LAB MANUAL
ON
SNORT- NETWORK INTRUSION DETECTION SYSTEM

ESTABLISHMENT OF ADVANCED LABORATORY FOR CYBER SECURITY TRAINING TO TECHNICAL TEACHERS

DEPARTMENT OF INFORMATION MANAGEMENT AND EMERGING ENGINEERING

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

GOVERNMENT OF INDIA

Principal Investigator: Prof. Maitreyee Dutta

Co Investigator: Prof. Shyam Sundar Pattnaik

PREPARED BY:

Prof. Maitreyee Dutta and Ms. Shweta Sharma (Technical Assistant)

Table of Contents

MANUAL-8: SNORT- Network Intrusion Detection System

INTRODUCTION TO SNORT

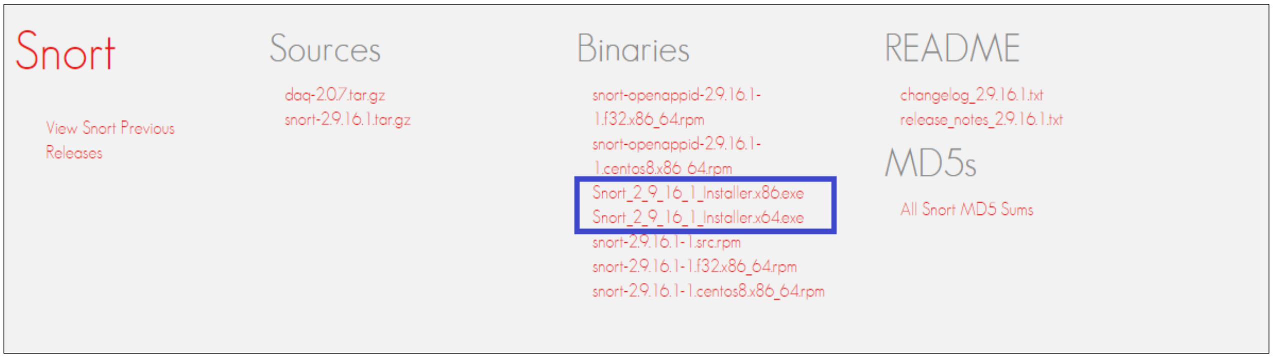
- Snort is an open source tool [1] for Intrusion Detection and Prevention System.
- It uses a series of rules that help define malicious network activities and uses those rules to find packets that match against them and generates alerts for users.
- Snort has three primary uses:
    - As a packet sniffer like tcpdump
    - As a packet logger — which is useful for network traffic debugging
    - As a full-blown network intrusion prevention system

FEATURES OF SNORT

- **RULES**: To generate rules to identify various kinds of scans such as TCP scan, UDP scan, FIN scan, etc.
- **ATTACK DETECTION**: To detect network scanning attacks, DoS attack, malware attack, etc.

HOW TO DOWNLOAD AND INSTALL SNORT TOOL

Step 1: Visit the website- https://www.snort.org/downloads to download Snort tool for 32-bit or 64-bit Windows Operating system as shown in Figure 1. The downloaded Snort tool is shown in Figure 2.



Snort

View Snort Previous Releases

Sources

daq-2.0.7.tar.gz
snort-2.9.16.1.tar.gz

Binaries

snort-openappid-2.9.16.1-1.f32.x86_64.rpm
snort-openappid-2.9.16.1-1.centos8.x86_64.rpm
Snort_2_9_16_1_Installer.x86.exe
Snort_2_9_16_1_Installer.x64.exe
snort-2.9.16.1-1.src.rpm
snort-2.9.16.1-1.f32.x86_64.rpm
snort-2.9.16.1-1.centos8.x86_64.rpm

README

changelog_2.9.16.1.txt
release_notes_2.9.16.1.txt

MD5s

All Snort MD5 Sums

Figure 1: Downloading Snort Tool for Windows Operating System

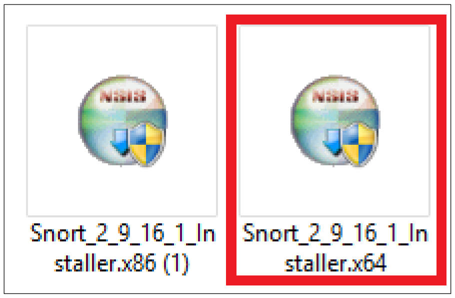
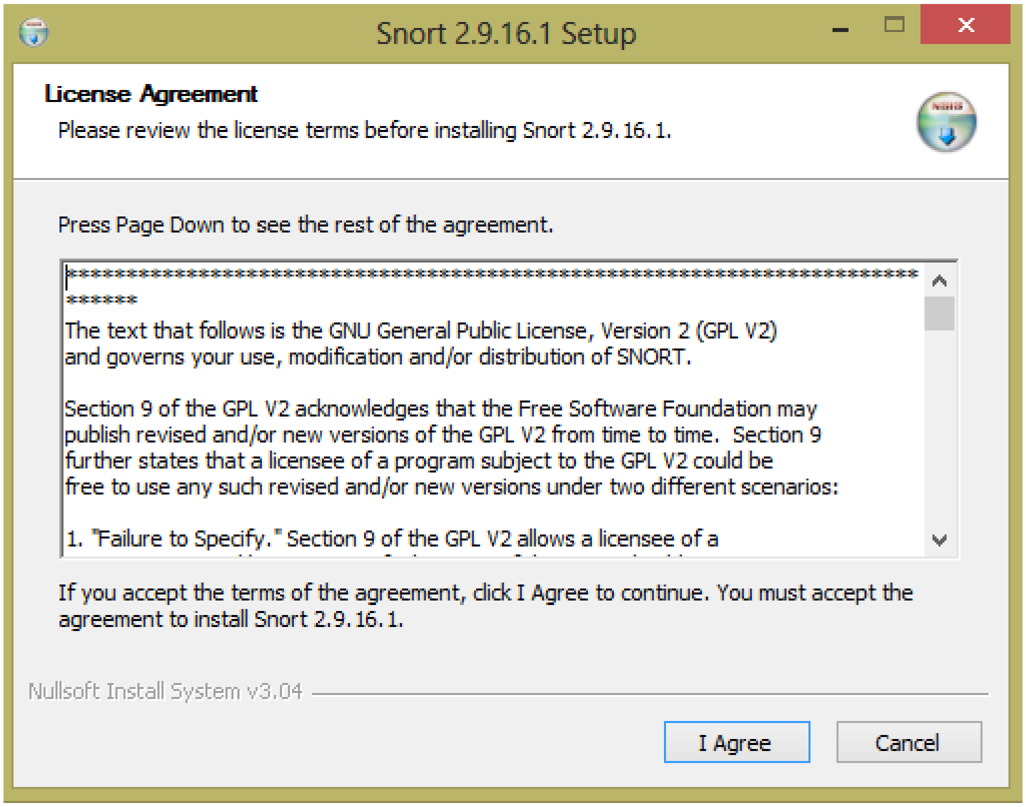

Snort_2_9_16_1_Installer.x86 (1)
Snort_2_9_16_1_Installer.x64

Figure 2: Downloaded Snort Tool in Windows Operating System

Step 2: After downloading the Snort tool, double click on it for installation. It will show a license agreement on the users' screen as shown in Figure 3. Click on "I Agree" button.



Snort 2.9.16.1 Setup

License Agreement

Please review the license terms before installing Snort 2.9.16.1.

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
```

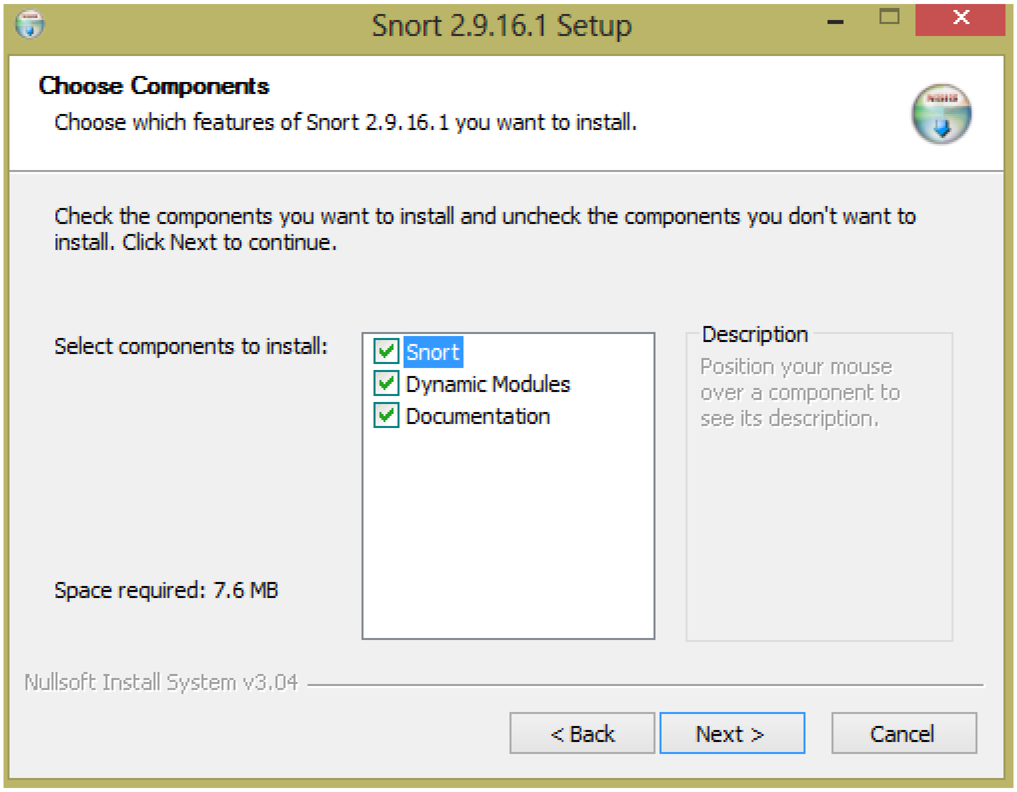
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Snort 2.9.16.1.

Nullsoft Install System v3.04

Figure 3: License Agreement

Step 3: Select the Snort, Dynamic Modules, and Documentation components and click on Next button as shown in Figure 4.

Step 4: Choose a destination folder by clicking on Browse button as shown in Figure 5. The default path is “C:/Snort” to install the Snort tool. After successful installation, a message with “snort has successfully been installed” will display on the screen as shown in Figure 6. Press OK button to close it.



Snort 2.9.16.1 Setup

Choose Components

Choose which features of Snort 2.9.16.1 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Snort
☑ Dynamic Modules
☑ Documentation

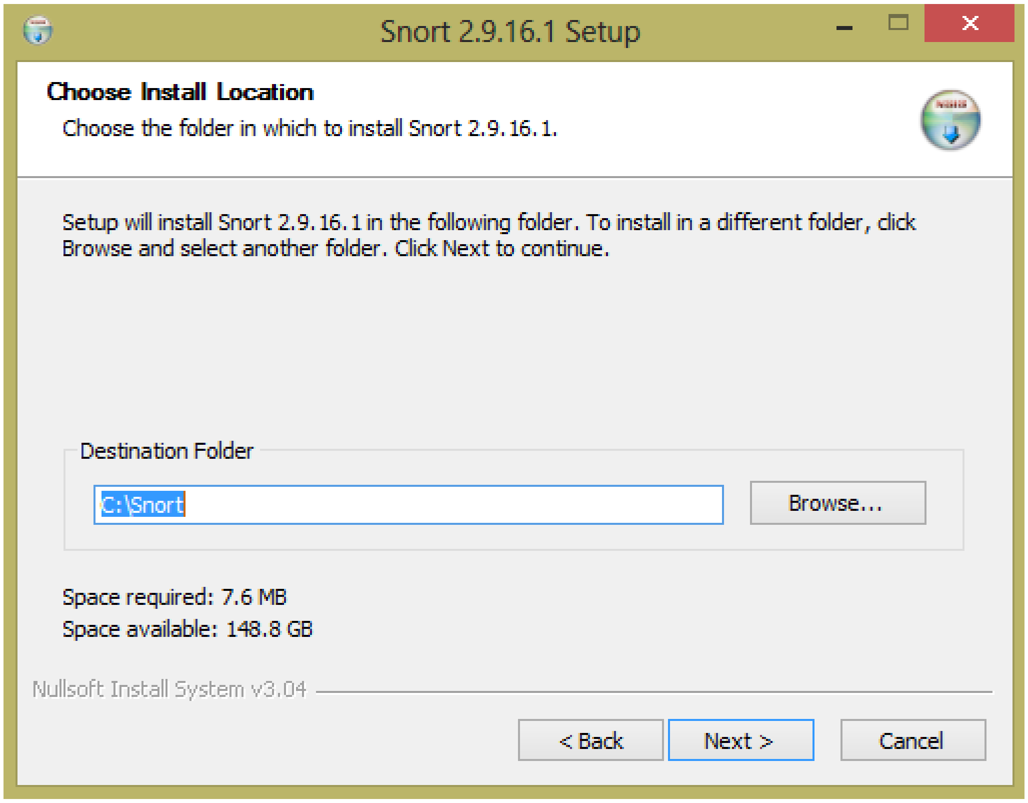
Space required: 7.6 MB

Description

Position your mouse over a component to see its description.

Nullsoft Install System v3.04

Figure 4: Components of Snort



Choose Install Location

Choose the folder in which to install Snort 2.9.16.1.

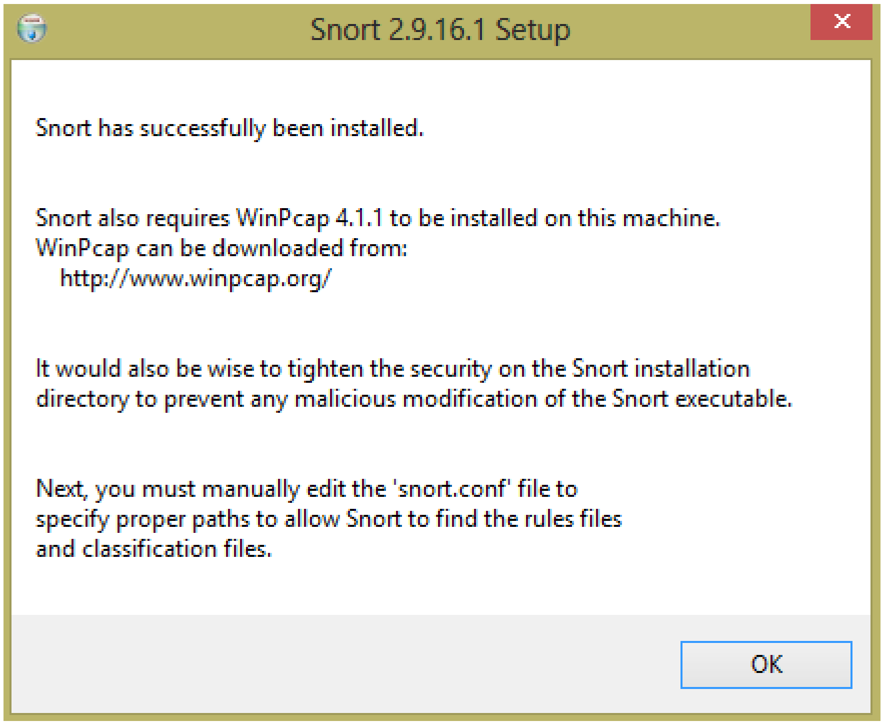
Setup will install Snort 2.9.16.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Snort

Space required: 7.6 MB
Space available: 148.8 GB

Nullsoft Install System v3.04

Figure 5: Installation of Snort



Snort has successfully been installed.

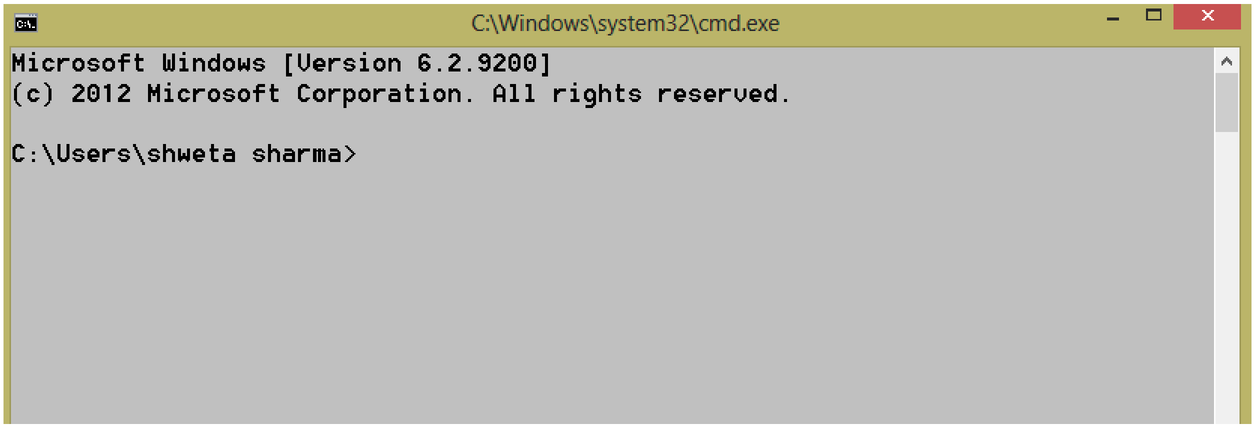
Snort also requires WinPcap 4.1.1 to be installed on this machine.
WinPcap can be downloaded from:
 http://www.winpcap.org/

It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.

Next, you must manually edit the 'snort.conf' file to specify proper paths to allow Snort to find the rules files and classification files.

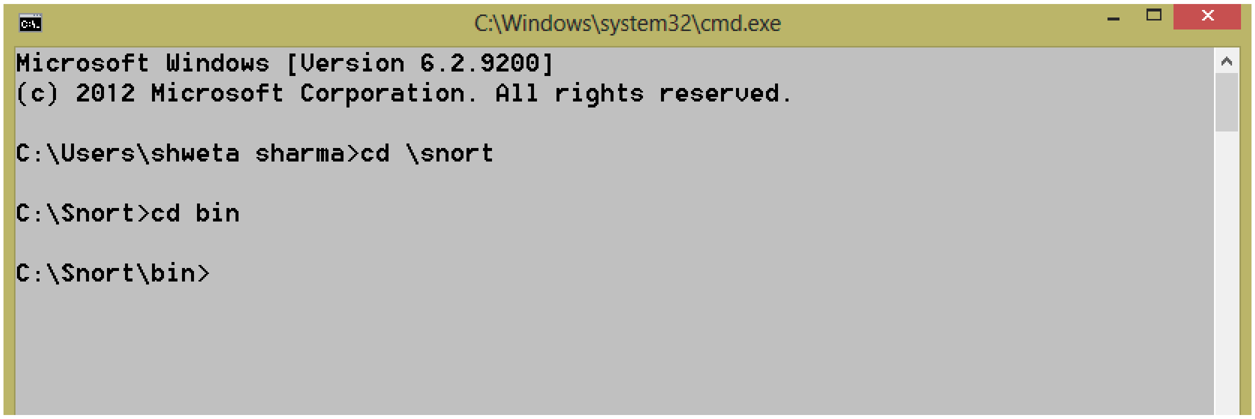
Figure 6: Successful Installation of Snort

Step 5: Open a command prompt as shown in Figure 7. Type the path where Snort has been installed (i.e., cd \snort) and press Enter as shown in Figure 8. Type “cd bin” to go to bin folder.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\shweta sharma>
```

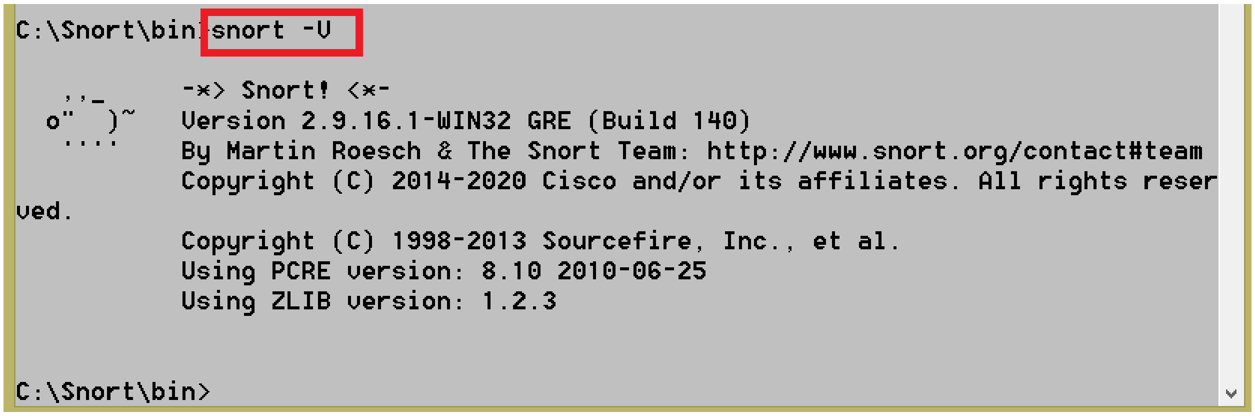
Figure 7: Command Prompt



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\shweta sharma>cd \snort

C:\Snort>cd bin

C:\Snort\bin>
```

Figure 8: Open bin Folder

Step 6: Type “snort –V” in command prompt to check the version of Snort tool as shown in Figure 9.

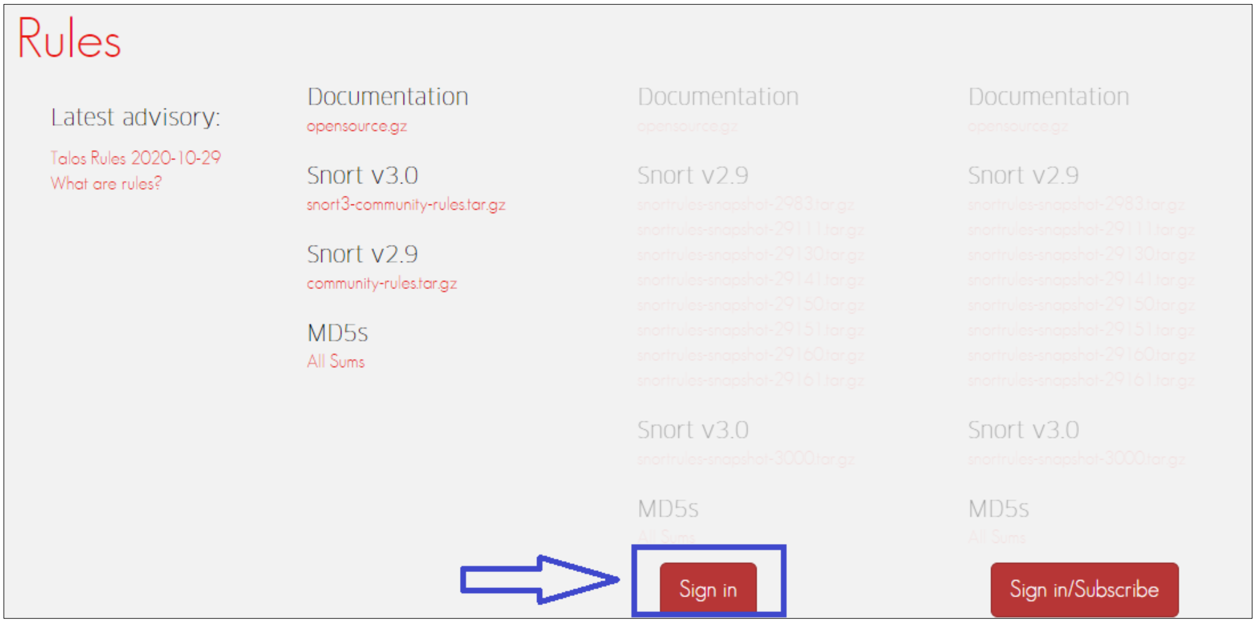


```
C:\Snort\bin>snort -V

   ,,_     -*> 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


C:\Snort\bin>
```

Figure 9: Version of Snort Tool

HOW TO DOWNLOAD THE RULES

<u>Step 7:</u> Visit the website- https://www.snort.org/downloads to download the rules. Click on "Sign in" button to create an account or login as shown in Figure 10.



Rules

Latest advisory:
Talos Rules 2020-10-29
What are rules?

Documentation
opensource.gz

Snort v3.0
snort3-community-rules.tar.gz

Snort v2.9
community-rules.tar.gz

MD5s
All Sums

Documentation
opensource.gz

Snort v2.9
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29150.tar.gz
snortrules-snapshot-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz

Snort v3.0
snortrules-snapshot-3000.tar.gz

MD5s
All Sums

Sign in

Documentation
opensource.gz

Snort v2.9
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29150.tar.gz
snortrules-snapshot-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz

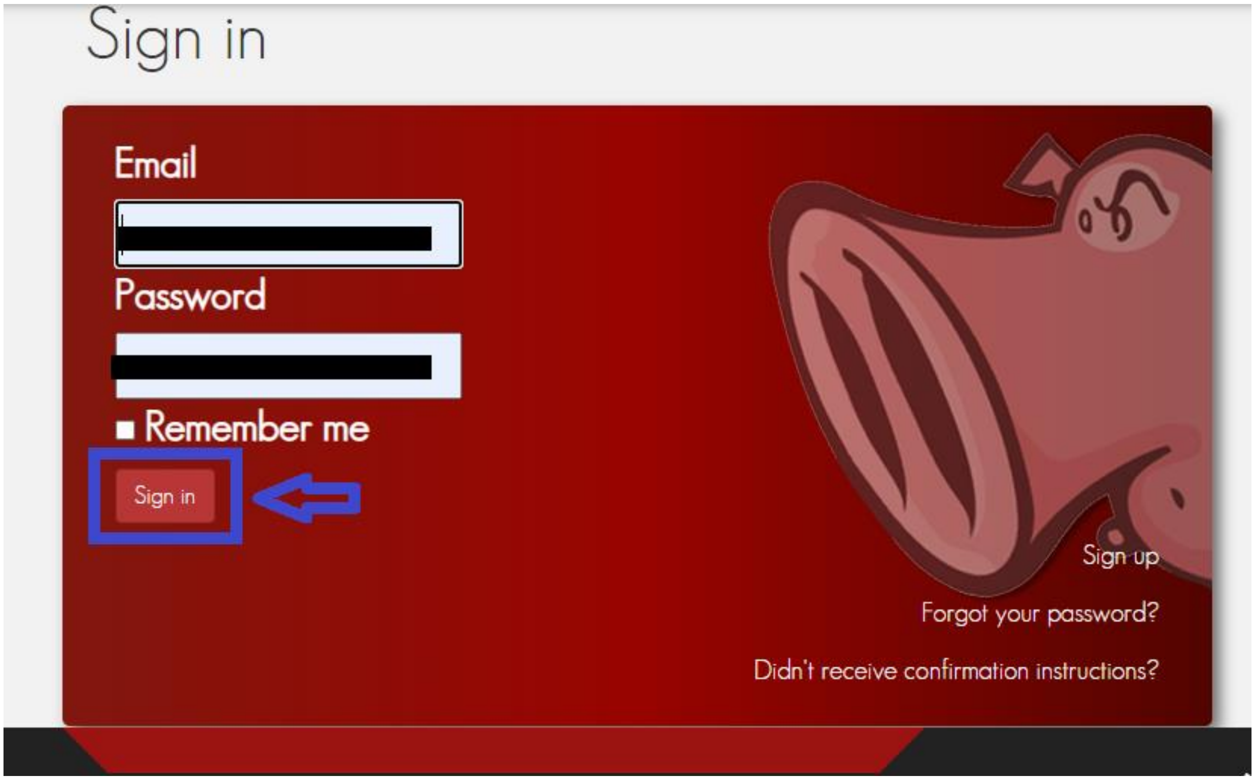
Snort v3.0
snortrules-snapshot-3000.tar.gz

MD5s
All Sums

Sign in/Subscribe

Figure 10: Create an Account to Download the Rules

Step 8: Fill Email address and password to Sign in as shown in Figure 11.



Sign in

Email

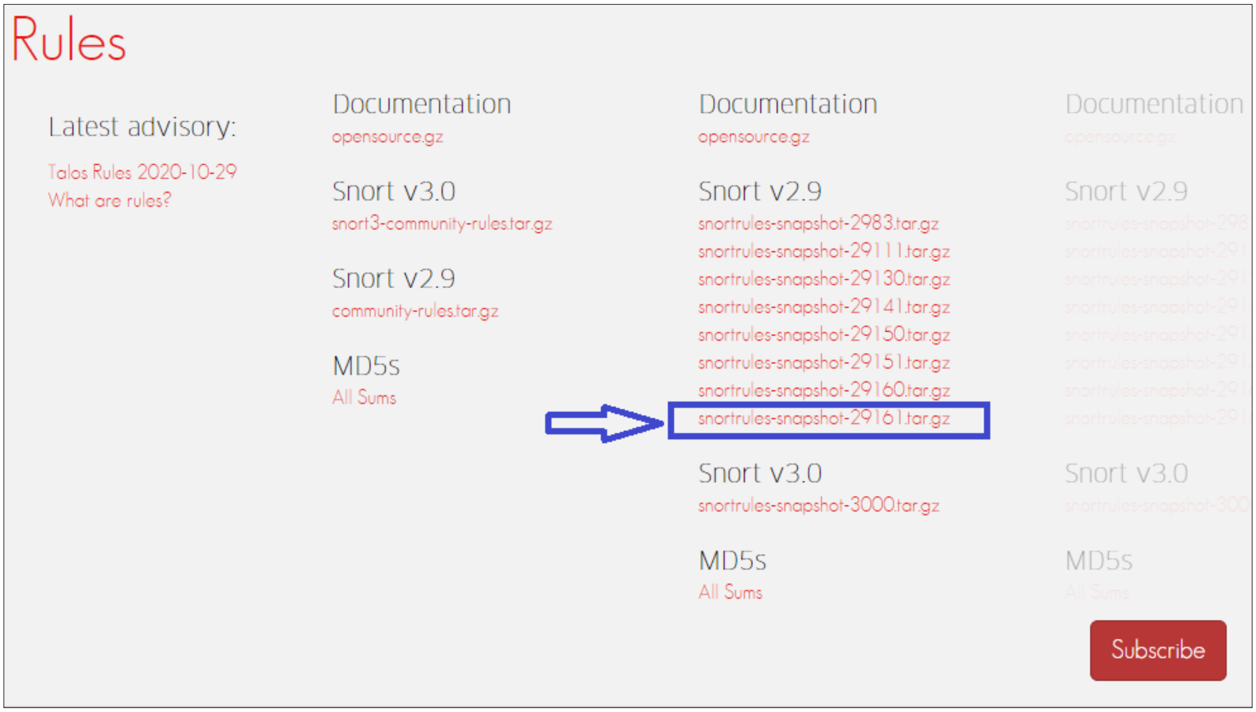
[redacted]

Password

[redacted]

Figure 11: Sign in after Filling Email Address and Password

Step 9: The rules can be downloaded after successful sign in as shown in Figure 12. A compressed folder “snortrules-snapshot-29161.tar.gz” will be downloaded in the personal computer. Unzip the compressed folder as shown in Figure 13.



Rules

Latest advisory:

Talos Rules 2020-10-29

What are rules?

Documentation

opensource.gz

Snort v3.0

snort3-community-rules.tar.gz

Snort v2.9

community-rules.tar.gz

MD5s

All Sums

Documentation

opensource.gz

Snort v2.9

snortrules-snapshot-2983.tar.gz

snortrules-snapshot-29111.tar.gz

snortrules-snapshot-29130.tar.gz

snortrules-snapshot-29141.tar.gz

snortrules-snapshot-29150.tar.gz

snortrules-snapshot-29151.tar.gz

snortrules-snapshot-29160.tar.gz

snortrules-snapshot-29161.tar.gz

Snort v3.0

snortrules-snapshot-3000.tar.gz

MD5s

All Sums

Documentation

opensource.gz

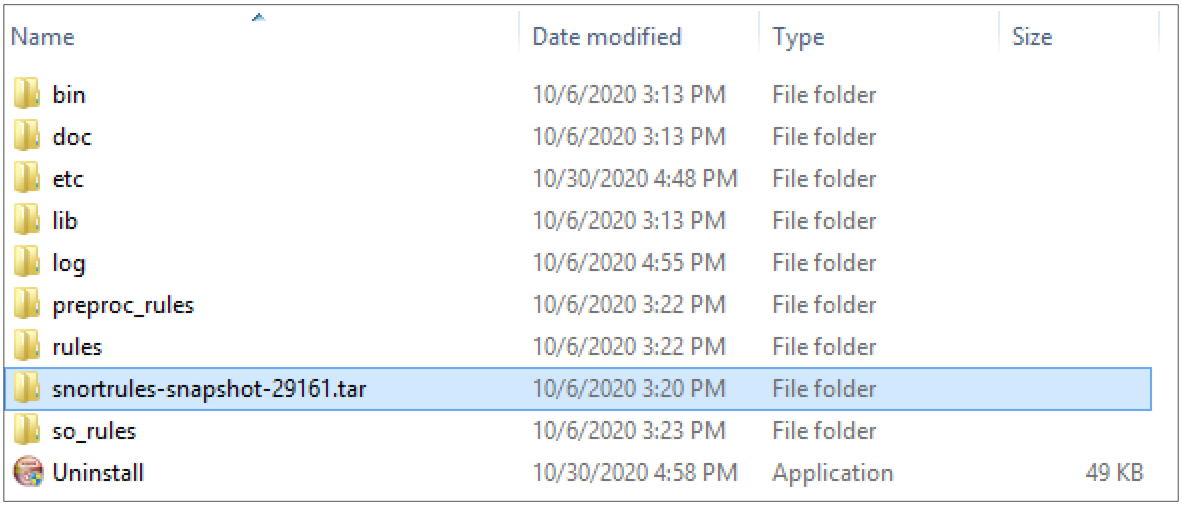
Snort v2.9

Snort v3.0

MD5s

All Sums

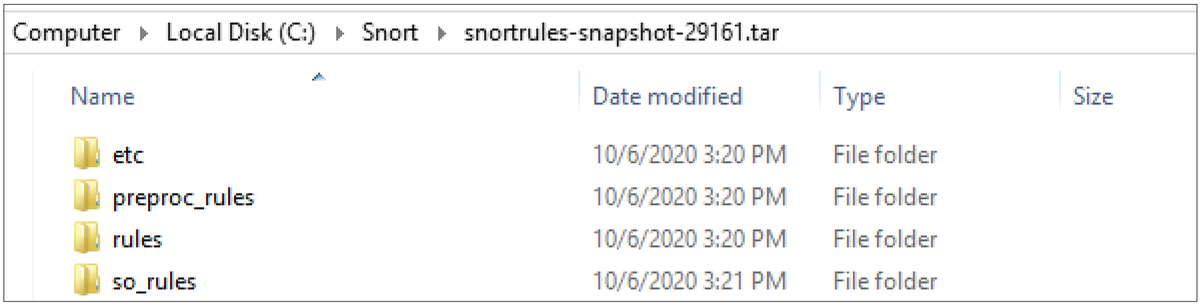
Figure 12: Download the Snort Rules



Name	Date modified	Type	Size
bin	10/6/2020 3:13 PM	File folder	
doc	10/6/2020 3:13 PM	File folder	
etc	10/30/2020 4:48 PM	File folder	
lib	10/6/2020 3:13 PM	File folder	
log	10/6/2020 4:55 PM	File folder	
preproc_rules	10/6/2020 3:22 PM	File folder	
rules	10/6/2020 3:22 PM	File folder	
snortrules-snapshot-29161.tar	10/6/2020 3:20 PM	File folder	
so_rules	10/6/2020 3:23 PM	File folder	
Uninstall	10/30/2020 4:58 PM	Application	49 KB

Figure 13: Unzip the Snortrules Folder

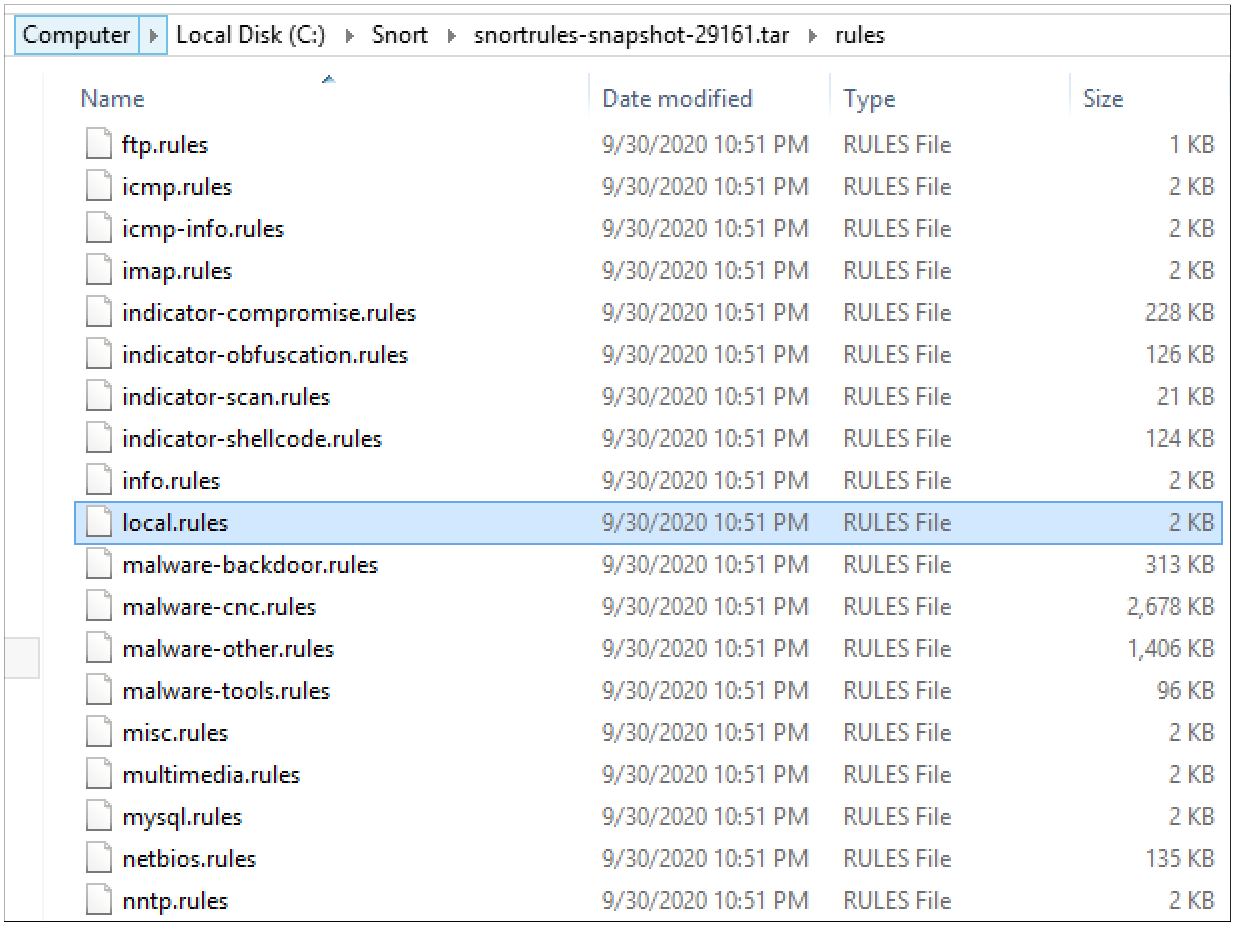
Step 10: Open the “snortrules-snapshot-29161.tar” folder and find “rules” folder as shown in Figure 14. Open the “rules” folder and copy all the rules present inside it as shown in Figure 15.



Computer ▸ Local Disk (C:) ▸ Snort ▸ snortrules-snapshot-29161.tar

Name	Date modified	Type	Size
etc	10/6/2020 3:20 PM	File folder	
preproc_rules	10/6/2020 3:20 PM	File folder	
rules	10/6/2020 3:20 PM	File folder	
so_rules	10/6/2020 3:21 PM	File folder	

Figure 14: Open the rules Folder

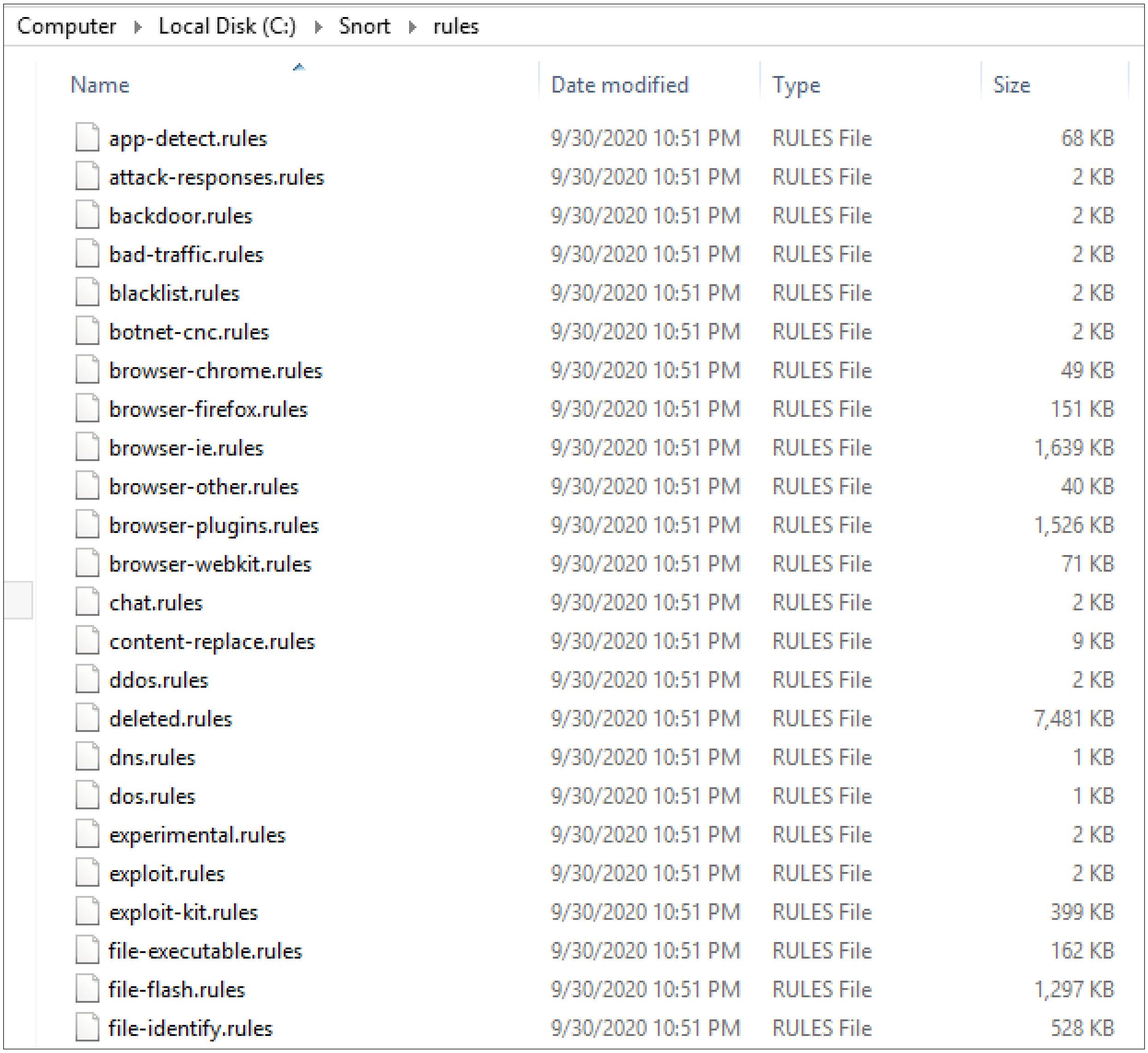


Computer ▸ Local Disk (C:) ▸ Snort ▸ snortrules-snapshot-29161.tar ▸ rules

Name	Date modified	Type	Size
ftp.rules	9/30/2020 10:51 PM	RULES File	1 KB
icmp.rules	9/30/2020 10:51 PM	RULES File	2 KB
icmp-info.rules	9/30/2020 10:51 PM	RULES File	2 KB
imap.rules	9/30/2020 10:51 PM	RULES File	2 KB
indicator-compromise.rules	9/30/2020 10:51 PM	RULES File	228 KB
indicator-obfuscation.rules	9/30/2020 10:51 PM	RULES File	126 KB
indicator-scan.rules	9/30/2020 10:51 PM	RULES File	21 KB
indicator-shellcode.rules	9/30/2020 10:51 PM	RULES File	124 KB
info.rules	9/30/2020 10:51 PM	RULES File	2 KB
local.rules	9/30/2020 10:51 PM	RULES File	2 KB
malware-backdoor.rules	9/30/2020 10:51 PM	RULES File	313 KB
malware-cnc.rules	9/30/2020 10:51 PM	RULES File	2,678 KB
malware-other.rules	9/30/2020 10:51 PM	RULES File	1,406 KB
malware-tools.rules	9/30/2020 10:51 PM	RULES File	96 KB
misc.rules	9/30/2020 10:51 PM	RULES File	2 KB
multimedia.rules	9/30/2020 10:51 PM	RULES File	2 KB
mysql.rules	9/30/2020 10:51 PM	RULES File	2 KB
netbios.rules	9/30/2020 10:51 PM	RULES File	135 KB
nntp.rules	9/30/2020 10:51 PM	RULES File	2 KB

Figure 15: Copy the Rules files

Step 11: Go to “C:\Snort\rules” and paste all the rules files as shown in Figure 16.



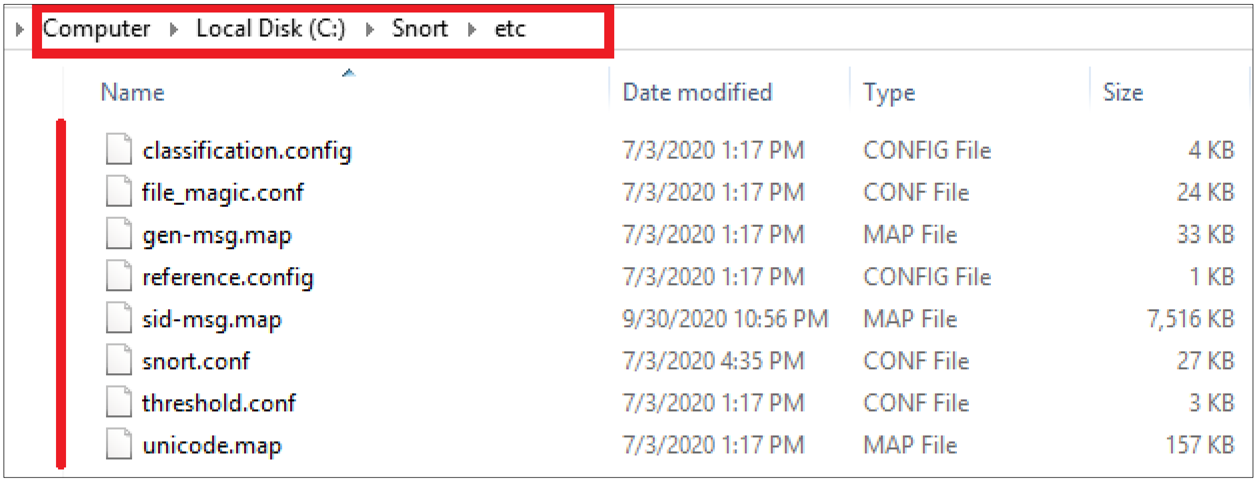
Computer ▸ Local Disk (C:) ▸ Snort ▸ rules

Name	Date modified	Type	Size
app-detect.rules	9/30/2020 10:51 PM	RULES File	68 KB
attack-responses.rules	9/30/2020 10:51 PM	RULES File	2 KB
backdoor.rules	9/30/2020 10:51 PM	RULES File	2 KB
bad-traffic.rules	9/30/2020 10:51 PM	RULES File	2 KB
blacklist.rules	9/30/2020 10:51 PM	RULES File	2 KB
botnet-cnc.rules	9/30/2020 10:51 PM	RULES File	2 KB
browser-chrome.rules	9/30/2020 10:51 PM	RULES File	49 KB
browser-firefox.rules	9/30/2020 10:51 PM	RULES File	151 KB
browser-ie.rules	9/30/2020 10:51 PM	RULES File	1,639 KB
browser-other.rules	9/30/2020 10:51 PM	RULES File	40 KB
browser-plugins.rules	9/30/2020 10:51 PM	RULES File	1,526 KB
browser-webkit.rules	9/30/2020 10:51 PM	RULES File	71 KB
chat.rules	9/30/2020 10:51 PM	RULES File	2 KB
content-replace.rules	9/30/2020 10:51 PM	RULES File	9 KB
ddos.rules	9/30/2020 10:51 PM	RULES File	2 KB
deleted.rules	9/30/2020 10:51 PM	RULES File	7,481 KB
dns.rules	9/30/2020 10:51 PM	RULES File	1 KB
dos.rules	9/30/2020 10:51 PM	RULES File	1 KB
experimental.rules	9/30/2020 10:51 PM	RULES File	2 KB
exploit.rules	9/30/2020 10:51 PM	RULES File	2 KB
exploit-kit.rules	9/30/2020 10:51 PM	RULES File	399 KB
file-executable.rules	9/30/2020 10:51 PM	RULES File	162 KB
file-flash.rules	9/30/2020 10:51 PM	RULES File	1,297 KB
file-identify.rules	9/30/2020 10:51 PM	RULES File	528 KB

Figure 16: Paste the copied files in the rules folder of Snort

HOW TO EDIT THE SNORT.CONF FILE

Step 12: Go to “C:\Snort\etc” to open the snort.conf file as shown in Figure 17.

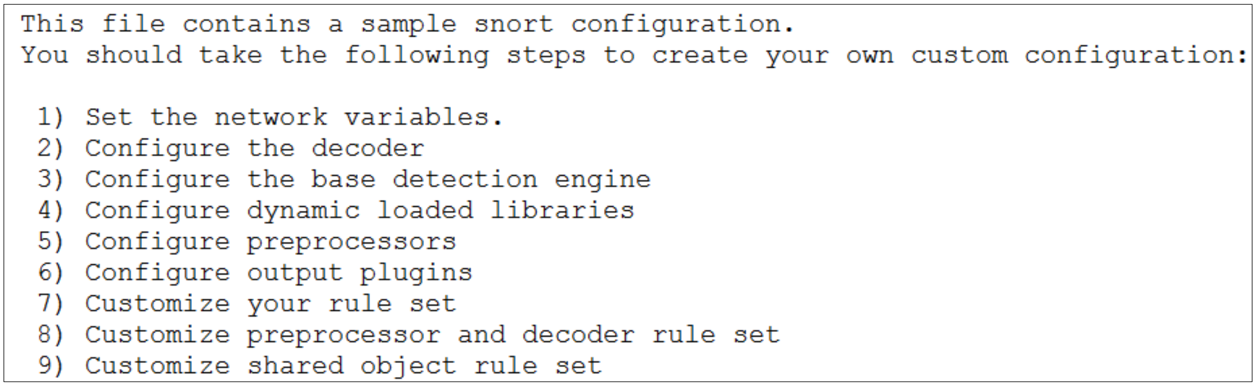


Computer ▸ Local Disk (C:) ▸ Snort ▸ etc

Name	Date modified	Type	Size
classification.config	7/3/2020 1:17 PM	CONFIG File	4 KB
file_magic.conf	7/3/2020 1:17 PM	CONF File	24 KB
gen-msg.map	7/3/2020 1:17 PM	MAP File	33 KB
reference.config	7/3/2020 1:17 PM	CONFIG File	1 KB
sid-msg.map	9/30/2020 10:56 PM	MAP File	7,516 KB
snort.conf	7/3/2020 4:35 PM	CONF File	27 KB
threshold.conf	7/3/2020 1:17 PM	CONF File	3 KB
unicode.map	7/3/2020 1:17 PM	MAP File	157 KB

Figure 17: Conf Files

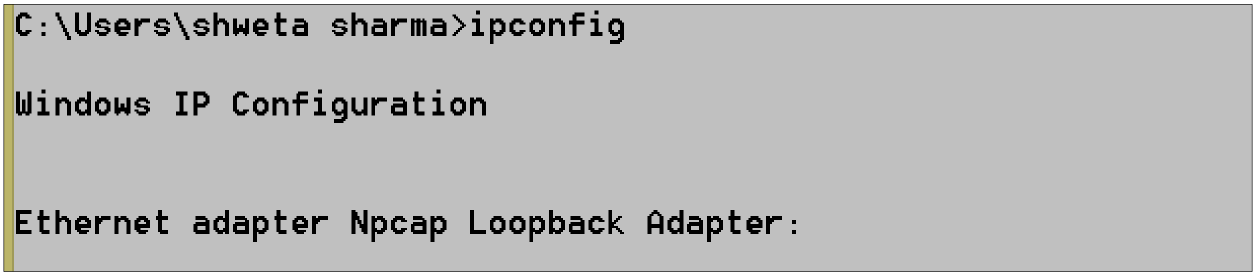
Step 13: There are a total number of 9 steps to edit in snort.conf file as shown in Figure 18.



```
This file contains a sample snort configuration.
You should take the following steps to create your own custom configuration:

 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
```

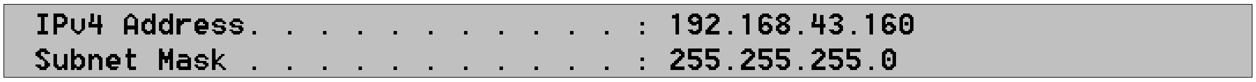
Figure 18: Open the snort.conf File

Step 14: Open the command prompt and type "ipconfig" as shown in Figure 19. The IP address of the personal computer or laptop will be displayed on the command prompt as shown in Figure 20.



```
C:\Users\shweta sharma>ipconfig

Windows IP Configuration


Ethernet adapter Npcap Loopback Adapter:
```

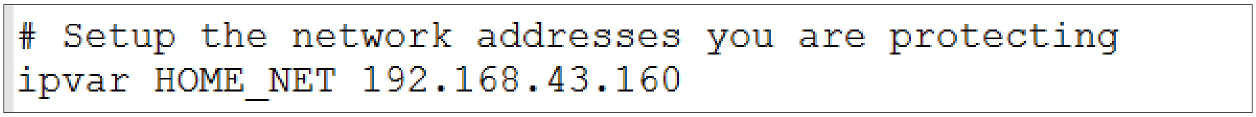
Figure 19: Command prompt



```
 IPv4 Address. . . . . . . . . . . : 192.168.43.160
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

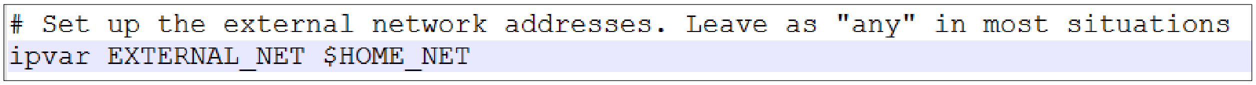
Figure 20: Check the IP address

Step 15: Set the network variables in Step 1 of snort.conf file by typing the IP address (192.168.43.160) found in step 13 as shown in Figure 21. Set up the external network address as home network ($HOME_NET) as shown in Figure 22.



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

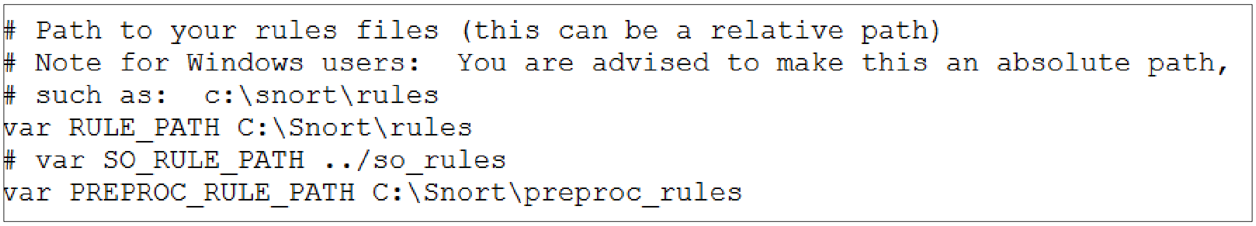
Figure 21: Type the IP Address as HOME_NET



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

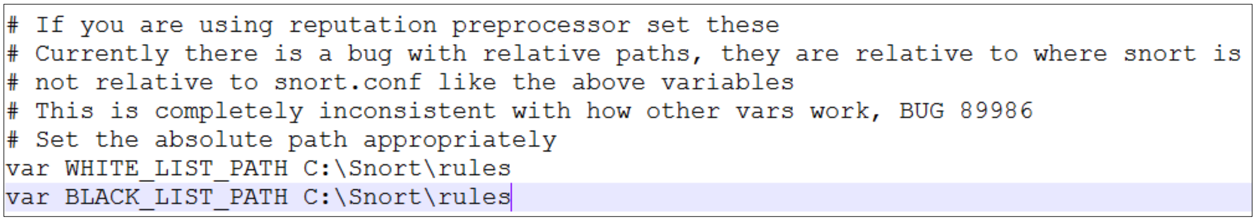
Figure 22: Set up the External Network Address as HOME_NET

Step 16: Set the path of the rules files as “C:\Snort\rules” and “C:\Snort\preproc_rules” as shown in Figure 23. Set the white list and black list path as to “C:\Snort\rules” as shown in Figure 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
```

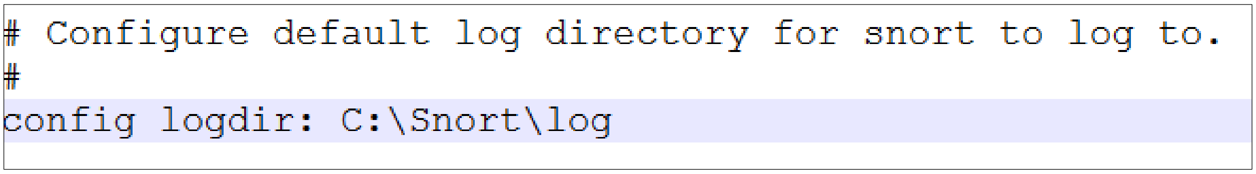
Figure 23: Set the path of the rules



```
# 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
```

Figure 24: Set the path of the White List and Black List

Step 17: 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 25.

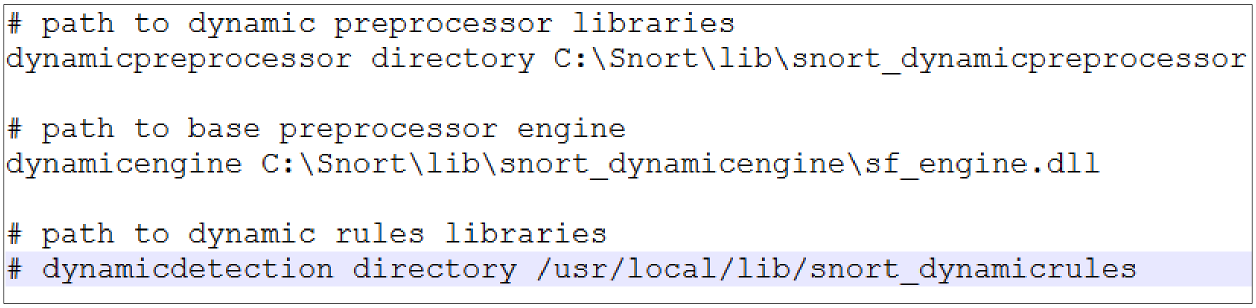


```
# Configure default log directory for snort to log to.
#
config logdir: C:\Snort\log
```

Figure 25: Set the path of the log Directory

Step 18: There is no change in Step 3 (Configure the base detection engine) of snort.conf file.

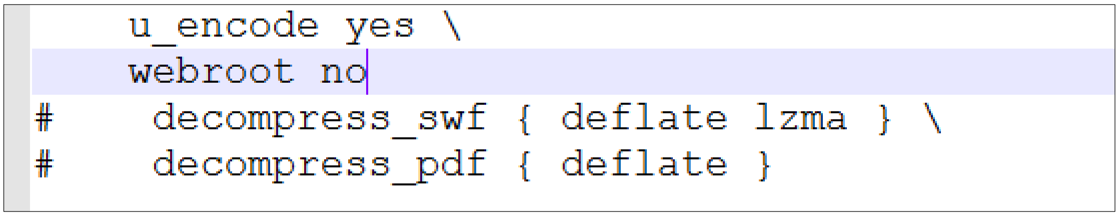
Step 19: Configure dynamic loaded libraries in Step 4 of snort.conf file by setting the path of the dynamic preprocessor libraries as “C:\Snort\lib\snort_dynamicpreprocessor” and base preprocessor engine as “C:\Snort\lib\snort_dynamicengine\sf_engine.dll” as shown in Figure 26.



```
# 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
```

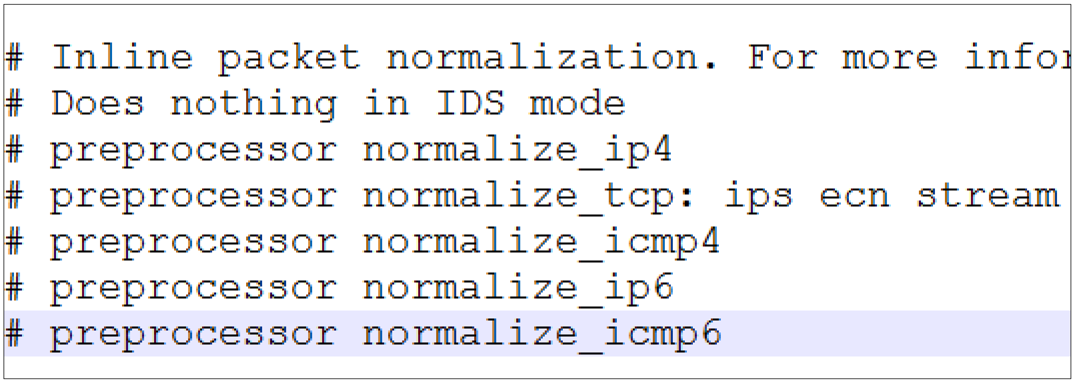
Figure 26: Set the path of the Libraries and Engines

Step 20: 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 27. Also, put the preprocessors in comments as shown in Figure 28. Also, put the preprocessor bo in comments as shown in Figure 29. Delete comment from preprocessor sfportscan as shown in Figure 30.



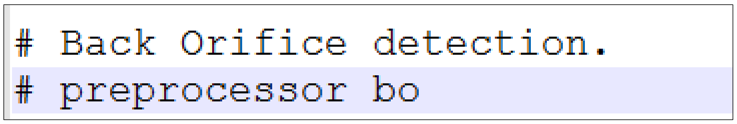
```
    u_encode yes \
    webroot no
#    decompress_swf { deflate lzma } \
#    decompress_pdf { deflate }
```

Figure 27: Set webroot



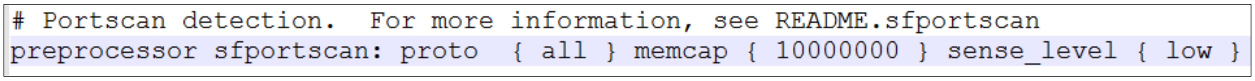
```
# Inline packet normalization. For more infor
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```

Figure 28: Put preprocessor in comments



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

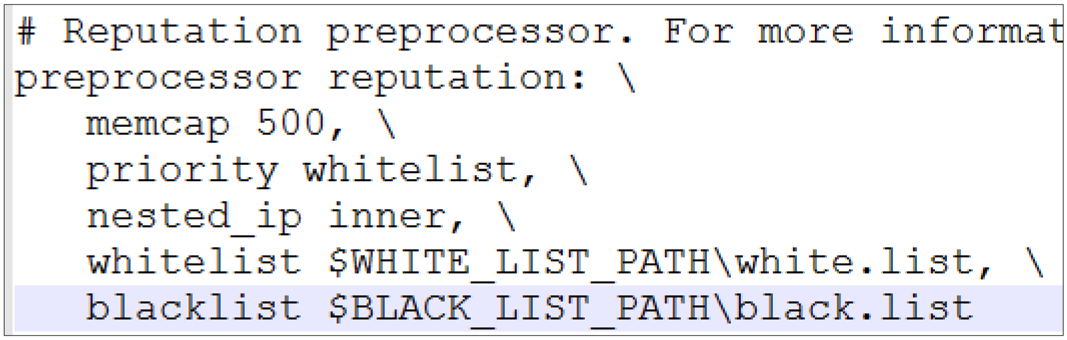
Figure 29: Put preprocessor bo in comments



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

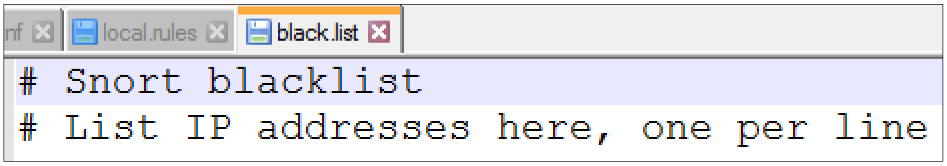
Figure 30: Delete Comment from preprocessor sfportscan

Step 21: Set path to white list and black list as shown in Figure 31. Create a new white list and black list as shown in Figure 32 and Figure 33. Save these files in rules directory as shown in Figure 34.



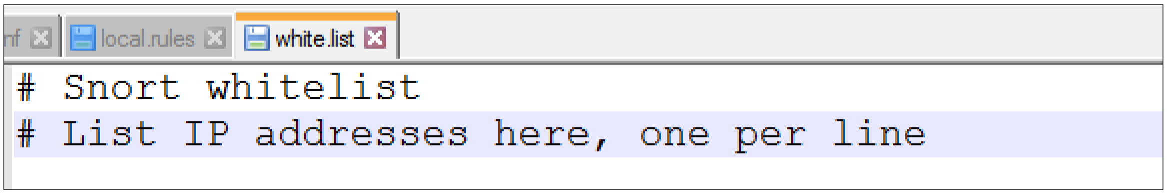
```
# Reputation preprocessor. For more informat
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\white.list, \
   blacklist $BLACK_LIST_PATH\black.list
```

Figure 31: Set Path to White and Black list



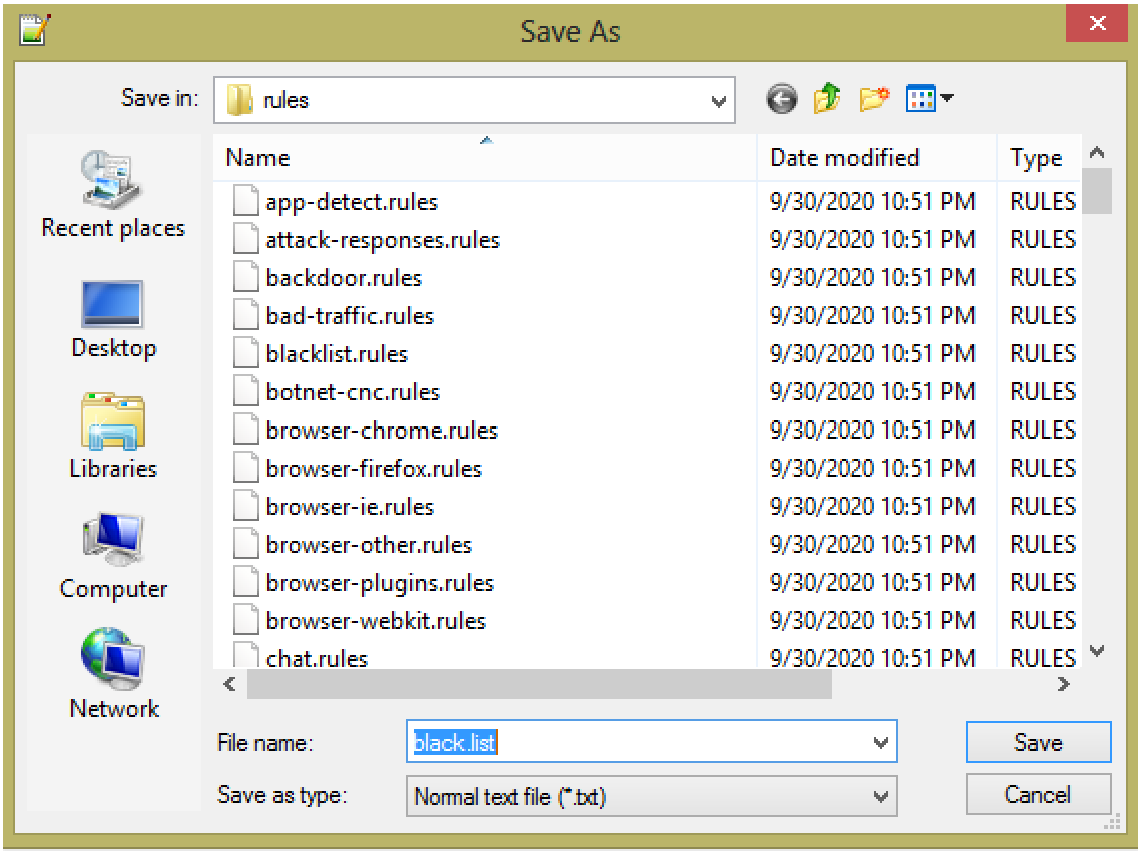
```
# Snort blacklist
# List IP addresses here, one per line
```

Figure 32: Create a Black list



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

Figure 33: Create a White list



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

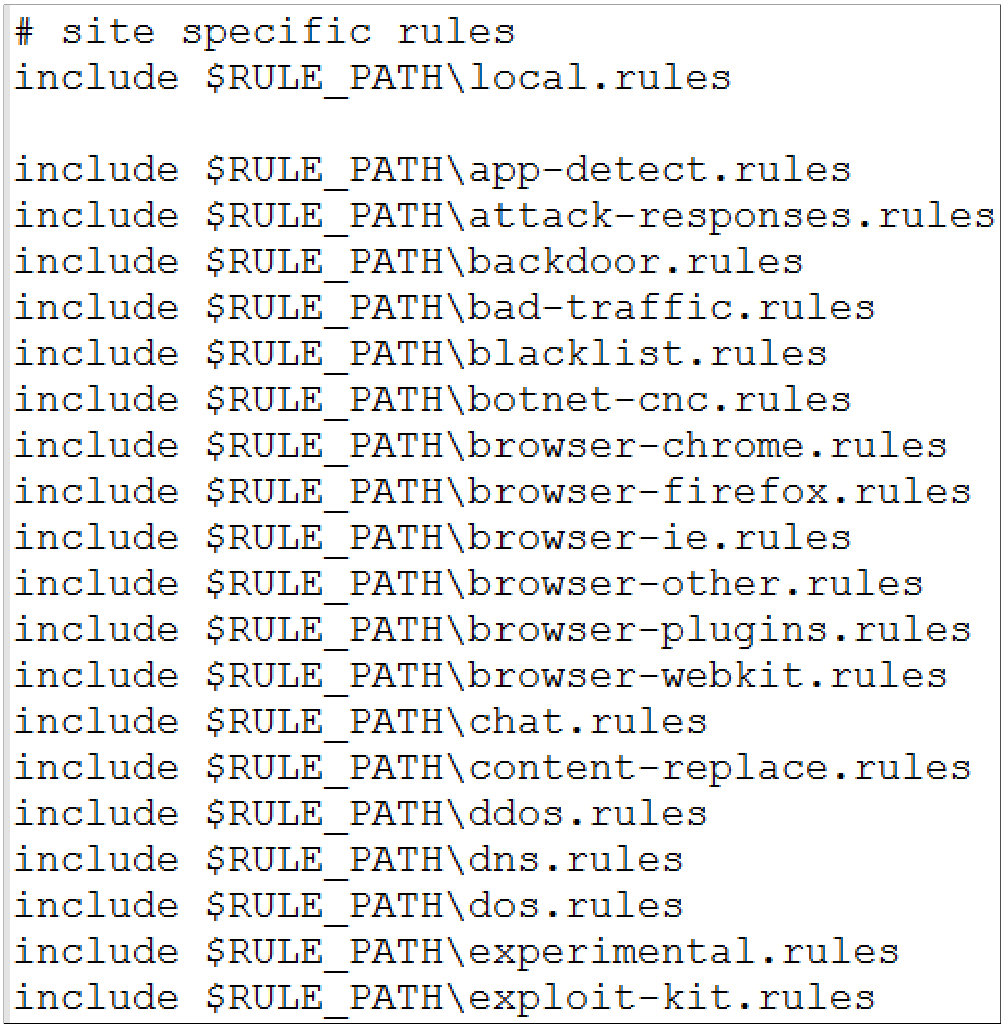
File name: black.list

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

Figure 34: Save Black List in rules Directory

<u>Step 22:</u> There is no change in Step 6 (Configure output plugins) of snort.conf file.

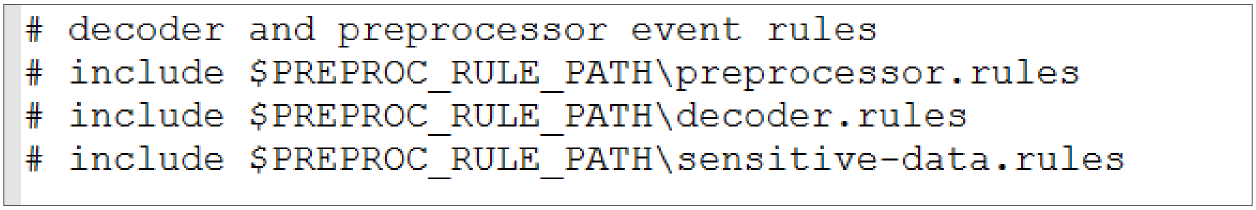
<u>Step 23:</u> Customize rule set in Step 7 of snort.conf file by replacing the forward slash "/" with backslash "\" as shown in Figure 35 (applicable for Windows operating system).



```
# 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
```

Figure 35: Save Black List in rules Directory

<u>Step 24:</u> Customize preprocessor and decoder alerts in Step 8 of snort.conf file by replacing the forward slash "/" with backslash "\" as shown in Figure 36 (applicable for Windows operating system).

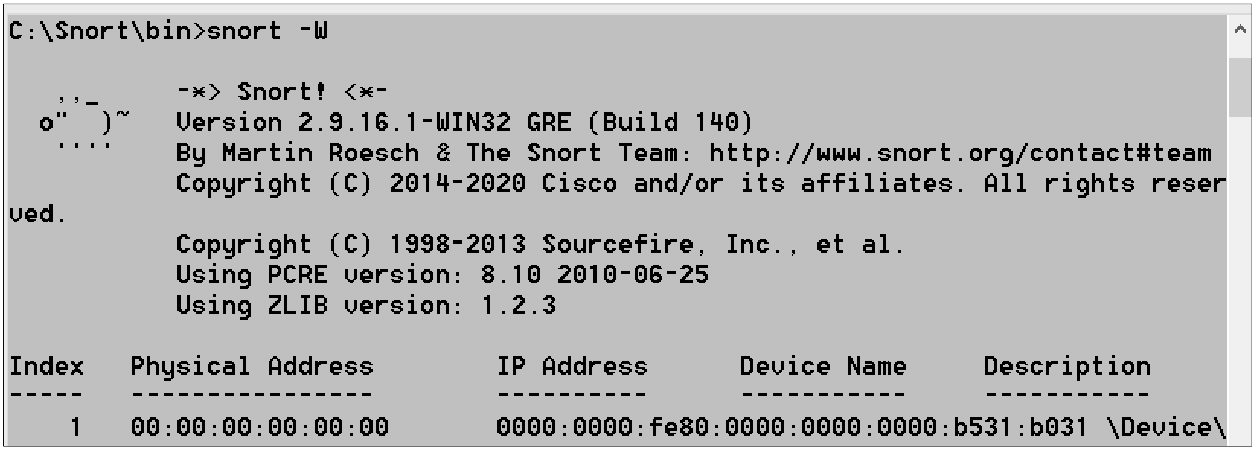


```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

Figure 36: Put Decoders and Preprocessors Rules in Comments

<u>Step 25:</u> There is no change in Step 9 (Customize shared object snort rules) of snort.conf file.

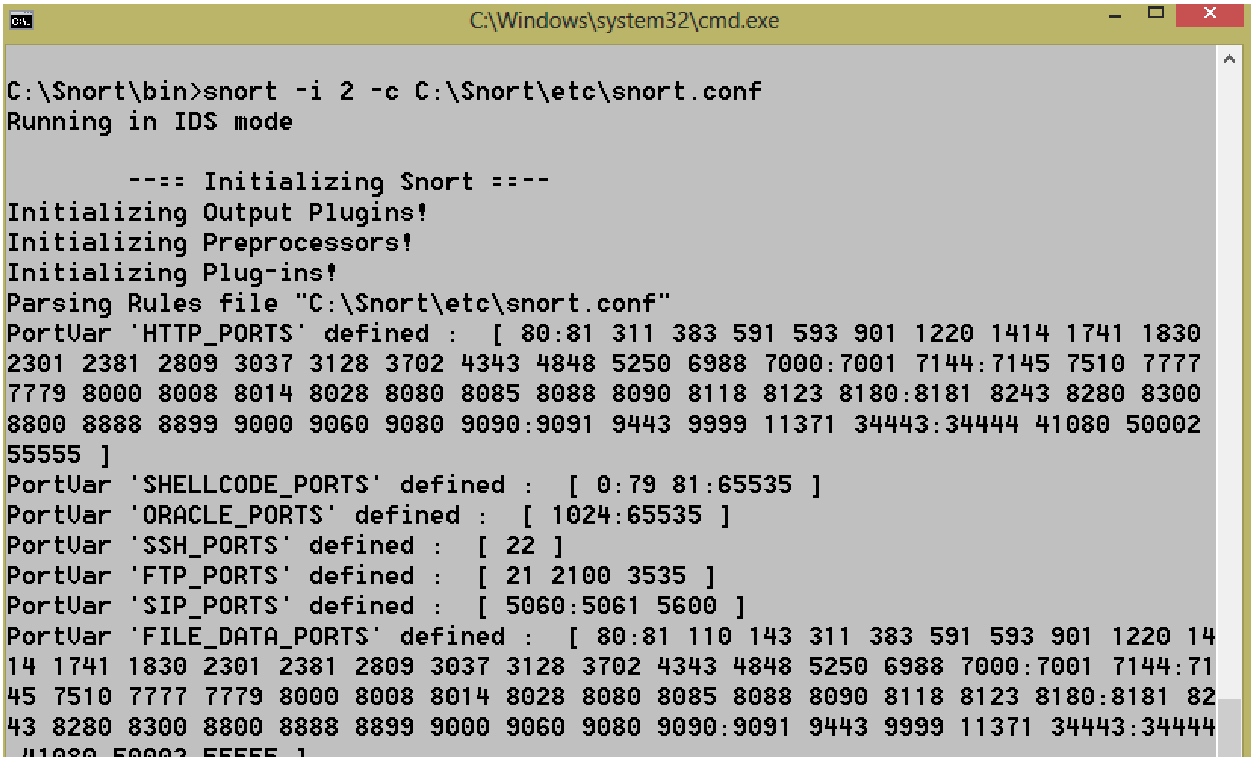
<u>Step 26:</u> Open the command prompt and go to “C:\Snort\bin” and type “snort –W” to check the available interface as shown in Figure 37.



```
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\
```

Figure 37: Check the Interface

<u>Step 27:</u> Execute the Snort tool in the command prompt by typing “snort –i 2 –c C:\Snort\etc\snort.conf” as shown in Figure 38 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 ]
```

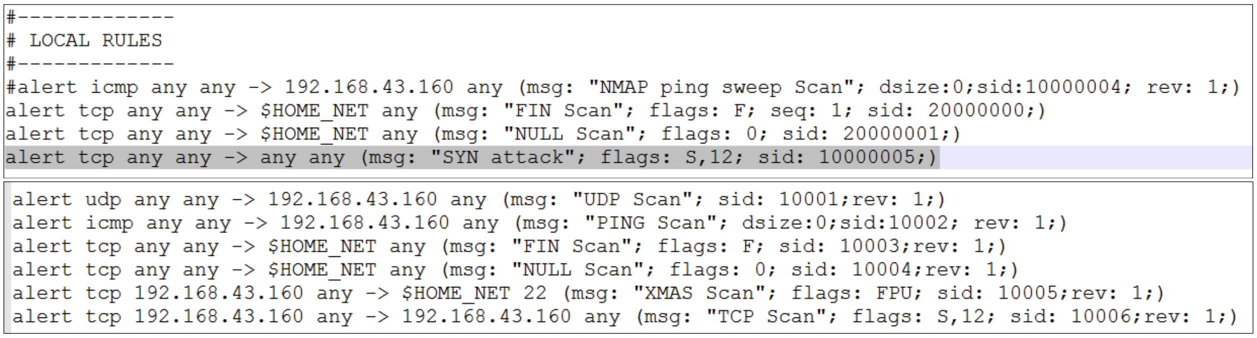
Figure 38: Execute Snort Tool

HOW TO WRITE RULES TO DETECT SCANNING ATTACKS

__Step 28:__ 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;)

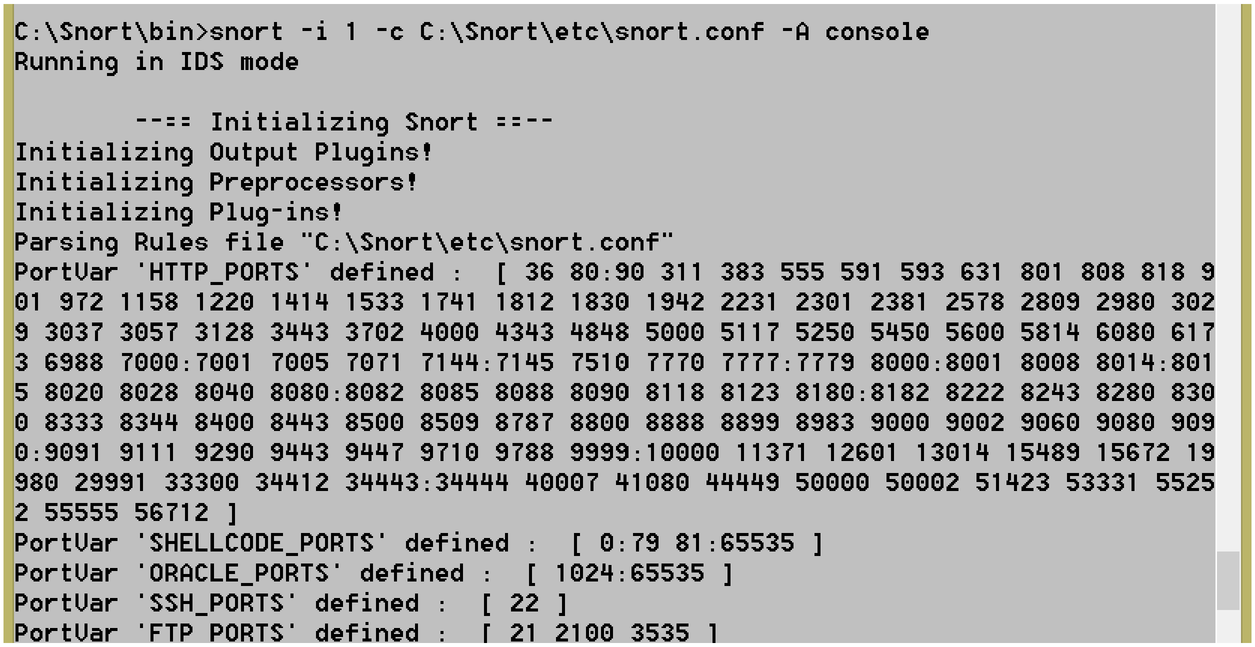


```
#-------------
# LOCAL RULES
#-------------
#alert icmp any any -> 192.168.43.160 any (msg: "NMAP ping sweep Scan"; dsize:0;sid:10000004; rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "FIN Scan"; flags: F; seq: 1; sid: 20000000;)
alert tcp any any -> $HOME_NET any (msg: "NULL Scan"; flags: 0;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

Figure 39: Adding Rules in local.rules

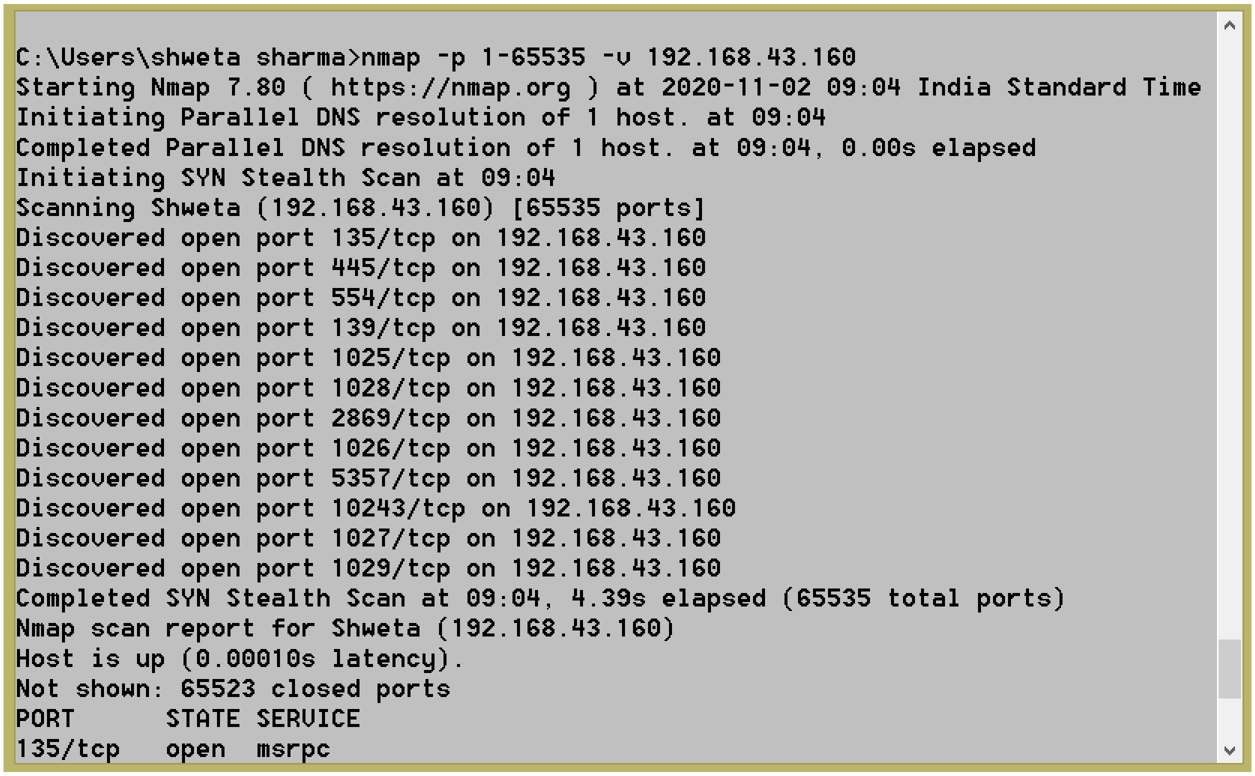
Step 29: Execute Snort in IDS mode by typing “snort –i 1 –c C:\Snort\etc\snort.conf –A console” in the command prompt and press Enter as shown in Figure 40.



```
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 ]
```

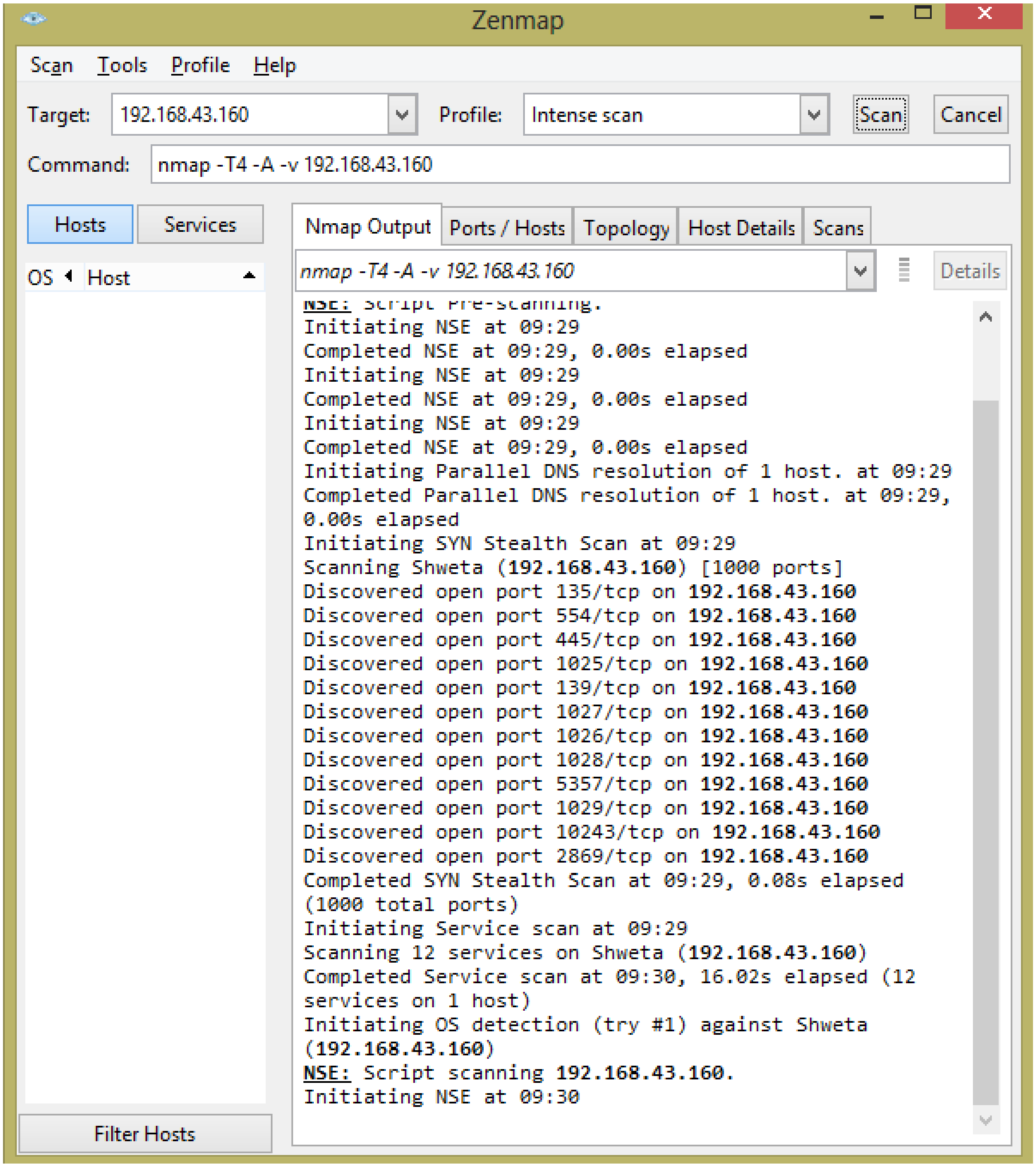
Figure 40: Running Snort in IDS mode

<u>Step 30:</u> Perform network scanning attacks with nmap by typing “nmap –p 1-65535 –v 192.168.43.160” in the command prompt as shown in Figure 41 where *p* is the port number and *v* is the verbose mode. The network scanning attacks can be performed with Zenmap tool as shown in Figure 42.



```
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
```

Figure 41: Network Scanning Attack with Nmap Tool



Target: 192.168.43.160

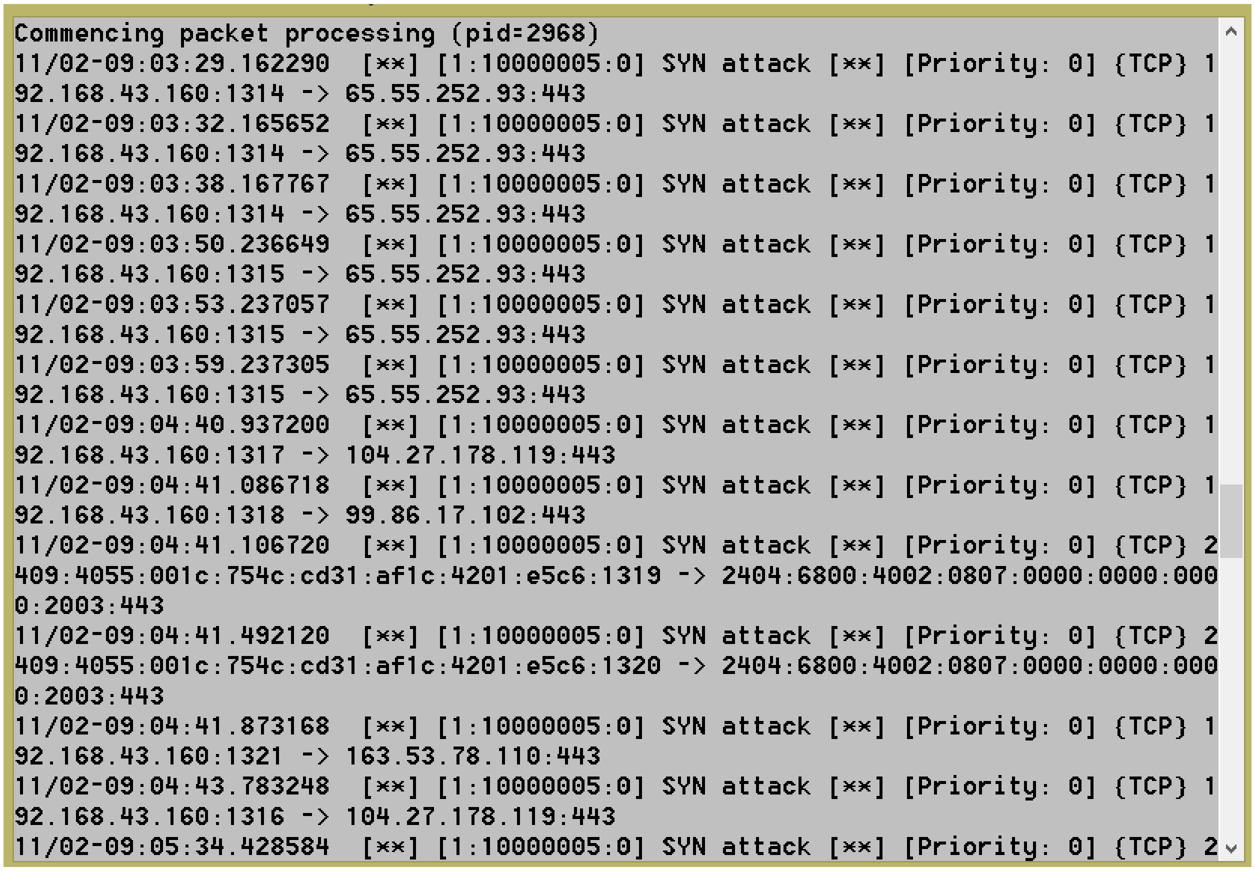
Profile: Intense scan

Command: 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
```

Figure 42: Network Scanning Attack with Zenmap Tool

<u>Step 29:</u> The network scanning attacks are detected by Snort IDS as shown in Figure 43.



```
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
```

Figure 43: Detection of Network Scanning Attack with Snort IDS

COUNTERMEASURES

The following countermeasures must be followed:

- Always disable SNMP and SMB on hosts if not using it for a particular period of time.
- Block the SNMP ports (UDP ports 161 and 162) and SMB ports (TCP port 139 and 445) at the network perimeter.
- There’s technically a “U” that’s part of the solution: upgrade. Upgrading systems (at least the ones you can) to

SNMP version 3 and SMB version 2 can resolve many of the well-known SNMP and SMB security weaknesses.

REFERENCES

[1] Snort, 2020, https://www.snort.org/ (accessed Dec. 24, 2020).