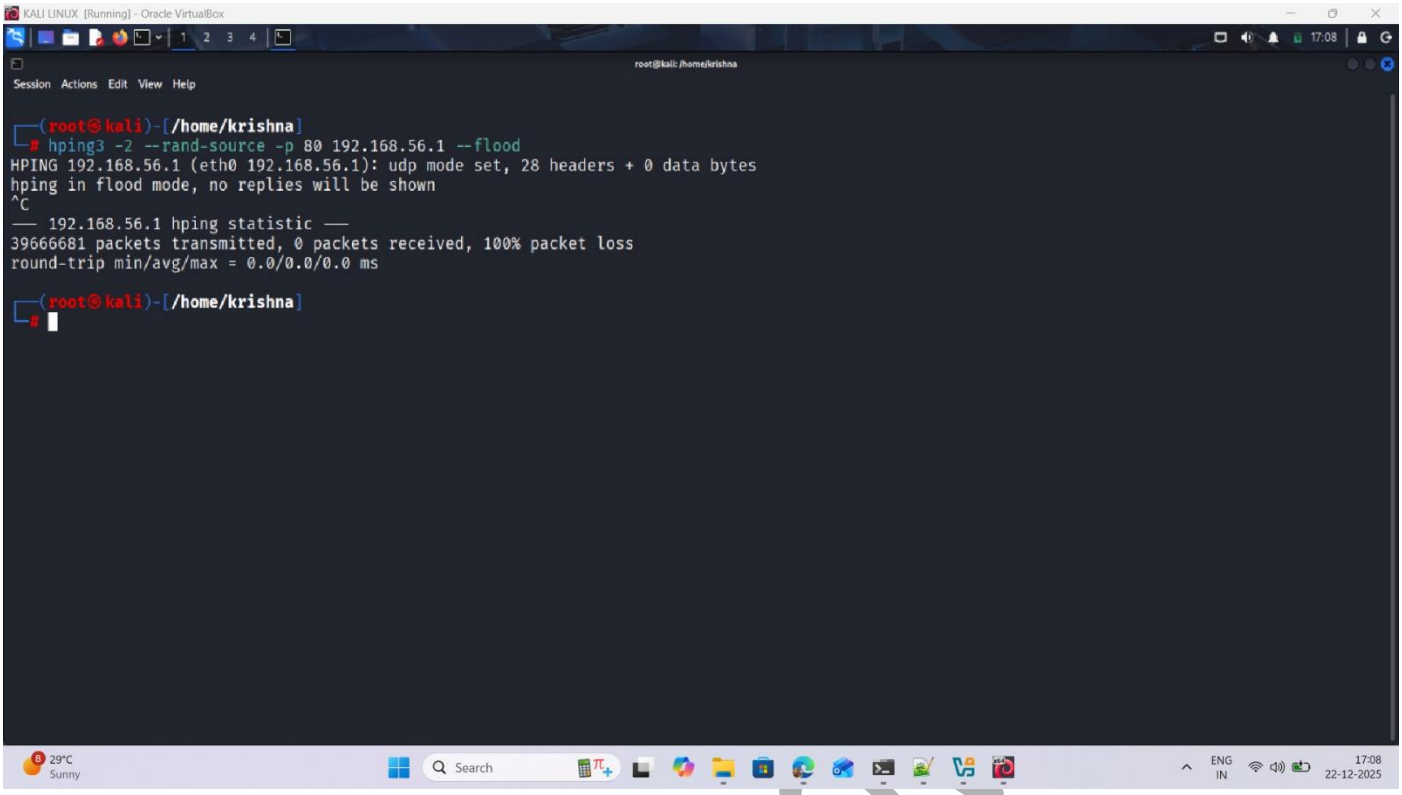
2 . Traffic Injection: The command targets the destination IP on port 80 using the --flood flag for maximum speed.

3 . Source Spoofing: The --rand-source flag randomizes the origin IP of every packet to hide the attacker's identity.

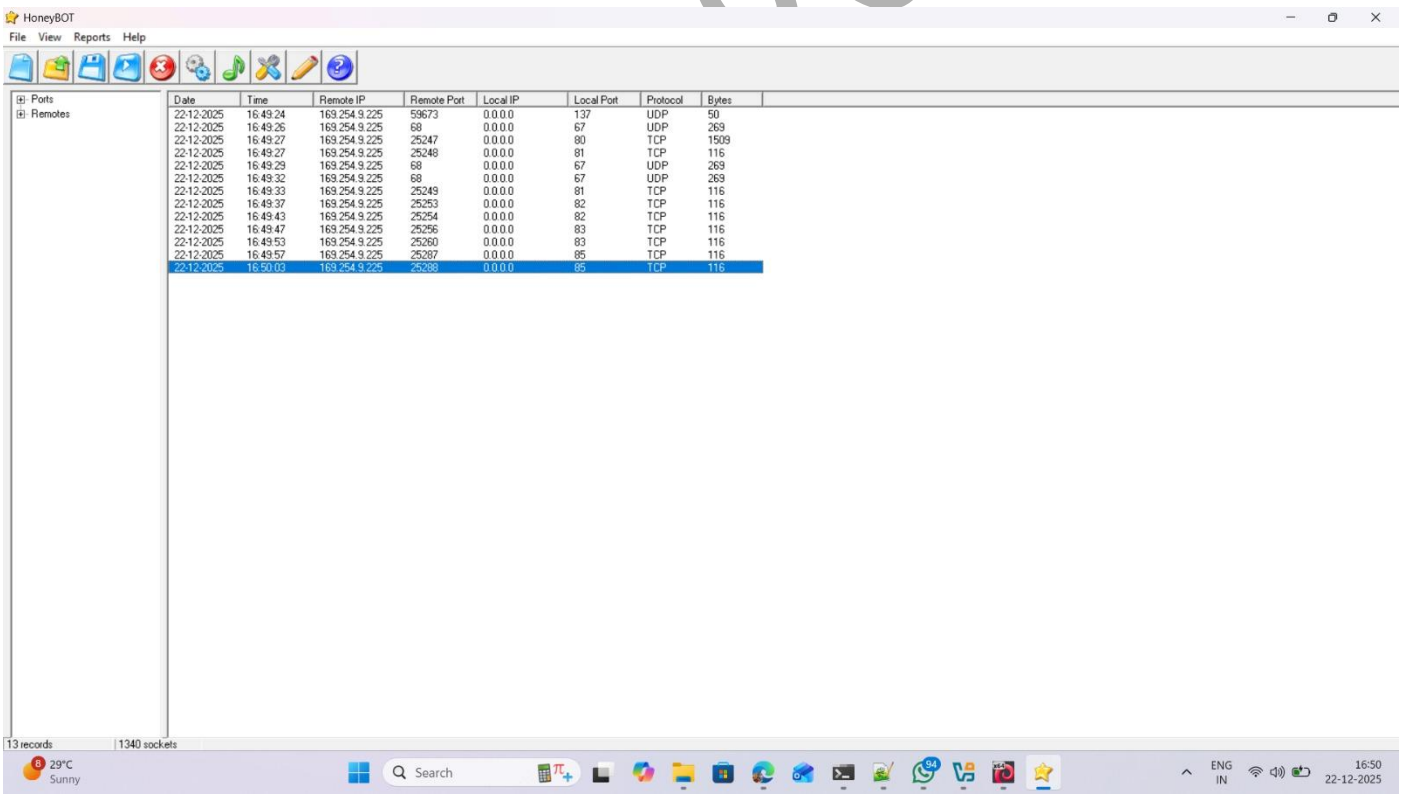
4 . Target Impact: Over 3.9 million packets overwhelm the target's network interface, causing 100% packet loss for legitimate traffic.

5 . Honeypot Capture: The HoneyBOT system on the target side intercepts these connection attempts.

6 . Incident Logging: HoneyBOT records the date, time, and specific ports being hit for security analysis.


KALI LINUX [Running] - Oracle VirtualBox
Session Actions Edit View Help
root@kali: /home/krishna
(root㉿kali)-[/home/krishna]
hping3 -2 --rand-source -p 80 192.168.56.1 --flood
HPING 192.168.56.1 (eth0 192.168.56.1): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.56.1 hping statistic —
39666681 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
(root㉿kali)-[/home/krishna]
#

1.1


HoneyBOT
File View Reports Help
Ports
Remotes
Date Time Remote IP Remote Port Local IP Local Port Protocol Bytes
22-12-2025 16:49:24 169.254.9.225 59673 0.0.0.0 137 UDP 50
22-12-2025 16:49:26 169.254.9.225 68 0.0.0.0 67 UDP 269
22-12-2025 16:49:27 169.254.9.225 25247 0.0.0.0 80 TCP 1509
22-12-2025 16:49:27 169.254.9.225 25248 0.0.0.0 81 TCP 116
22-12-2025 16:49:29 169.254.9.225 68 0.0.0.0 67 UDP 269
22-12-2025 16:49:32 169.254.9.225 68 0.0.0.0 67 UDP 269
22-12-2025 16:49:33 169.254.9.225 25249 0.0.0.0 81 TCP 116
22-12-2025 16:49:37 169.254.9.225 25253 0.0.0.0 82 TCP 116
22-12-2025 16:49:43 169.254.9.225 25254 0.0.0.0 82 TCP 116
22-12-2025 16:49:47 169.254.9.225 25256 0.0.0.0 83 TCP 116
22-12-2025 16:49:53 169.254.9.225 25260 0.0.0.0 83 TCP 116
22-12-2025 16:49:57 169.254.9.225 25287 0.0.0.0 85 TCP 116
22-12-2025 16:50:03 169.254.9.225 25288 0.0.0.0 85 TCP 116
13 records
1340 sockets

1.2