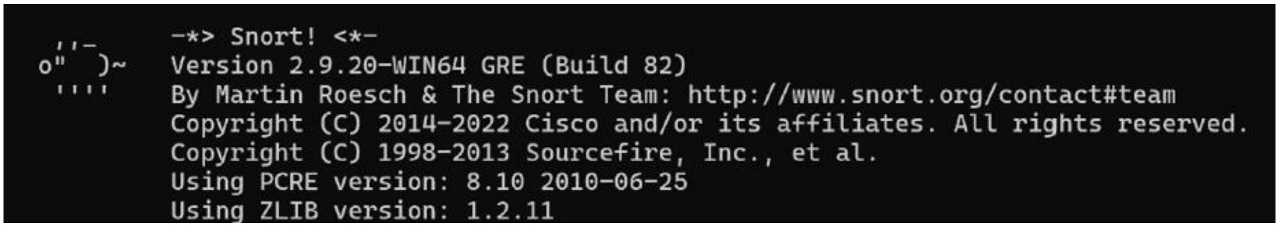
Name: Akash Panicker

UID:2021300089

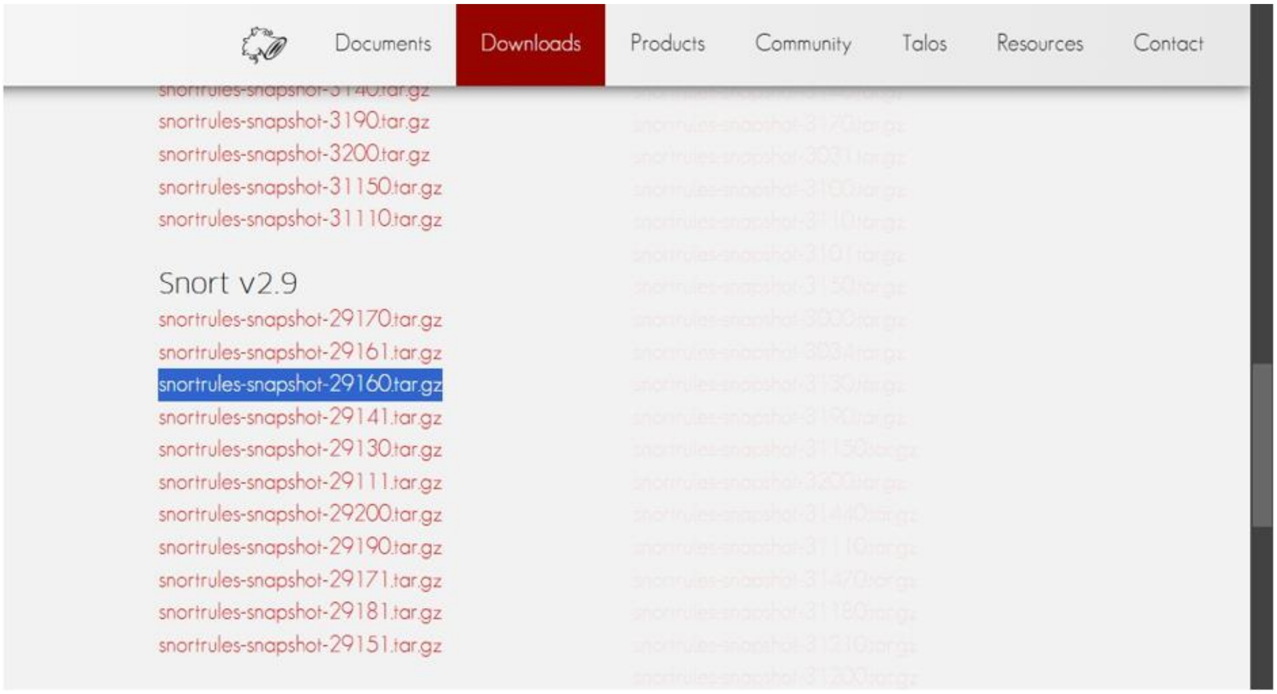
Batch: 2

Step 1) Download Snort from snort.org and choose the destination folder (default: C:\Snort).



```
   ,,_     -*> 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
```

Step 2) Download and Configure Rules (First you have to sign in to enable it)

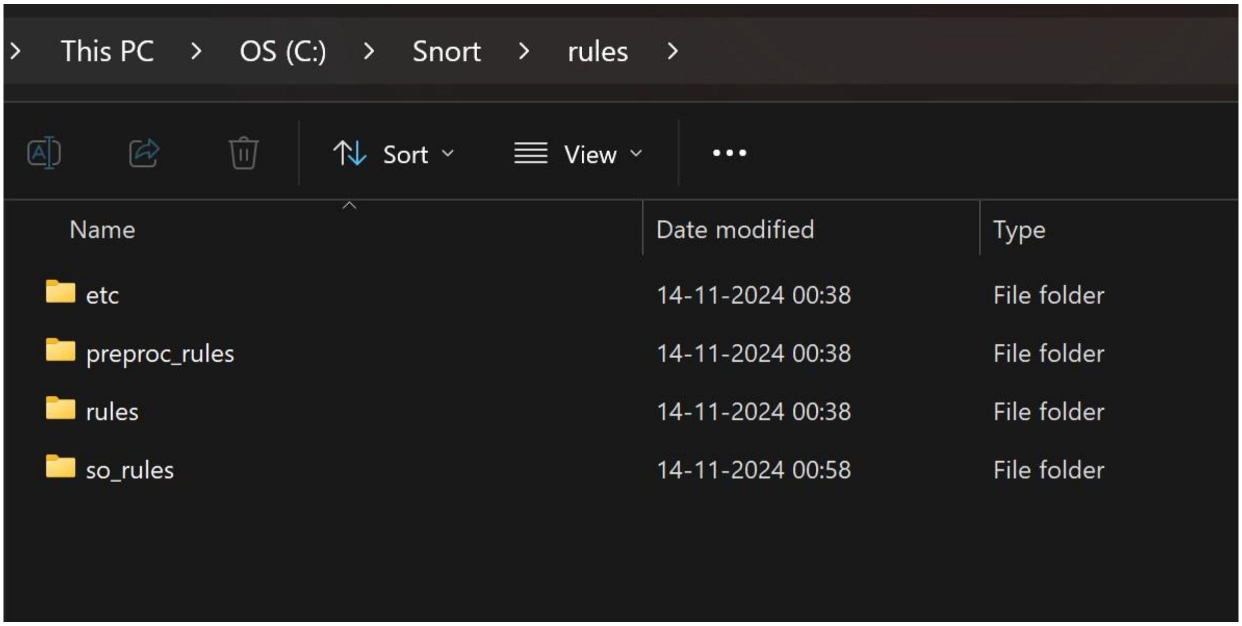


snortrules-snapshot-3140.tar.gz
snortrules-snapshot-3190.tar.gz
snortrules-snapshot-3200.tar.gz
snortrules-snapshot-31150.tar.gz
snortrules-snapshot-31110.tar.gz

Snort v2.9

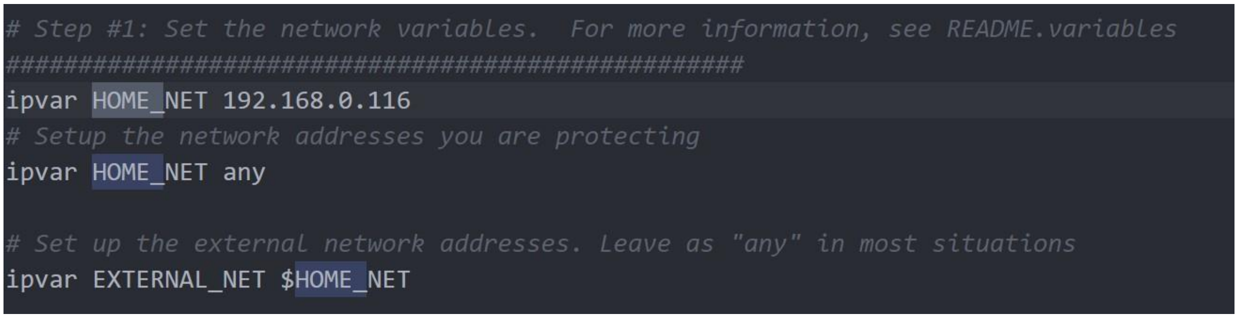
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-29161.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29200.tar.gz
snortrules-snapshot-29190.tar.gz
snortrules-snapshot-29171.tar.gz
snortrules-snapshot-29181.tar.gz
snortrules-snapshot-29151.tar.gz

Step 3) Extract this rule to C:\Snort\rules

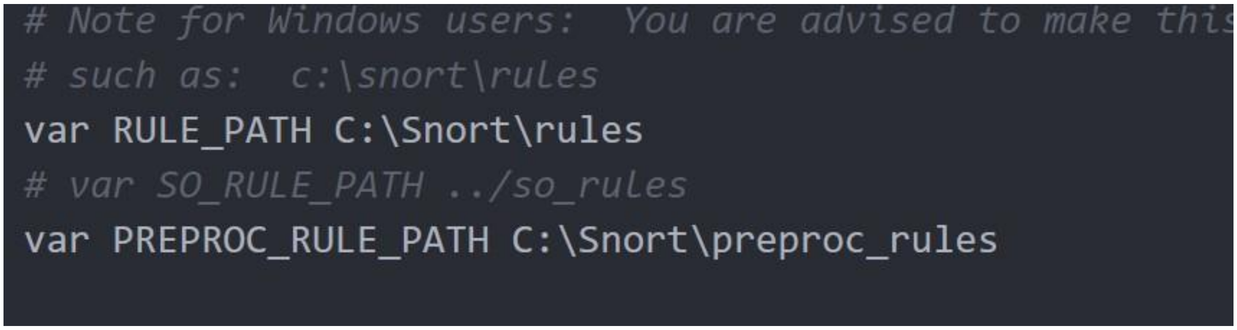


Name	Date modified	Type
etc	14-11-2024 00:38	File folder
preproc_rules	14-11-2024 00:38	File folder
rules	14-11-2024 00:38	File folder
so_rules	14-11-2024 00:58	File folder

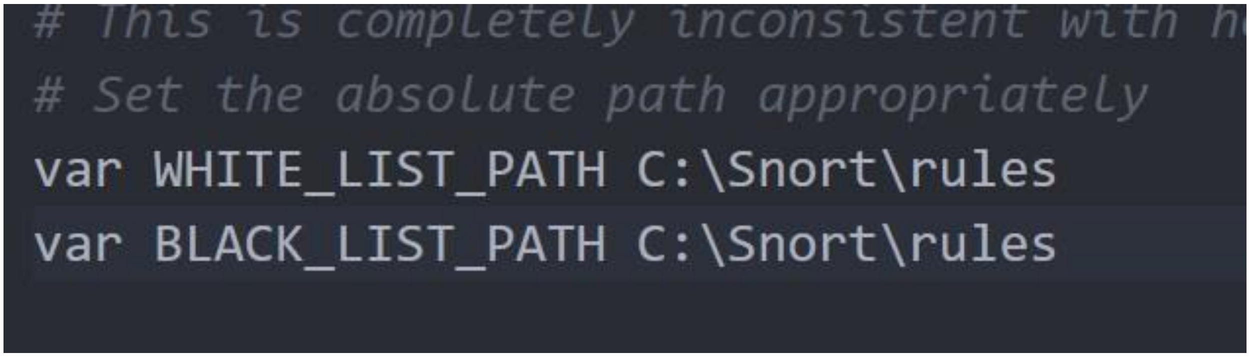
Step 4) Editing the snort.conf file



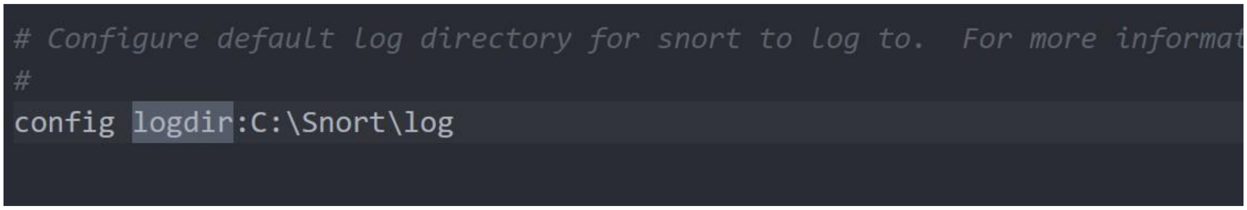
```
# Step #1: Set the network variables.  For more information, see README.variables
###################################################
ipvar HOME_NET 192.168.0.116
# Setup the network addresses you are protecting
ipvar HOME_NET any

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



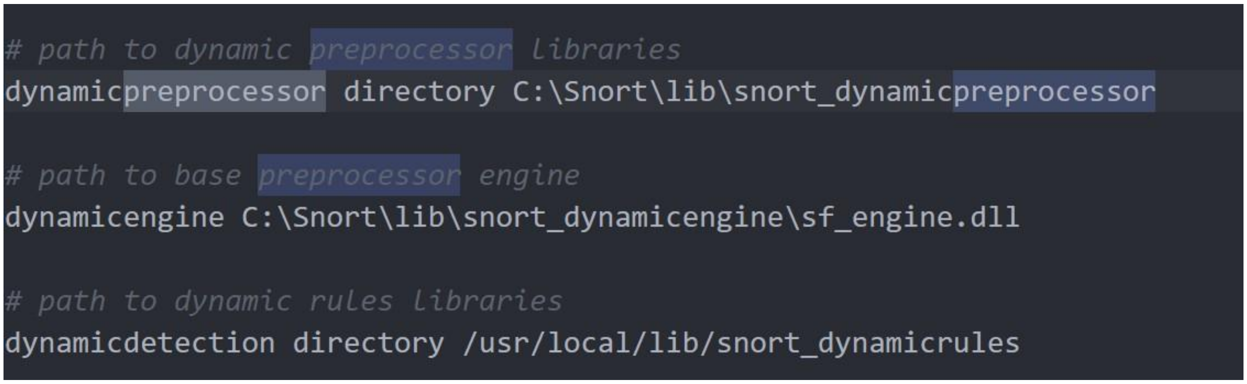
```
# Note for Windows users:  You are advised to make this
# such as:  c:\snort\rules
var RULE_PATH C:\Snort\rules
# var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```



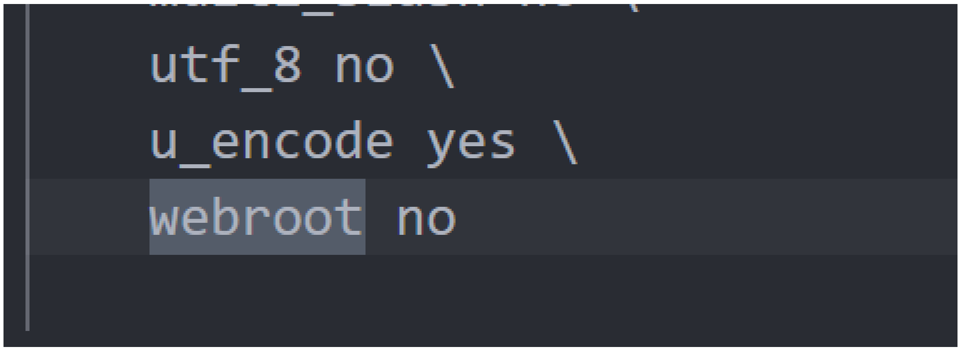
```
# This is completely inconsistent with h
# Set the absolute path appropriately
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```



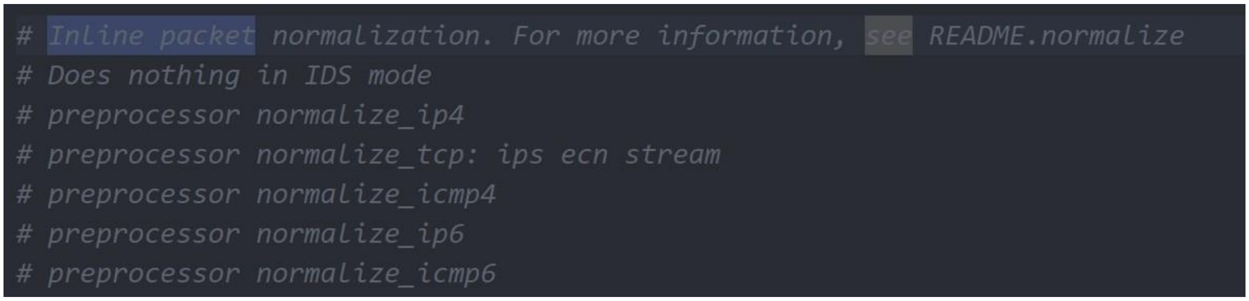
```
# Configure default log directory for snort to log to.  For more informat
#
config logdir:C:\Snort\log
```



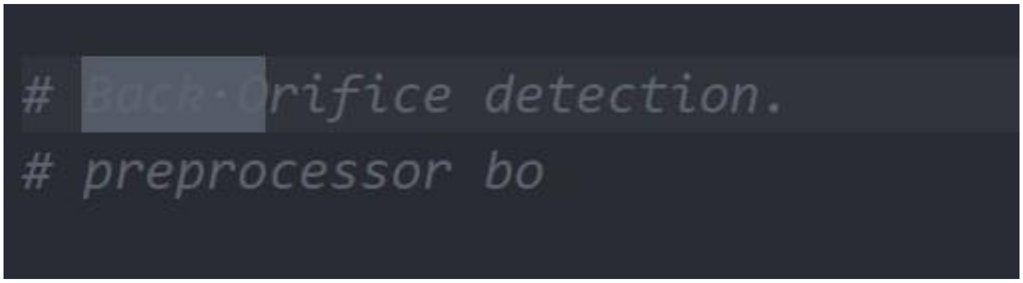
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# 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
```



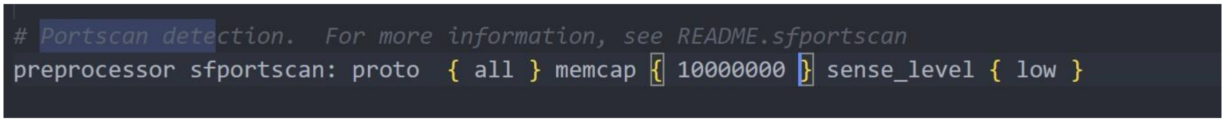
```
    multi_slash no \
    utf_8 no \
    u_encode yes \
    webroot no
```



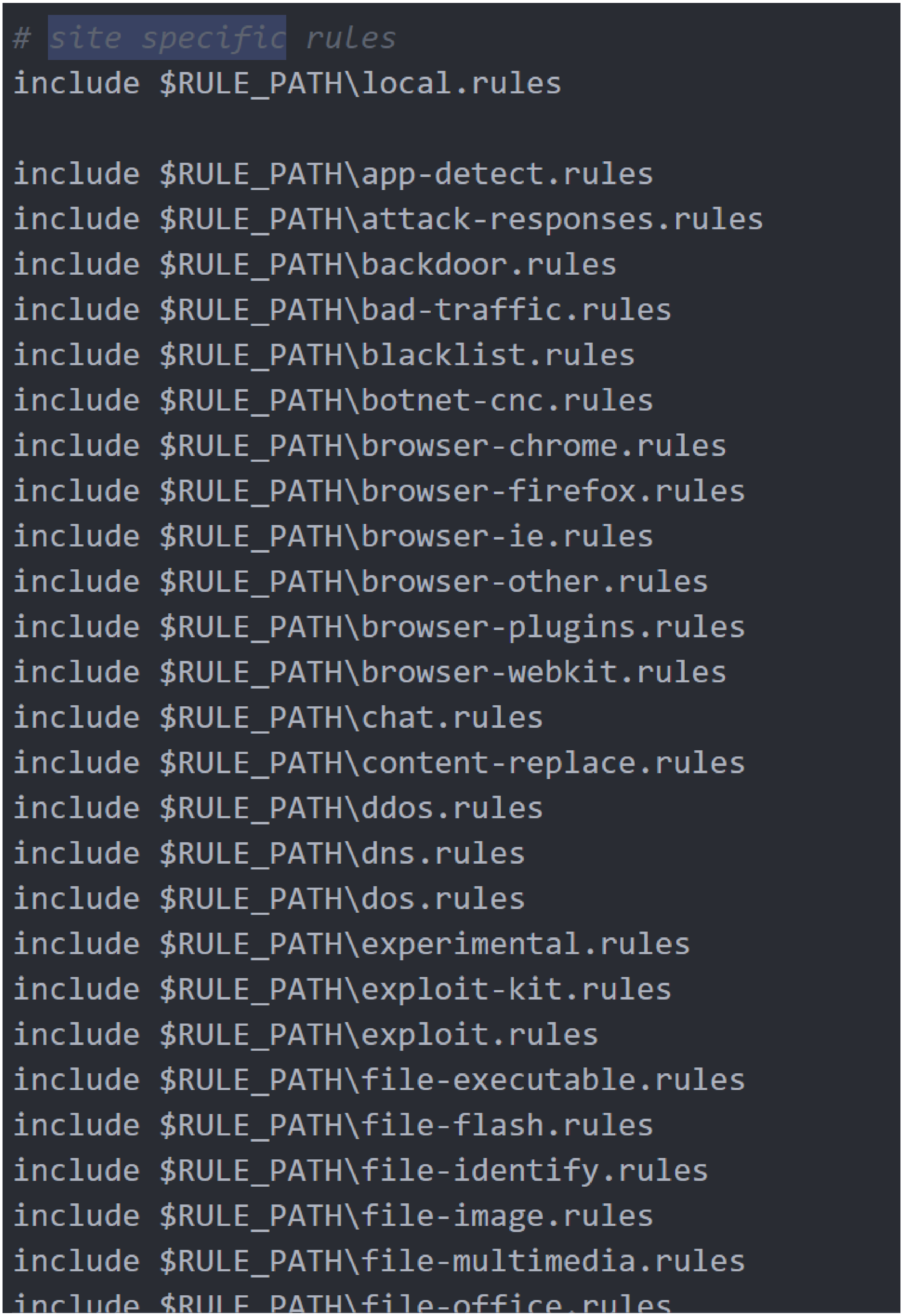
```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```



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

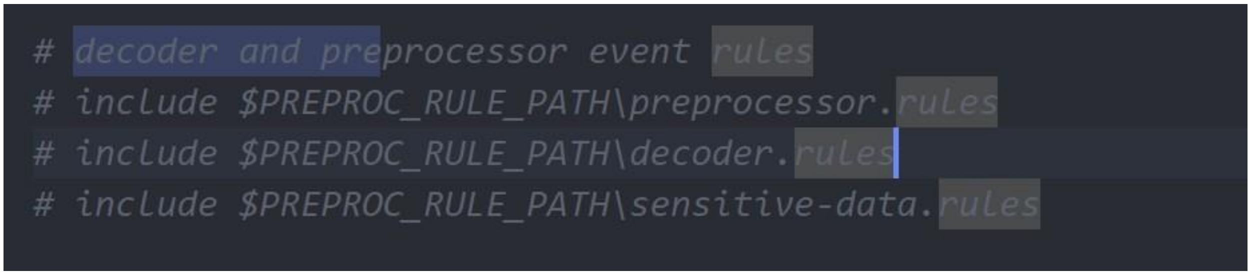


```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```



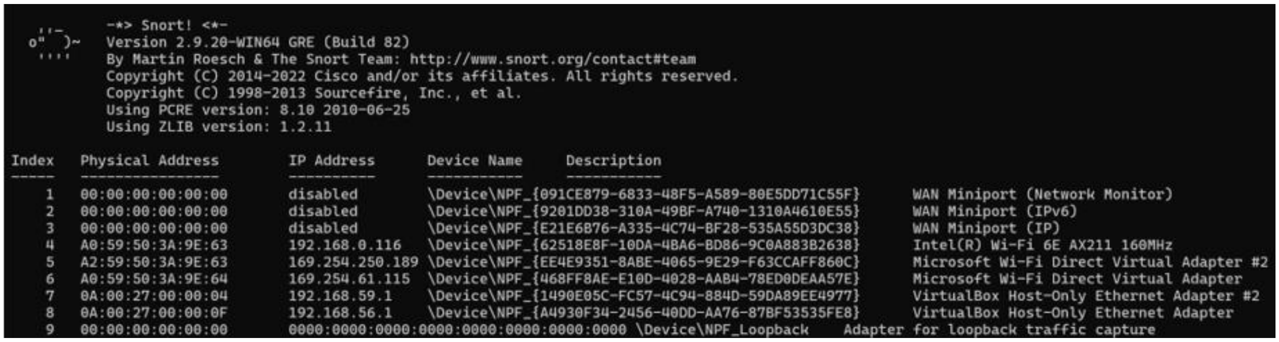
```
# site specific rules
include $RULE_PATH\local.rules

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
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
```

replacing the forward slash “/” with backslash “\”



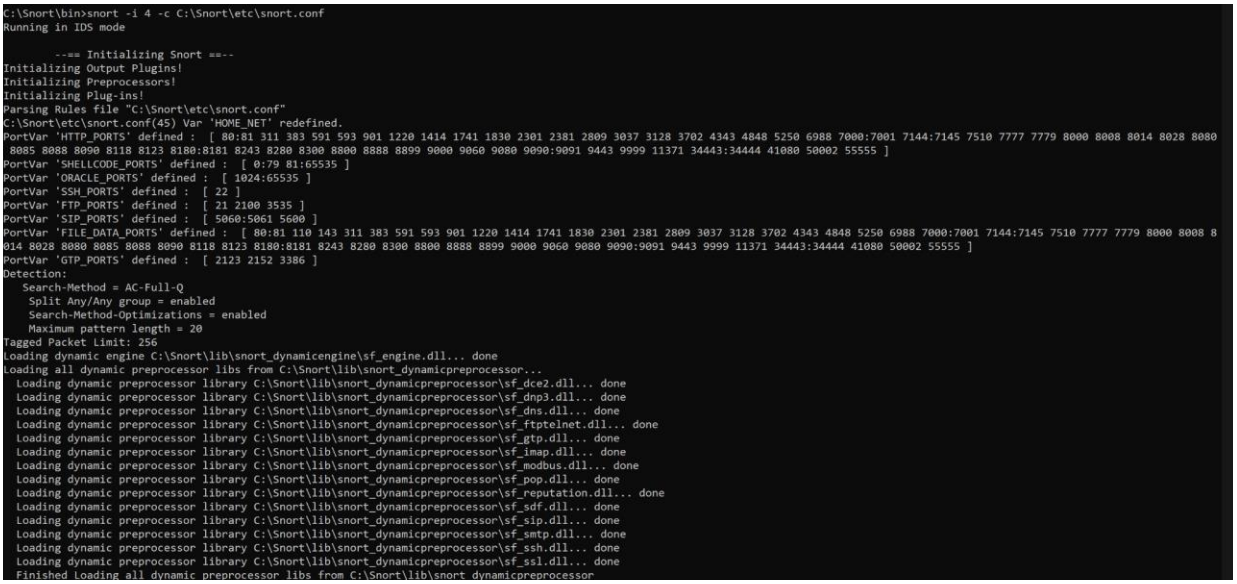
```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

Put Decoders and Preprocessors Rules in Comments



```
   ,,_     -*> 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_{091CE879-6833-48F5-A589-80E5DD71C55F}      WAN Miniport (Network Monitor)
    2  00:00:00:00:00:00       disabled        \Device\NPF_{9201DD38-310A-49BF-A740-1310A4610E55}      WAN Miniport (IPv6)
    3  00:00:00:00:00:00       disabled        \Device\NPF_{E21E6B76-A335-4C74-BF28-535A55D3DC38}      WAN Miniport (IP)
    4  A0:59:50:3A:9E:63       192.168.0.116   \Device\NPF_{62518E8F-10DA-4BA6-BD86-9C0A883B2638}      Intel(R) Wi-Fi 6E AX211 160MHz
    5  A2:59:50:3A:9E:63       169.254.250.189 \Device\NPF_{EE4E9351-8ABE-4065-9E29-F63CCAFF860C}      Microsoft Wi-Fi Direct Virtual Adapter #2
    6  A0:59:50:3A:9E:64       169.254.61.115  \Device\NPF_{468FF8AE-E10D-4028-AAB4-78ED0DEAA57E}      Microsoft Wi-Fi Direct Virtual Adapter
    7  0A:00:27:00:00:04       192.168.59.1    \Device\NPF_{1490E05C-FC57-4C94-884D-59DA89EE4977}      VirtualBox Host-Only Ethernet Adapter #2
    8  0A:00:27:00:00:0F       192.168.56.1    \Device\NPF_{A4930F34-2456-40DD-AA76-87BF53535FE8}      VirtualBox Host-Only Ethernet Adapter
    9  00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
```

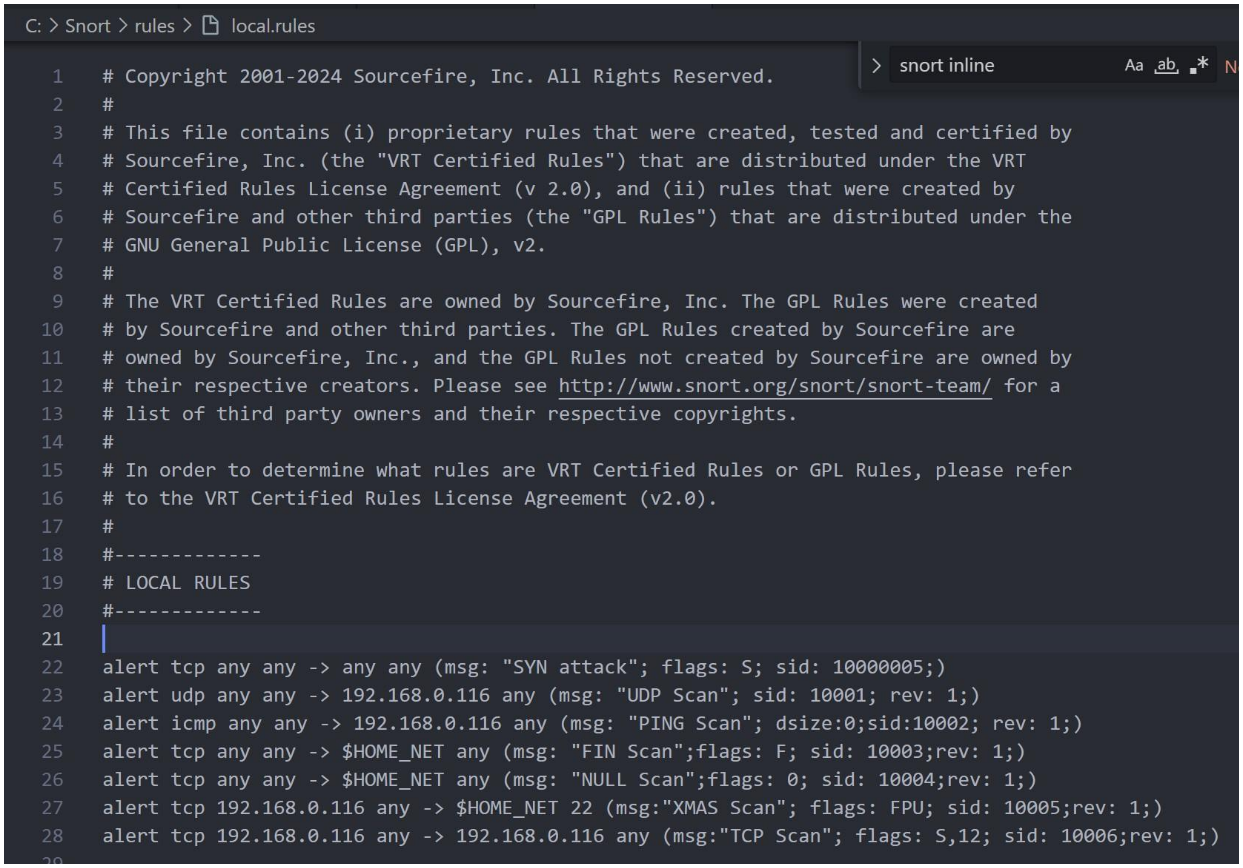
Check the Interface



```
C:\Snort\bin>snort -i 4 -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"
C:\Snort\etc\snort.conf(45) Var 'HOME_NET' redefined.
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 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8
014 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 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor
```

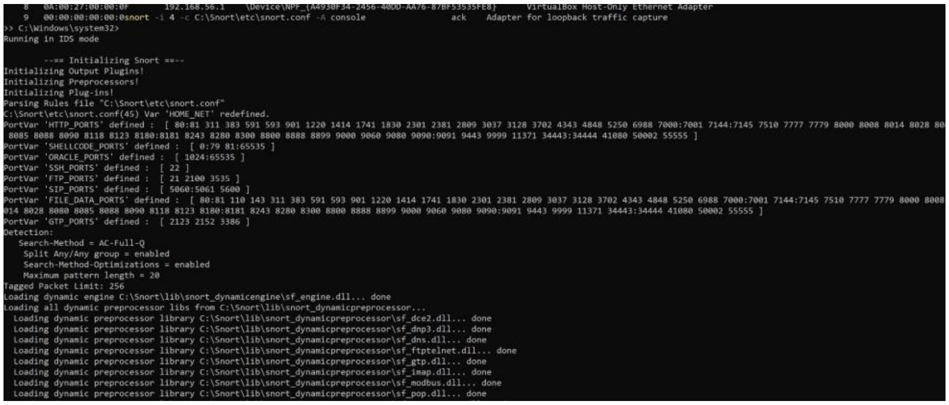
Execute the Snort tool in the command prompt by typing “snort –i 2 –c C:\Snort\etc\snort.conf

WRITE RULES TO DETECT SCANNING ATTACKS



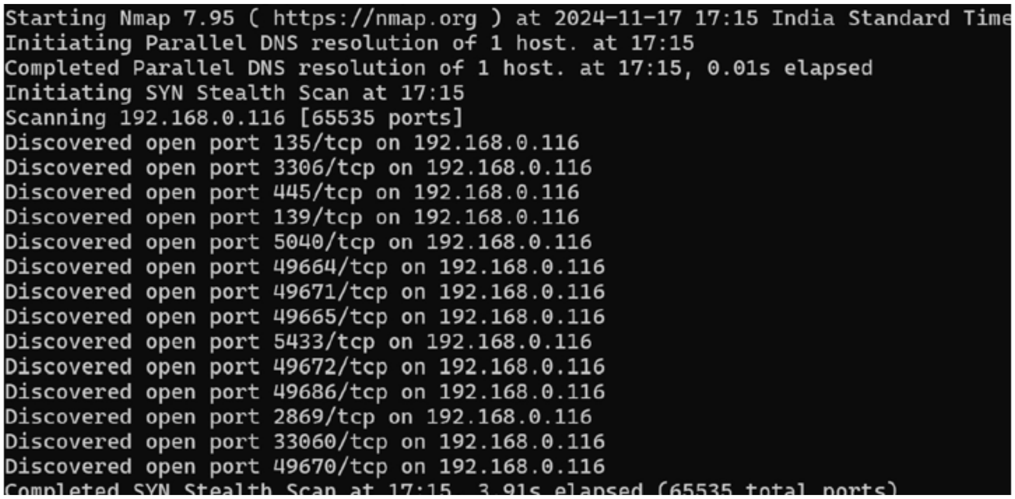
```
# Copyright 2001-2024 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

alert tcp any any -> any any (msg: "SYN attack"; flags: S; sid: 10000005;)
alert udp any any -> 192.168.0.116 any (msg: "UDP Scan"; sid: 10001; rev: 1;)
alert icmp any any -> 192.168.0.116 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 192.168.0.116 any -> $HOME_NET 22 (msg:"XMAS Scan"; flags: FPU; sid: 10005;rev: 1;)
alert tcp 192.168.0.116 any -> 192.168.0.116 any (msg:"TCP Scan"; flags: S,12; sid: 10006;rev: 1;)
```

Adding Rules in local.rules



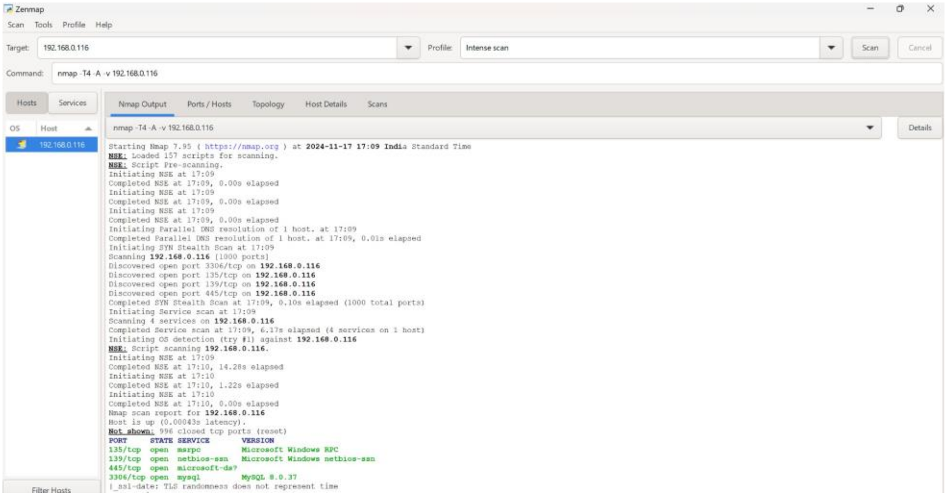
```
    8   0A:00:27:00:00:0F      192.168.56.1    \Device\NPF_{A4930F34-2456-40DD-AA76-87BF53535FE8}      VirtualBox Host-Only Ethernet Adapter
    9   00:00:00:00:00:00snort -i 4 -c C:\Snort\etc\snort.conf -A console               ack    Adapter for loopback traffic capture
>> C:\Windows\system32>
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
C:\Snort\etc\snort.conf(45) Var 'HOME_NET' redefined.
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 80
 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 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008
014 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 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine C:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from C:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library C:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
```

Running Snort in IDS mode



```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-17 17:15 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 17:15
Completed Parallel DNS resolution of 1 host. at 17:15, 0.01s elapsed
Initiating SYN Stealth Scan at 17:15
Scanning 192.168.0.116 [65535 ports]
Discovered open port 135/tcp on 192.168.0.116
Discovered open port 3306/tcp on 192.168.0.116
Discovered open port 445/tcp on 192.168.0.116
Discovered open port 139/tcp on 192.168.0.116
Discovered open port 5040/tcp on 192.168.0.116
Discovered open port 49664/tcp on 192.168.0.116
Discovered open port 49671/tcp on 192.168.0.116
Discovered open port 49665/tcp on 192.168.0.116
Discovered open port 5433/tcp on 192.168.0.116
Discovered open port 49672/tcp on 192.168.0.116
Discovered open port 49686/tcp on 192.168.0.116
Discovered open port 2869/tcp on 192.168.0.116
Discovered open port 33060/tcp on 192.168.0.116
Discovered open port 49670/tcp on 192.168.0.116
Completed SYN Stealth Scan at 17:15, 3.91s elapsed (65535 total ports)
```

Network Scanning Attack with Nmap Tool



Target: 192.168.0.116

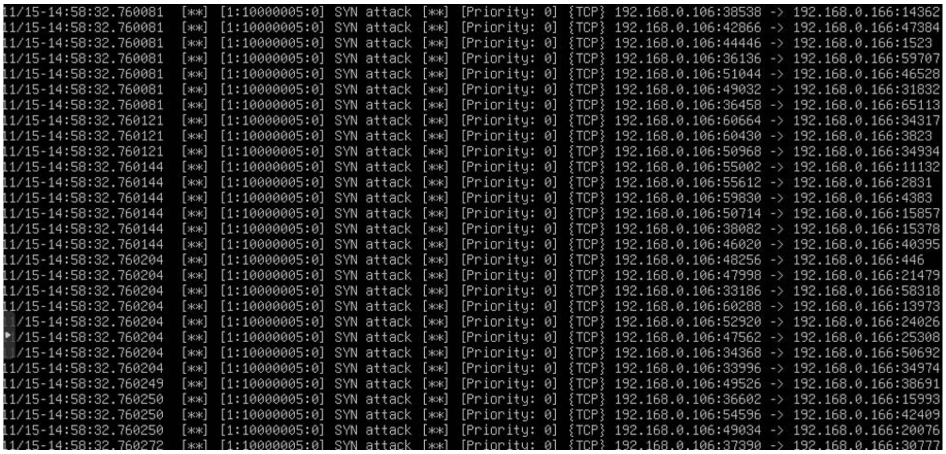
Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.116

192.168.0.116

```
nmap -T4 -A -v 192.168.0.116
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-17 17:09 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating NSE at 17:09
Completed NSE at 17:09, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:09
Completed Parallel DNS resolution of 1 host. at 17:09, 0.01s elapsed
Initiating SYN Stealth Scan at 17:09
Scanning 192.168.0.116 [1000 ports]
Discovered open port 3306/tcp on 192.168.0.116
Discovered open port 135/tcp on 192.168.0.116
Discovered open port 139/tcp on 192.168.0.116
Discovered open port 445/tcp on 192.168.0.116
Completed SYN Stealth Scan at 17:09, 0.10s elapsed (1000 total ports)
Initiating Service scan at 17:09
Scanning 4 services on 192.168.0.116
Completed Service scan at 17:09, 6.17s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.116
NSE: Script scanning 192.168.0.116.
Initiating NSE at 17:09
Completed NSE at 17:10, 14.28s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 1.22s elapsed
Initiating NSE at 17:10
Completed NSE at 17:10, 0.00s elapsed
Nmap scan report for 192.168.0.116
Host is up (0.00043s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL 8.0.37
|_ssl-date: TLS randomness does not represent time
```

Network Scanning Attack with Zenmap Tool



```
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:38538 -> 192.168.0.166:14362
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:42866 -> 192.168.0.166:47384
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:44446 -> 192.168.0.166:1523
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:36136 -> 192.168.0.166:59707
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:51044 -> 192.168.0.166:46528
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:49032 -> 192.168.0.166:31832
11/15-14:58:32.760081  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:36458 -> 192.168.0.166:65113
11/15-14:58:32.760121  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:60664 -> 192.168.0.166:34317
11/15-14:58:32.760121  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:60430 -> 192.168.0.166:3823
11/15-14:58:32.760121  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:50968 -> 192.168.0.166:34934
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:55002 -> 192.168.0.166:11132
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:55612 -> 192.168.0.166:2831
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:59830 -> 192.168.0.166:4383
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:50714 -> 192.168.0.166:15857
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:38082 -> 192.168.0.166:15378
11/15-14:58:32.760144  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:46020 -> 192.168.0.166:40395
11/15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:48256 -> 192.168.0.166:446
11/15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:47998 -> 192.168.0.166:21479
11/15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:33186 -> 192.168.0.166:58318
11/15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:60288 -> 192.168.0.166:13973
  /15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:52920 -> 192.168.0.166:24026
  /15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:47562 -> 192.168.0.166:25308
  /15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:34368 -> 192.168.0.166:50692
11/15-14:58:32.760204  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:33996 -> 192.168.0.166:34974
11/15-14:58:32.760249  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:49526 -> 192.168.0.166:38691
11/15-14:58:32.760250  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:36602 -> 192.168.0.166:15993
11/15-14:58:32.760250  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:54596 -> 192.168.0.166:42409
11/15-14:58:32.760250  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:49034 -> 192.168.0.166:20076
11/15-14:58:32.760272  [**] [1:10000005:0] SYN attack [**] [Priority: 0] {TCP} 192.168.0.106:37390 -> 192.168.0.166:30777
```

Detection of Network Scanning Attack with Snort IDS