Practical 8

Information & Network Security

Aim: Intrusion Detection System:
Set up and configure an intrusion detection system (IDS) to monitor network traffic and detect potential security breaches or malicious activities.

Definition: An Intrusion Detection System (IDS) is a security tool used to monitor network traffic or system activities for malicious actions or policy violations. It helps identify and alert administrators about potential security breaches, unauthorised access, or other malicious activities within a network or system.

Choose an IDS Solution

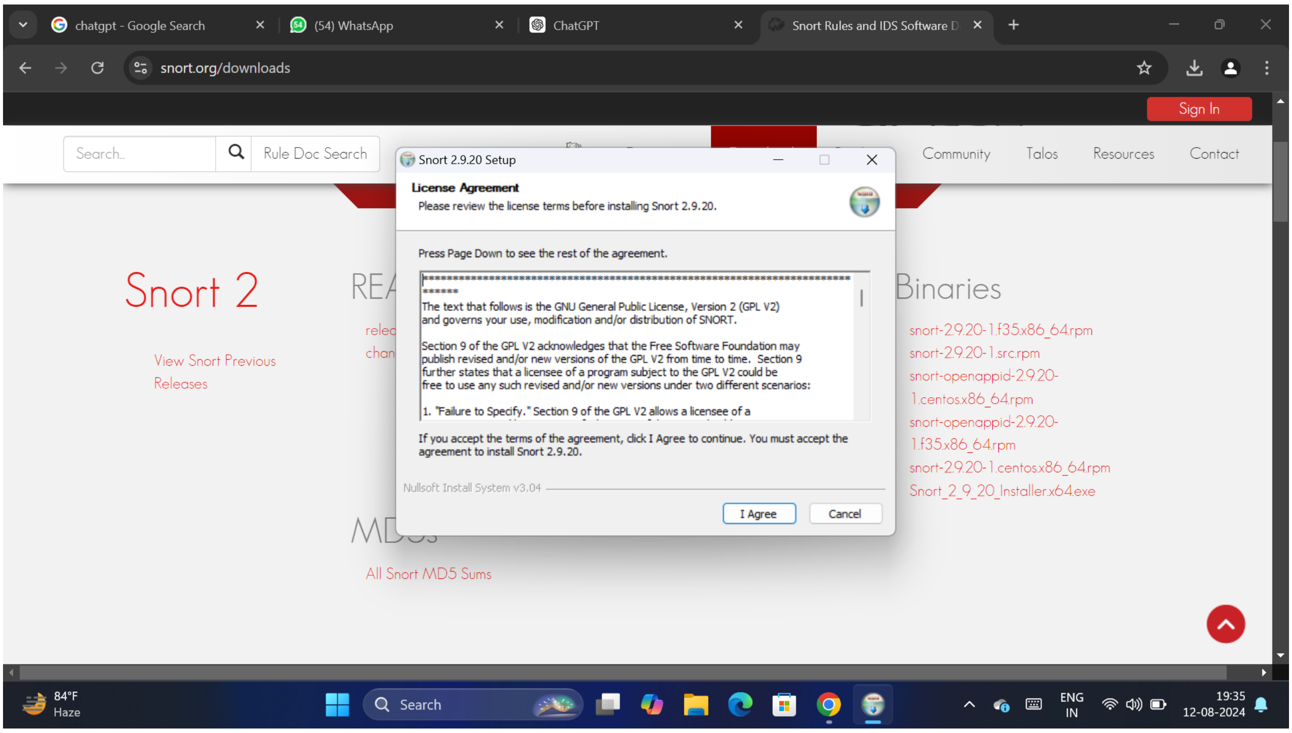
- **Snort**: A popular open-source IDS that can analyse real-time traffic and perform packet logging.

- **Suricata**: Another open-source IDS/IPS that offers multi-threading, making it faster than Snort.

- **OSSEC**: A host-based IDS (HIDS) that focuses on log analysis and integrity checking.

In our case we will use SNORT IDS.

Step 1: Download and Install Snort and it's rules.


chatgpt - Google Search
(54) WhatsApp
ChatGPT
Snort Rules and IDS Software D
snort.org/downloads
Sign In
Search..
Rule Doc Search
Community
Talos
Resources
Contact
Snort 2
View Snort Previous Releases
REA
relea
chan
Binaries
snort-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.src.rpm
snort-openappid-2.9.20-1.centos.x86_64.rpm
snort-openappid-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.centos.x86_64.rpm
Snort_2_9_20_Installer.x64.exe
MD5s
All Snort MD5 Sums
84°F
Haze
Search
ENG
IN
19:35
12-08-2024

Snort 2.9.20 Setup

License Agreement

Please review the license terms before installing Snort 2.9.20.

Press Page Down to see the rest of the agreement.

```
******************************************************************************
******
The text that follows is the GNU General Public License, Version 2 (GPL V2)
and governs your use, modification and/or distribution of SNORT.

Section 9 of the GPL V2 acknowledges that the Free Software Foundation may
publish revised and/or new versions of the GPL V2 from time to time.  Section 9
further states that a licensee of a program subject to the GPL V2 could be
free to use any such revised and/or new versions under two different scenarios:

1. "Failure to Specify." Section 9 of the GPL V2 allows a licensee of a
```

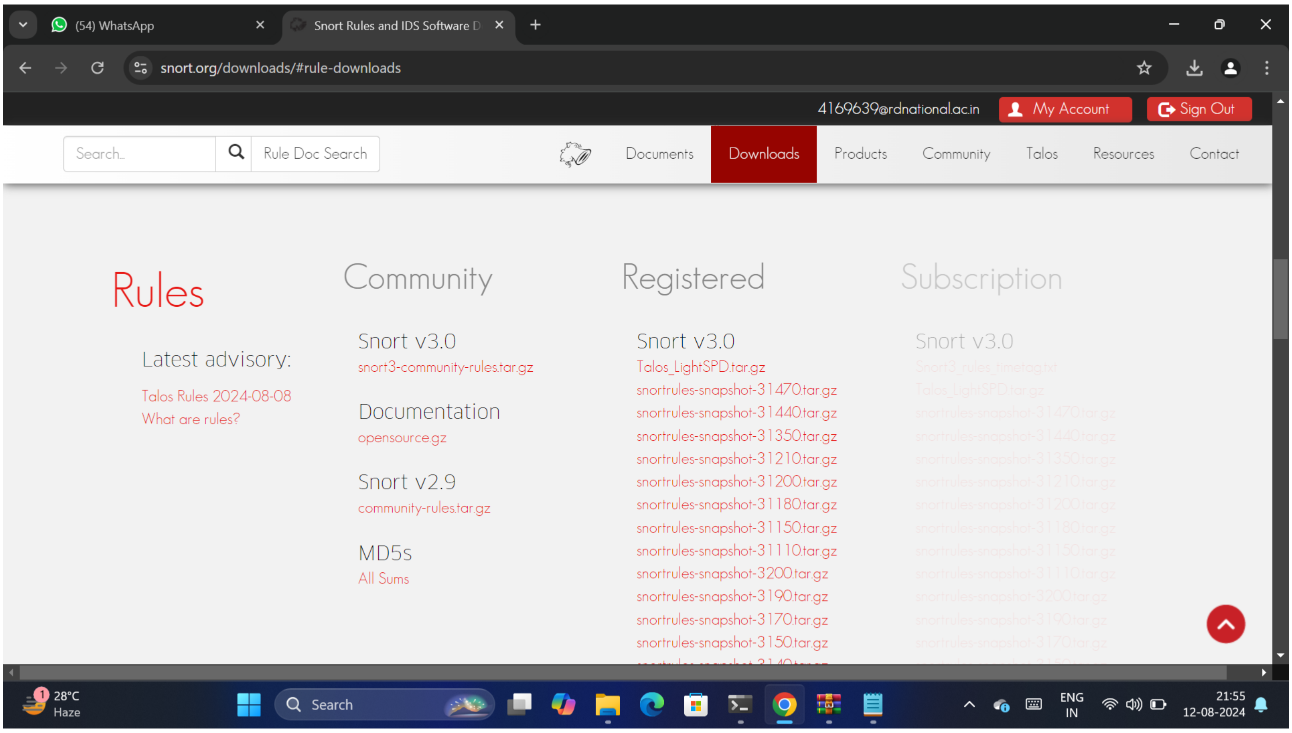
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Snort 2.9.20.

Nullsoft Install System v3.04

Practical 8

Information & Network Security

- **Register and Download the Registered Snort Rules:**



Rules

Latest advisory:

Talos Rules 2024-08-08

What are rules?

Community

Snort v3.0

snort3-community-rules.tar.gz

Documentation

opensource.gz

Snort v2.9

community-rules.tar.gz

MD5s

All Sums

Registered

Snort v3.0

Talos_LightSPD.tar.gz

snortrules-snapshot-31470.tar.gz

snortrules-snapshot-31440.tar.gz

snortrules-snapshot-31350.tar.gz

snortrules-snapshot-31210.tar.gz

snortrules-snapshot-31200.tar.gz

snortrules-snapshot-31180.tar.gz

snortrules-snapshot-31150.tar.gz

snortrules-snapshot-31110.tar.gz

snortrules-snapshot-3200.tar.gz

snortrules-snapshot-3190.tar.gz

snortrules-snapshot-3170.tar.gz

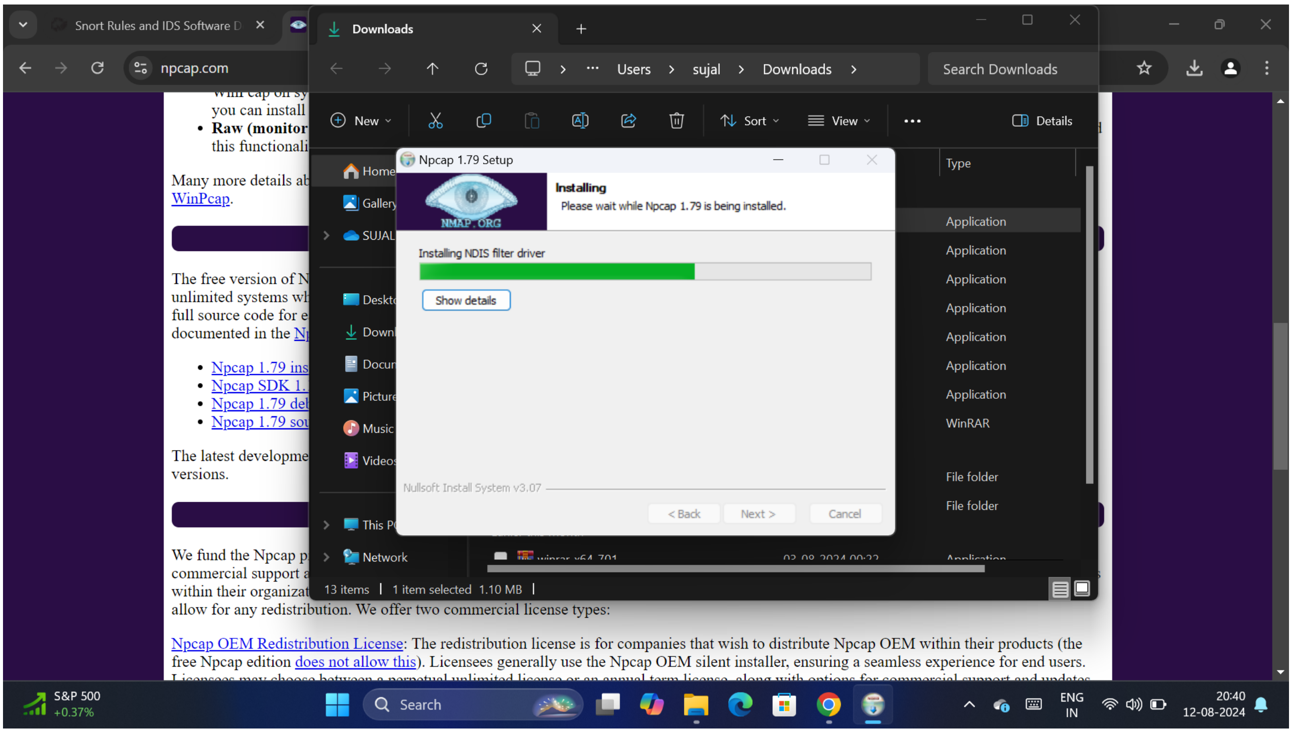
snortrules-snapshot-3150.tar.gz

Subscription

Snort v3.0

- **Extract the snortrules-snapshot-29111.tar.gz folder.**
- **Copy the files of the rules folder from the snortrules-snapshot-29111.tar.gz and paste it in the rules folder which is inside the Snort Directory.**

Step 2: Install Ncap



Npcap 1.79 Setup

Installing

Please wait while Npcap 1.79 is being installed.

Installing NDIS filter driver

Show details

Nullsoft Install System v3.07

< Back | Next > | Cancel

you can install

- **Raw (monitor** this functionali

Many more details ab WinPcap.

The free version of N unlimited systems wh full source code for e documented in the Np

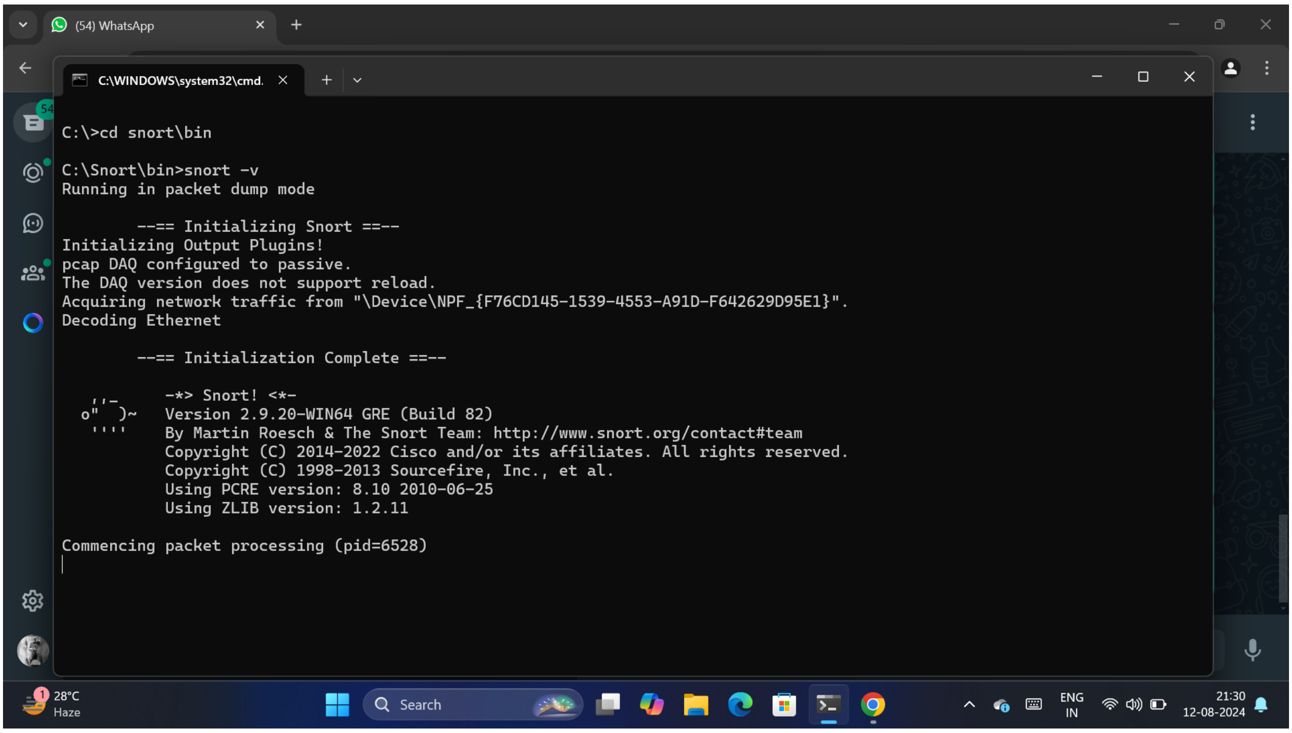
- Npcap 1.79 ins
- Npcap SDK 1.
- Npcap 1.79 de
- Npcap 1.79 sou

The latest developme versions.

We fund the Npcap p commercial support a within their organizat allow for any redistribution. We offer two commercial license types:

Npcap OEM Redistribution License: The redistribution license is for companies that wish to distribute Npcap OEM within their products (the free Npcap edition does not allow this). Licensees generally use the Npcap OEM silent installer, ensuring a seamless experience for end users.

- **Verify The Download:**

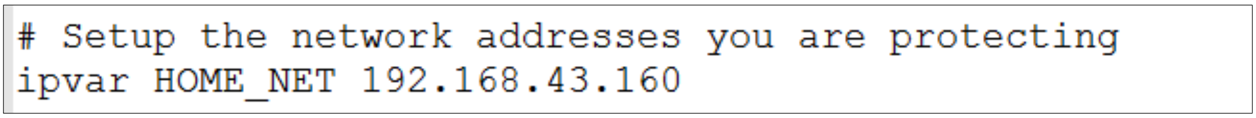


```
C:\>cd snort\bin

C:\Snort\bin>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{F76CD145-1539-4553-A91D-F642629D95E1}".
Decoding Ethernet

        --== 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

Commencing packet processing (pid=6528)
```

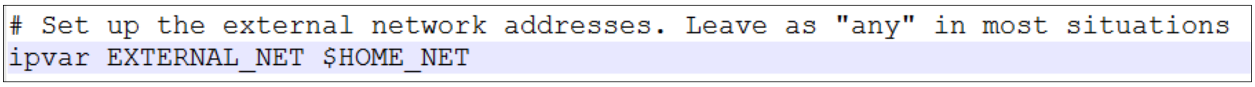
Step 3: Config Snort.

Open the *"snort.conf"* file from the etc folder which is inside the Snort Folder and make this changes:

- **Set the network variables in Step 1 of snort.conf file by typing the IP address (Of your Host). Set up the external network address as home network ($HOME_NET).**

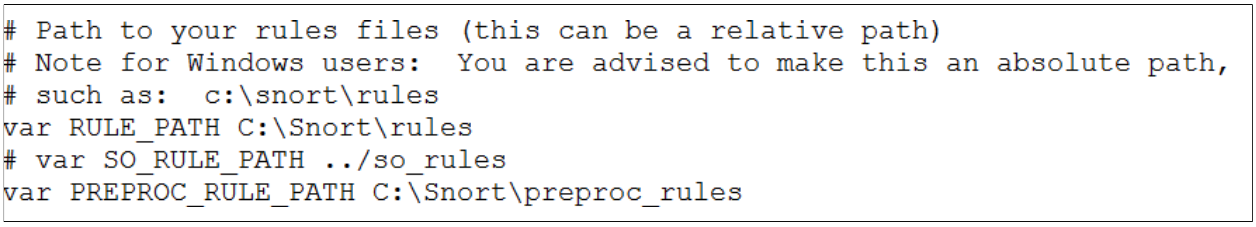


```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.43.160
```

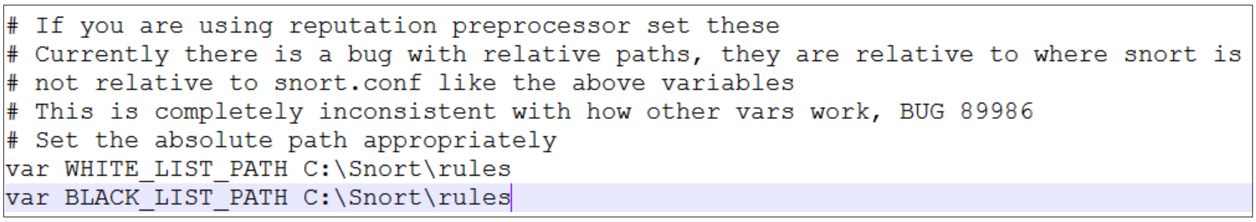


```
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET $HOME_NET
```

- **Set the path of the rules files as "C:\Snort\rules" and "C:\Snort\preproc_rules" as shown in Figure below. Set the white list and black list path as to "C:\Snort\rules" as shown in Figure.**

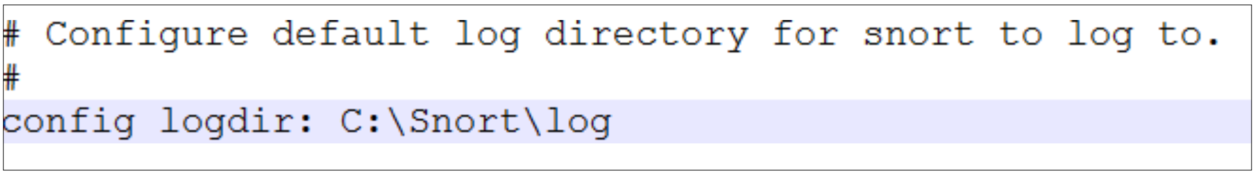


```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH C:\Snort\rules
# var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```



```
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# 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
```

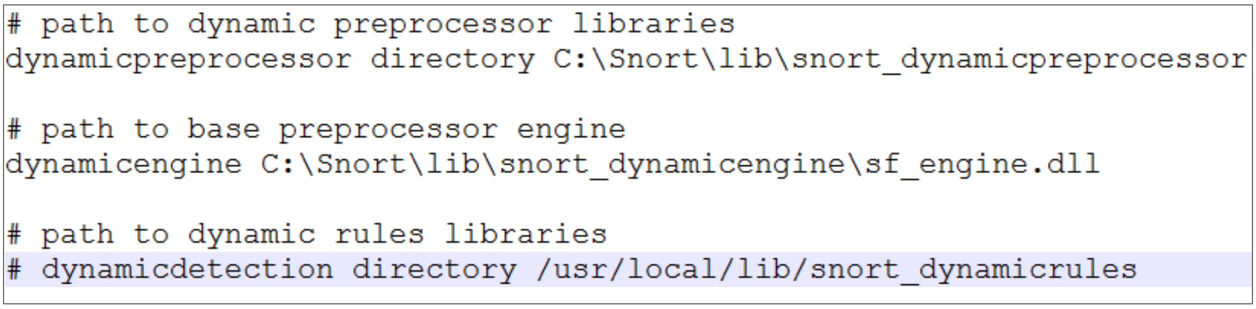
- **Configure the decoder in Step 2 of snort.conf file by setting the path of the log directory as “C:\Snort\log” as shown in Figure.**



```
# Configure default log directory for snort to log to.
#
config logdir: C:\Snort\log
```

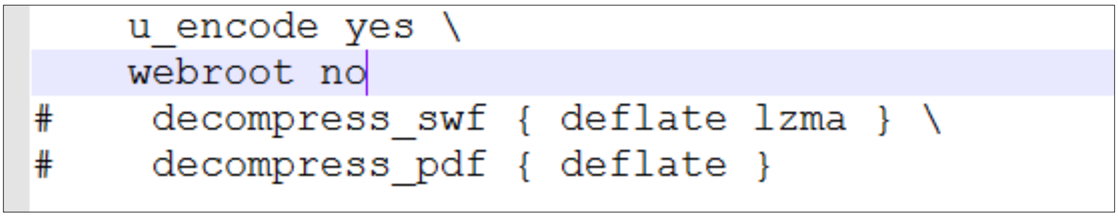
- **There is no change in Step 3 (Configure the base detection engine) of snort.conf file.**

- **Configure dynamic loaded libraries in Step 4 of snort.conf file by setting the path “C:\Snort\lib\snort_dynamicpreprocessor” and base preprocessor engine as “C:\Snort\lib\snort_dynamicengine\sf_engine.dll” as shown in Figure.**

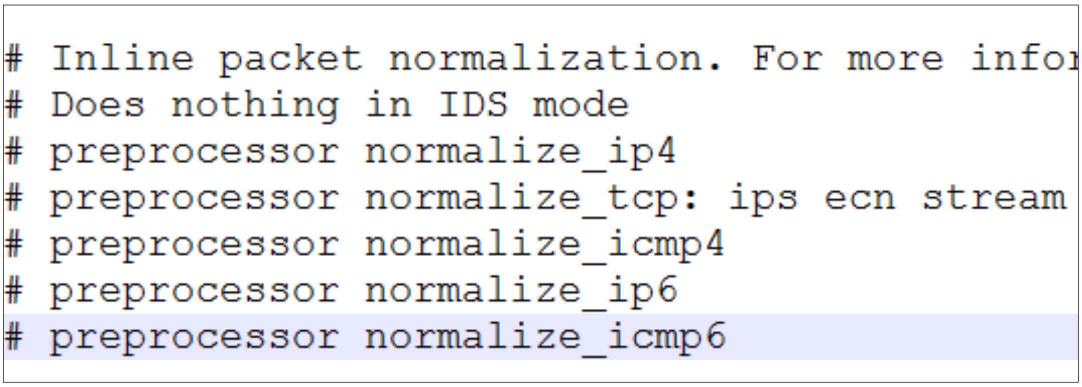


```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# 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
```

- **Configure preprocessors in Step 5 of snort.conf file by removing the "\" and putting decompress_swf and decompress_pdf in comments as shown in Figure. Also, put the preprocessors in comments as shown in Figure. Also, put the preprocessor bo in comments as shown in Figure. Delete comment from preprocessor sfportscan as shown in Figure.**

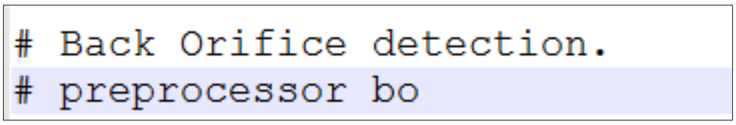


```
    u_encode yes \
    webroot no
#     decompress_swf { deflate lzma } \
#     decompress_pdf { deflate }
```

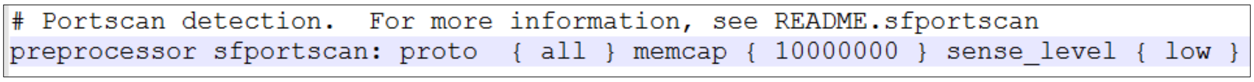


```
# Inline packet normalization. For more infor
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```

Put preprocessor in comments



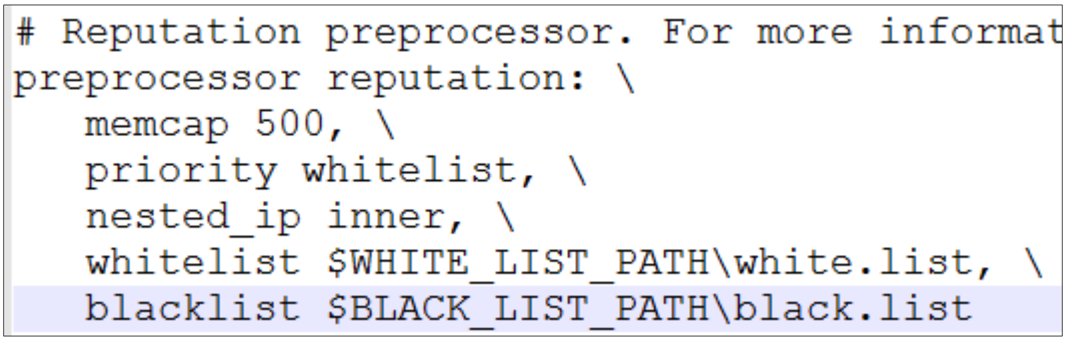
```
# Back Orifice detection.
# preprocessor bo
```



```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

Delete Comment from preprocessor sfportscan

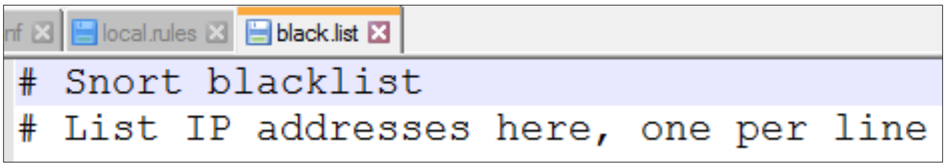
- Set path to white list and black list as shown in Figure. Create a new white list and black list as shown in Figure. Save these files in rules directory.



```
# Reputation preprocessor. For more informat
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\white.list, \
   blacklist $BLACK_LIST_PATH\black.list
```

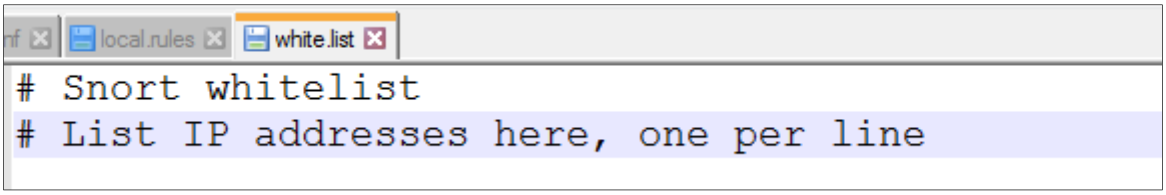
Set Path to White and Black list

Create a Black list



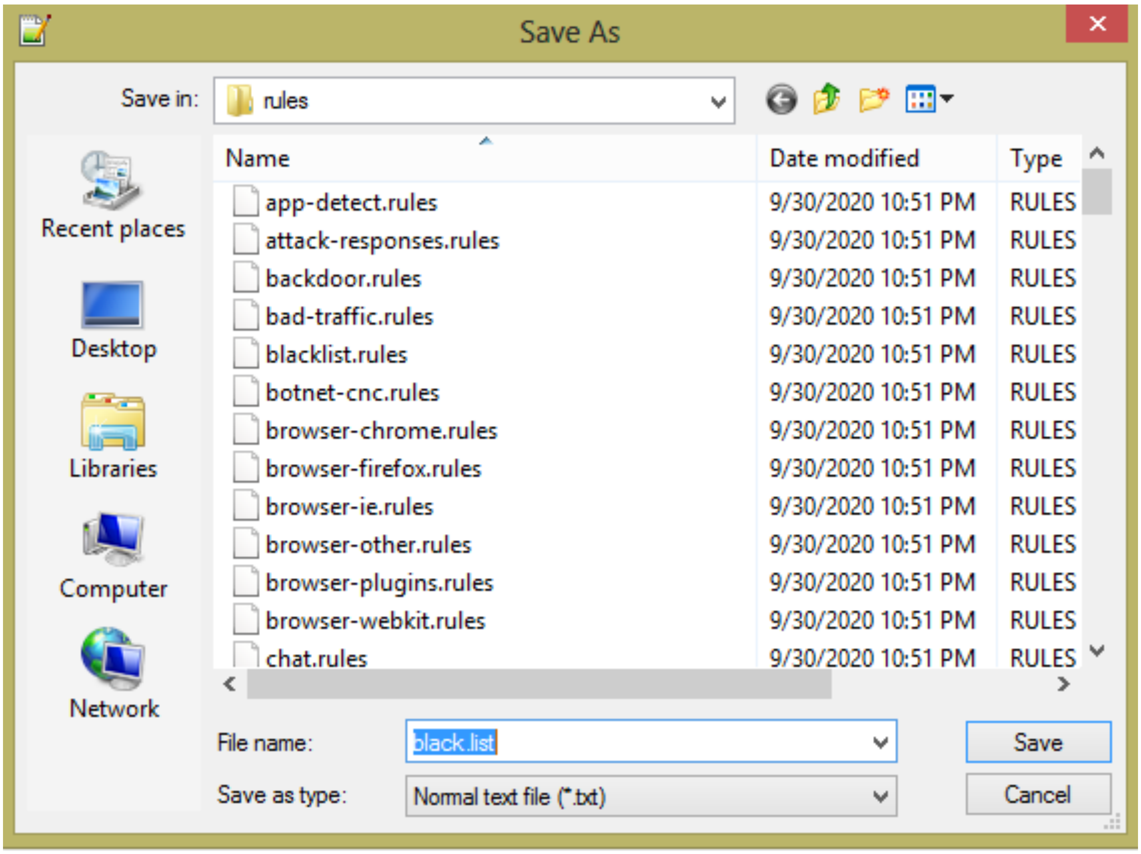
```
# Snort blacklist
# List IP addresses here, one per line
```

Create a White list



```
# Snort whitelist
# List IP addresses here, one per line
```

Save Black List in rules Directory



Save in: rules

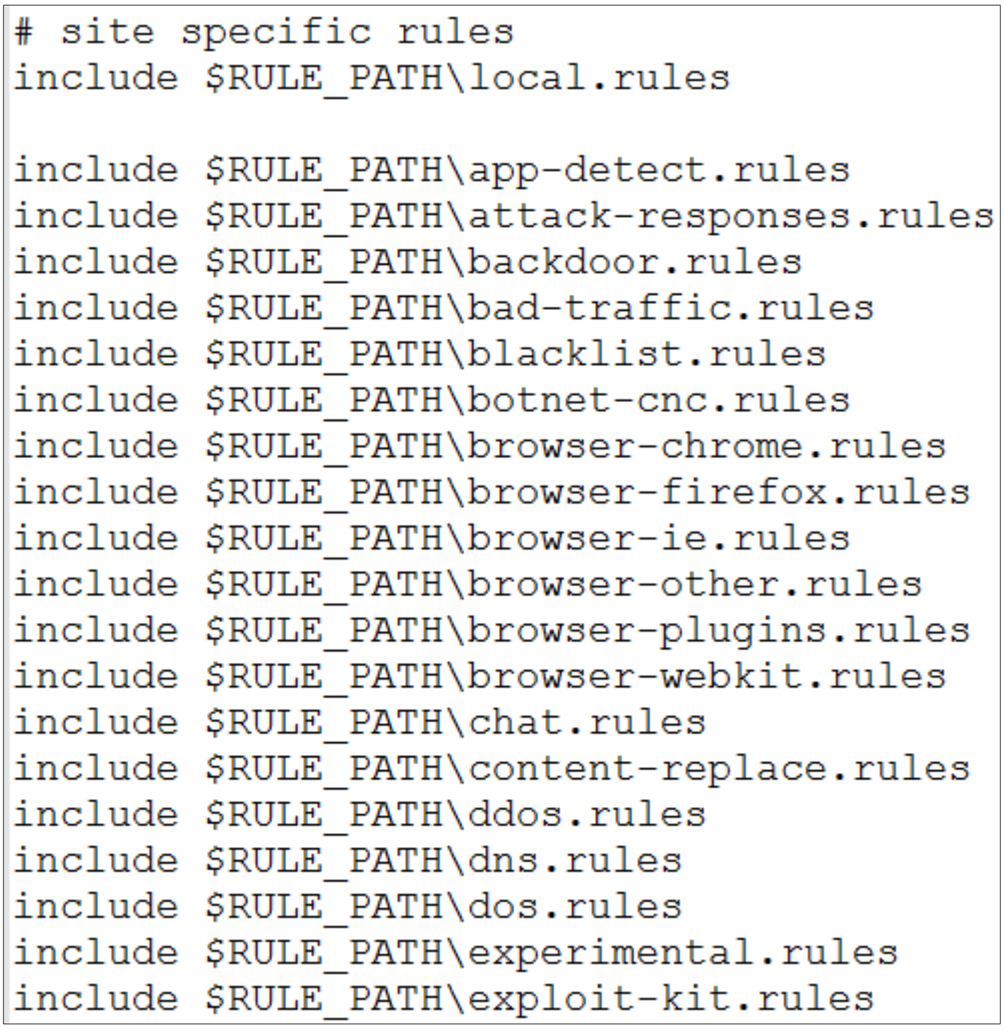
Name	Date modified	Type
app-detect.rules	9/30/2020 10:51 PM	RULES
attack-responses.rules	9/30/2020 10:51 PM	RULES
backdoor.rules	9/30/2020 10:51 PM	RULES
bad-traffic.rules	9/30/2020 10:51 PM	RULES
blacklist.rules	9/30/2020 10:51 PM	RULES
botnet-cnc.rules	9/30/2020 10:51 PM	RULES
browser-chrome.rules	9/30/2020 10:51 PM	RULES
browser-firefox.rules	9/30/2020 10:51 PM	RULES
browser-ie.rules	9/30/2020 10:51 PM	RULES
browser-other.rules	9/30/2020 10:51 PM	RULES
browser-plugins.rules	9/30/2020 10:51 PM	RULES
browser-webkit.rules	9/30/2020 10:51 PM	RULES
chat.rules	9/30/2020 10:51 PM	RULES

File name: black.list

Save as type: Normal text file (*.txt)

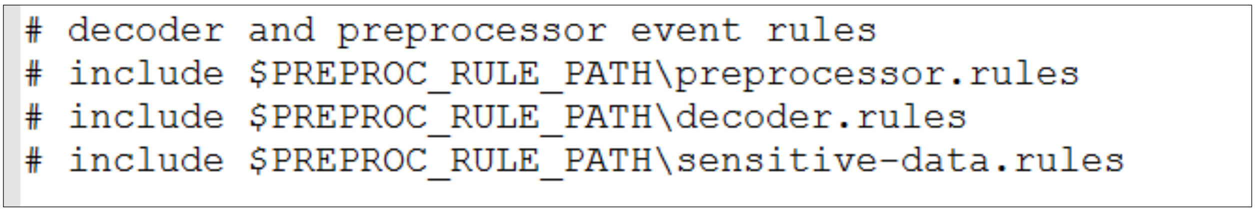
- **There is no change in Step 6 (Configure output plugins) of snort.conf file.**

- **Customize rule set in Step 7 of snort.conf file by replacing the forward slash “/” with backslash “\” as shown below (applicable for Windows operating system).**



```
# site specific rules
include $RULE_PATH\local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
```

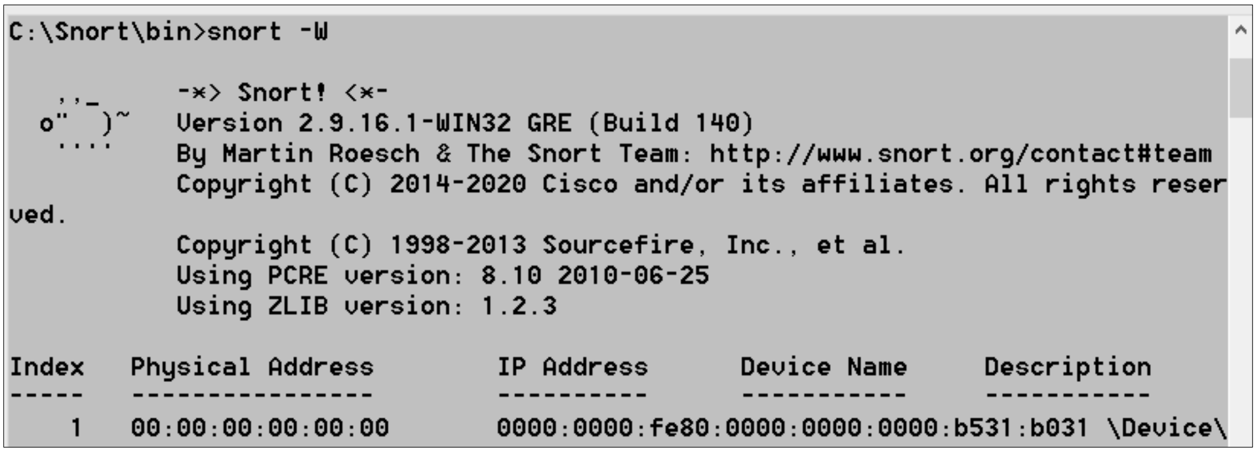
- **Customize preprocessor and decoder alerts in Step 8 of snort.conf file by replacing the forward slash "/" with backslash "\" as shown in Figure (applicable for Windows operating system).**



```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

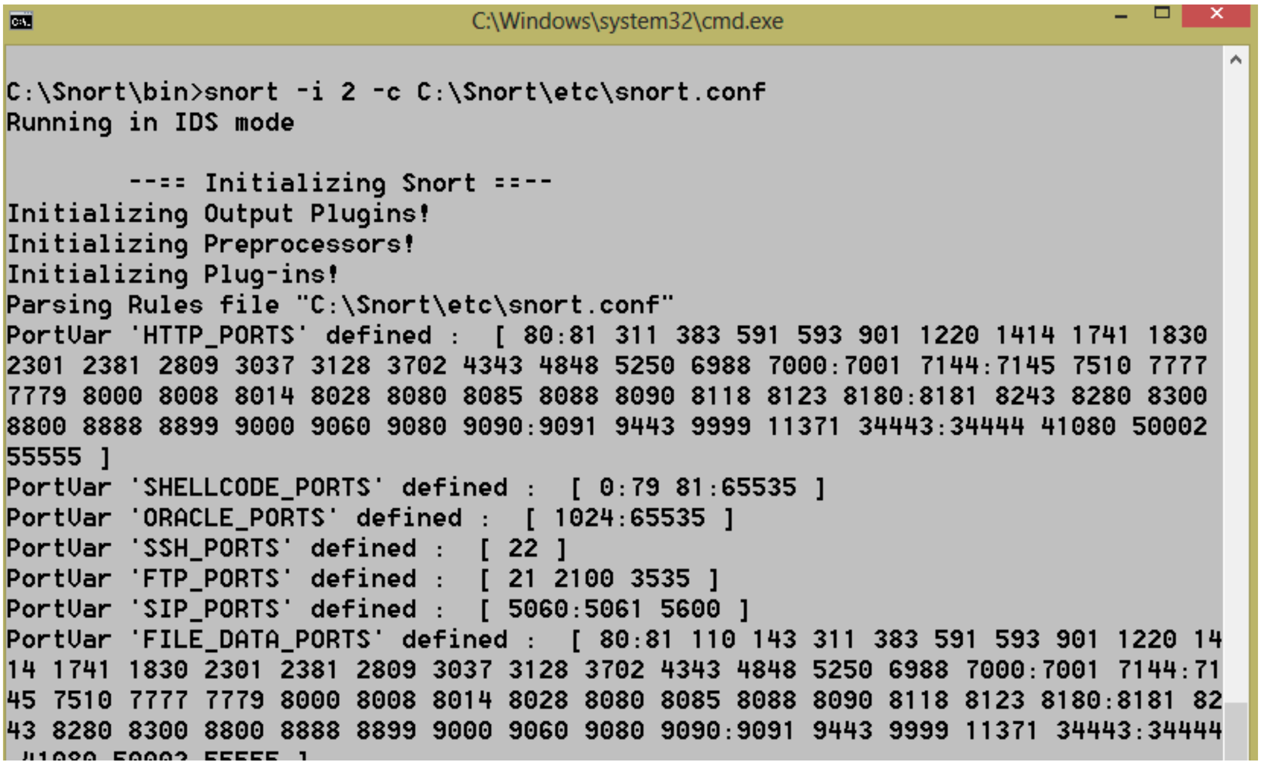
- **There is no change in Step 9 (Customize shared object snort rules) of snort.conf file.**

Step 4: Open the command prompt and go to "C:\Snort\bin" and type "snort –W" to check the available interface.



```
C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16.1-WIN32 GRE (Build 140)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:b531:b031  \Device\
```

- Execute the Snort tool in the command prompt by typing "snort –i 2 –c C:\Snort\etc\snort.conf" where *i* is the interface *c* is the configuration file.

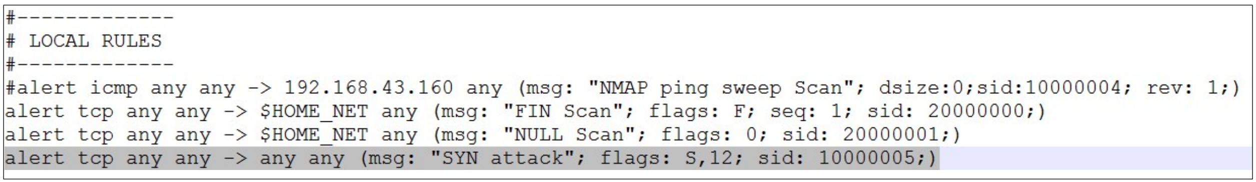


```
C:\Snort\bin>snort -i 2 -c C:\Snort\etc\snort.conf
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 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 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002
55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 14
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
 41080 50002 55555 ]
```

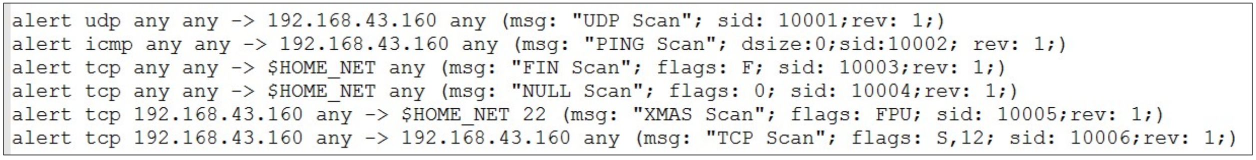
Execute Snort Tool

Step 4: **After running Snort in IDS mode, the next step is to write rules in “local.rules” file as shown in Figure 39. For example, the following rules can be added to detect SYN attack, UDP scan, PINK scan, FIN scan, NULL scan, XMAS scan, and TCP scan.**

- **alert tcp any any -> any any (msg: "SYN attack"; flags: S,12; sid: 10000005;)**
- **alert udp any any -> 192.168.43.160 any (msg: "UDP Scan"; sid: 10001;rev:1;)**
- **alert icmp any any -> 192.168.43.160 any (msg: "PING Scan"; dsize:0;sid:10002; rev: 1;)**
- **alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; sid: 10003;rev: 1;)**
- **alert tcp any any -> $HOME_NET any (msg: "NULL Scan"; flags: 0; sid: 10004;rev: 1;)**
- **alert tcp 192.168.43.160 any -> $HOME_NET 22 (msg: "XMAS Scan"; flags: FPU; sid: 10005;rev: 1;)**
- **alert tcp 192.168.43.160 any -> 192.168.43.160 any (msg: "TCP Scan"; flags: S,12; sid: 10006;rev: 1;)**

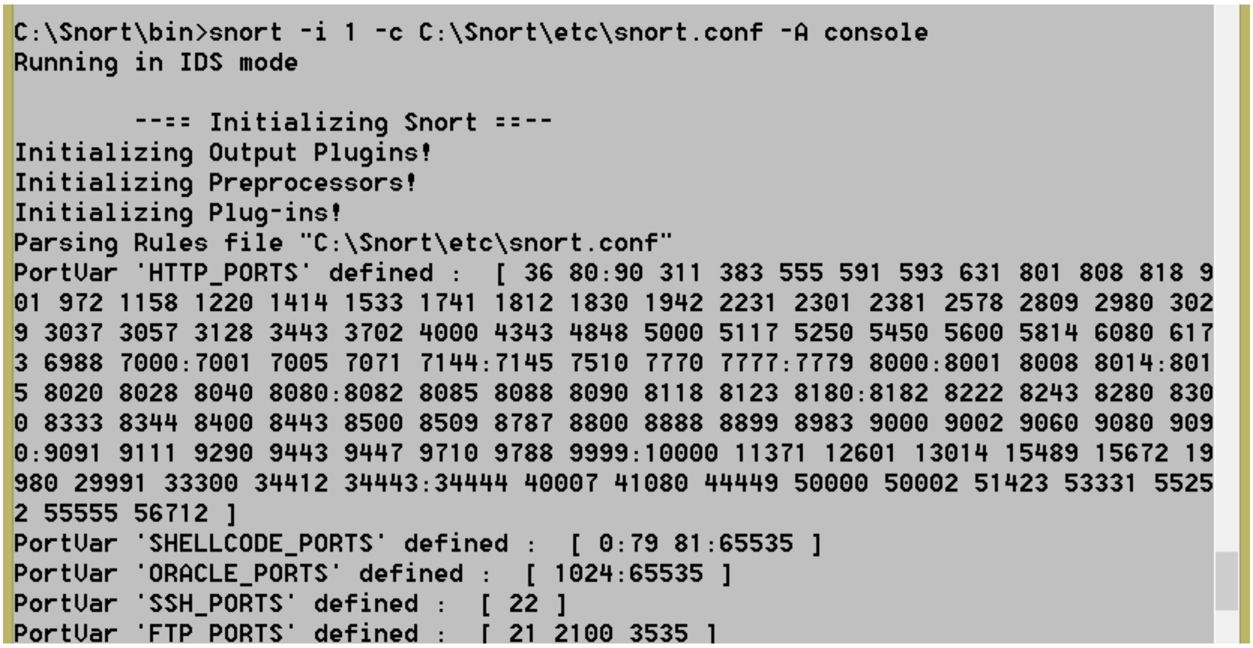


```
#-------------
# LOCAL RULES
#-------------
#alert icmp any any -> 192.168.43.160 any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; seq: 1; sid: 20000000;)
alert tcp any any -> $HOME_NET any (msg: "NULL Scan"; flags: 0; sid: 20000001;)
alert tcp any any -> any any (msg: "SYN attack"; flags: S,12; sid: 10000005;)
```



```
alert udp any any -> 192.168.43.160 any (msg: "UDP Scan"; sid: 10001;rev: 1;)
alert icmp any any -> 192.168.43.160 any (msg: "PING Scan"; dsize:0;sid:10002; rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; sid: 10003;rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "NULL Scan"; flags: 0; sid: 10004;rev: 1;)
alert tcp 192.168.43.160 any -> $HOME_NET 22 (msg: "XMAS Scan"; flags: FPU; sid: 10005;rev: 1;)
alert tcp 192.168.43.160 any -> 192.168.43.160 any (msg: "TCP Scan"; flags: S,12; sid: 10006;rev: 1;)
```

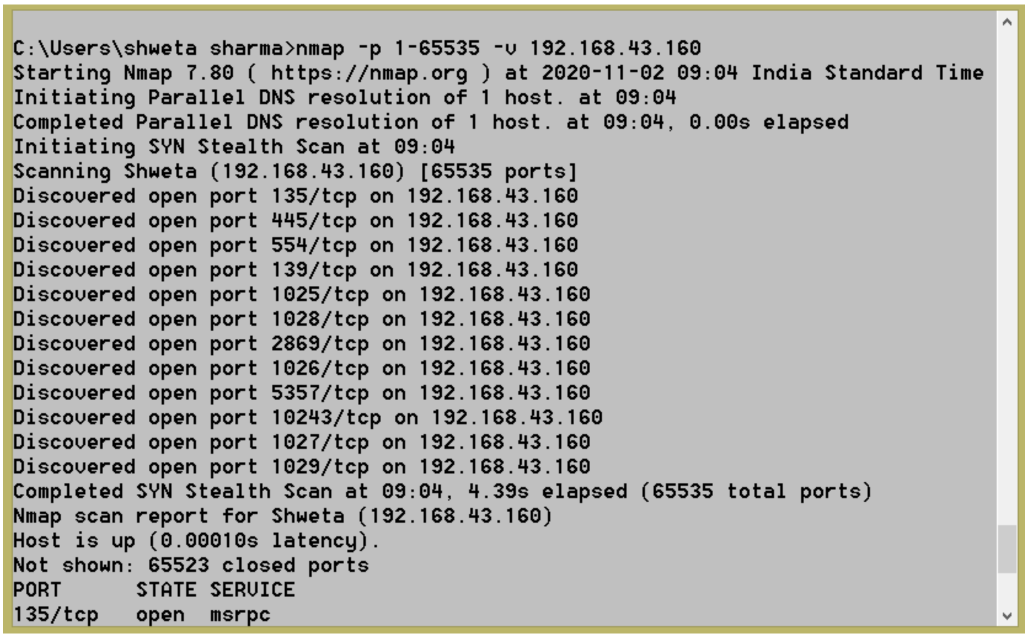
Step 4: Execute Snort in IDS mode by typing "snort –i 1 –c C:\Snort\etc\snort.conf –A console" in the command prompt and press Enter.



```
C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 383 555 591 593 631 801 808 818 9
01 972 1158 1220 1414 1533 1741 1812 1830 1942 2231 2301 2381 2578 2809 2980 302
9 3037 3057 3128 3443 3702 4000 4343 4848 5000 5117 5250 5450 5600 5814 6080 617
3 6988 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008 8014:801
5 8020 8028 8040 8080:8082 8085 8088 8090 8118 8123 8180:8182 8222 8243 8280 830
0 8333 8344 8400 8443 8500 8509 8787 8800 8888 8899 8983 9000 9002 9060 9080 909
0:9091 9111 9290 9443 9447 9710 9788 9999:10000 11371 12601 13014 15489 15672 19
980 29991 33300 34412 34443:34444 40007 41080 44449 50000 50002 51423 53331 5525
2 55555 56712 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
```

- **Perform network scanning attacks with nmap by typing "nmap –p 1-65535 –v 192.168.43.160" in the command prompt. where *p* is the port number and *v* is the verbose mode. The network scanning attacks can be performed with Zenmap tool.**

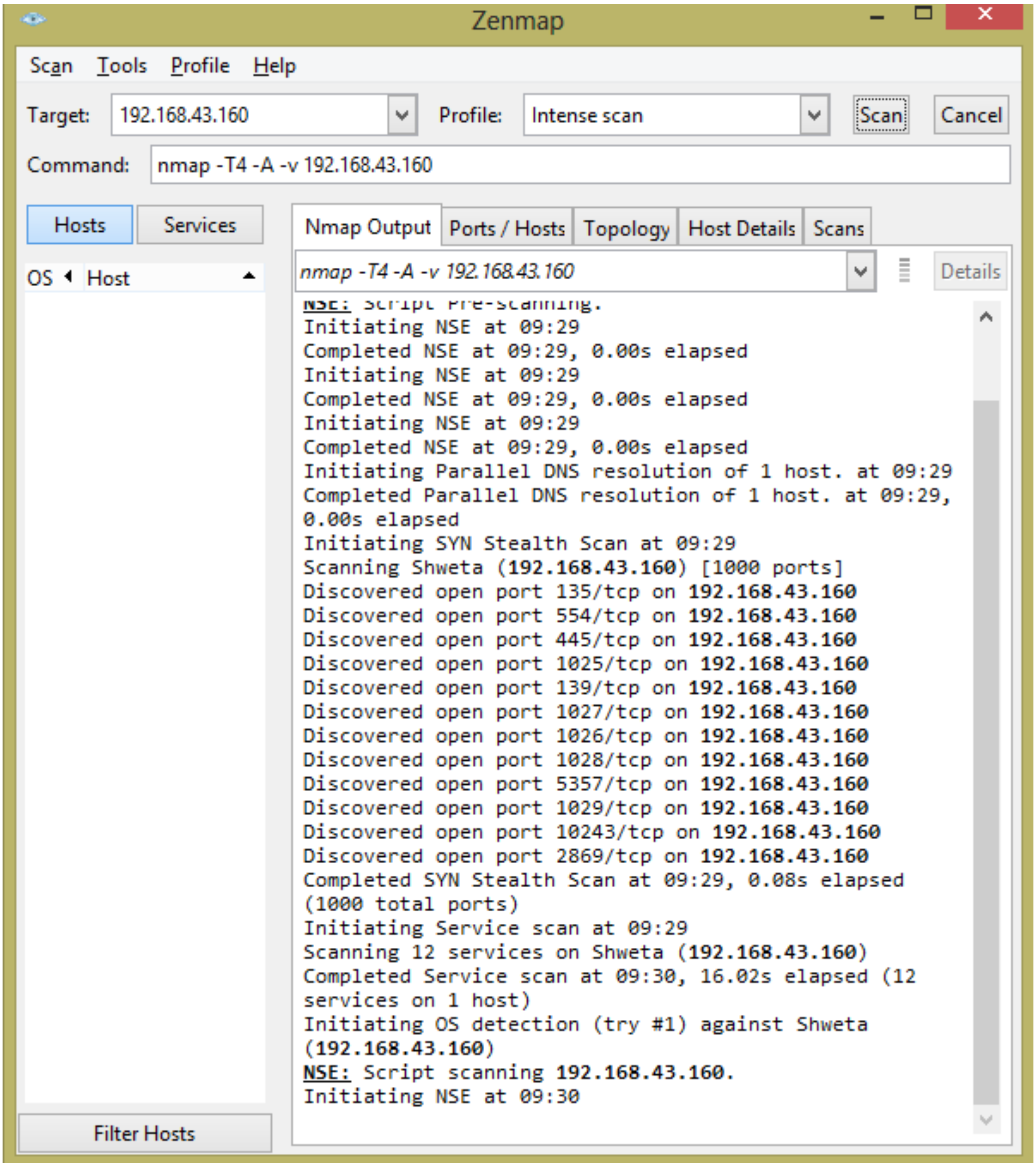
Network Scanning Attack with Nmap Tool



```
C:\Users\shweta sharma>nmap -p 1-65535 -v 192.168.43.160
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-02 09:04 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 09:04
Completed Parallel DNS resolution of 1 host. at 09:04, 0.00s elapsed
Initiating SYN Stealth Scan at 09:04
Scanning Shweta (192.168.43.160) [65535 ports]
Discovered open port 135/tcp on 192.168.43.160
Discovered open port 445/tcp on 192.168.43.160
Discovered open port 554/tcp on 192.168.43.160
Discovered open port 139/tcp on 192.168.43.160
Discovered open port 1025/tcp on 192.168.43.160
Discovered open port 1028/tcp on 192.168.43.160
Discovered open port 2869/tcp on 192.168.43.160
Discovered open port 1026/tcp on 192.168.43.160
Discovered open port 5357/tcp on 192.168.43.160
Discovered open port 10243/tcp on 192.168.43.160
Discovered open port 1027/tcp on 192.168.43.160
Discovered open port 1029/tcp on 192.168.43.160
Completed SYN Stealth Scan at 09:04, 4.39s elapsed (65535 total ports)
Nmap scan report for Shweta (192.168.43.160)
Host is up (0.00010s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
```

Practical 8

Network Scanning Attack with Zenmap Tool



Target: 192.168.43.160

Profile: Intense scan

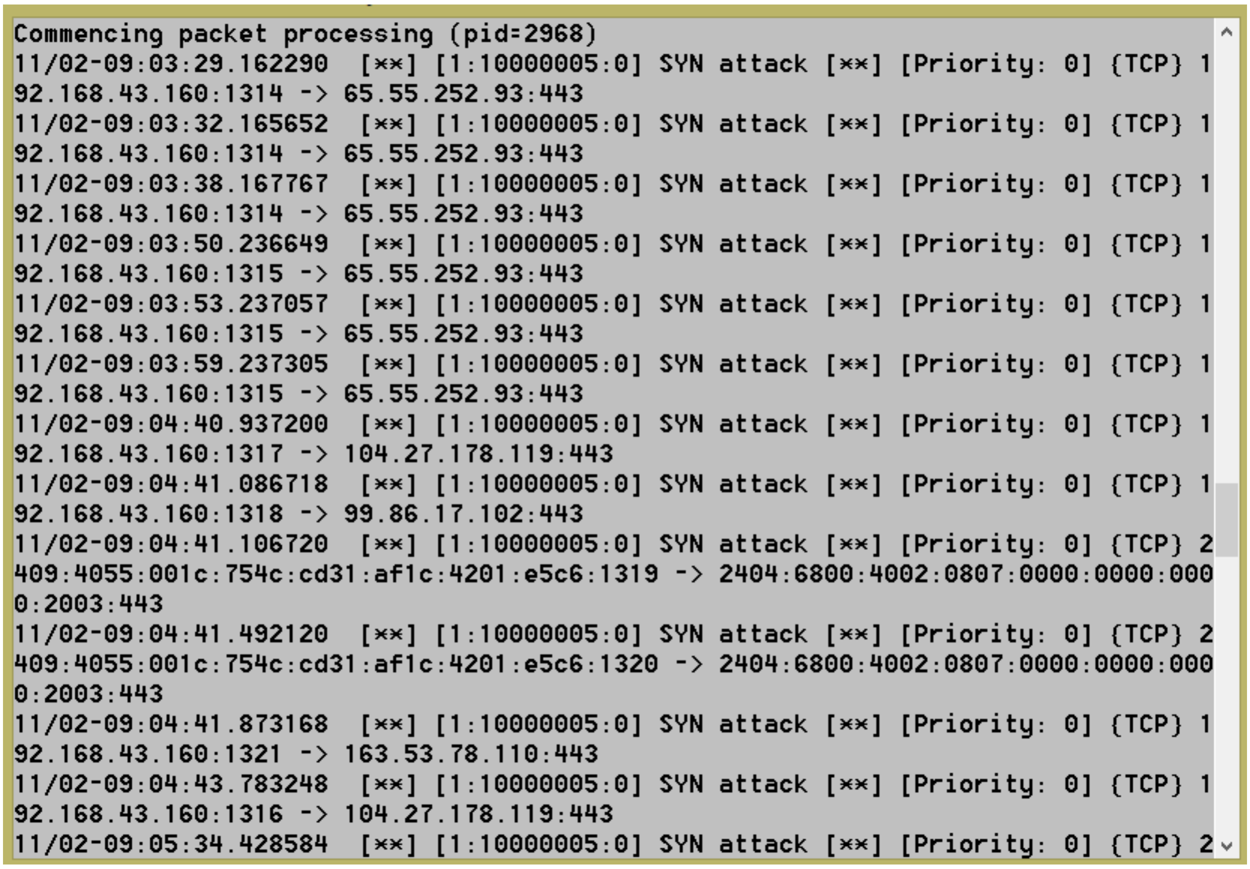
Command: nmap -T4 -A -v 192.168.43.160

nmap -T4 -A -v 192.168.43.160

```
NSE: Script Pre-scanning.
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Initiating NSE at 09:29
Completed NSE at 09:29, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:29
Completed Parallel DNS resolution of 1 host. at 09:29,
0.00s elapsed
Initiating SYN Stealth Scan at 09:29
Scanning Shweta (192.168.43.160) [1000 ports]
Discovered open port 135/tcp on 192.168.43.160
Discovered open port 554/tcp on 192.168.43.160
Discovered open port 445/tcp on 192.168.43.160
Discovered open port 1025/tcp on 192.168.43.160
Discovered open port 139/tcp on 192.168.43.160
Discovered open port 1027/tcp on 192.168.43.160
Discovered open port 1026/tcp on 192.168.43.160
Discovered open port 1028/tcp on 192.168.43.160
Discovered open port 5357/tcp on 192.168.43.160
Discovered open port 1029/tcp on 192.168.43.160
Discovered open port 10243/tcp on 192.168.43.160
Discovered open port 2869/tcp on 192.168.43.160
Completed SYN Stealth Scan at 09:29, 0.08s elapsed
(1000 total ports)
Initiating Service scan at 09:29
Scanning 12 services on Shweta (192.168.43.160)
Completed Service scan at 09:30, 16.02s elapsed (12
services on 1 host)
Initiating OS detection (try #1) against Shweta
(192.168.43.160)
NSE: Script scanning 192.168.43.160.
Initiating NSE at 09:30
```

Practical 8

- **The network scanning attacks are detected by Snort IDS.**



```
Commencing packet processing (pid=2968)
11/02-09:03:29.162290  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:32.165652  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:38.167767  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1314 -> 65.55.252.93:443
11/02-09:03:50.236649  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:03:53.237057  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:03:59.237305  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1315 -> 65.55.252.93:443
11/02-09:04:40.937200  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1317 -> 104.27.178.119:443
11/02-09:04:41.086718  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1318 -> 99.86.17.102:443
11/02-09:04:41.106720  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
409:4055:001c:754c:cd31:af1c:4201:e5c6:1319 -> 2404:6800:4002:0807:0000:0000:000
0:2003:443
11/02-09:04:41.492120  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
409:4055:001c:754c:cd31:af1c:4201:e5c6:1320 -> 2404:6800:4002:0807:0000:0000:000
0:2003:443
11/02-09:04:41.873168  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1321 -> 163.53.78.110:443
11/02-09:04:43.783248  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 1
92.168.43.160:1316 -> 104.27.178.119:443
11/02-09:05:34.428584  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 2
```

Detection of Network Scanning Attack with Snort IDS