Experiment 10

Aim: Study of Network security : Set up Snort and study the logs.

Roll No.	70
Name	MAYURI SHRIDATTA YERANDE
Class	D15-B
Subject	Internet Security Lab
LO Mapped	LO6: Demonstrate the network security system using open source tools.

AIM: Study of Network security: Set up Snort and study the logs.

THEORY:

SNORT is a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity. Using SNORT, network admins can spot denial-of-service (DoS) attacks and distributed DoS (DDoS) attacks, Common Gateway Interface (CGI) attacks, buffer overflows, and stealth port scans. SNORT creates a series of rules that define malicious network activity, identify malicious packets, and send alerts to users.

There are various features that make SNORT useful for network admins to monitor their systems and detect malicious activity. These include:

- Real-time Traffic Monitor

SNORT can be used to monitor the traffic that goes in and out of a network. It will monitor traffic in real time and issue alerts to users when it discovers potentially malicious packets or threats on Internet Protocol (IP) networks.

- Packet Logging

SNORT enables packet logging through its packet logger mode, which means it logs packets to the disk. In this mode, SNORT collects every packet and logs it in a hierarchical directory based on the host network's IP address.

- Analysis of Protocol

SNORT can perform protocol analysis, which is a network sniffing process that captures data in protocol layers for additional analysis. This enables the network admin to further examine potentially malicious data packets, which is crucial in, for example, Transmission Control Protocol/IP (TCP/IP) stack protocol specification.

- Content Matching

SNORT collates rules by the protocol, such as IP and TCP, then by ports, and then by those with content and those without. Rules that do have content use a multi-pattern matcher that increases performance, especially when it comes to protocols like the Hypertext Transfer Protocol (HTTP). Rules that do not have content are always evaluated, which negatively affects performance.

- OS Fingerprinting

Operating system (OS) fingerprinting uses the concept that all platforms have a unique TCP/IP stack. Through this process, SNORT can be used to determine the OS platform being used by a system that accesses a network.

- Can Be Installed in Any Network Environment

SNORT can be deployed on all operating systems, including Linux and Windows, and as part of all network environments.

- Open Source

As a piece of open-source software, SNORT is free and available for anyone who wants to use an IDS or IPS to monitor and protect their network.

- Rules Are Easy to Implement

SNORT rules are easy to implement and get network monitoring and protection up and running. Its rule language is also very flexible, and creating new rules is pretty simple, enabling network admins to differentiate regular internet activity from anomalous or malicious activity.

IMPLEMENTATION:

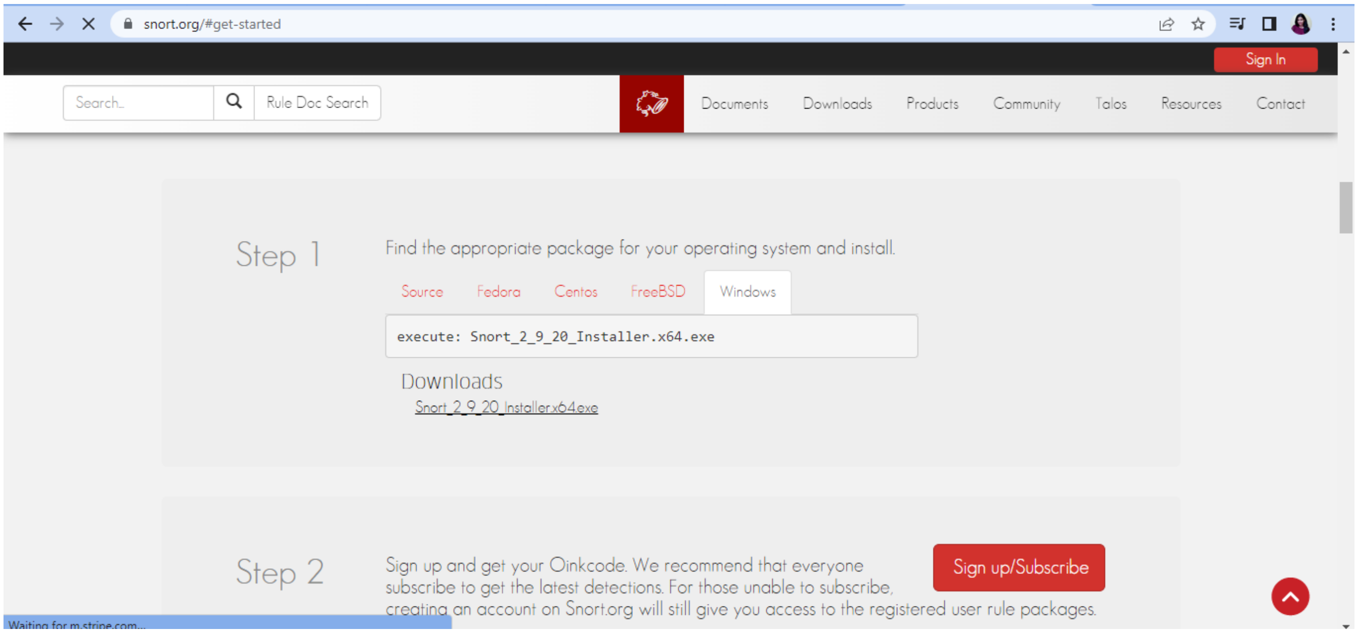
Installation

Download link for WinPcap: https://www.winpcap.org/default.htm

Download nPCAP: https://npcap.com/

Link for Snort: https://www.snort.org/

- In Snort, Go to “Get started”
- Click on Windows and download the exe file.



Step 1

Find the appropriate package for your operating system and install.

```
execute: Snort_2_9_20_Installer.x64.exe
```

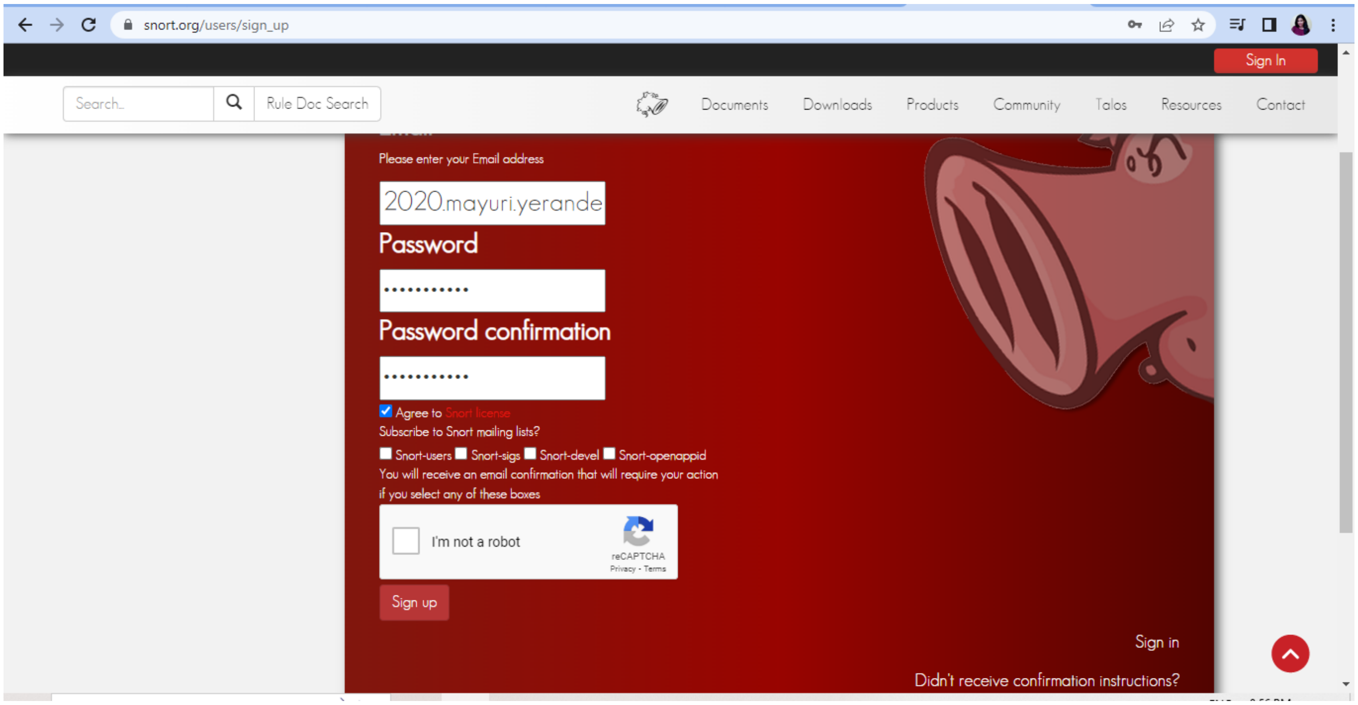
Downloads

Snort_2_9_20_Installer.x64.exe

Step 2

Sign up and get your Oinkcode. We recommend that everyone subscribe to get the latest detections. For those unable to subscribe, creating an account on Snort.org will still give you access to the registered user rule packages.

- Sign up into Snort



Please enter your Email address

2020.mayuri.yerande

Password

•••••••••••

Password confirmation

•••••••••••

☑ Agree to Snort license

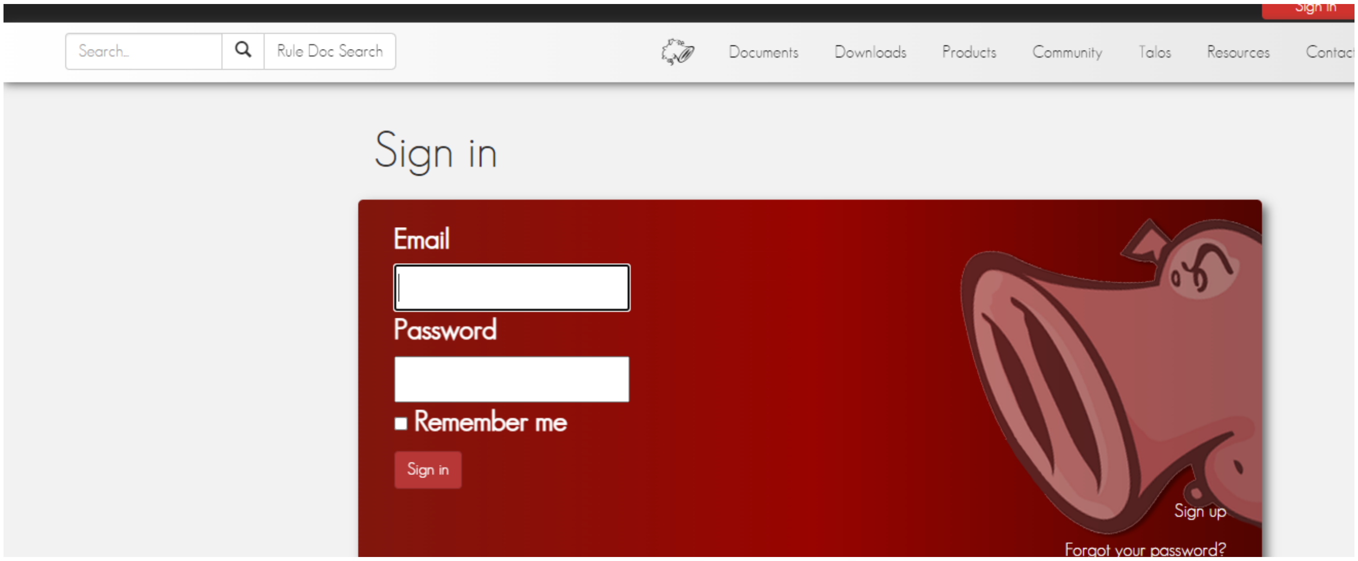
Subscribe to Snort mailing lists?

□ Snort-users □ Snort-sigs □ Snort-devel □ Snort-openappid

You will receive an email confirmation that will require your action if you select any of these boxes

□ I'm not a robot

- You will receive a mail for verification, After that sign in



Sign in

Email

Password

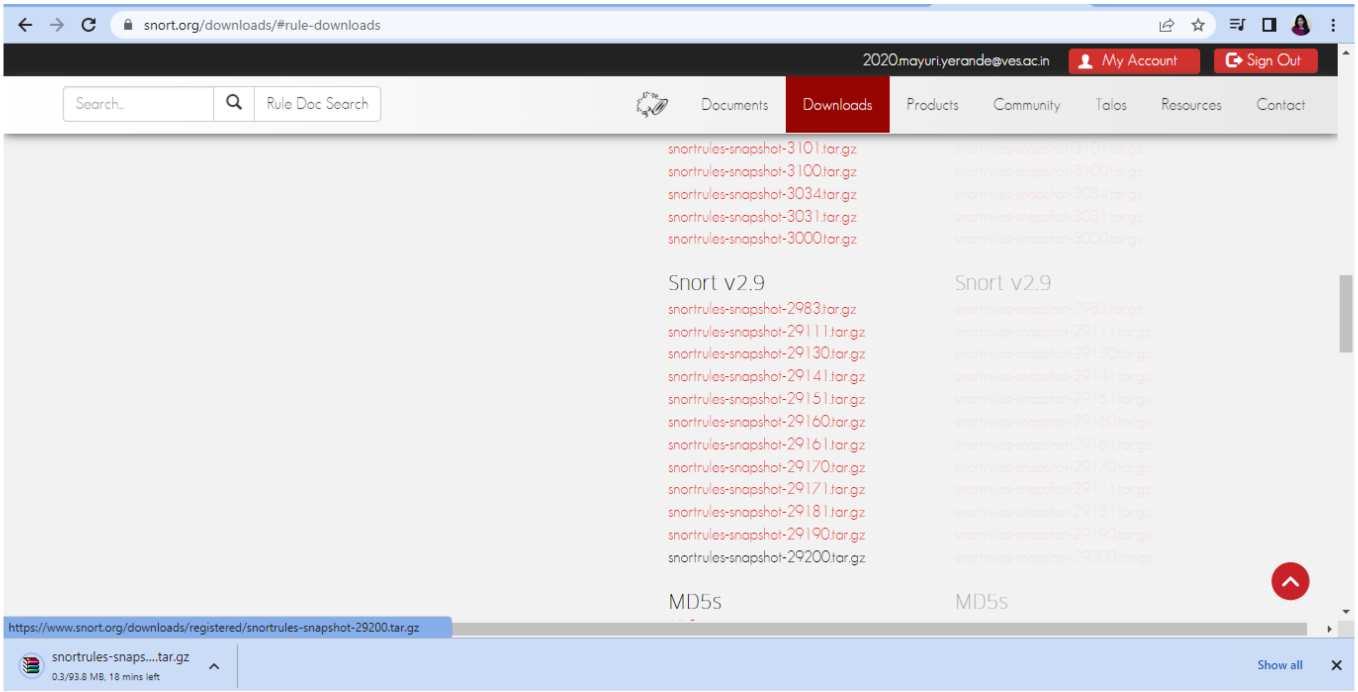
■ Remember me

Sign in

Sign up

Forgot your password?

- Go to rules and download the rules according to the version of snort you downloaded



snort.org/downloads/#rule-downloads

2020.mayuri.yerande@ves.ac.in

snortrules-snapshot-3101.tar.gz
snortrules-snapshot-3100.tar.gz
snortrules-snapshot-3034.tar.gz
snortrules-snapshot-3031.tar.gz
snortrules-snapshot-3000.tar.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-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-29171.tar.gz
snortrules-snapshot-29181.tar.gz
snortrules-snapshot-29190.tar.gz
snortrules-snapshot-29200.tar.gz

MD5s

snortrules-snapshot-3101.tar.gz
snortrules-snapshot-3100.tar.gz
snortrules-snapshot-3034.tar.gz
snortrules-snapshot-3031.tar.gz
snortrules-snapshot-3000.tar.gz

Snort v2.9

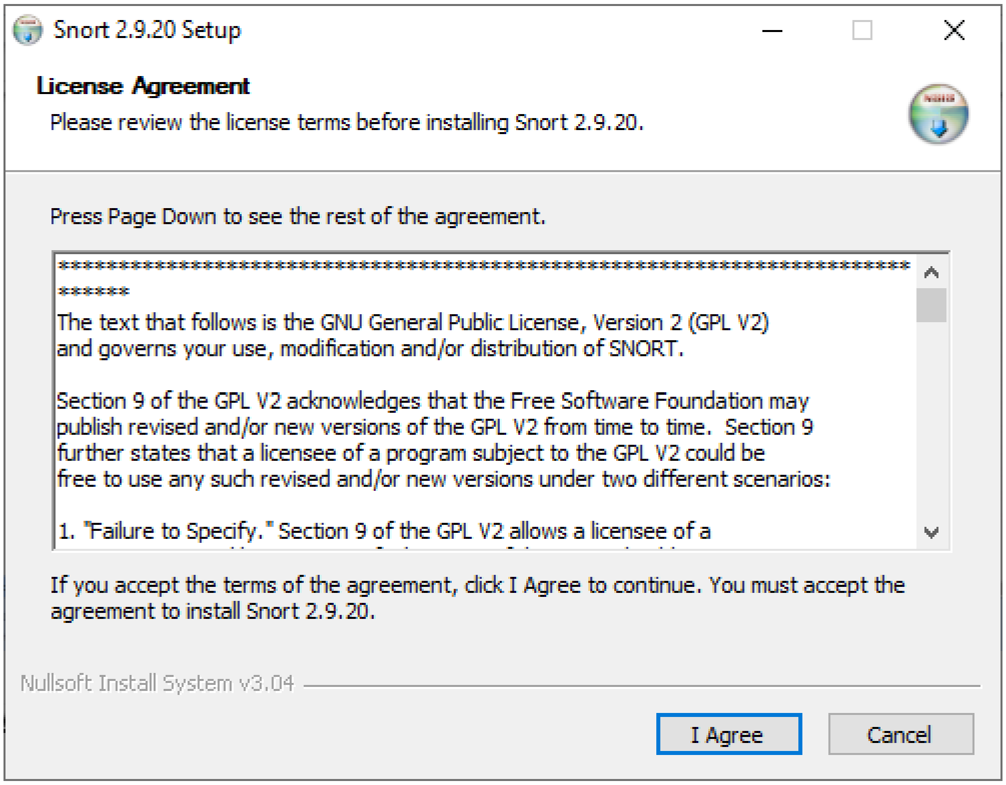
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-29171.tar.gz
snortrules-snapshot-29181.tar.gz
snortrules-snapshot-29190.tar.gz
snortrules-snapshot-29200.tar.gz

MD5s

https://www.snort.org/downloads/registered/snortrules-snapshot-29200.tar.gz

snortrules-snaps....tar.gz
0.3/93.8 MB, 18 mins left

- Install WinPcap and Npcap on your machine
- Installation of Snort



Snort 2.9.20 Setup

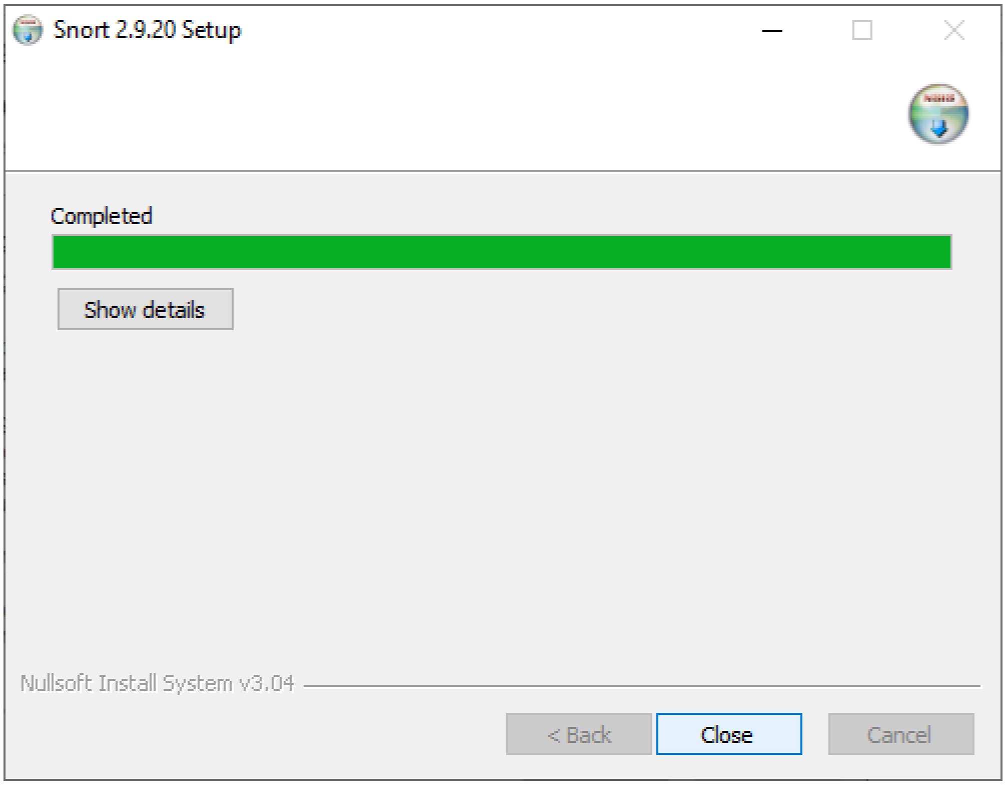
License Agreement

Please review the license terms before installing Snort 2.9.20.

Press Page Down to see the rest of the agreement.

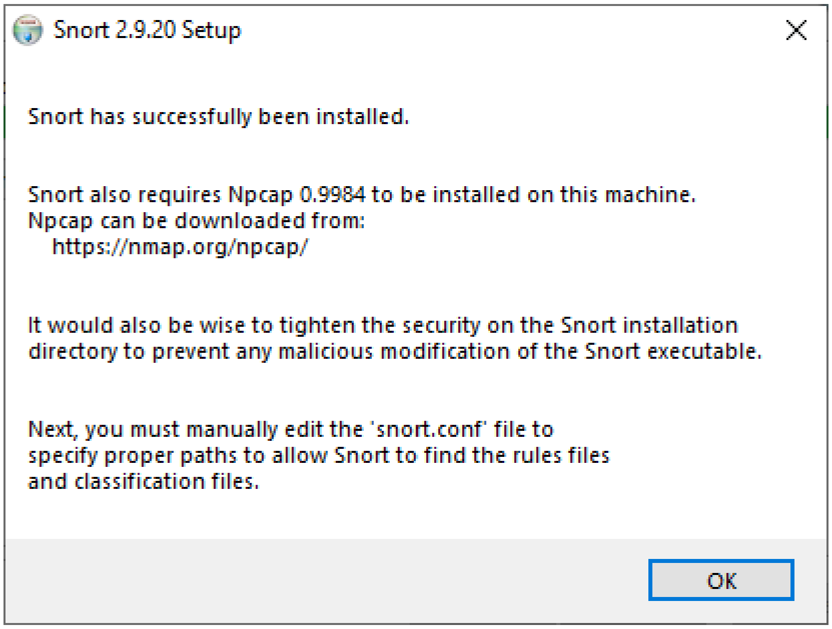
```
*****************************************************************************
******
The text that follows is the GNU General Public License, Version 2 (GPL V2)
and governs your use, modification and/or distribution of SNORT.

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.



Snort 2.9.20 Setup

Completed



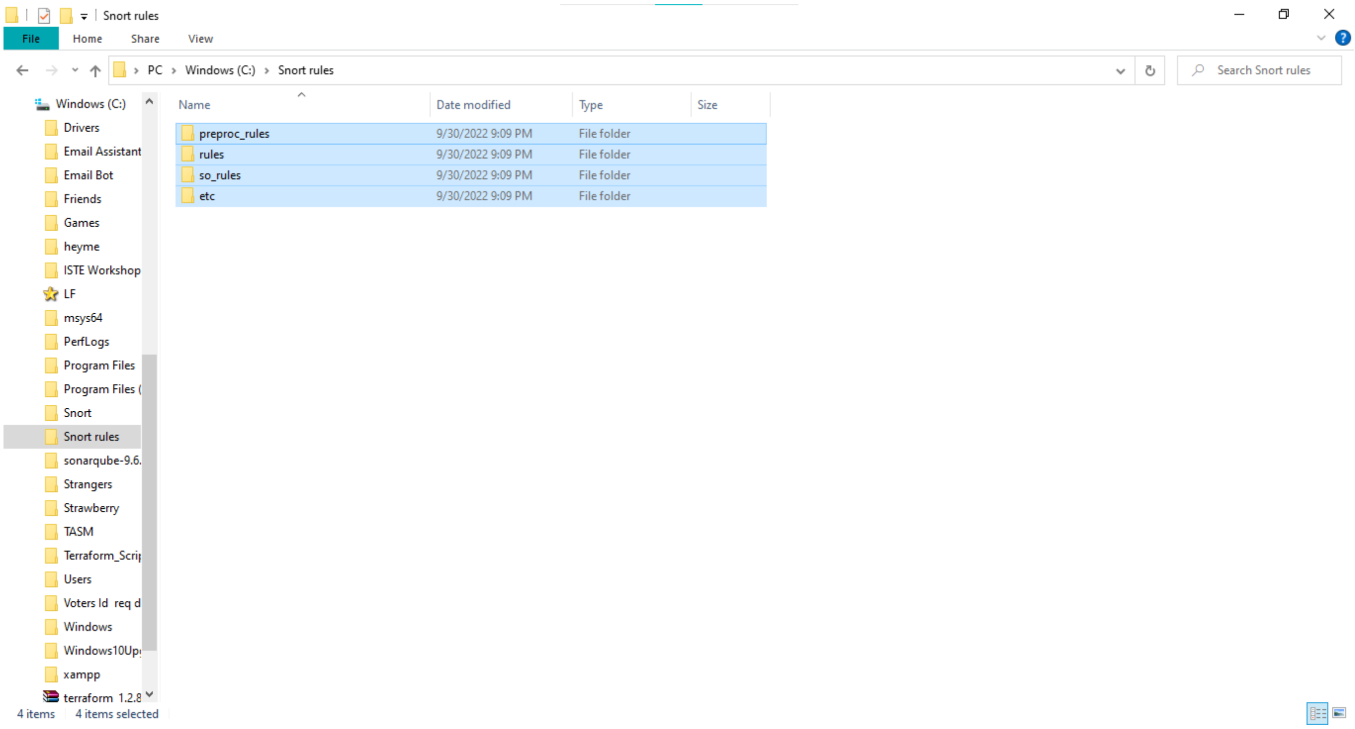
Snort has successfully been installed.

Snort also requires Npcap 0.9984 to be installed on this machine.
Npcap can be downloaded from:
https://nmap.org/npcap/

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.

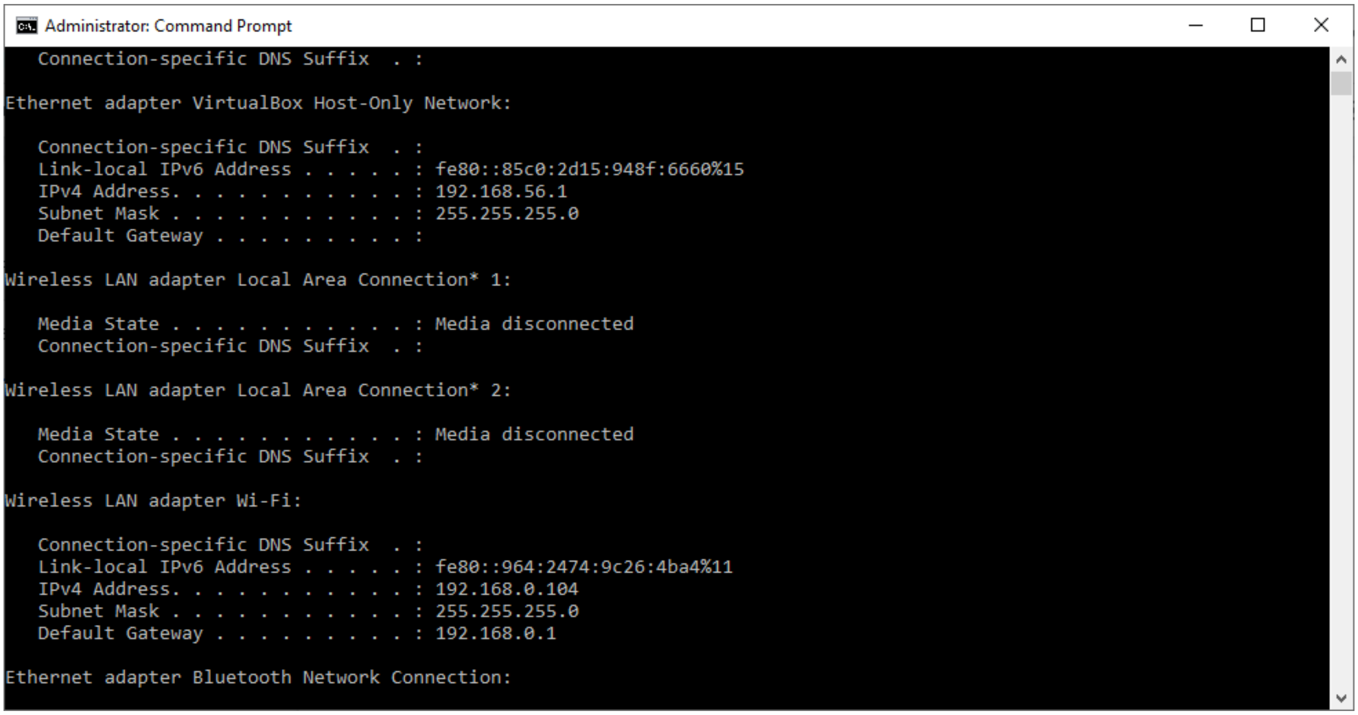
- Extract the rules file and put it into a folder named “snort rules”



Name	Date modified	Type	Size
preproc_rules	9/30/2022 9:09 PM	File folder	
rules	9/30/2022 9:09 PM	File folder	
so_rules	9/30/2022 9:09 PM	File folder	
etc	9/30/2022 9:09 PM	File folder	

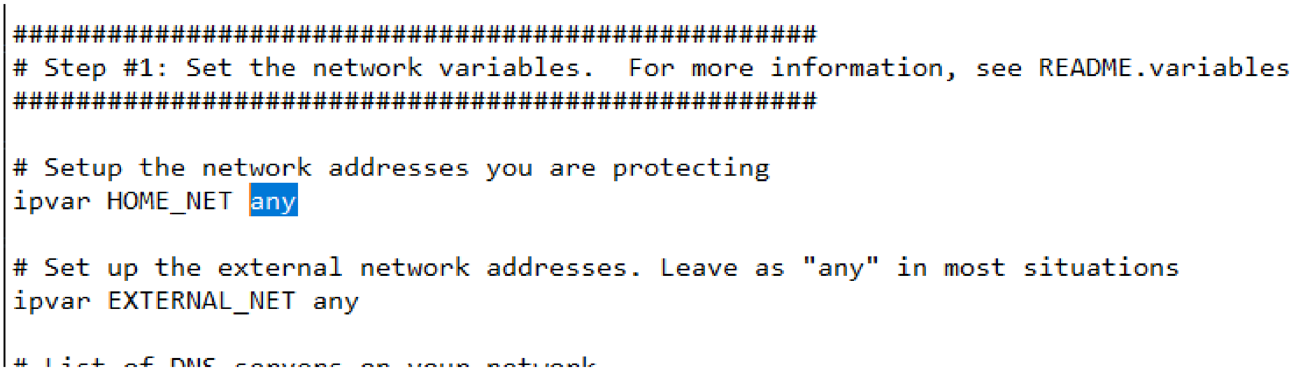
Configuration of Snort:

- Now open your snort.conf file via notepad from the “etc” folder.
- Find “Default gateway” of your device by putting “ipconfig” on your administrator cmd.



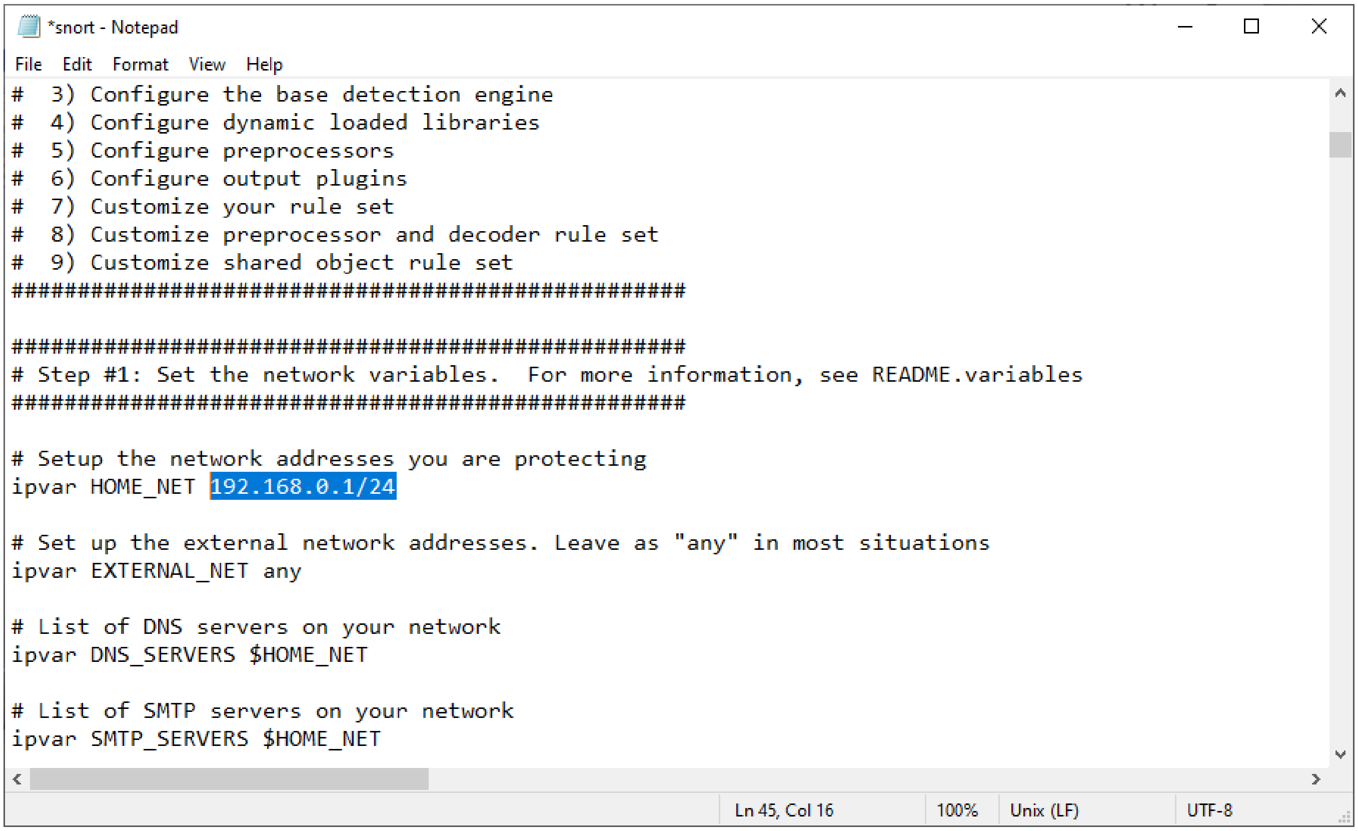
```
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::85c0:2d15:948f:6660%15
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::964:2474:9c26:4ba4%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:
```

- Remove “any”



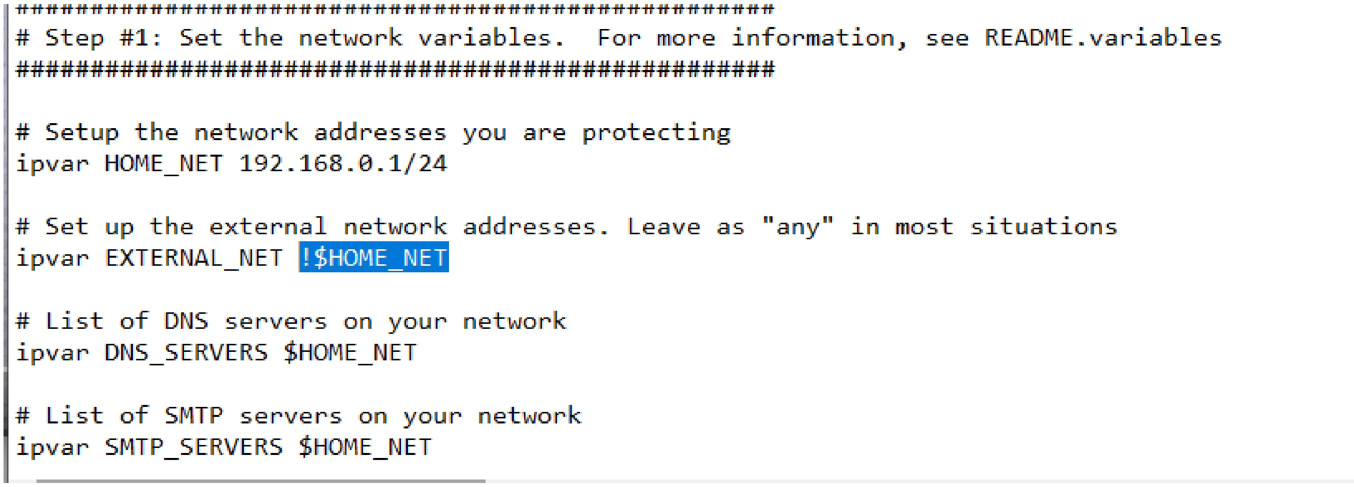
```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# 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 any

# List of DNS servers on your network
```

- And add your address there with /24



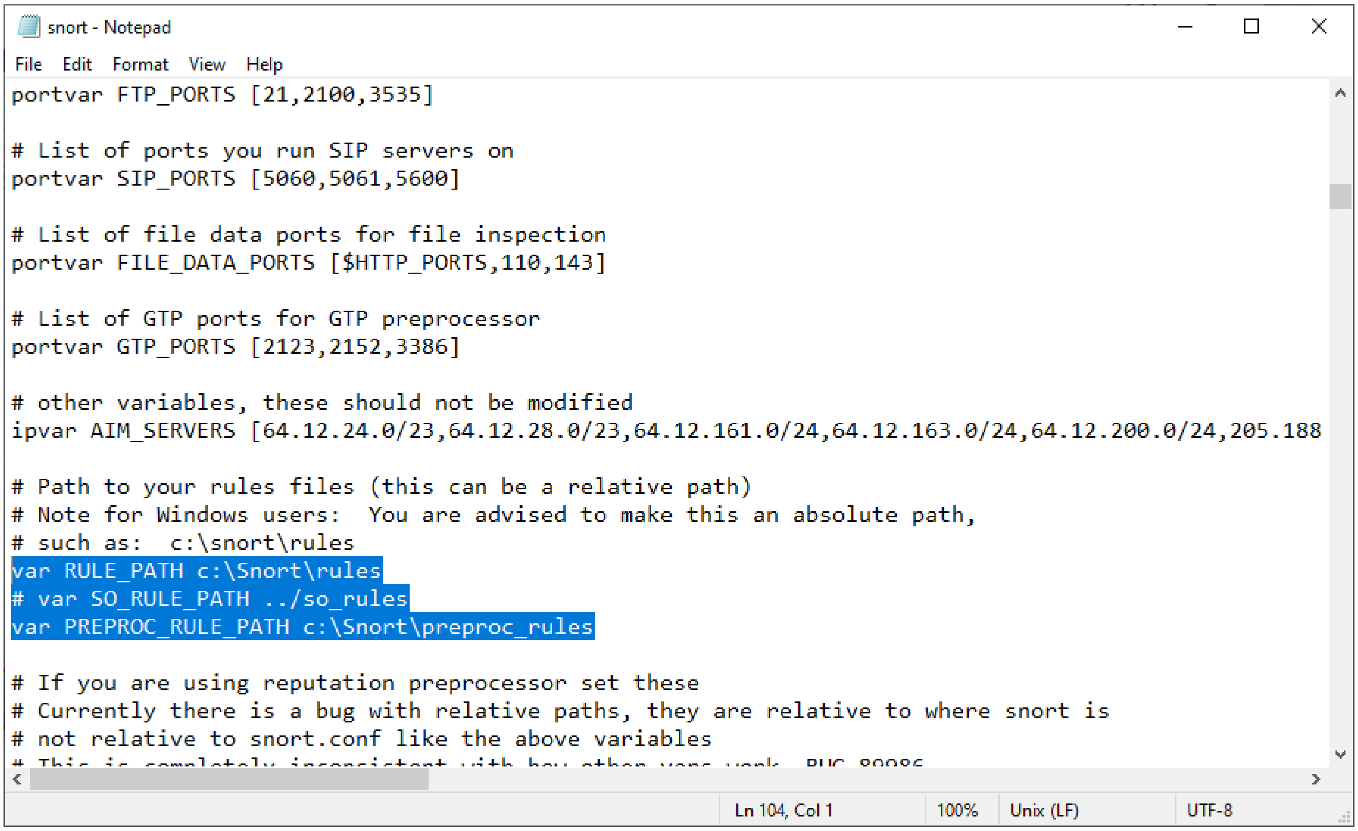
```
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

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

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.1/24

# 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
```

- Add “!$HOME_NET” instead of “any” in the line specified.

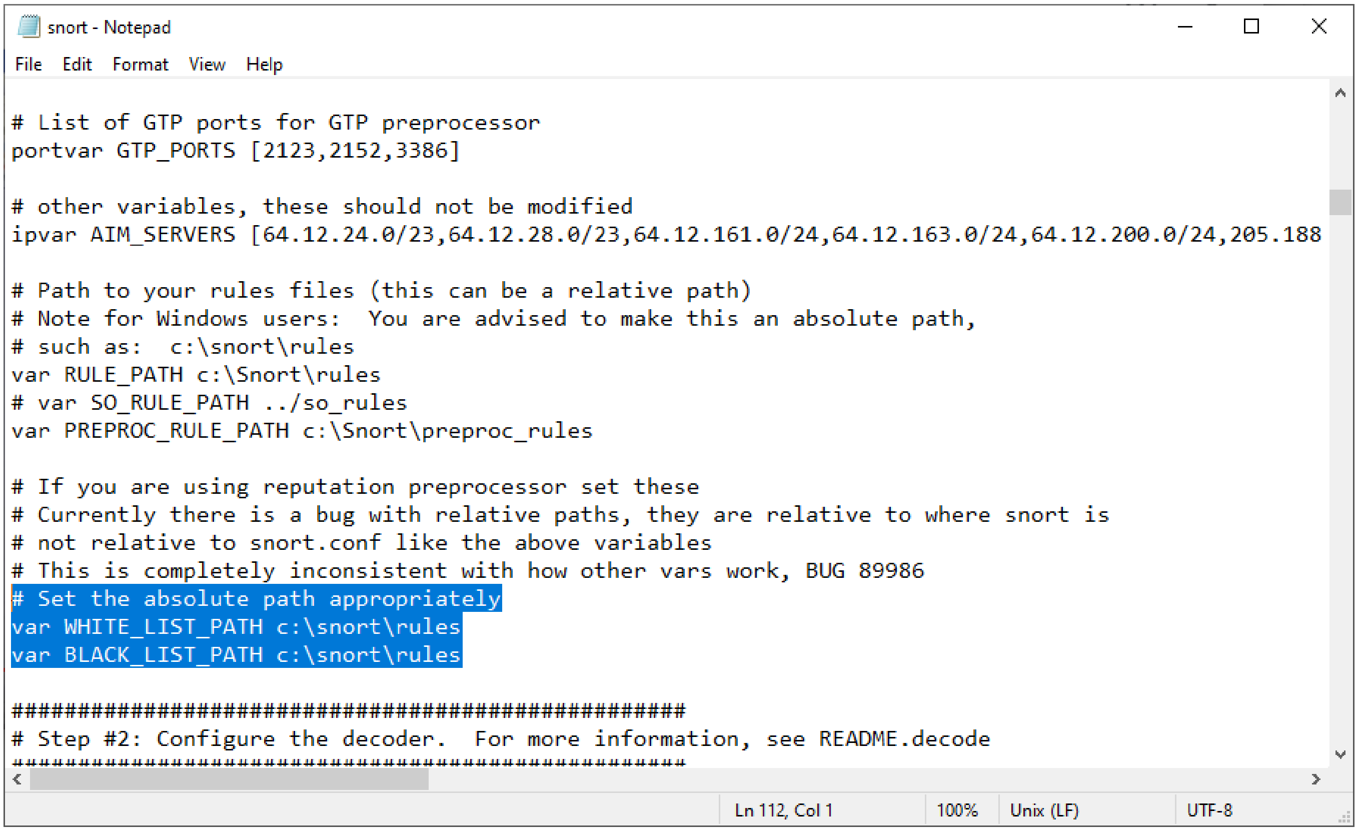


```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.1/24

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

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

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

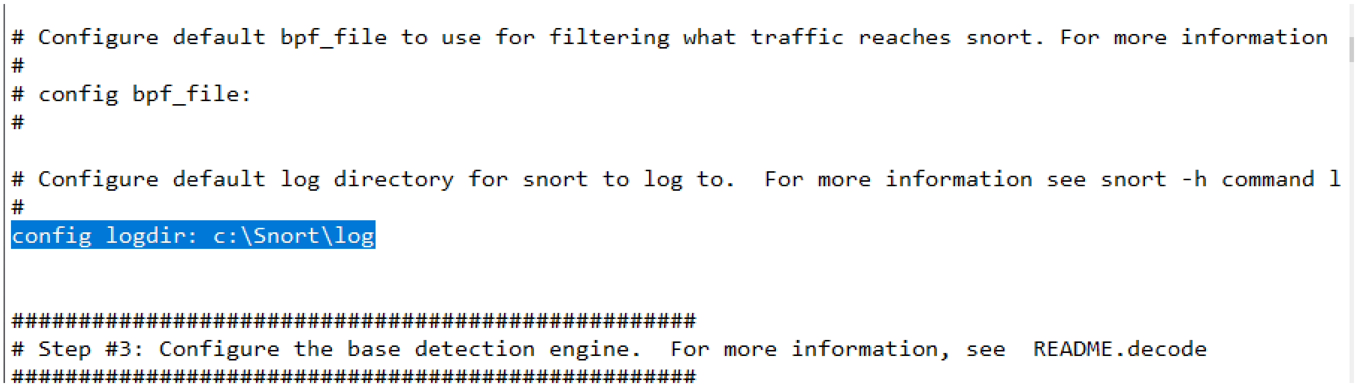
- Do the following changes:



```
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 [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188

# 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
```

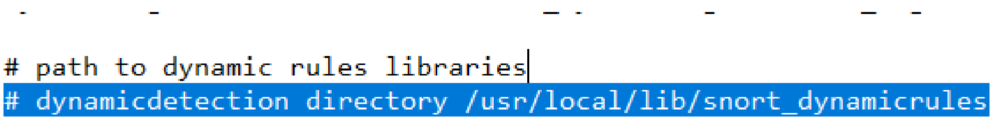


```

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188

# 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

###################################################
# Step #2: Configure the decoder.  For more information, see README.decode
###################################################
```



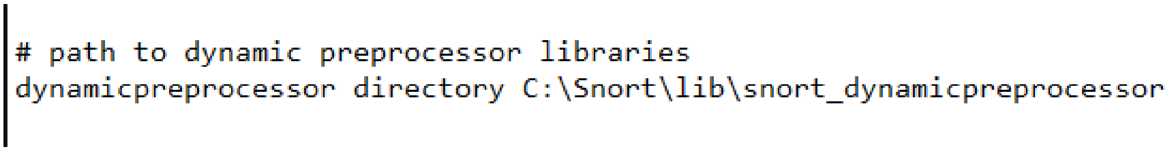
```
# Configure default bpf_file to use for filtering what traffic reaches snort. For more information
#
# config bpf_file:
#

# Configure default log directory for snort to log to.  For more information see snort -h command l
#
config logdir: c:\Snort\log


#####################################################
# Step #3: Configure the base detection engine.  For more information, see  README.decode
#####################################################
```

- We are not gonna use this line so hashtag it



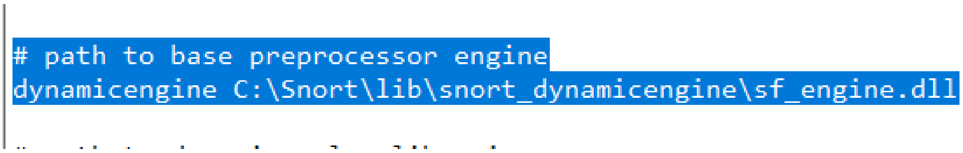
```
# path to dynamic rules libraries
# dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

- Change the path to the path of your device



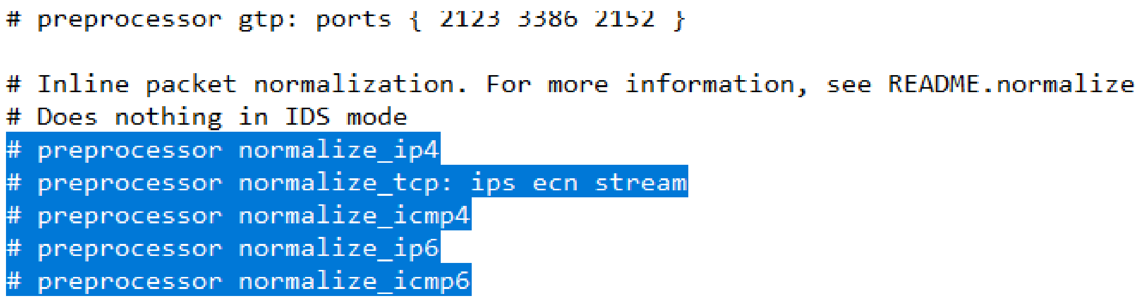
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
```

- Make the following changes

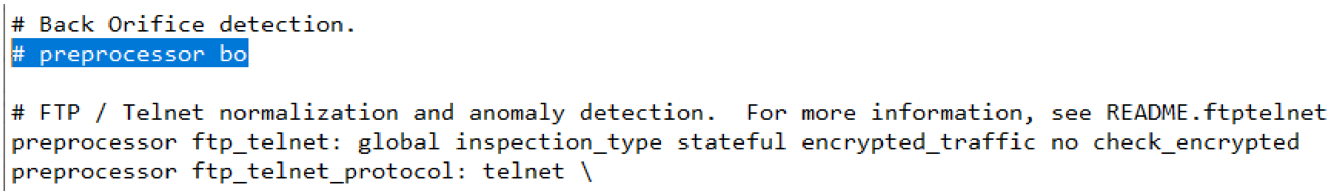


```
# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

- Comment these lines from the file

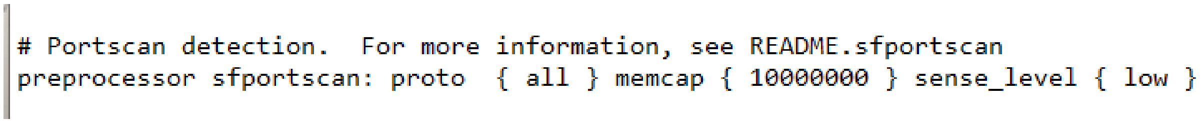


```
# preprocessor gtp: ports { 2123 3386 2152 }

# 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
```



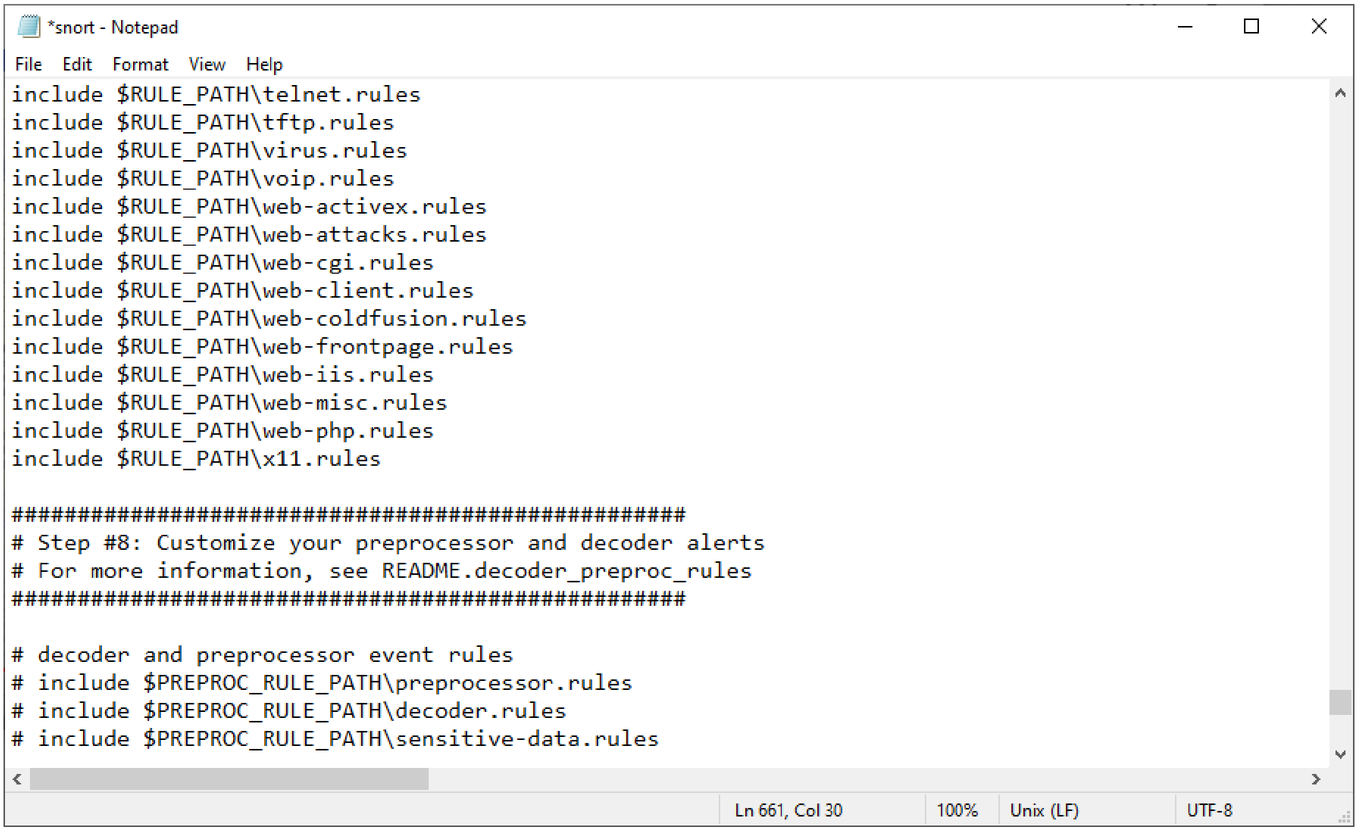
```
# Back Orifice detection.
# preprocessor bo

# FTP / Telnet normalization and anomaly detection.  For more information, see README.ftptelnet
preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no check_encrypted
preprocessor ftp_telnet_protocol: telnet \
```

- We are going to need line 418 so we will comment out



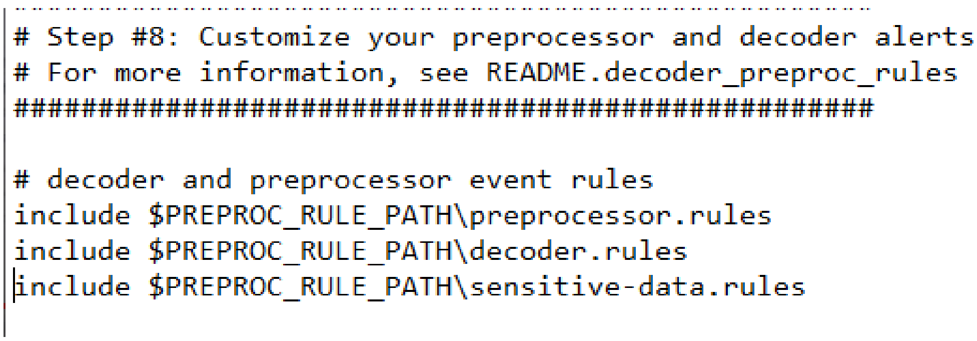
```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

- In step 7 and step 8 of the file
- replace all “/” with “\”



```
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
```

In step 8, comment out those lines since we r going to use them

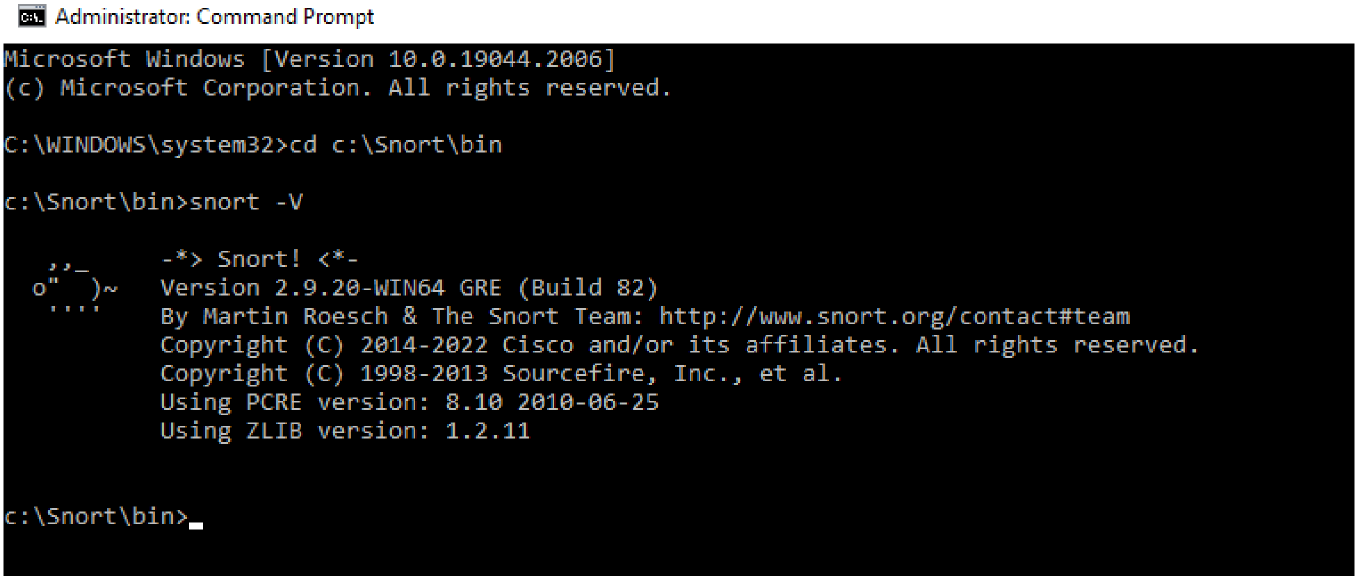


```
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
###################################################

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

- Thus we are done with the configuration.

Testing of snort:-

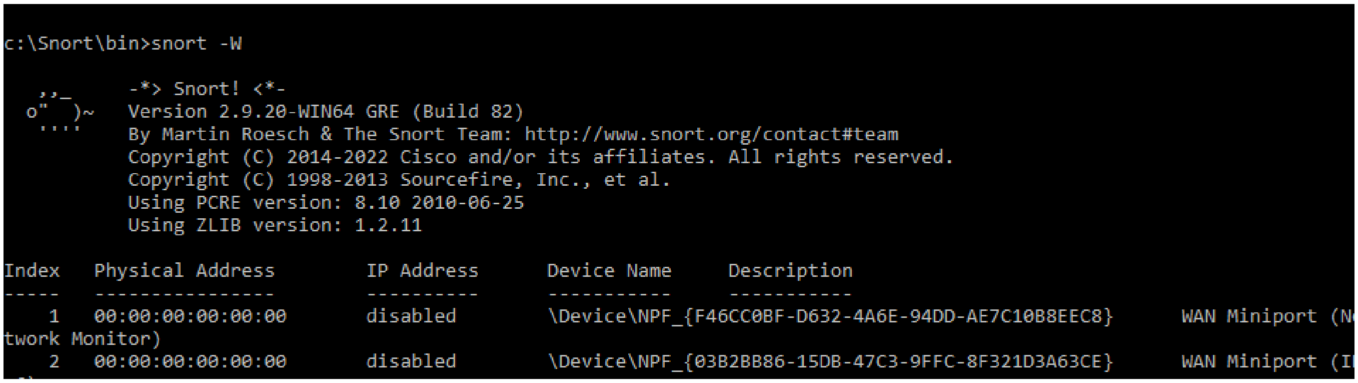
- Change the directory to Snort
- Command to check version: **snort -V**



Administrator: Command Prompt

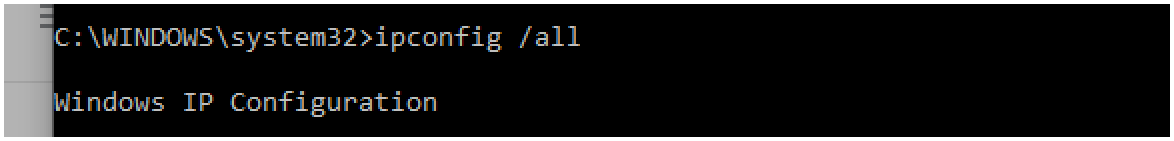
```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd c:\Snort\bin

c:\Snort\bin>snort -V

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


c:\Snort\bin>_
```

- Command to check interfaces present in our device: snort -W



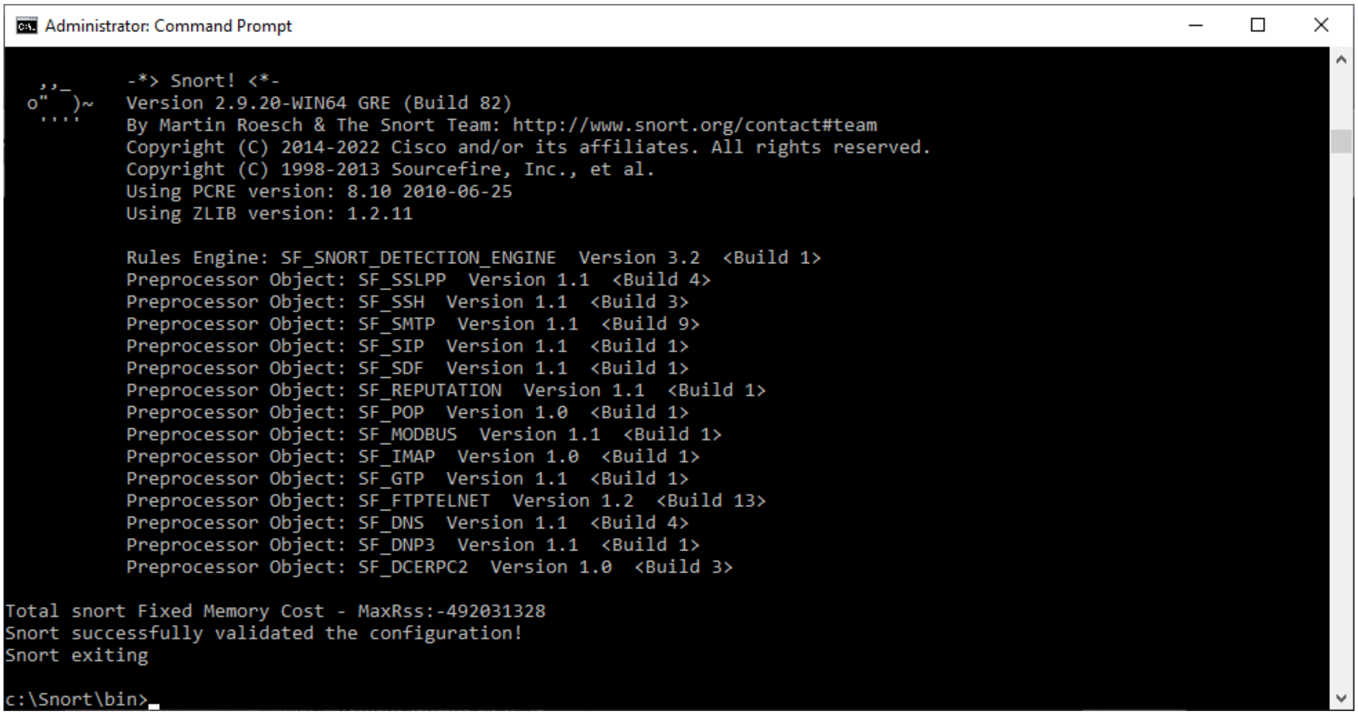
```
c:\Snort\bin>snort -W

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

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{F46CC0BF-D632-4A6E-94DD-AE7C10B8EEC8}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{03B2BB86-15DB-47C3-9FFC-8F321D3A63CE}      WAN Miniport (I
```

- Enter the command “ipconig /all” on new command administrative prompt



```
C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration
```

- compare values in both the command prompts
- Command to check if snort is successully configured: snort -i 1 -c c:\Snort\etc\snort.conf -T



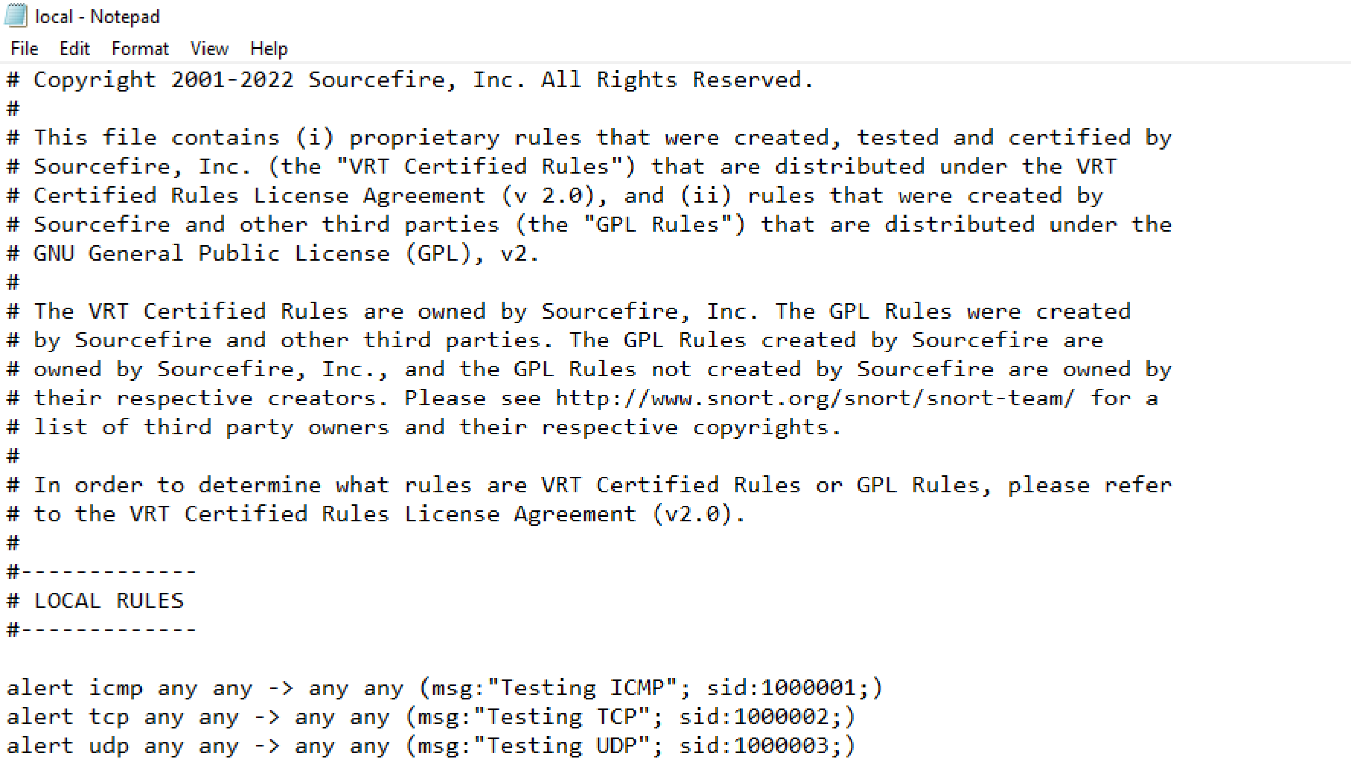
```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           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:-492031328
Snort successfully validated the configuration!
Snort exiting

c:\Snort\bin>_
```

- Go into the “local.rules” file
- add these alerts into it**(Alert Log)**

alert icmp any any -> any any (msg:"Testing ICMP";sid:1000001;)

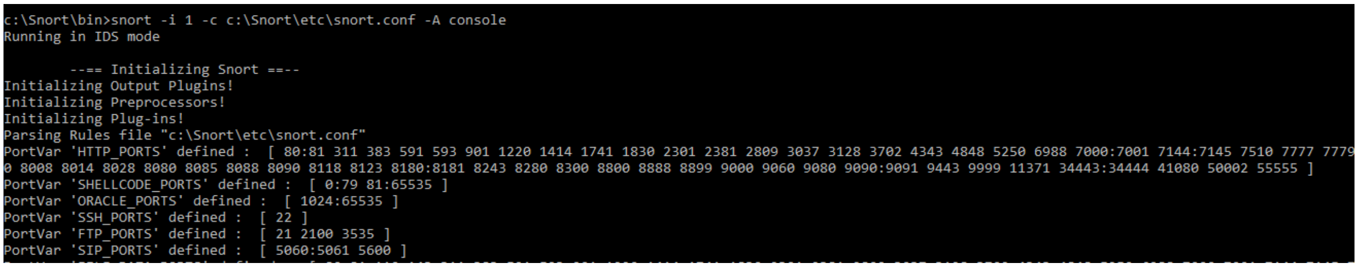
alert tcp any any -> any any (msg:"Testing TCP";sid:1000002;)

alert udp any any -> any any (msg:"Testing UDP";sid:1000003;)

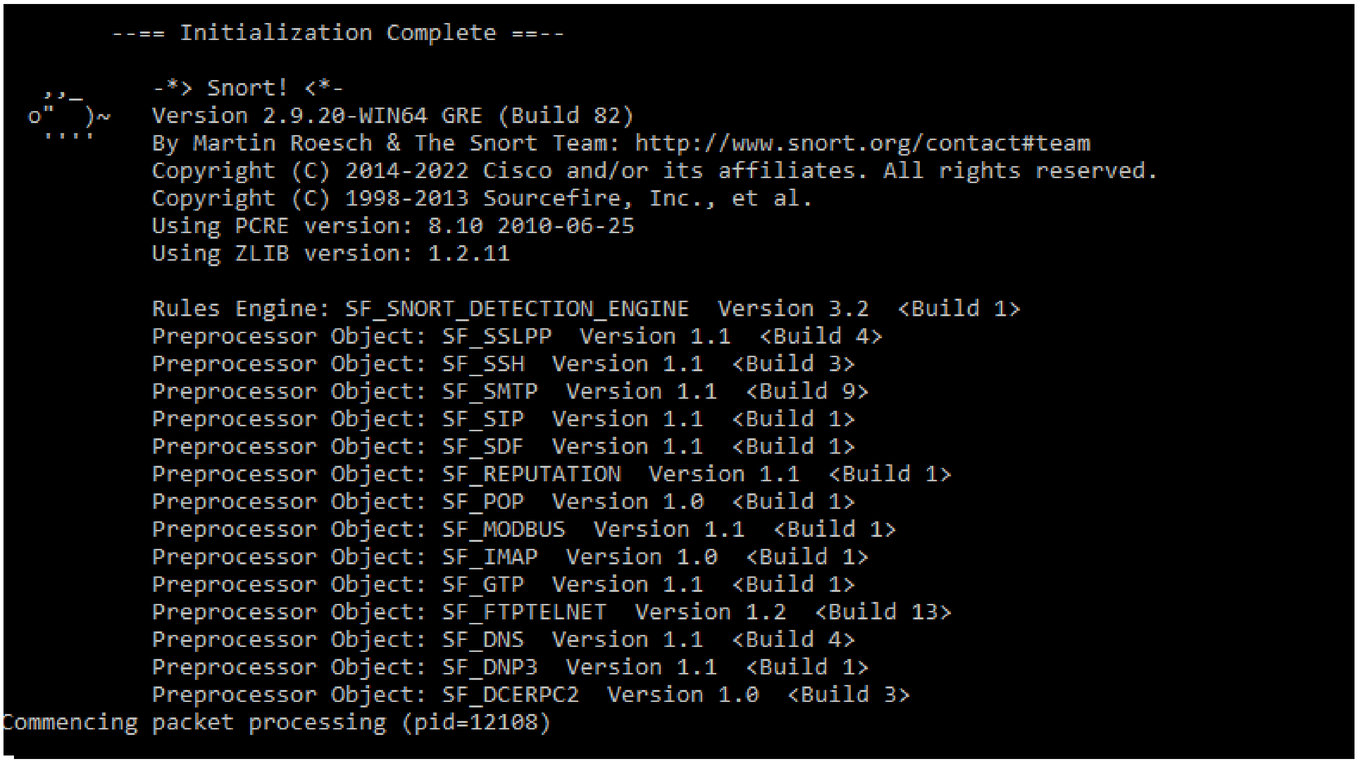


```
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were 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 icmp any any -> any any (msg:"Testing ICMP"; sid:1000001;)
alert tcp any any -> any any (msg:"Testing TCP"; sid:1000002;)
alert udp any any -> any any (msg:"Testing UDP"; sid:1000003;)
```

- Command to do ping test: snort -i 1 -c c:\Snort\etc\snort.conf -A console

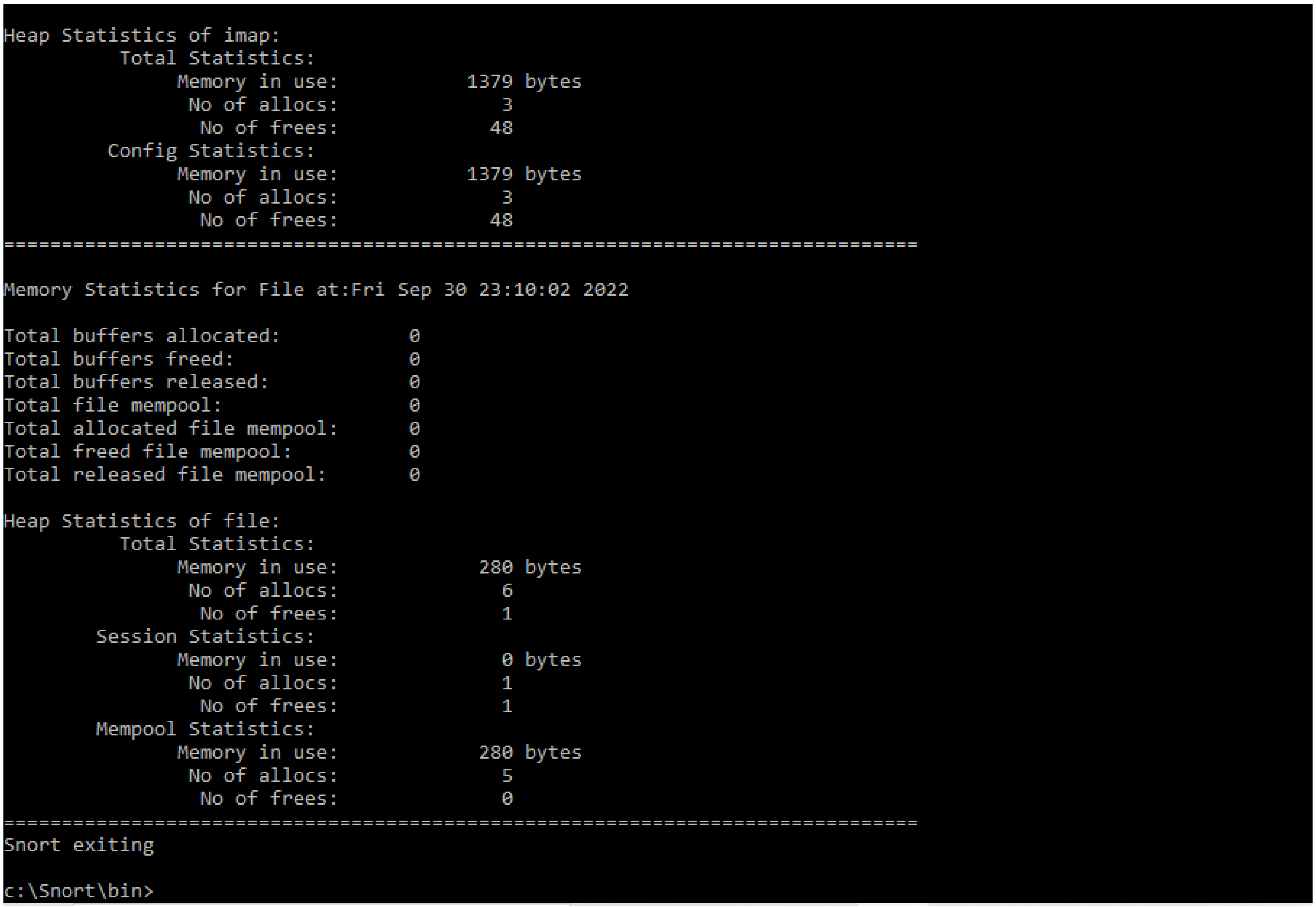


```
c:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf -A console
Running in IDS mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 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
0 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 ]
```



```
        --== 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>
Commencing packet processing (pid=12108)
```

- You will see the packets are being processed.
- Open youtube,or any other site to see the packets
- Enter “ctrl c” to top the packets



```
Heap Statistics of imap:
          Total Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
         Config Statistics:
               Memory in use:           1379 bytes
                No of allocs:              3
                 No of frees:             48
===============================================================================

Memory Statistics for File at:Fri Sep 30 23:10:02 2022

Total buffers allocated:           0
Total buffers freed:               0
Total buffers released:            0
Total file mempool:                0
Total allocated file mempool:      0
Total freed file mempool:          0
Total released file mempool:       0

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

c:\Snort\bin>
```

CONCLUSION: Thus We have successfully set up snort and studied the logs.