NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

LAB 12

LAB 12: Study of Network security : Set up Snort and study the logs.

ROLL NO	52
NAME	Sarvesh Patil
CLASS	D15A
SUBJECT	Internet Security Lab
LO MAPPED	LO6: Demonstrate the network security system using open source tools.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

AIM:

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

INTRODUCTION:

SNORT :

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.

SNORT is a free-to-use open-source piece of software that can be deployed by individuals and organizations. The SNORT rule language determines which network traffic should be collected and what should happen when it detects malicious packets. This snorting meaning can be used in the same way as sniffers and network intrusion detection systems to discover malicious packets or as a full network IPS solution that monitors network activity and detects and blocks potential attack vectors.

Features :

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

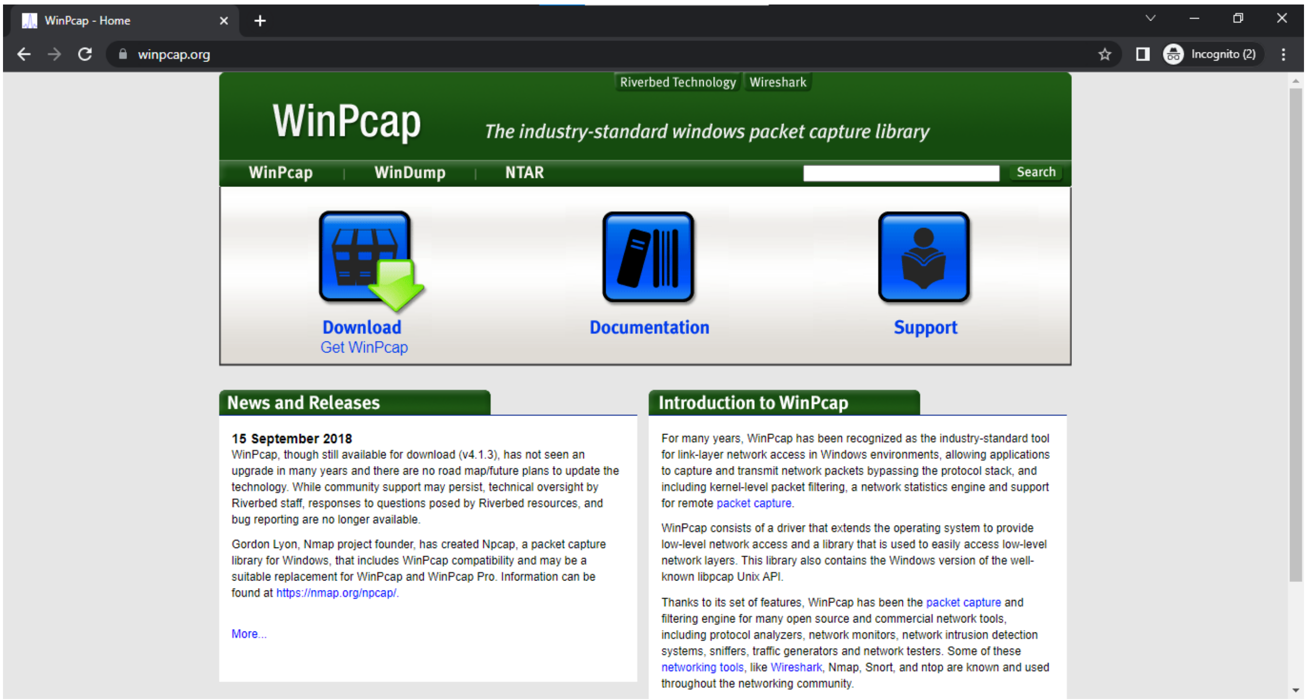
6. Can Be Installed in Any Network Environment : SNORT can be deployed on all operating systems, including Linux and Windows, and as part of all network environments.

7. 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.

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

RESULTS :

1. Get the WinPcap installer by browsing to http://www.winpcap.org and clicking on the link for the Version 4.1.3 installer for Windows.



News and Releases

15 September 2018
WinPcap, though still available for download (v4.1.3), has not seen an upgrade in many years and there are no road map/future plans to update the technology. While community support may persist, technical oversight by Riverbed staff, responses to questions posed by Riverbed resources, and bug reporting are no longer available.

Gordon Lyon, Nmap project founder, has created Npcap, a packet capture library for Windows, that includes WinPcap compatibility and may be a suitable replacement for WinPcap and WinPcap Pro. Information can be found at https://nmap.org/npcap/.

More...

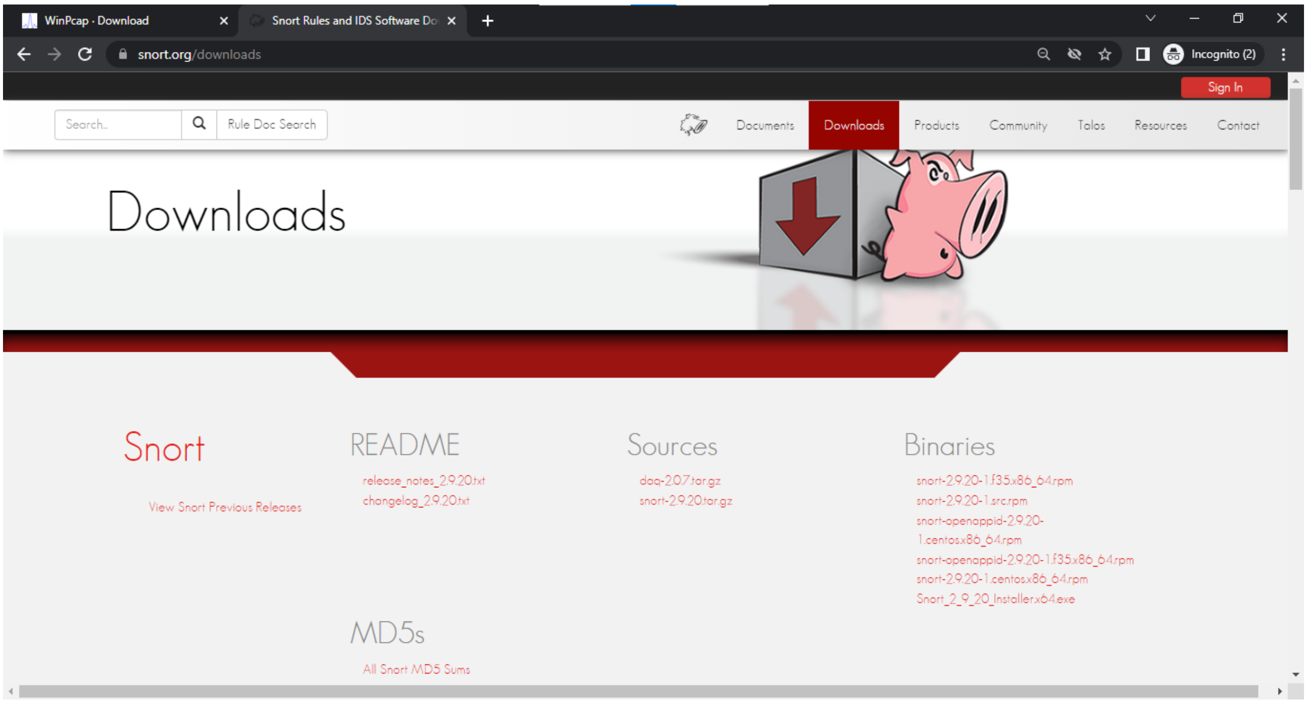
Introduction to WinPcap

For many years, WinPcap has been recognized as the industry-standard tool for link-layer network access in Windows environments, allowing applications to capture and transmit network packets bypassing the protocol stack, and including kernel-level packet filtering, a network statistics engine and support for remote packet capture.

WinPcap consists of a driver that extends the operating system to provide low-level network access and a library that is used to easily access low-level network layers. This library also contains the Windows version of the well-known libpcap Unix API.

Thanks to its set of features, WinPcap has been the packet capture and filtering engine for many open source and commercial network tools, including protocol analyzers, network monitors, network intrusion detection systems, sniffers, traffic generators and network testers. Some of these networking tools, like Wireshark, Nmap, Snort, and ntop are known and used throughout the networking community.

2. Get the latest version of Snort by browsing to https://www.snort.org and clicking on the link for the Windows installer.



Downloads

Snort

View Snort Previous Releases

README

release_notes_2.9.20.txt
changelog_2.9.20.txt

Sources

daq-2.0.7.tar.gz
snort-2.9.20.tar.gz

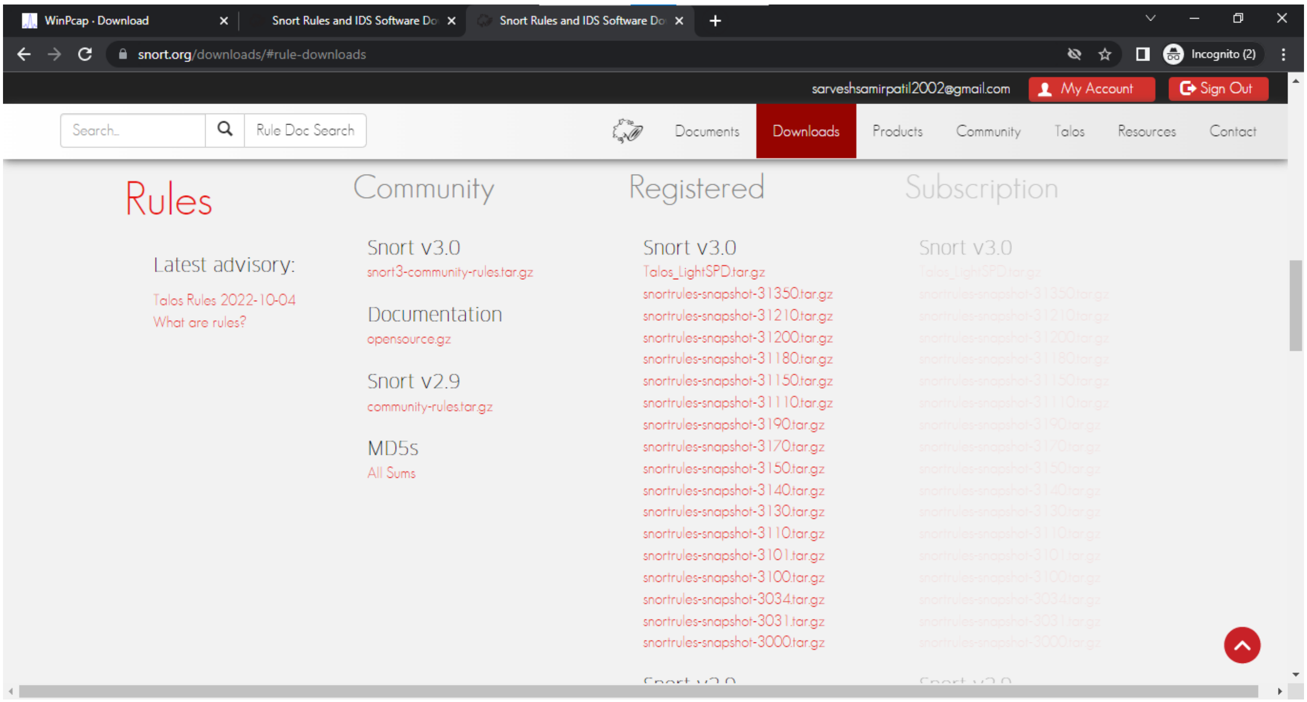
Binaries

snort-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.src.rpm
snort-openappid-2.9.20-1.centos.x86_64.rpm
snort-openappid-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.centos.x86_64.rpm
Snort_2_9_20_Installer.x64.exe

MD5s

All Snort MD5 Sums

3. Get the latest version of the rules by browsing to https://www.snort.org/downloads/#rule-downloads and clicking on the link for the current Registered User release.



snort.org/downloads/#rule-downloads

sarveshsamirpatil2002@gmail.com

Rules

Latest advisory:
Talos Rules 2022-10-04
What are rules?

Community

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

Documentation
opensource.gz

Snort v2.9
community-rules.tar.gz

MD5s
All Sums

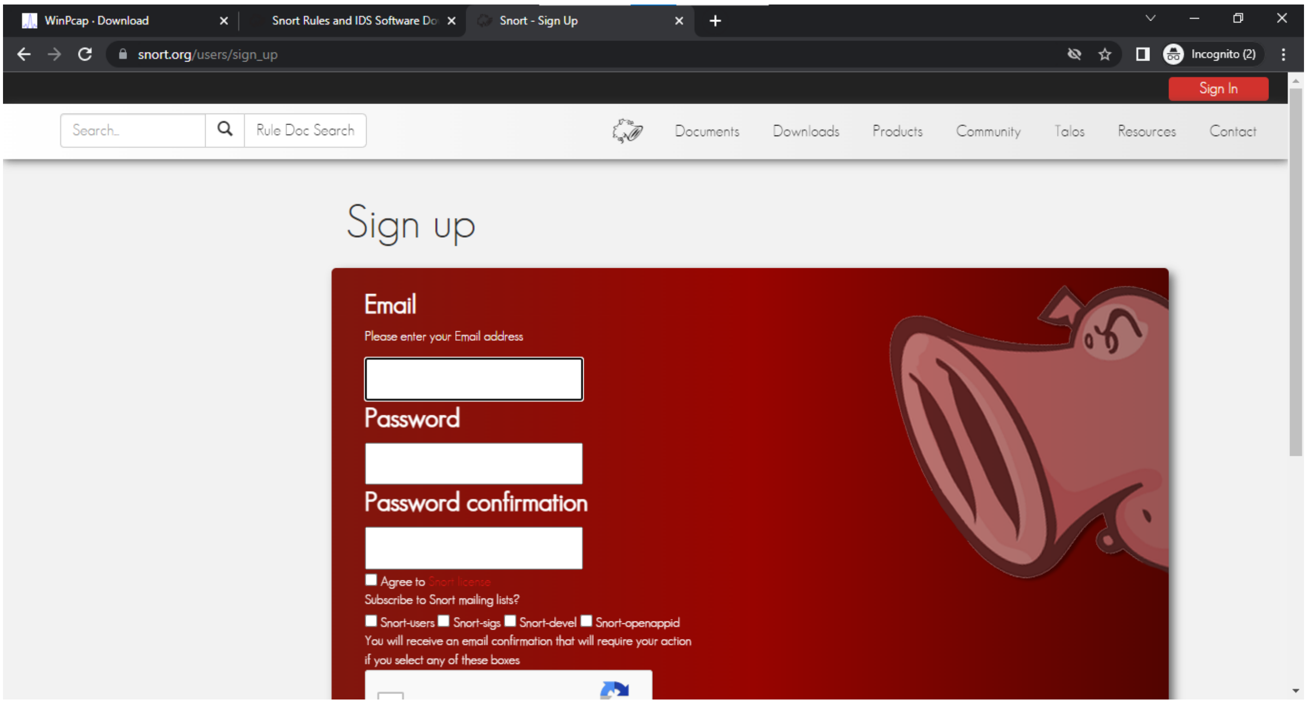
Registered

Snort v3.0
Talos_LightSPD.tar.gz
snortrules-snapshot-31350.tar.gz
snortrules-snapshot-31210.tar.gz
snortrules-snapshot-31200.tar.gz
snortrules-snapshot-31180.tar.gz
snortrules-snapshot-31150.tar.gz
snortrules-snapshot-31110.tar.gz
snortrules-snapshot-3190.tar.gz
snortrules-snapshot-3170.tar.gz
snortrules-snapshot-3150.tar.gz
snortrules-snapshot-3140.tar.gz
snortrules-snapshot-3130.tar.gz
snortrules-snapshot-3110.tar.gz
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

Subscription

Snort v3.0
Talos_LightSPD.tar.gz
snortrules-snapshot-31350.tar.gz
snortrules-snapshot-31210.tar.gz
snortrules-snapshot-31200.tar.gz
snortrules-snapshot-31180.tar.gz
snortrules-snapshot-31150.tar.gz
snortrules-snapshot-31110.tar.gz
snortrules-snapshot-3190.tar.gz
snortrules-snapshot-3170.tar.gz
snortrules-snapshot-3150.tar.gz
snortrules-snapshot-3140.tar.gz
snortrules-snapshot-3130.tar.gz
snortrules-snapshot-3110.tar.gz
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

Note that you must create an account (which is free) and log in to Snort.org in order to download the "registered" rules file or purchase an annual subscription to download the "subscriber” rules file.



snort.org/users/sign_up

Sign up

Email
Please enter your Email address

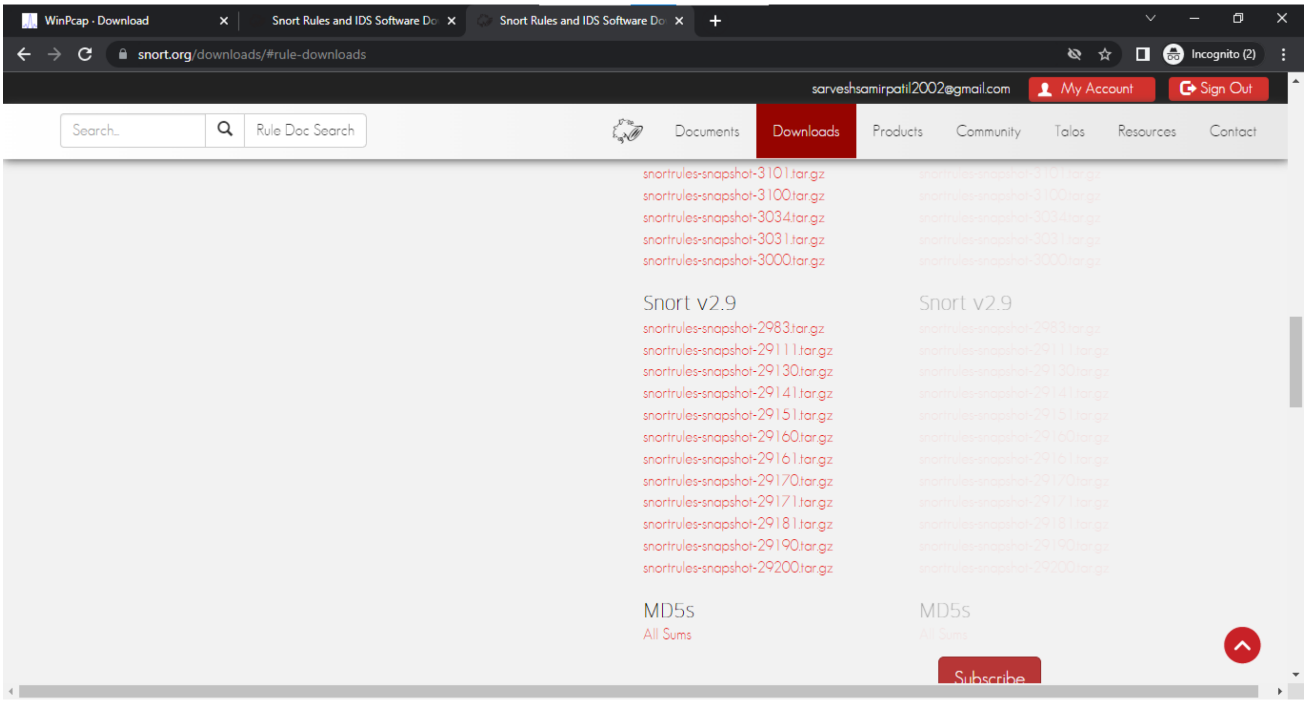
Password

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

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52

Select the rules of the same version of which you downloaded Snort.



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

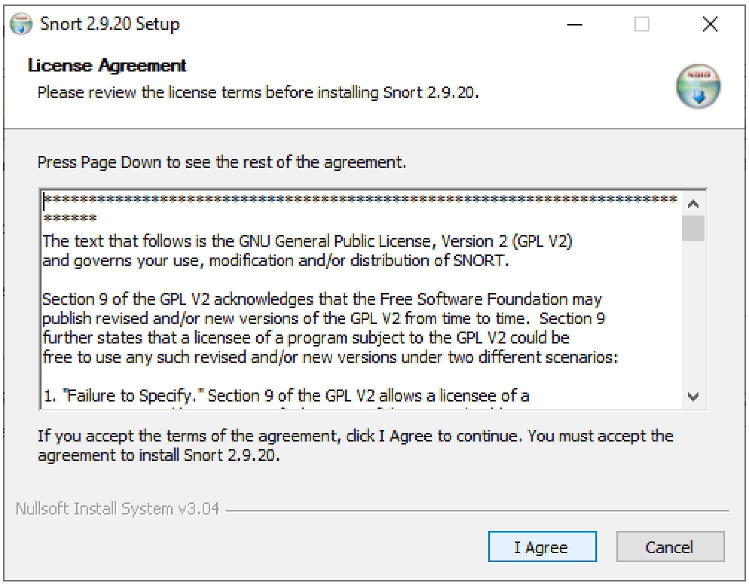
snortrules-snapshot-2983.tar.gz
snortrules-snapshot-29111.tar.gz
snortrules-snapshot-29130.tar.gz
snortrules-snapshot-29141.tar.gz
snortrules-snapshot-29151.tar.gz
snortrules-snapshot-29160.tar.gz
snortrules-snapshot-29161.tar.gz
snortrules-snapshot-29170.tar.gz
snortrules-snapshot-29171.tar.gz
snortrules-snapshot-29181.tar.gz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

MD5s
All Sums

Snort v2.9

MD5s
All Sums

4. Now install the programs (in the case of WinPcap and Snort) and extract the rules files in the case of the Snort rules package) :
   a) Double-click the WinPcap_4_1_3.exe installer file and follow the on-screen prompts. Typically no customization or configuration is required for this install, although on many systems a restart may be required to make sure the WinPcap netgroup packet filter (NPF) driver is running.
   b) Double-click the Snort_2_9_18_1_Installer.exe file and follow the on-screen prompts :
      I. Accept the license agreement.
      II. Choose the components (Snort, dynamic modules, documentation) you want to install. All are selected by default.



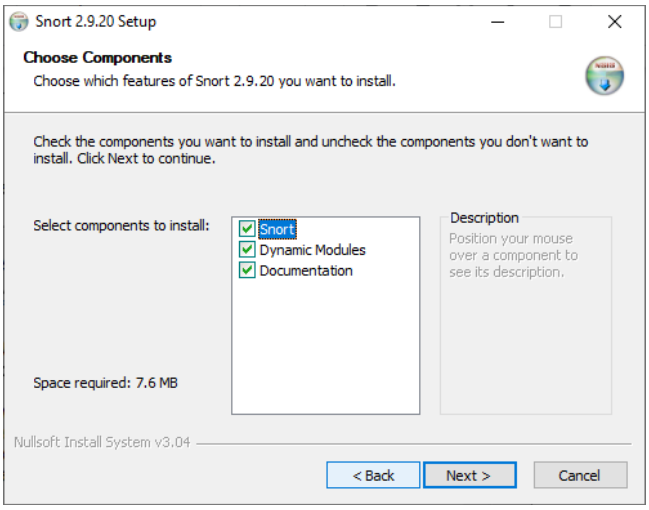
License Agreement

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

Choose Components

Choose which features of Snort 2.9.20 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

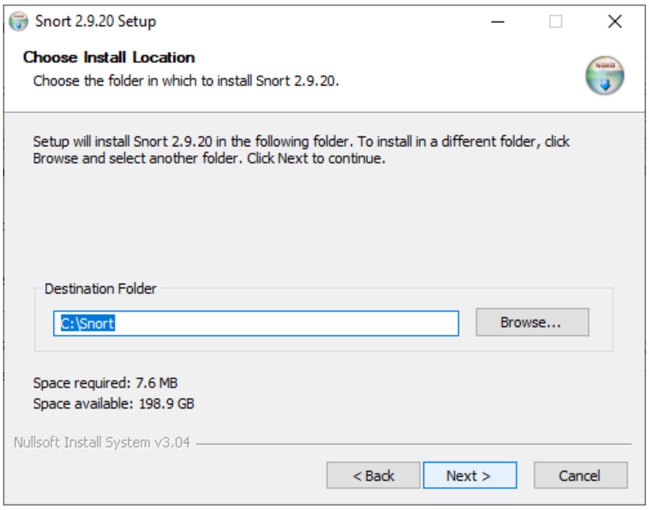
Description

Position your mouse over a component to see its description.

Space required: 7.6 MB

Nullsoft Install System v3.04

III. By default the installer creates a root directory for Snort at c:\Snort, although you can specify a different directory if desired. When you select "Next" the installation executes.



Snort 2.9.20 Setup

Choose Install Location

Choose the folder in which to install Snort 2.9.20.

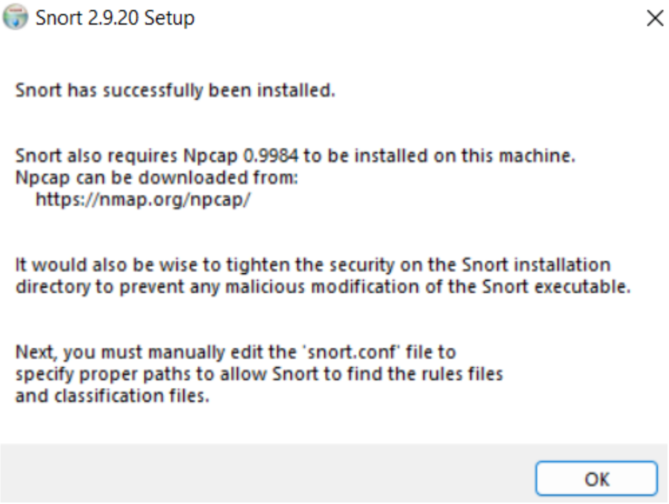
Setup will install Snort 2.9.20 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Snort

Space required: 7.6 MB
Space available: 198.9 GB

Nullsoft Install System v3.04

IV. At the end of the installation, the program displays a message that Snort has successfully been installed. The message includes a note that WinPcap is required (it refers to 4.1.1 although 4.1.3 is the current version), recommends tightening security on Snort, and directs you to edit the snort.conf file.



Snort 2.9.20 Setup

Snort has successfully been installed.

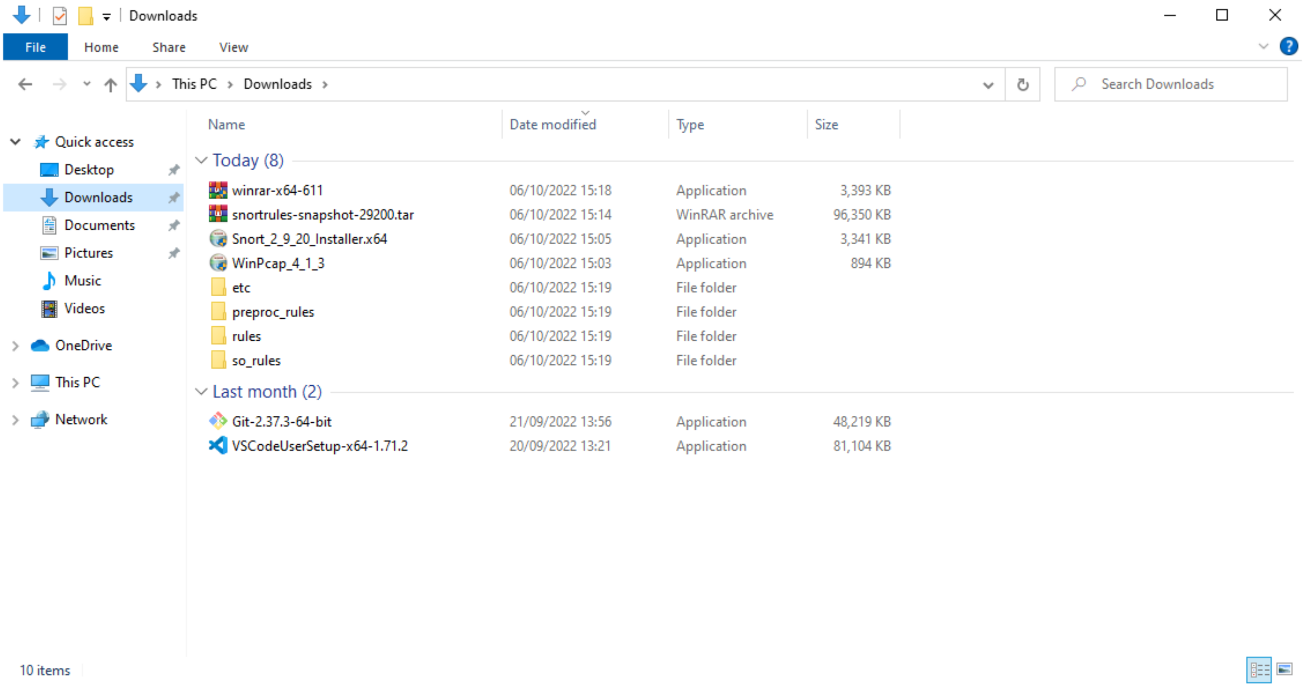
Snort also requires Npcap 0.9984 to be installed on this machine.
Npcap can be downloaded from:
https://nmap.org/npcap/

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.

5. Open the Snort rules package. Depending on your operating system, Windows may be able to open the zipped archive automatically, or you can use a utility such as WinZip, 7Zip, or WinRAR to open it.

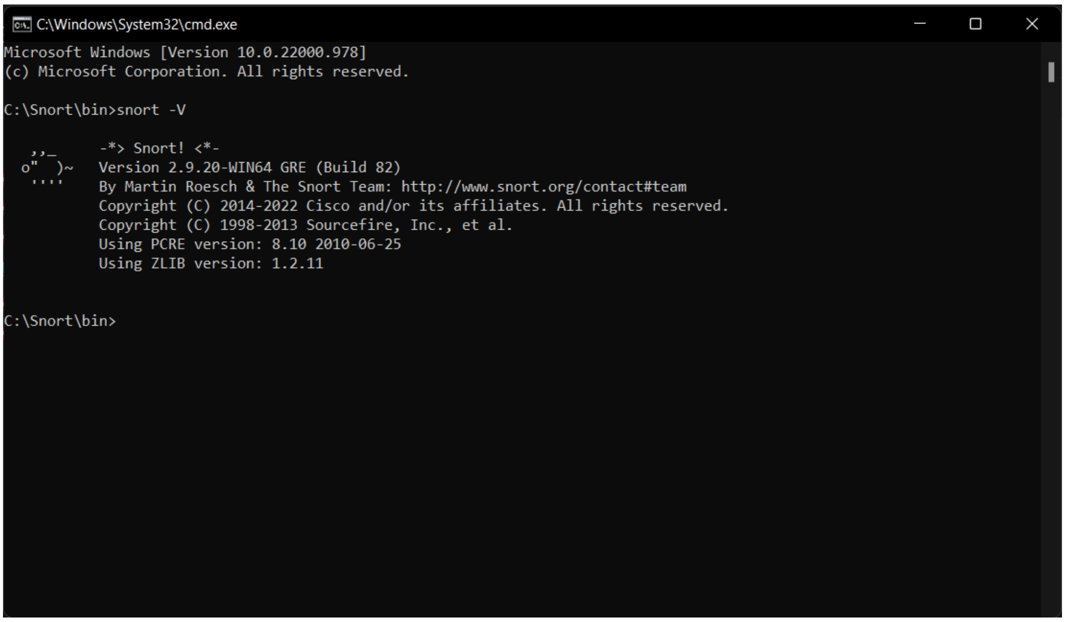
1) Create a subfolder under c:\Snort called rules, and another called preproc_rules.
2) Extract the contents of the rules folder in the archive to c:\Snort rules
3) Extract the contents of the preproc_rules folder in the archive to c:\Snort preproc_rules
4) Ignore the so_rules folder, while Sourcefire offers pre-compiled versions of the shared object rules for many Linux distributions, no such option exists for Windows. Compiling the Snort shared object rules to run on Windows is well beyond the technical scope of this course.
5) Also ignore the contents of the etc folder in the archive.



Name	Date modified	Type	Size
Today (8)			
winrar-x64-611	06/10/2022 15:18	Application	3,393 KB
snortrules-snapshot-29200.tar	06/10/2022 15:14	WinRAR archive	96,350 KB
Snort_2_9_20_Installer.x64	06/10/2022 15:05	Application	3,341 KB
WinPcap_4_1_3	06/10/2022 15:03	Application	894 KB
etc	06/10/2022 15:19	File folder	
preproc_rules	06/10/2022 15:19	File folder	
rules	06/10/2022 15:19	File folder	
so_rules	06/10/2022 15:19	File folder	
Last month (2)			
Git-2.37.3-64-bit	21/09/2022 13:56	Application	48,219 KB
VSCodeUserSetup-x64-1.71.2	20/09/2022 13:21	Application	81,104 KB

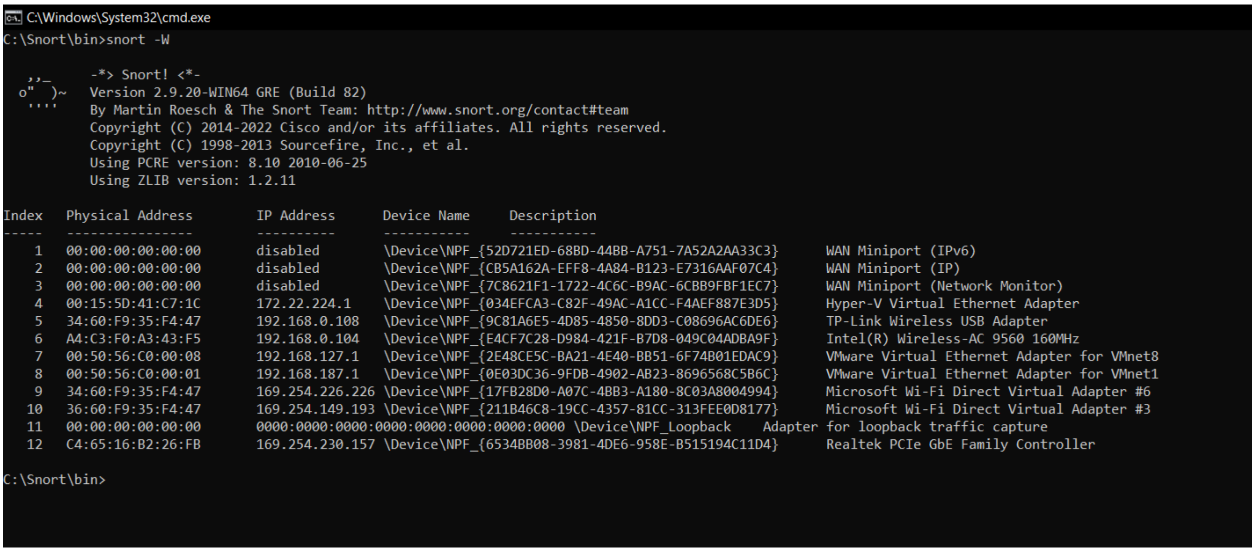
Once you have completed installing these components, you can check to see if the program responds:

a) Check the installed version for Snort: **C:\Snort\bin/snort -V**



```
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

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>
```

b) You should also check to see what network adapters are on your system, so you can tell Snort to listen on the appropriate interface when it runs. To see a list of interfaces, run the command: **C:\Snort\bin/snort -W**



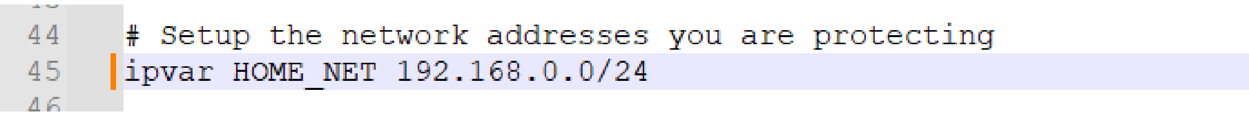
C:\Windows\System32\cmd.exe

```
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_{52D721ED-68BD-44BB-A751-7A52A2AA33C3}      WAN Miniport (IPv6)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{CB5A162A-EFF8-4A84-B123-E7316AAF07C4}      WAN Miniport (IP)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{7C8621F1-1722-4C6C-B9AC-6CBB9FBF1EC7}      WAN Miniport (Network Monitor)
    4   00:15:5D:41:C7:1C       172.22.224.1    \Device\NPF_{034EFCA3-C82F-49AC-A1CC-F4AEF887E3D5}      Hyper-V Virtual Ethernet Adapter
    5   34:60:F9:35:F4:47       192.168.0.108   \Device\NPF_{9C81A6E5-4D85-4850-8DD3-C08696AC6DE6}      TP-Link Wireless USB Adapter
    6   A4:C3:F0:A3:43:F5       192.168.0.104   \Device\NPF_{E4CF7C28-D984-421F-B7D8-049C04ADBA9F}      Intel(R) Wireless-AC 9560 160MHz
    7   00:50:56:C0:00:08       192.168.127.1   \Device\NPF_{2E48CE5C-BA21-4E40-BB51-6F74B01EDAC9}      VMware Virtual Ethernet Adapter for VMnet8
    8   00:50:56:C0:00:01       192.168.187.1   \Device\NPF_{0E03DC36-9FDB-4902-AB23-8696568C5B6C}      VMware Virtual Ethernet Adapter for VMnet1
    9   34:60:F9:35:F4:47       169.254.226.226 \Device\NPF_{17FB28D0-A07C-4BB3-A180-8C03A8004994}      Microsoft Wi-Fi Direct Virtual Adapter #6
   10   36:60:F9:35:F4:47       169.254.149.193 \Device\NPF_{211B46C8-19CC-4357-81CC-313FEE0D8177}      Microsoft Wi-Fi Direct Virtual Adapter #3
   11   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
   12   C4:65:16:B2:26:FB       169.254.230.157 \Device\NPF_{6534BB08-3981-4DE6-958E-B515194C11D4}      Realtek PCIe GbE Family Controller

C:\Snort\bin>
```

The next thing to do is to edit the snort.conf file to make it reflect the environment where your computer is running. You should make sure that when you edit the file, you are working on the one in c:\Snort\etc.

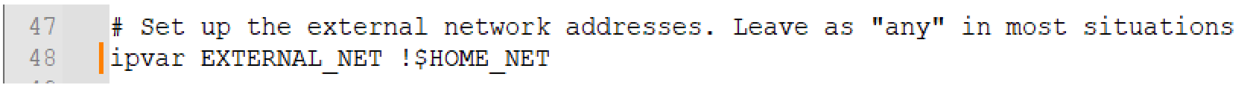
Now open the snort.conf file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.

1. Setup the network addresses you are protecting
   Note: Mention your own host IP addresses that you want to protect.



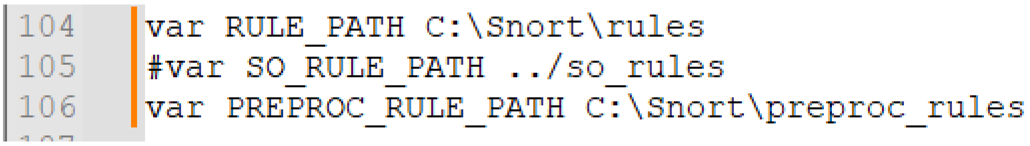
```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.0/24
```

2. Setup the external network into anything that is not the home network. That is why ! is used in the command it denotes ‘not’.



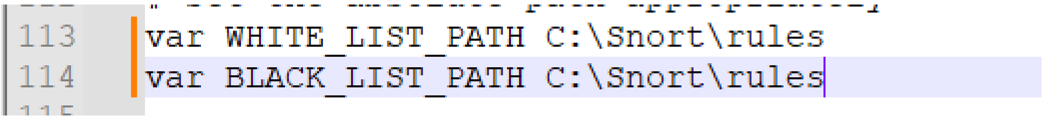
```
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
```

3. Now we have to define the directory for our rules and preproc rules folder.



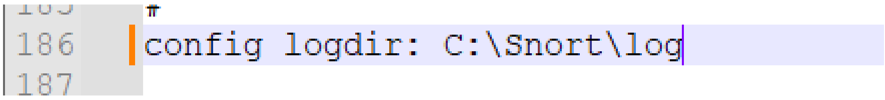
```
var RULE_PATH C:\Snort\rules
#var SO_RULE_PATH ../so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules
```

4. Now we have to set up our white list and black list path. It will be in our snorts' rule folder.



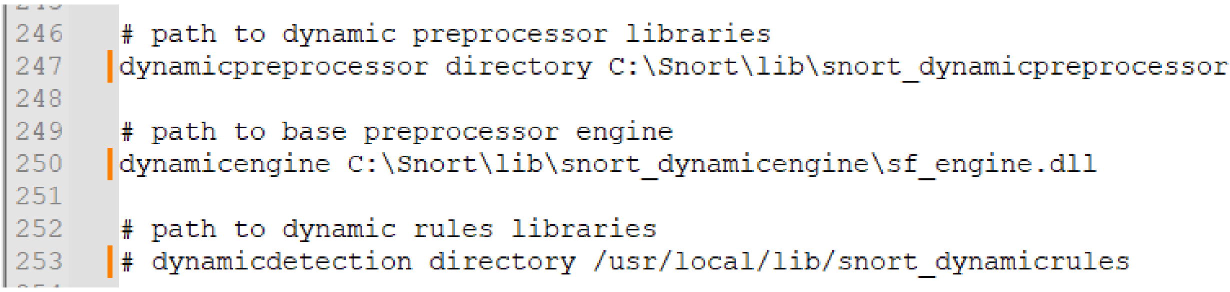
```
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

5. Next we have to enable the log directory, so that we store logs in our log folder. Uncomment this line.



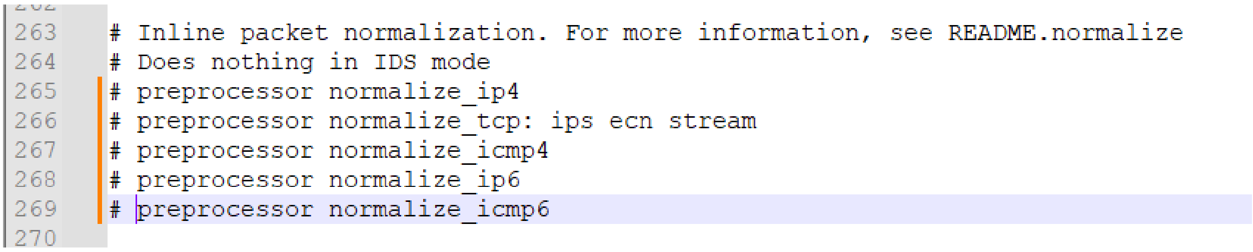
```
config logdir: C:\Snort\log
```

6. Now we will set the path to dynamic preprocessors and dynamic engine. Comment out the dynamic detection path.



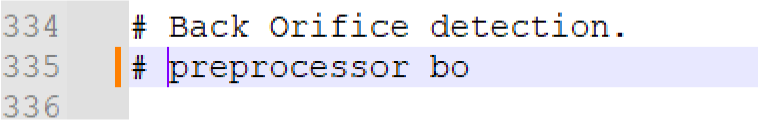
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# 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
```

7. Just comment out these lines. In doing so we are excluding packet normalization of different packets.



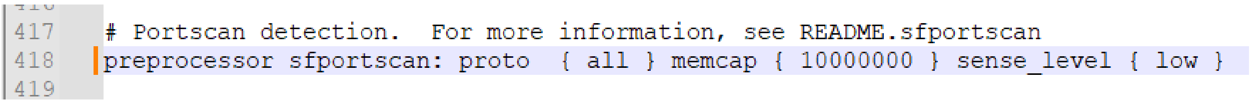
```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```

8. Comment out this line.



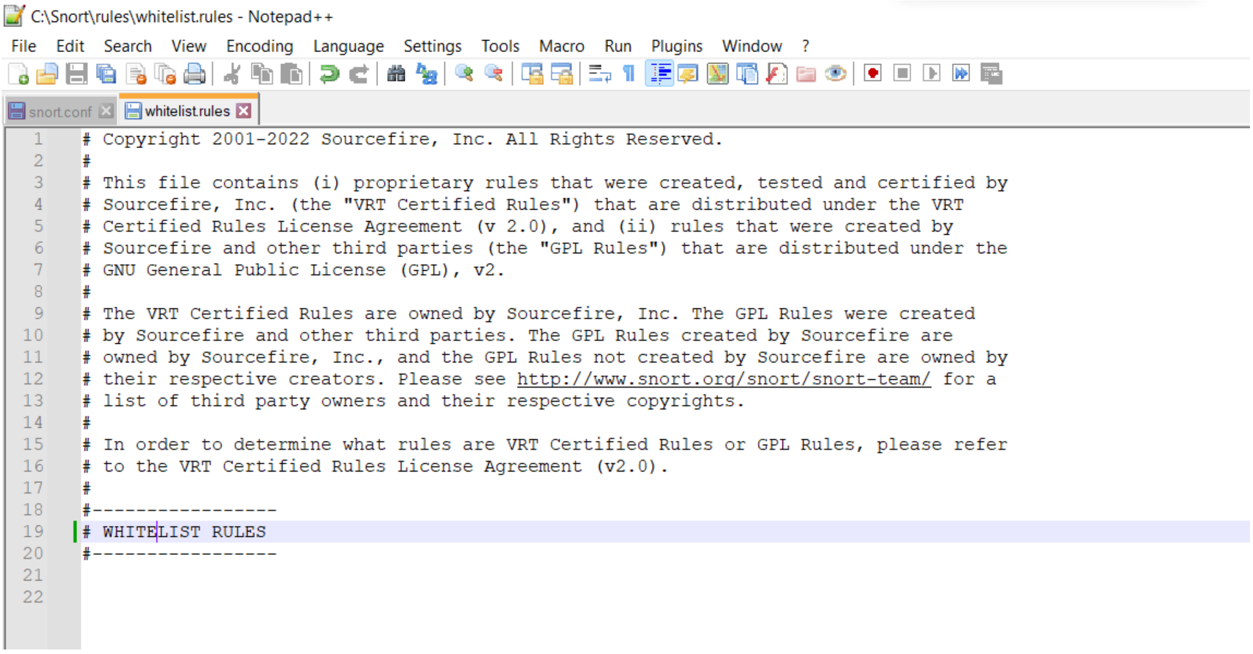
```
# Back Orifice detection.
# preprocessor bo
```

9. Uncomment the following line :



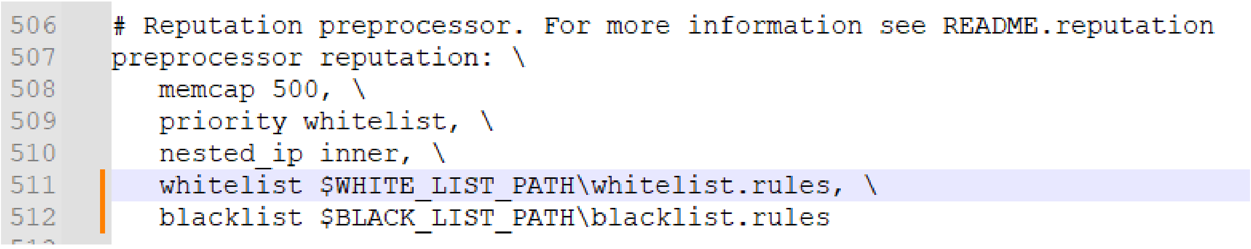
```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

10. Create a whitelist.rules file in the same folder.


C:\Snort\rules\whitelist.rules - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
whitelist.rules

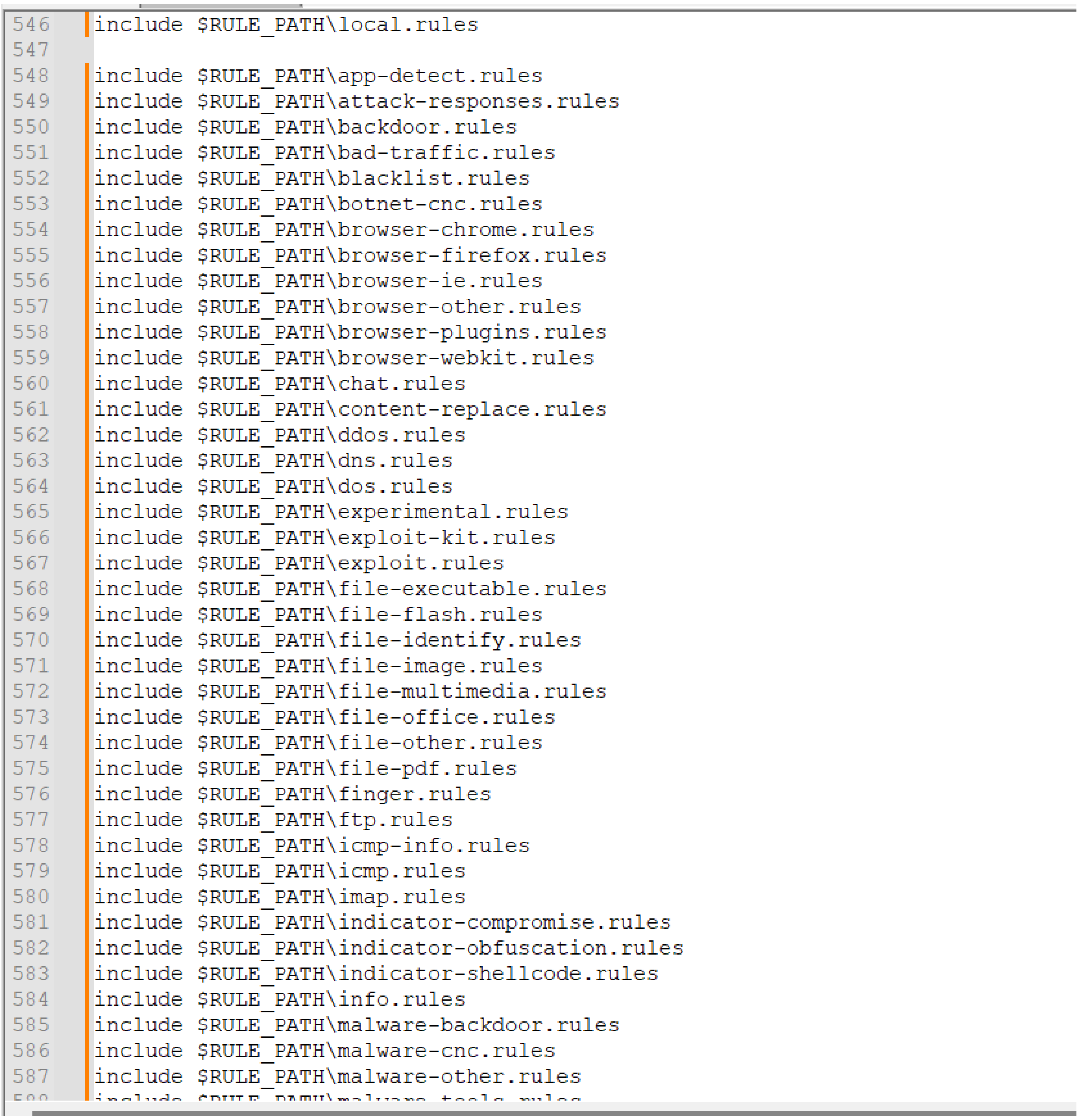
```
# Copyright 2001-2022 Sourcefire, Inc. All Rights Reserved.
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were 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).
#
#-----------------
# WHITELIST RULES
#-----------------
```

11. Scroll down to the reputation preprocessors. We will just change the name of the black list file and the white list file.



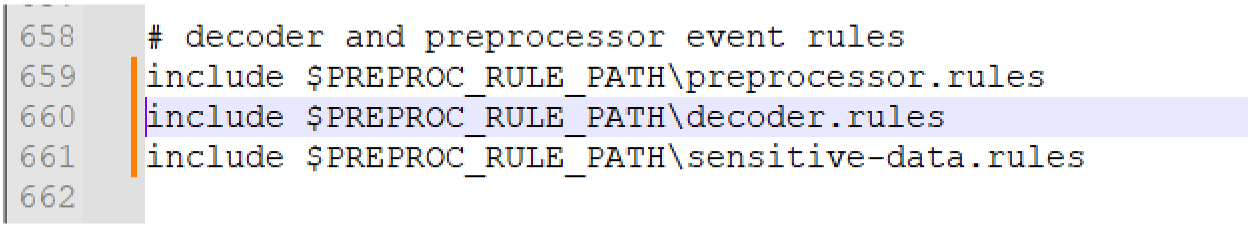
```
 # Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\whitelist.rules, \
   blacklist $BLACK_LIST_PATH\blacklist.rules
```

12. Convert the backslashes to forward slashes in lines till Step 8 mentioned in this file.



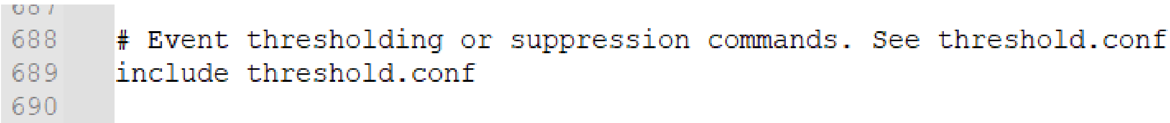
```
include $RULE_PATH\local.rules

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
include $RULE_PATH\file-other.rules
include $RULE_PATH\file-pdf.rules
include $RULE_PATH\finger.rules
include $RULE_PATH\ftp.rules
include $RULE_PATH\icmp-info.rules
include $RULE_PATH\icmp.rules
include $RULE_PATH\imap.rules
include $RULE_PATH\indicator-compromise.rules
include $RULE_PATH\indicator-obfuscation.rules
include $RULE_PATH\indicator-shellcode.rules
include $RULE_PATH\info.rules
include $RULE_PATH\malware-backdoor.rules
include $RULE_PATH\malware-cnc.rules
include $RULE_PATH\malware-other.rules
include $RULE_PATH\malware-tools.rules
```

13. Uncomment the below lines.



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

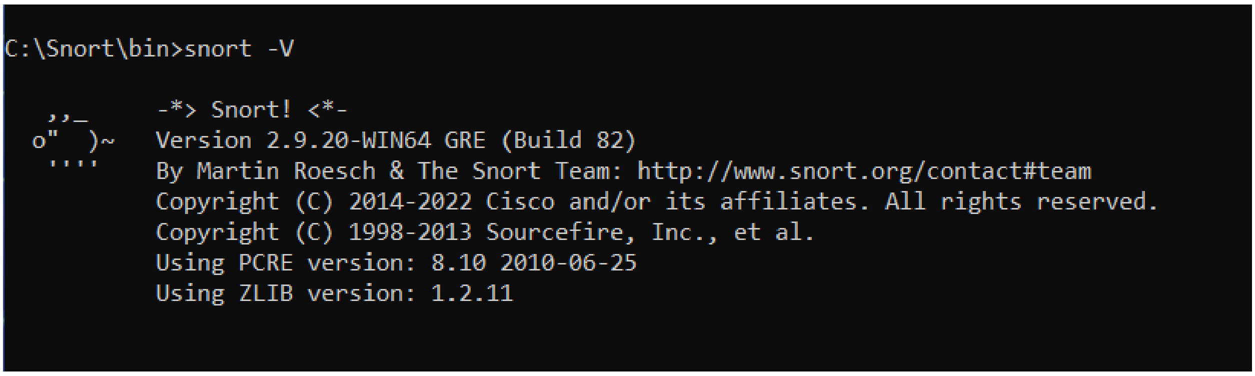
14. Now we just need to verify the presence of this command at the bottom of the snort.conf file.



```
# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
```

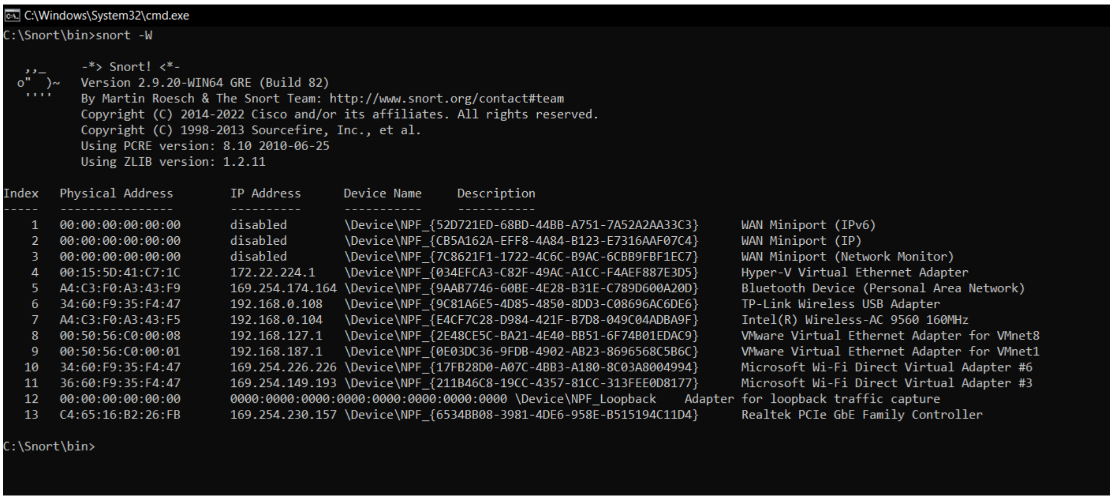
15. Click on Save file and save all changes to save the configuration file (snort.conf).

Now we test snort again by running Command prompt as admin. To check if it's running fine after all the configurations.



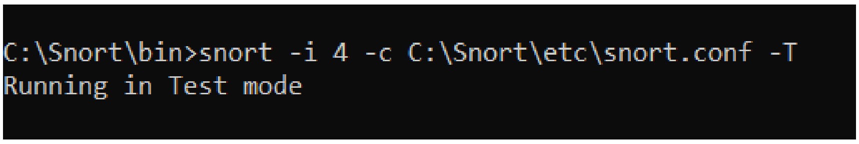
```
C:\Snort\bin>snort -V

   ,,_     -*> 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
```

We can also check the wireless interface cards from which we will be using snort by using the command below. We can see the list of our wireless interface cards through entering this command in the command prompt.

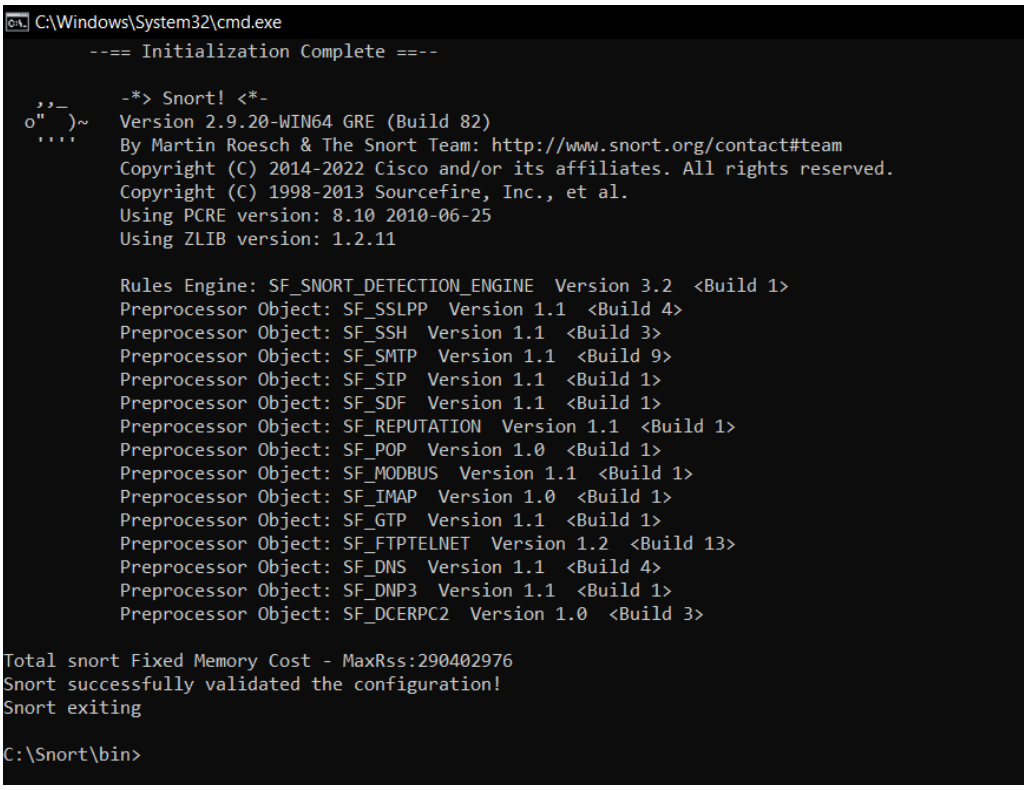


```
C:\Snort\bin>snort -W

   ,,_     -*> 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_{52D721ED-68BD-44BB-A751-7A52A2AA33C3}      WAN Miniport (IPv6)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{CB5A162A-EFF8-4A84-B123-E7316AAF07C4}      WAN Miniport (IP)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{7C8621F1-1722-4C6C-B9AC-6CBB9FBF1EC7}      WAN Miniport (Network Monitor)
    4   00:15:5D:41:C7:1C       172.22.224.1    \Device\NPF_{034EFCA3-C82F-49AC-A1CC-F4AEF887E3D5}      Hyper-V Virtual Ethernet Adapter
    5   A4:C3:F0:A3:43:F9       169.254.174.164 \Device\NPF_{9AAB7746-60BE-4E28-B31E-C789D600A20D}      Bluetooth Device (Personal Area Network)
    6   34:60:F9:35:F4:47       192.168.0.108   \Device\NPF_{9C81A6E5-4D85-4850-8DD3-C08696AC6DE6}      TP-Link Wireless USB Adapter
    7   A4:C3:F0:A3:43:F5       192.168.0.104   \Device\NPF_{E4CF7C28-D984-421F-B7D8-049C04ADBA9F}      Intel(R) Wireless-AC 9560 160MHz
    8   00:50:56:C0:00:08       192.168.127.1   \Device\NPF_{2E48CE5C-BA21-4E40-BB51-6F74B01EDAC9}      VMware Virtual Ethernet Adapter for VMnet8
    9   00:50:56:C0:00:01       192.168.187.1   \Device\NPF_{0E03DC36-9FDB-4902-AB23-8696568C5B6C}      VMware Virtual Ethernet Adapter for VMnet1
   10   34:60:F9:35:F4:47       169.254.226.226 \Device\NPF_{17FB28D0-A07C-4BB3-A180-8C03A8004994}      Microsoft Wi-Fi Direct Virtual Adapter #6
   11   36:60:F9:35:F4:47       169.254.149.193 \Device\NPF_{211B46C8-19CC-4357-81CC-313FEE0D8177}      Microsoft Wi-Fi Direct Virtual Adapter #3
   12   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
   13   C4:65:16:B2:26:FB       169.254.230.157 \Device\NPF_{6534BB08-3981-4DE6-958E-B515194C11D4}      Realtek PCIe GbE Family Controller

C:\Snort\bin>
```

Now we will enter a command to check validation of snort's configuration by choosing a specific wireless interface card (4) the rest of the command shows the config file path . The command is:



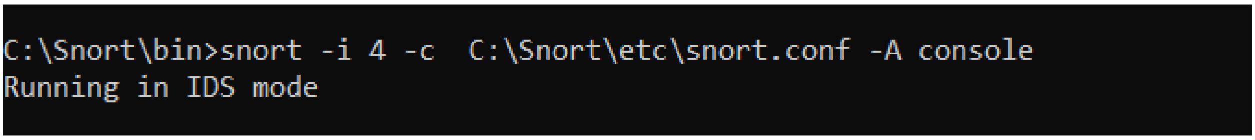
```
C:\Snort\bin>snort -i 4 -c C:\Snort\etc\snort.conf -T
Running in Test mode
```



C:\Windows\System32\cmd.exe

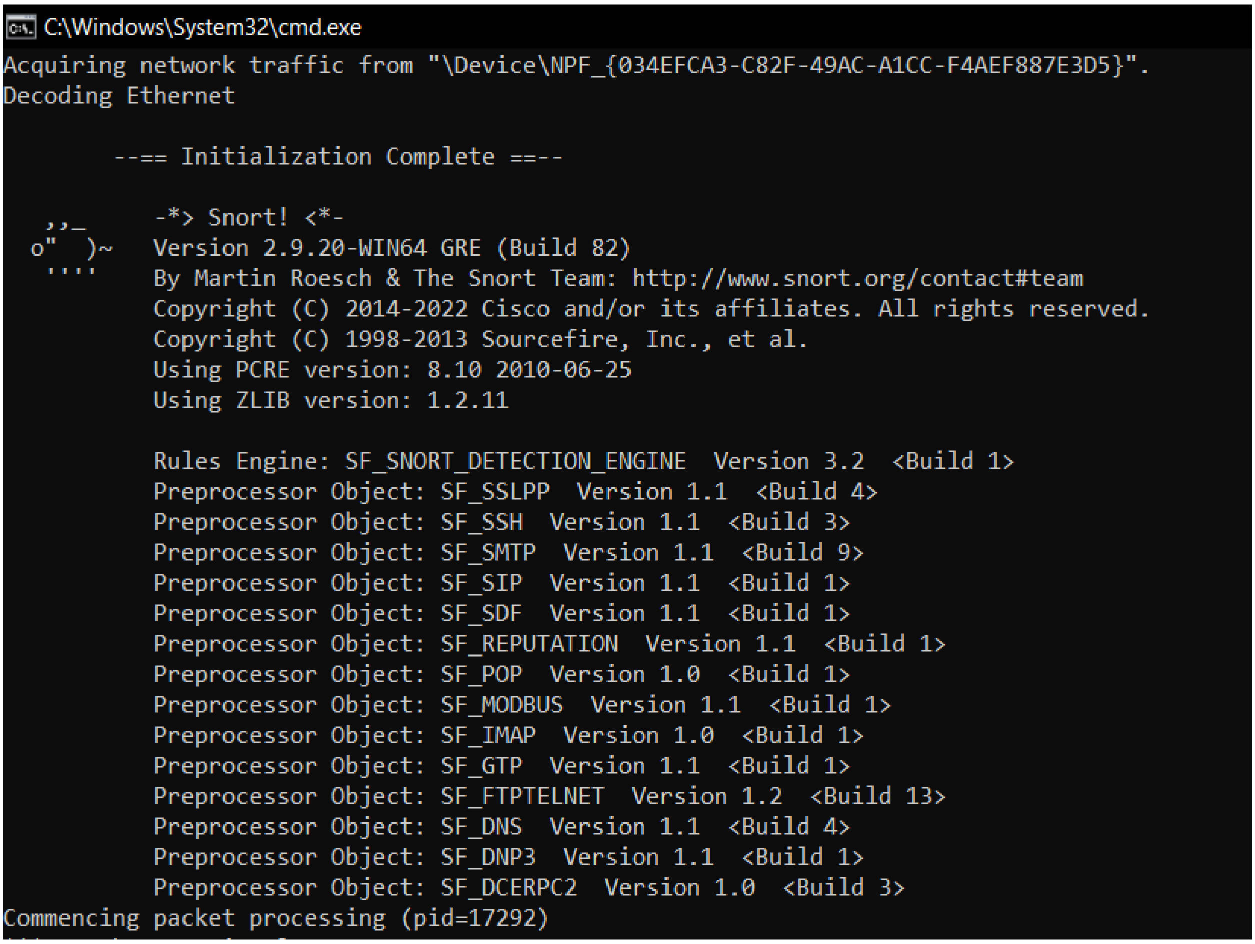
```
        --== Initialization Complete ==--

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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Total snort Fixed Memory Cost - MaxRss:290402976
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

If you load these rules by starting Snort with the -A console option, you can see the output on the screen as it happens. Note that the startup command shown below uses an interface 4, which is often the correct choice, but many systems have multiple network interfaces so it is a good idea to determine which one you want Snort to monitor by running the command snort -W to see the available interfaces.

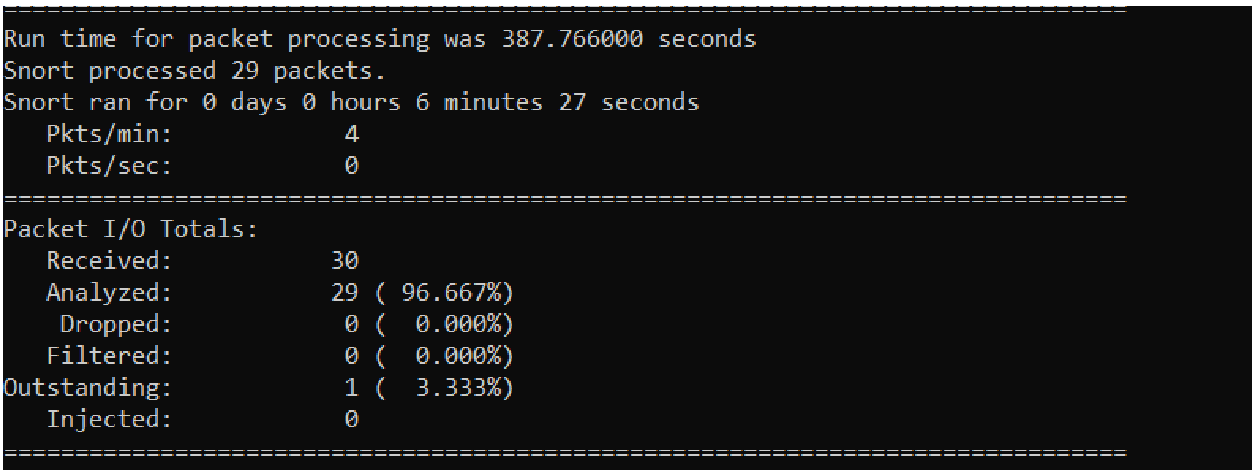


```
C:\Snort\bin>snort -i 4 -c  C:\Snort\etc\snort.conf -A console
Running in IDS mode
```

NAME: Sarvesh Patil
CLASS: D15A
ROLL NO: 52



```
C:\Windows\System32\cmd.exe
Acquiring network traffic from "\Device\NPF_{034EFCA3-C82F-49AC-A1CC-F4AEF887E3D5}".
Decoding Ethernet

        --== Initialization Complete ==--

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

           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=17292)
```



```
===============================================================================
Run time for packet processing was 387.766000 seconds
Snort processed 29 packets.
Snort ran for 0 days 0 hours 6 minutes 27 seconds
   Pkts/min:            4
   Pkts/sec:            0
===============================================================================
Packet I/O Totals:
   Received:           30
   Analyzed:           29 ( 96.667%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            1 (  3.333%)
   Injected:            0
===============================================================================
```

CONCLUSION:
Hence, we understood how to set up the Snort and also studied the logs.