Experiment 10

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

Roll No.	37
Name	Mikil Lalwani
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 network-based intrusion detection system that is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software. It can also be used as a packet sniffer to monitor the system in real-time. The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system. It is based on a library packet capture tool. The rules are fairly easy to create and implement and they can be deployed in any kind of operating system and any kind of network environment. The main reason for the popularity of this IDS over others is that it is free-to-use software and also open source because of which any user can be able to use it the way he wants.

Features:

1. Real-time traffic monitor
2. Packet logging
3. Analysis of protocol
4. Content matching
5. OS fingerprinting
6. Can be installed in any network environment.
7. Creates logs
8. Open Source
9. Rules are easy to implement
10. Installation Steps:

In Linux:
Step-1: wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
Step-2: tar xvzf snort-2.9.15.tar.gz
Step-3: cd snort-2.9.15
Step-4: ./configure –enable-sourcefire && make && sudo make install

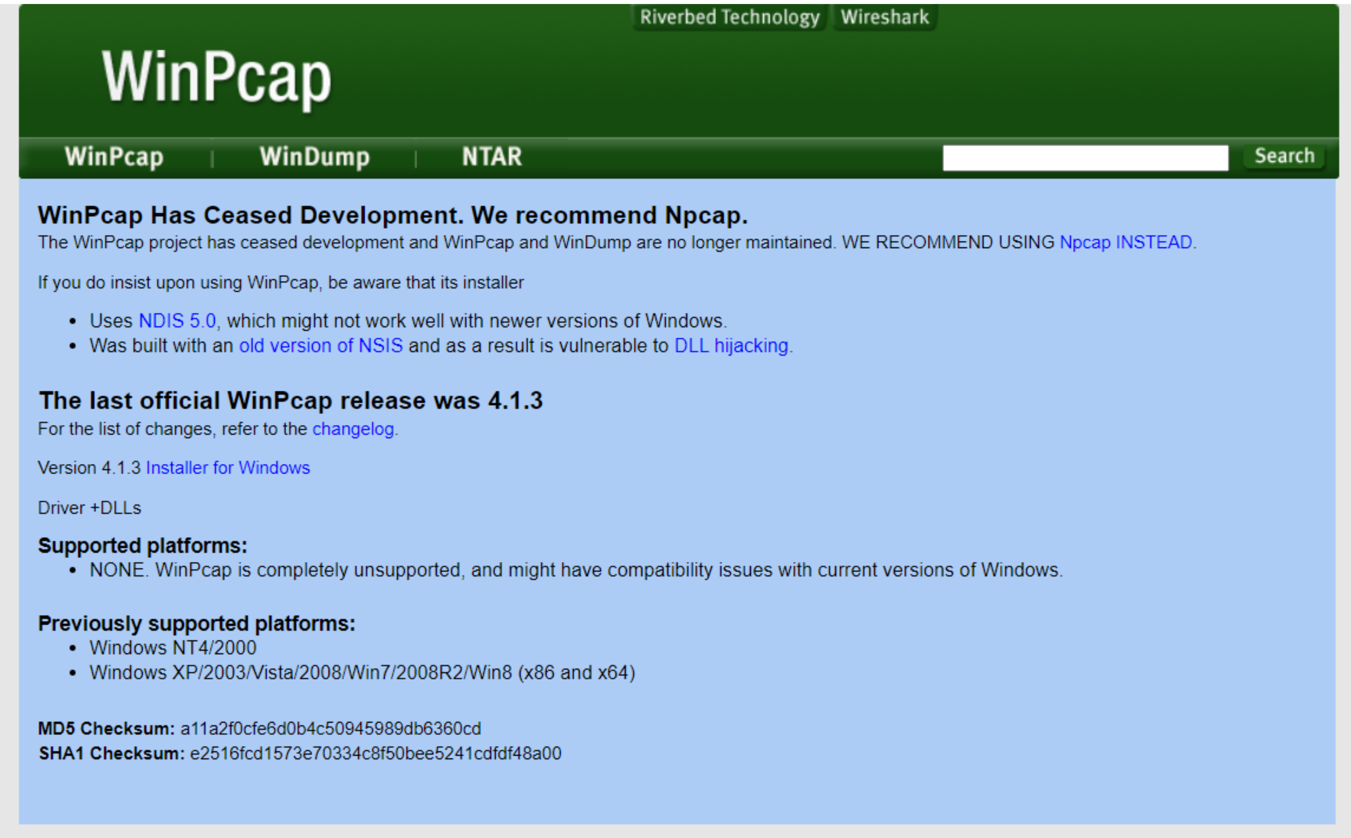
In Windows:
Step-1: Download SNORT installer from
https://www.snort.org/downloads/snort/Snort_2_9_15_Installer.exe
Step-1: Execute the Snort_2_9_15_Installer.exe
Basic Usages:
Sniffer Mode –
To print TCP/IP header use command ./snort -v
To print IP address along with header use command ./snort -vd

Packet Logging –
To store the packet in the disk you need to give the path where you want to store the logs. For this command is./snort -dev -l ./SnortLogs.

Activate network intrusion detection mode –
To start this mode use this command ./snort -dev -l ./SnortLogs -h 192.127.1.0/24 -c snort.conf

Procedure-

1. Download Winpcap, Snort, and Snort rules as shown below.



WinPcap Has Ceased Development. We recommend Npcap.

The WinPcap project has ceased development and WinPcap and WinDump are no longer maintained. WE RECOMMEND USING Npcap INSTEAD.

If you do insist upon using WinPcap, be aware that its installer

- Uses NDIS 5.0, which might not work well with newer versions of Windows.
- Was built with an old version of NSIS and as a result is vulnerable to DLL hijacking.

The last official WinPcap release was 4.1.3

For the list of changes, refer to the changelog.

Version 4.1.3 Installer for Windows

Driver +DLLs

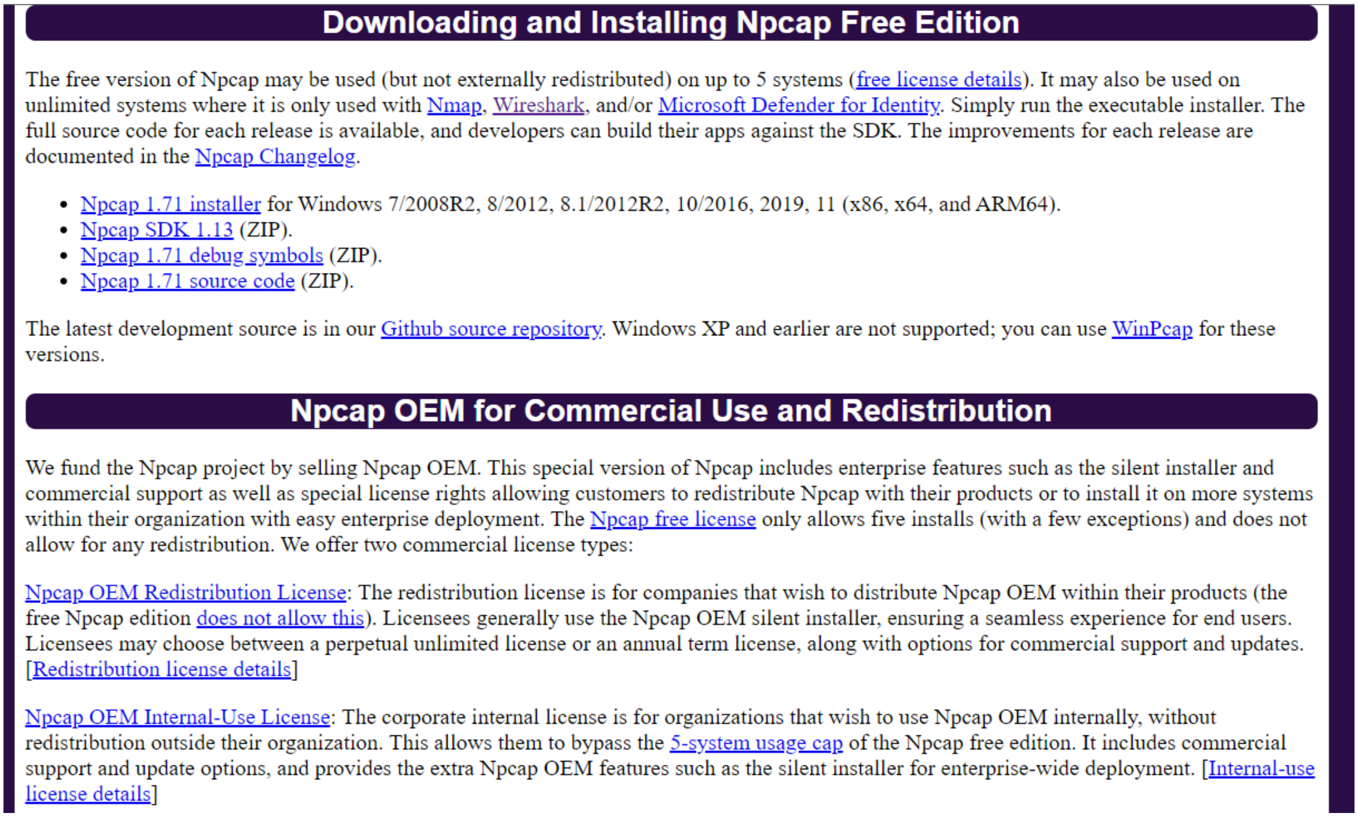
Supported platforms:

- NONE. WinPcap is completely unsupported, and might have compatibility issues with current versions of Windows.

Previously supported platforms:

- Windows NT4/2000
- Windows XP/2003/Vista/2008/Win7/2008R2/Win8 (x86 and x64)

MD5 Checksum: a11a2f0cfe6d0b4c50945989db6360cd
SHA1 Checksum: e2516fcd1573e70334c8f50bee5241cdfdf48a00



Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on unlimited systems where it is only used with Nmap, Wireshark, and/or Microsoft Defender for Identity. Simply run the executable installer. The full source code for each release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

- Npcap 1.71 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019, 11 (x86, x64, and ARM64).
- Npcap SDK 1.13 (ZIP).
- Npcap 1.71 debug symbols (ZIP).
- Npcap 1.71 source code (ZIP).

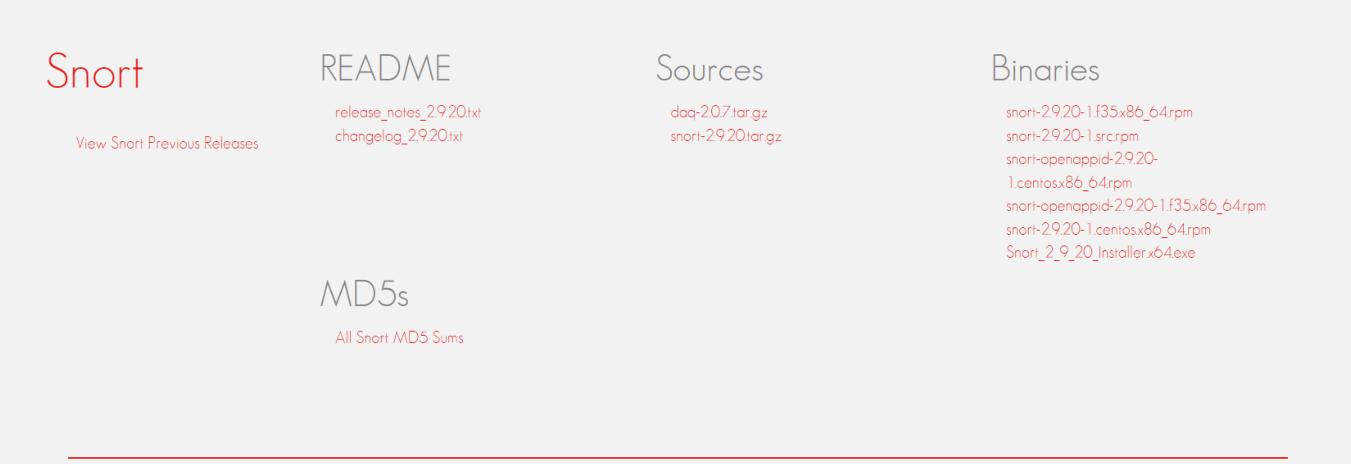
The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

Npcap OEM for Commercial Use and Redistribution

We fund the Npcap project by selling Npcap OEM. This special version of Npcap includes enterprise features such as the silent installer and commercial support as well as special license rights allowing customers to redistribute Npcap with their products or to install it on more systems within their organization with easy enterprise deployment. The Npcap free license only allows five installs (with a few exceptions) and does not allow for any redistribution. We offer two commercial license types:

Npcap OEM Redistribution License: The redistribution license is for companies that wish to distribute Npcap OEM within their products (the free Npcap edition does not allow this). Licensees generally use the Npcap OEM silent installer, ensuring a seamless experience for end users. Licensees may choose between a perpetual unlimited license or an annual term license, along with options for commercial support and updates. [Redistribution license details]

Npcap OEM Internal-Use License: The corporate internal license is for organizations that wish to use Npcap OEM internally, without redistribution outside their organization. This allows them to bypass the 5-system usage cap of the Npcap free edition. It includes commercial support and update options, and provides the extra Npcap OEM features such as the silent installer for enterprise-wide deployment. [Internal-use license details]



Snort

View Snort Previous Releases

README

release_notes_2.9.20.txt
changelog_2.9.20.txt

Sources

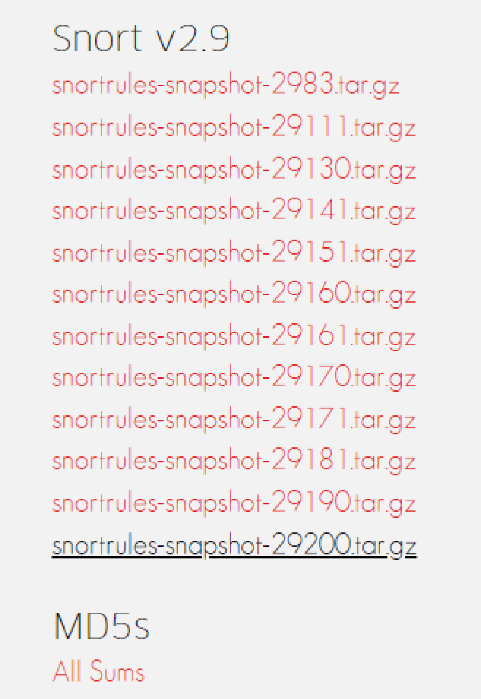
daq-2.0.7.tar.gz
snort-2.9.20.tar.gz

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



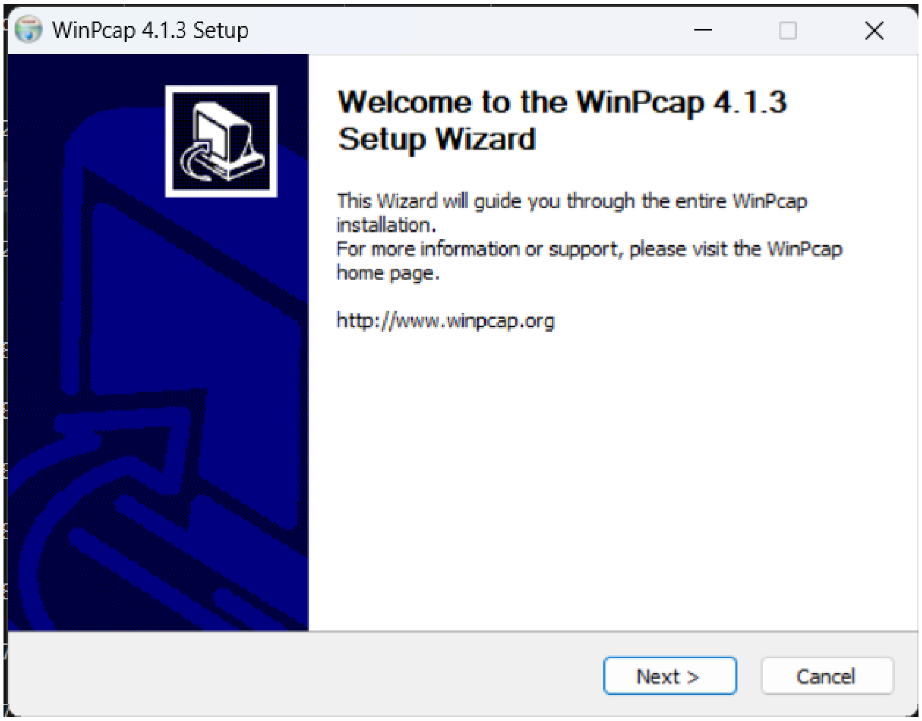
Snort v2.9

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

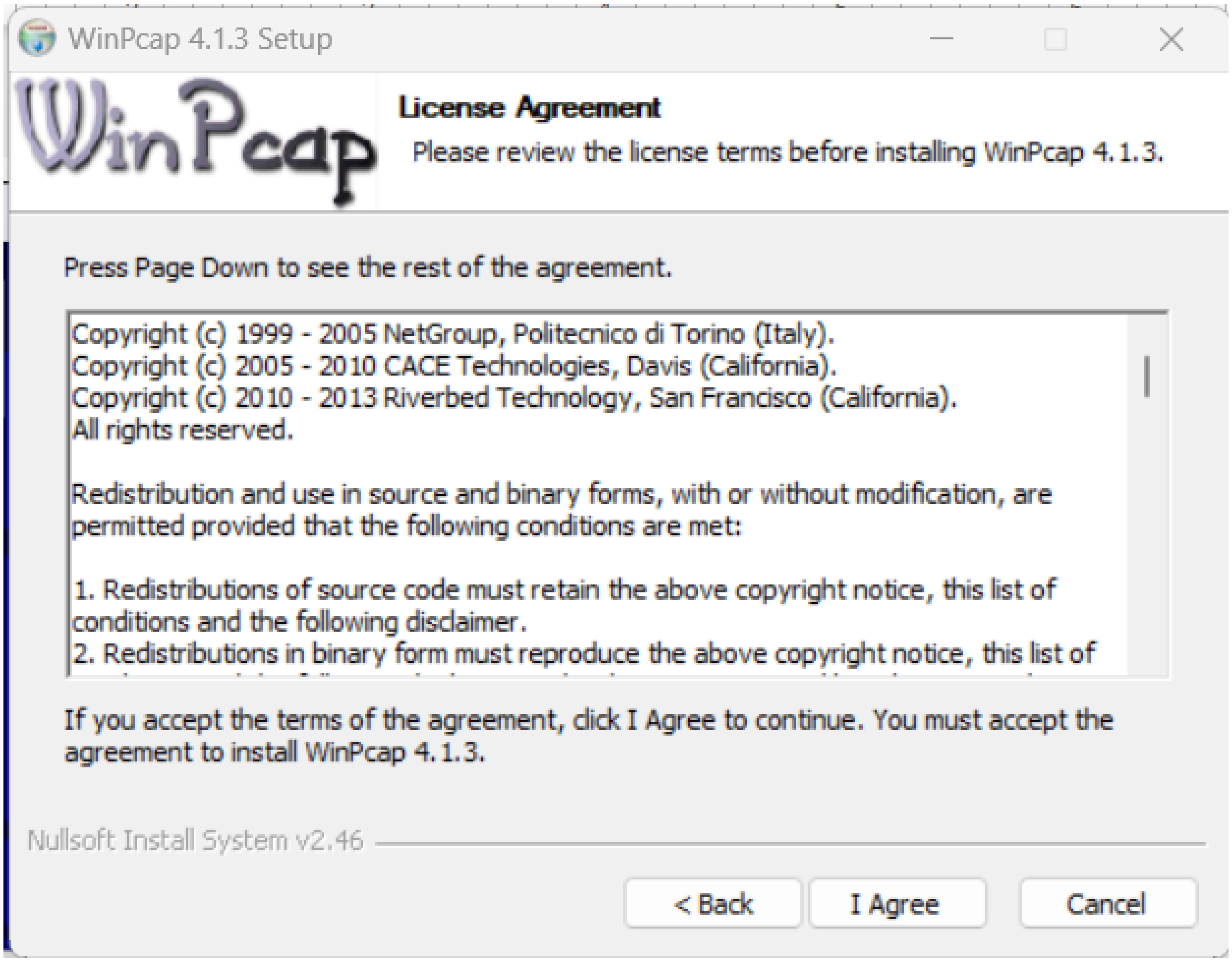
2. Install Snort, winpcap and npcap as shown below.



Welcome to the WinPcap 4.1.3 Setup Wizard

This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org



License Agreement

Please review the license terms before installing WinPcap 4.1.3.

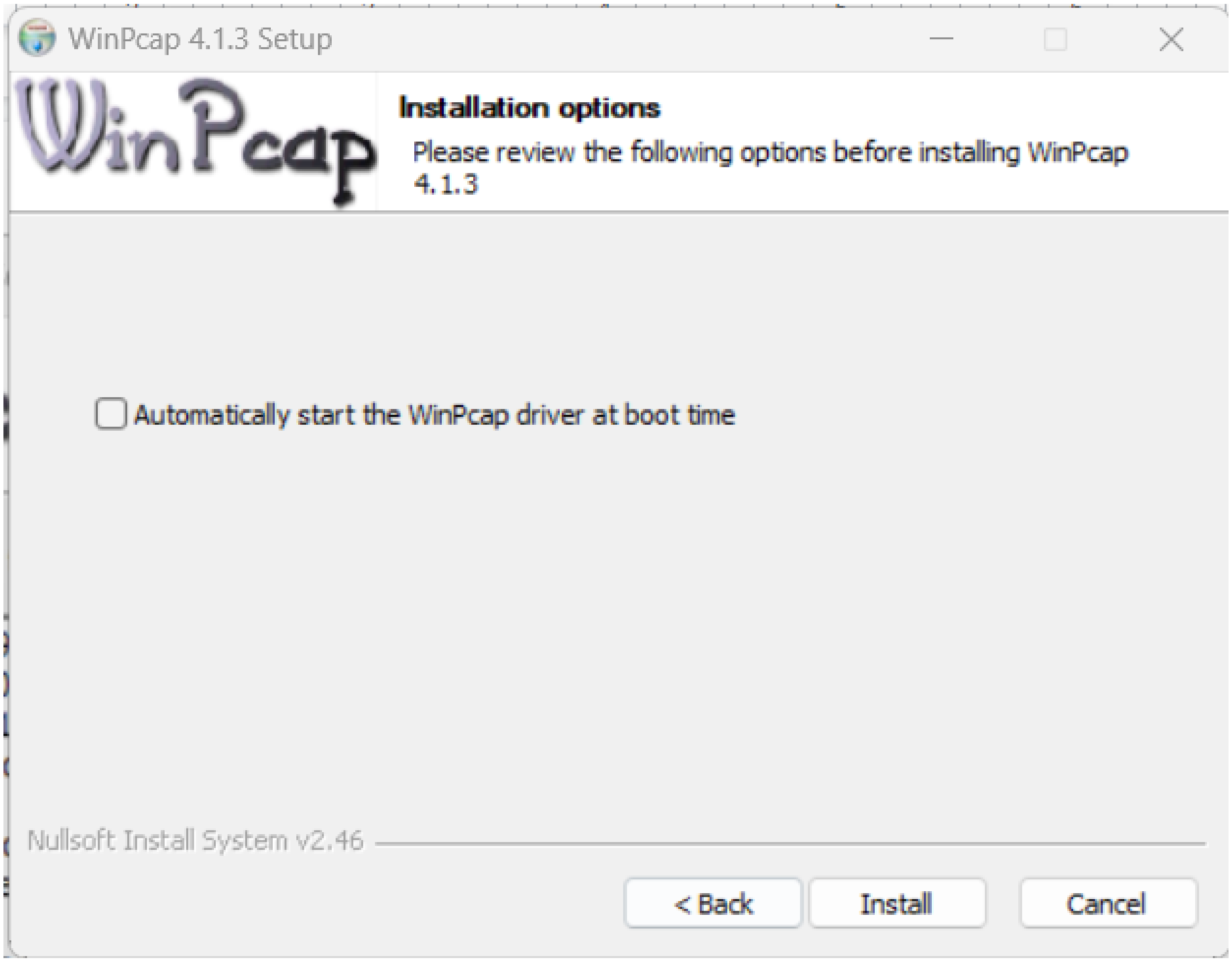
Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

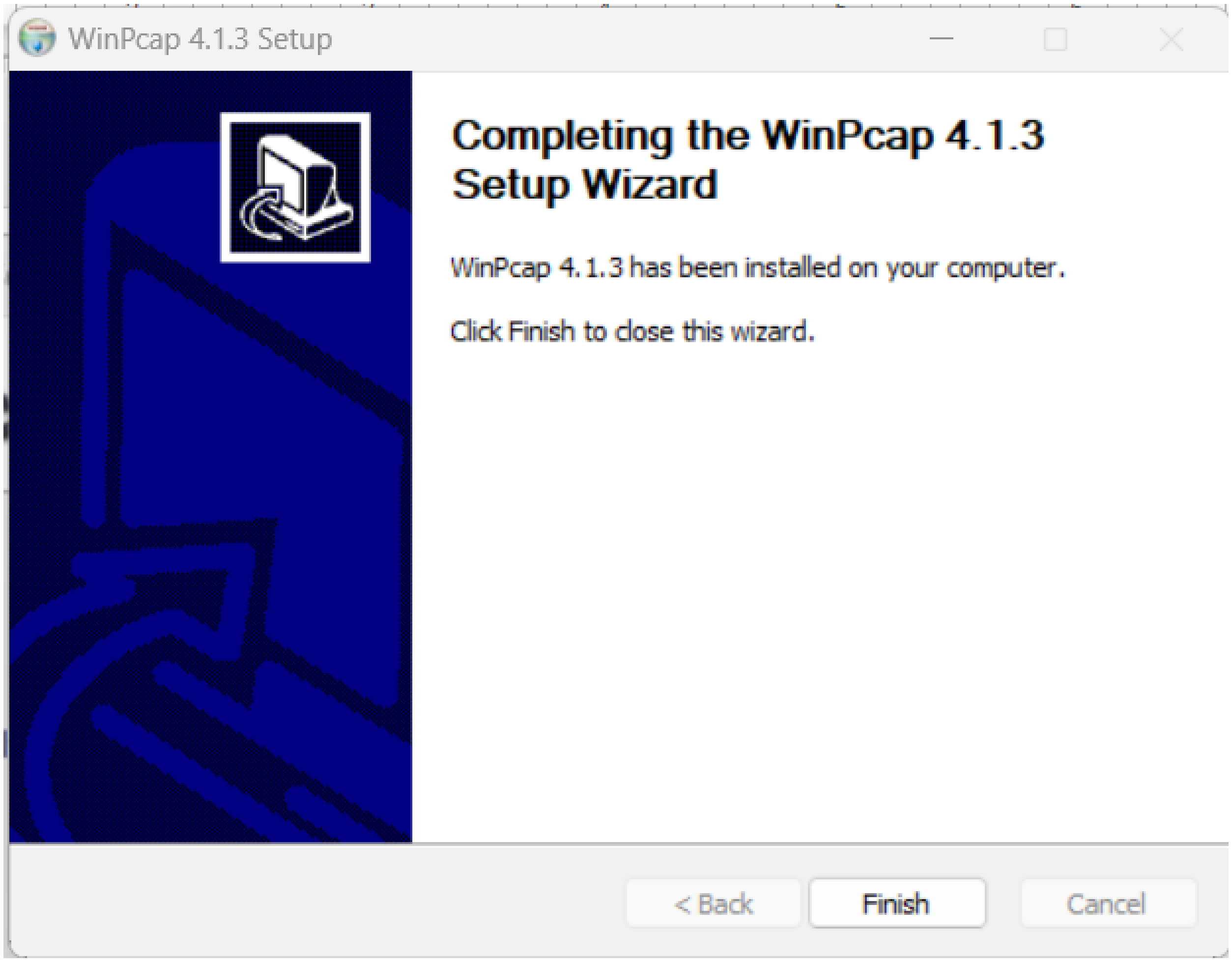
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.



Installation options

Please review the following options before installing WinPcap 4.1.3

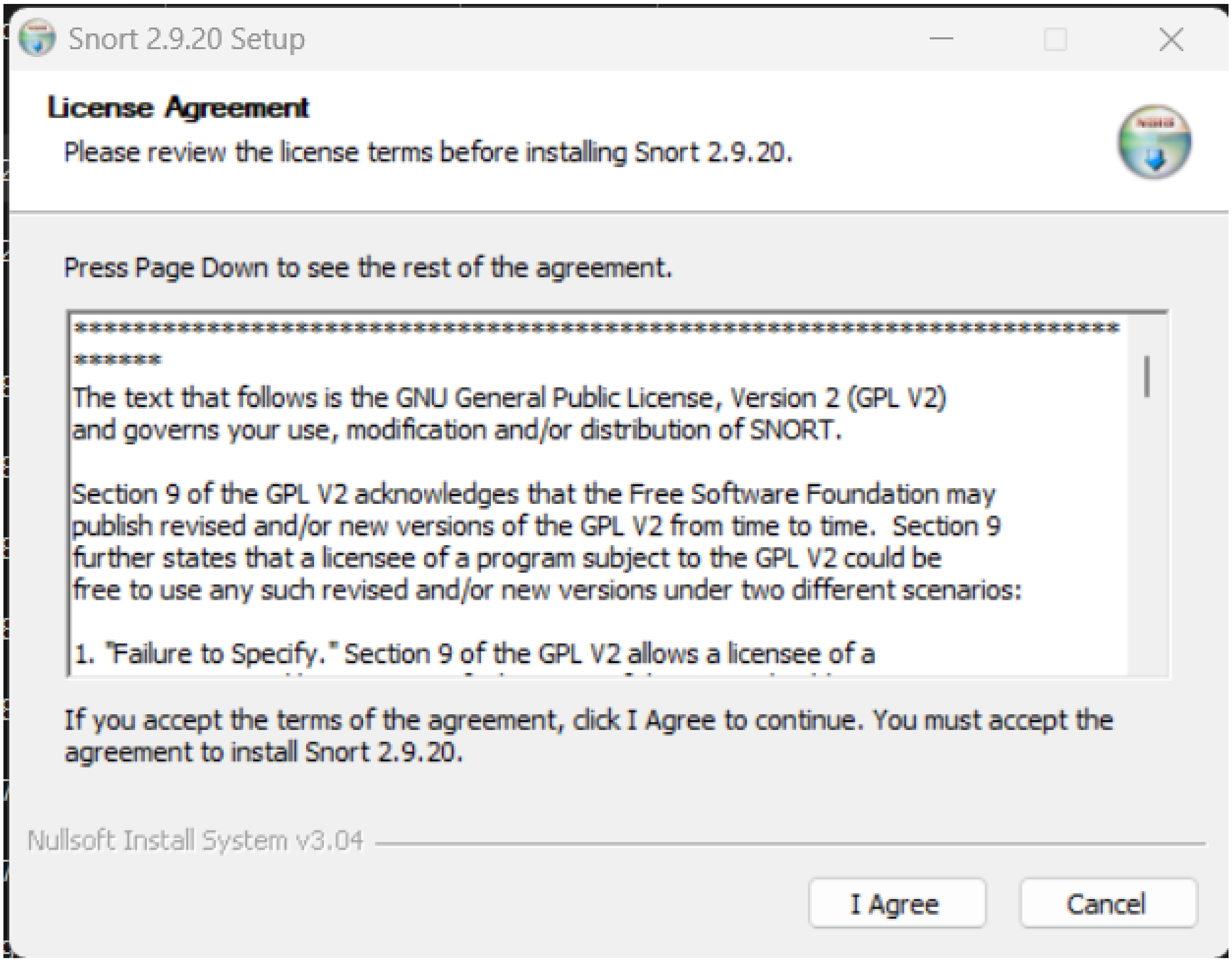
☐ Automatically start the WinPcap driver at boot time



Completing the WinPcap 4.1.3 Setup Wizard

WinPcap 4.1.3 has been installed on your computer.

Click Finish to close this wizard.



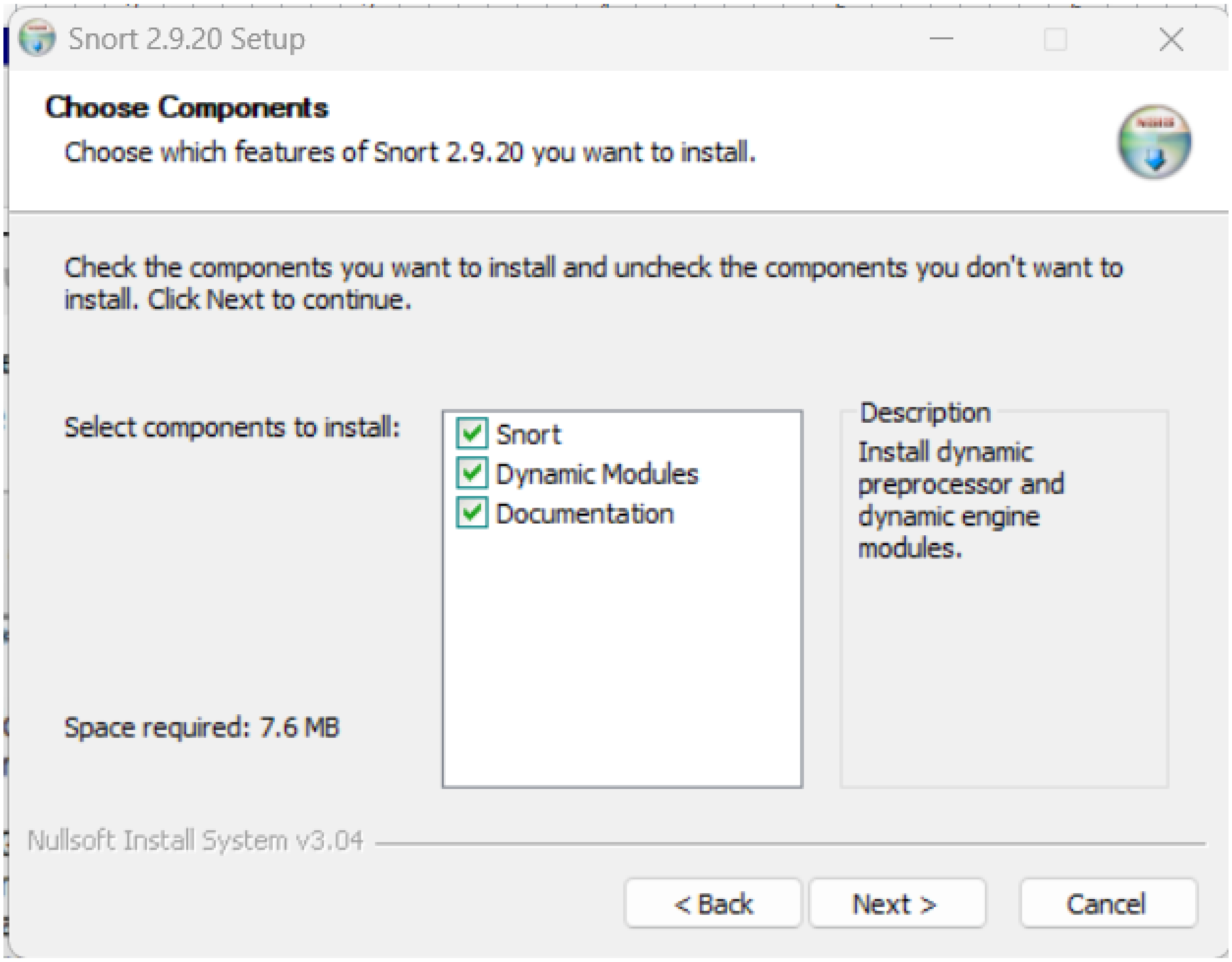
License Agreement

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:

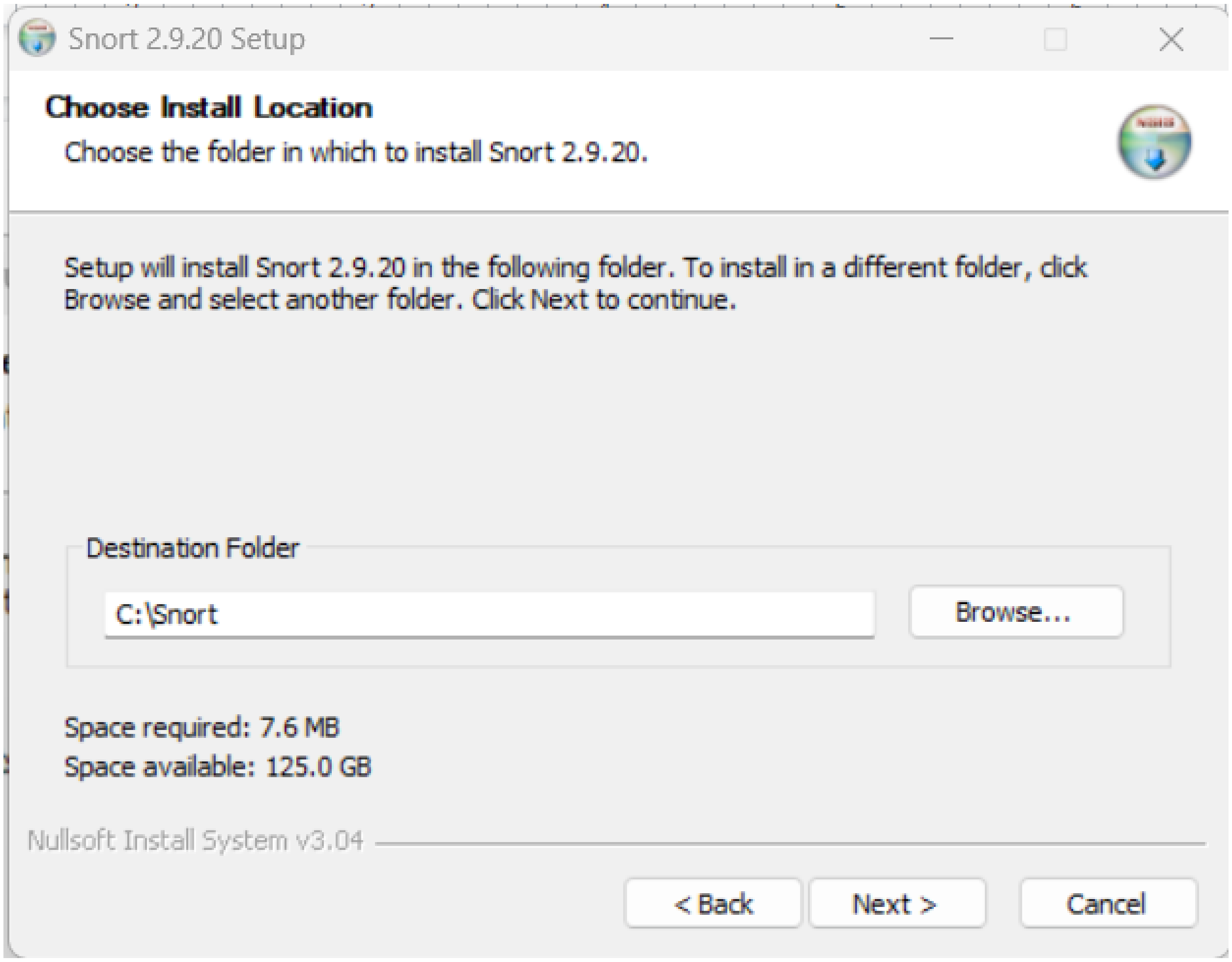
☑ Snort
☑ Dynamic Modules
☑ Documentation

Description

Install dynamic preprocessor and dynamic engine modules.

Space required: 7.6 MB

Nullsoft Install System v3.04



Snort 2.9.20 Setup

Choose Install Location

Choose the folder in which to install Snort 2.9.20.

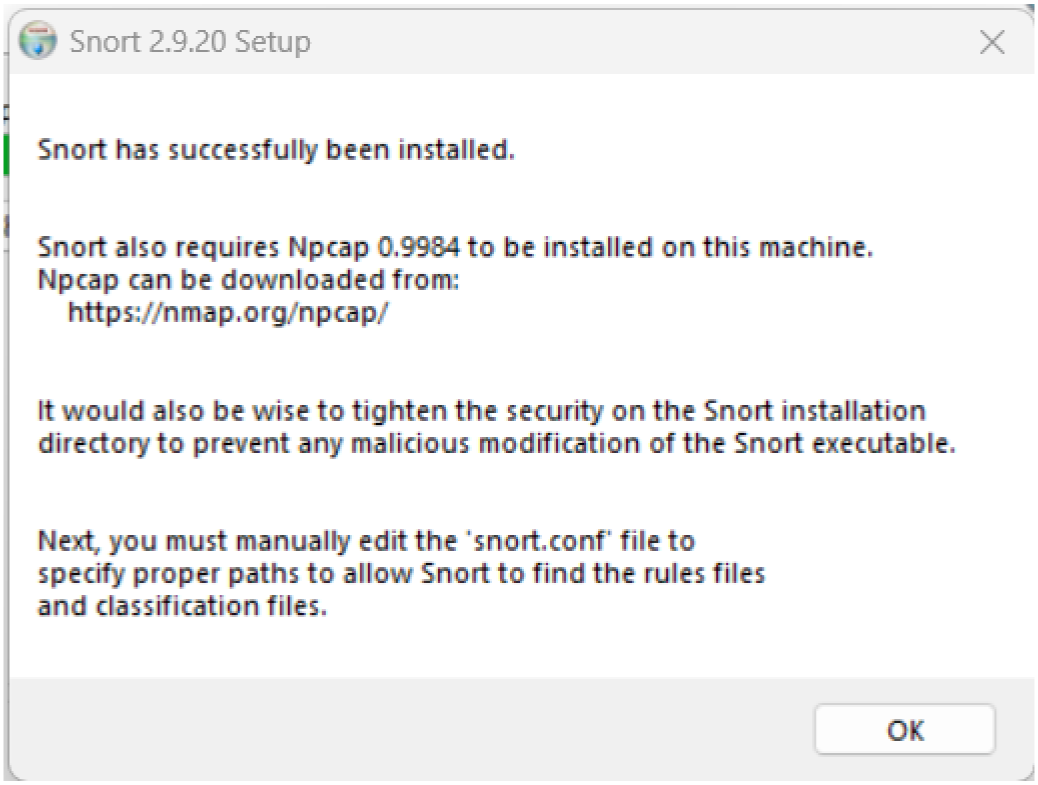
Setup will install Snort 2.9.20 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

C:\Snort

Space required: 7.6 MB
Space available: 125.0 GB

Nullsoft Install System v3.04



Snort 2.9.20 Setup

Snort has successfully been installed.

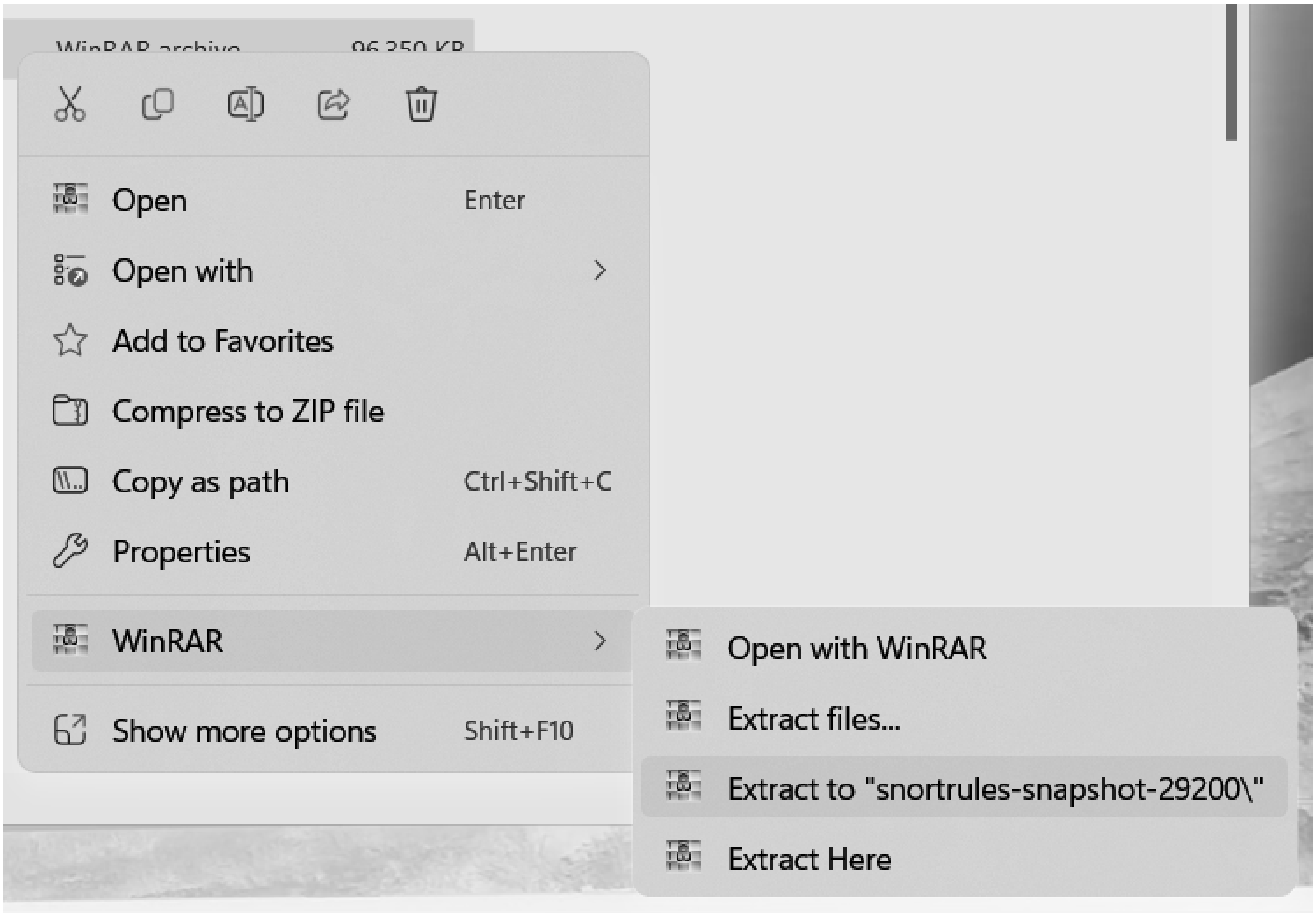
Snort also requires Npcap 0.9984 to be installed on this machine.
Npcap can be downloaded from:
https://nmap.org/npcap/

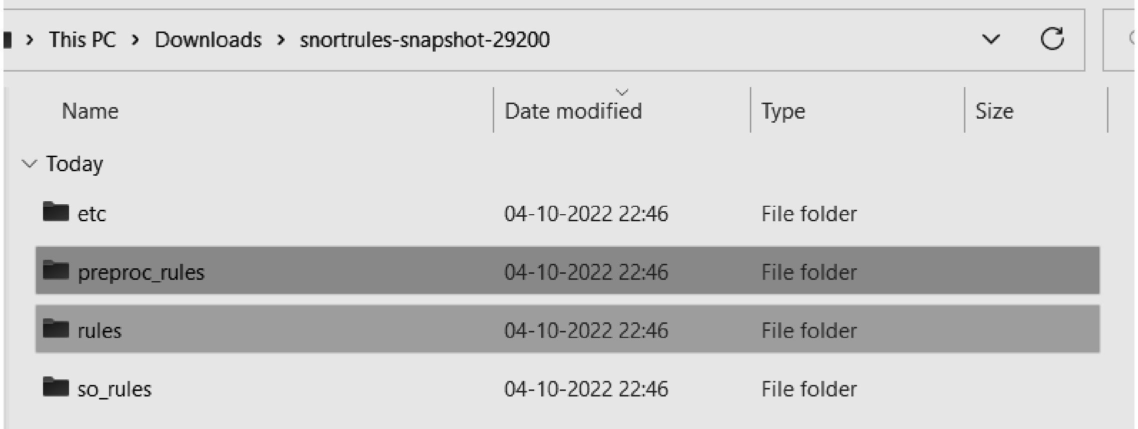
It would also be wise to tighten the security on the Snort installation directory to prevent any malicious modification of the Snort executable.

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

OK

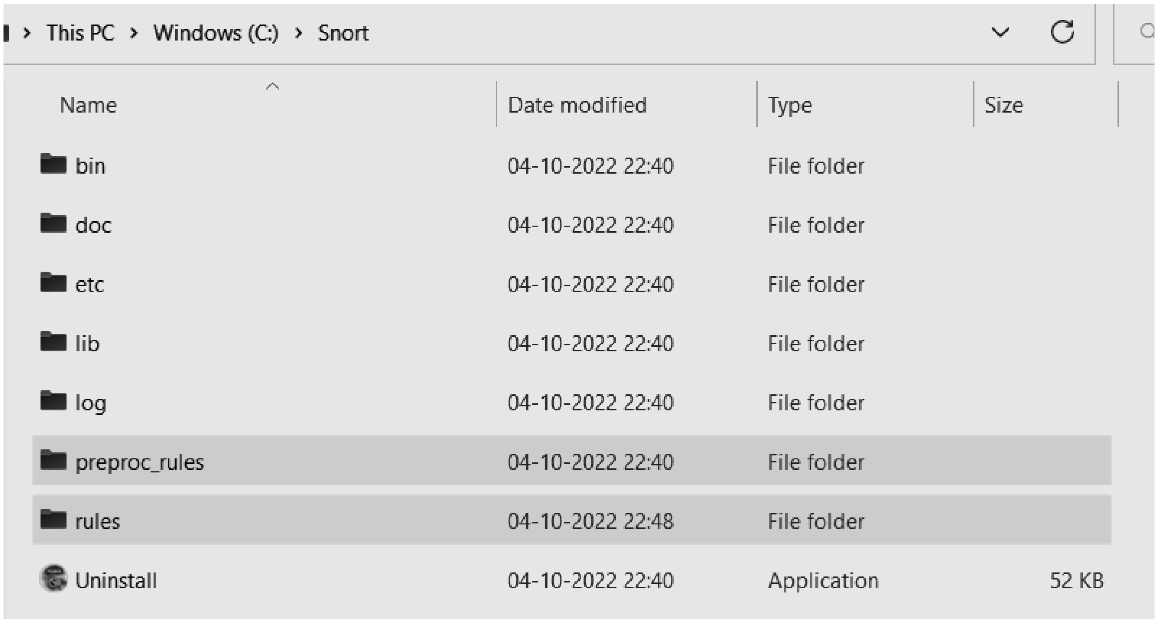
3. Extract snort rules and copy preproc_rules and rules to C:/Snort/ .





This PC > Downloads > snortrules-snapshot-29200

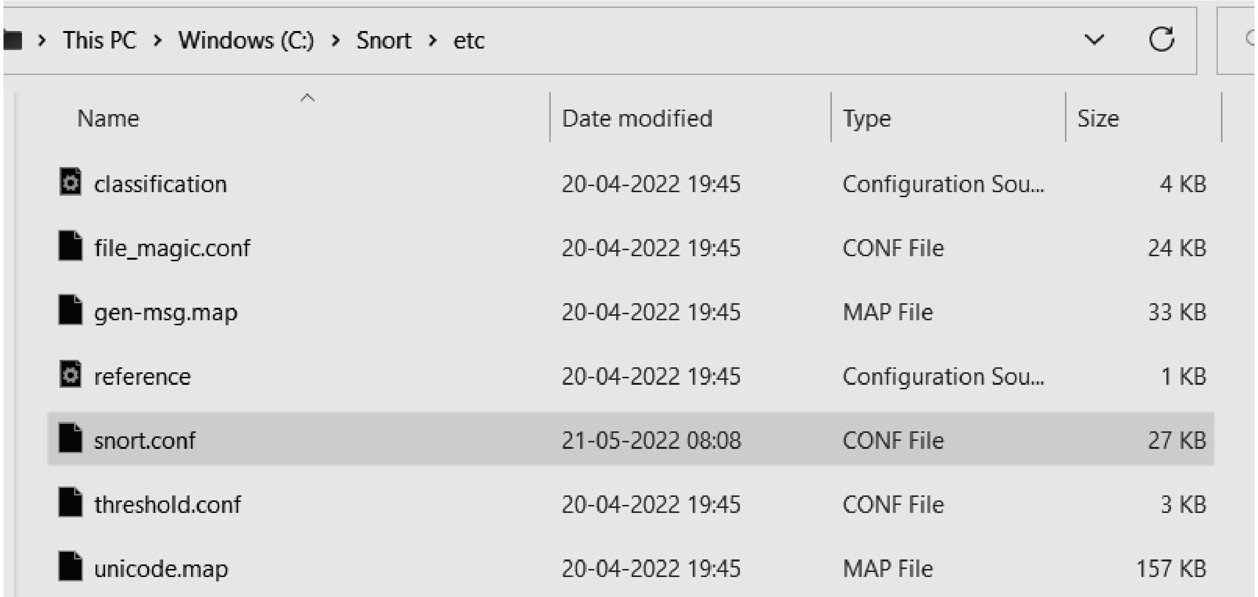
Name	Date modified	Type	Size
Today			
etc	04-10-2022 22:46	File folder	
preproc_rules	04-10-2022 22:46	File folder	
rules	04-10-2022 22:46	File folder	
so_rules	04-10-2022 22:46	File folder	



This PC > Windows (C:) > Snort

Name	Date modified	Type	Size
bin	04-10-2022 22:40	File folder	
doc	04-10-2022 22:40	File folder	
etc	04-10-2022 22:40	File folder	
lib	04-10-2022 22:40	File folder	
log	04-10-2022 22:40	File folder	
preproc_rules	04-10-2022 22:40	File folder	
rules	04-10-2022 22:48	File folder	
Uninstall	04-10-2022 22:40	Application	52 KB

4. Now we edit the config file.

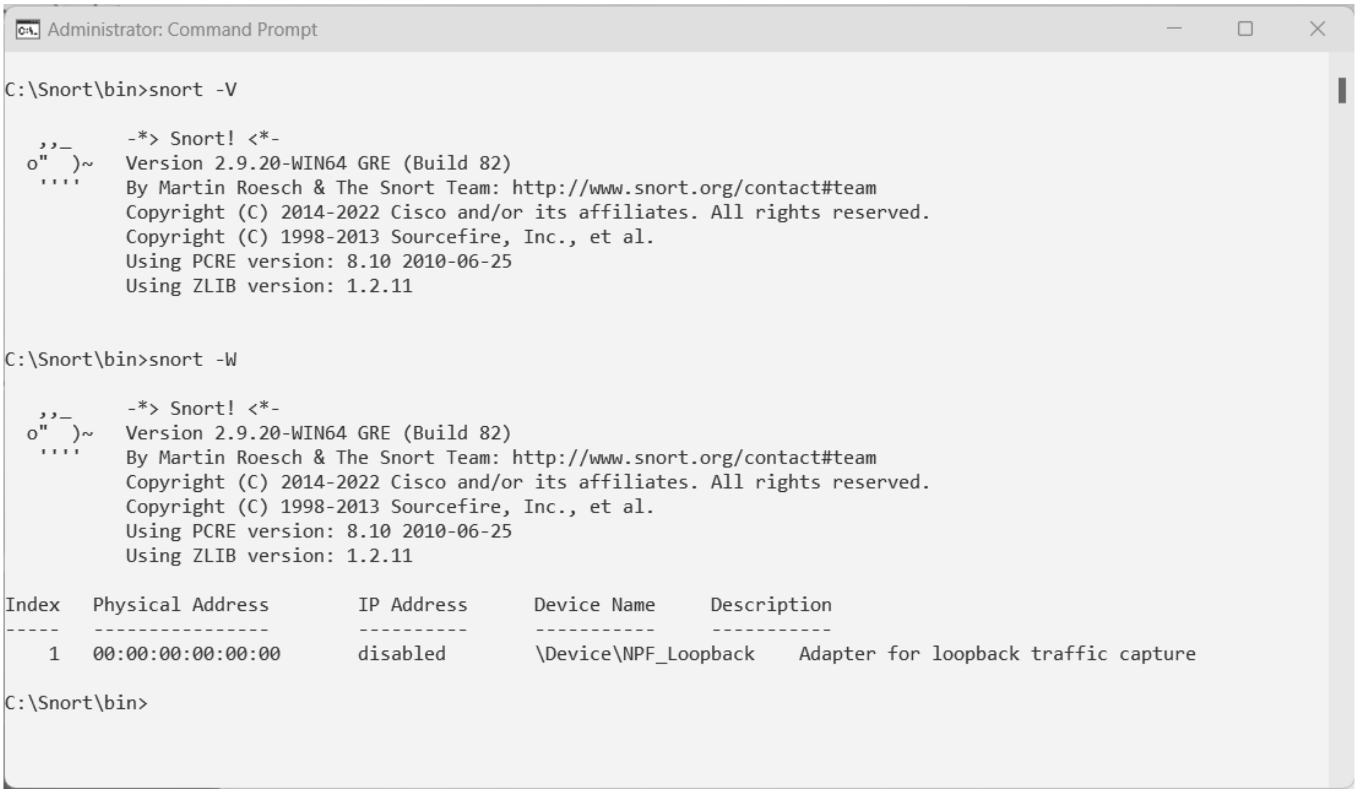


This PC > Windows (C:) > Snort > etc

Name	Date modified	Type	Size
classification	20-04-2022 19:45	Configuration Sou...	4 KB
file_magic.conf	20-04-2022 19:45	CONF File	24 KB
gen-msg.map	20-04-2022 19:45	MAP File	33 KB
reference	20-04-2022 19:45	Configuration Sou...	1 KB
snort.conf	21-05-2022 08:08	CONF File	27 KB
threshold.conf	20-04-2022 19:45	CONF File	3 KB
unicode.map	20-04-2022 19:45	MAP File	157 KB

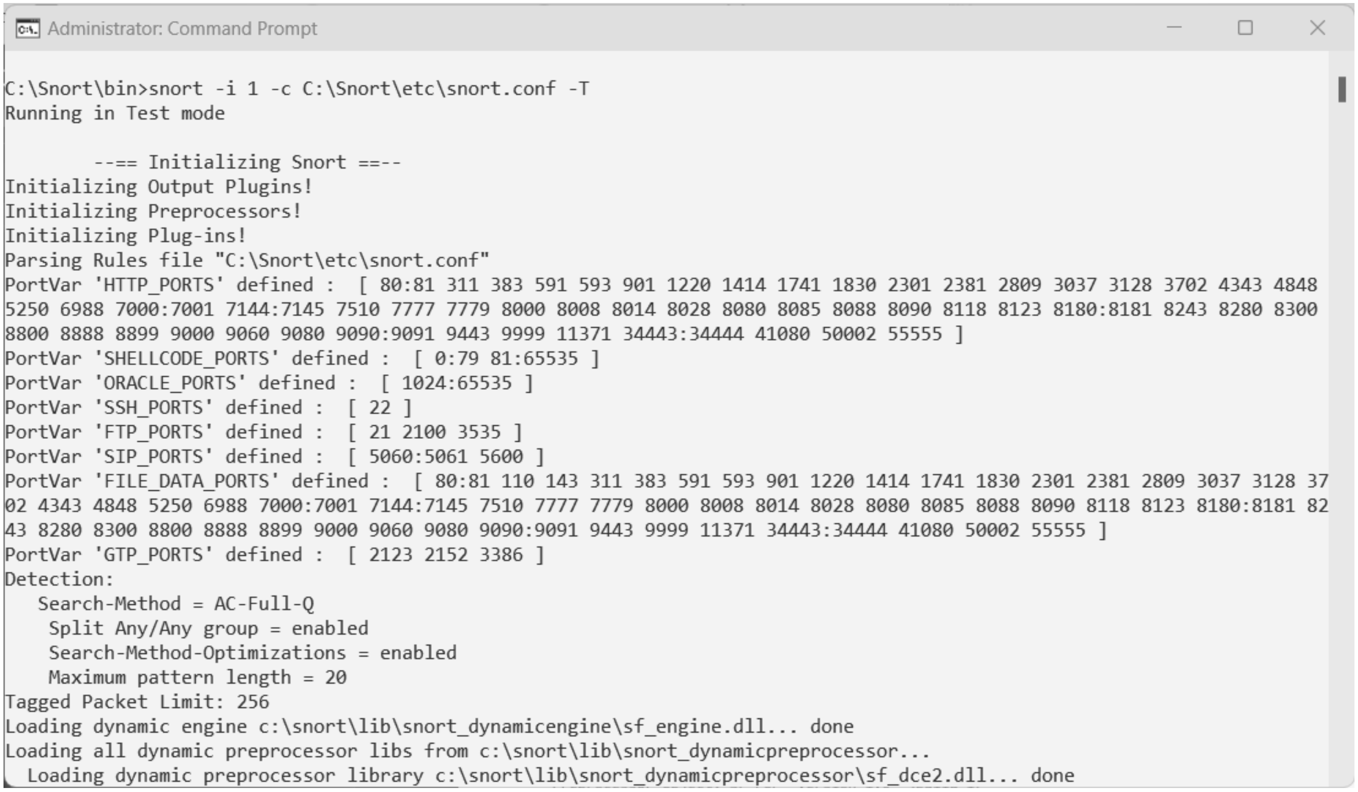
5. After installing Snort and Npcap enter these commands in the windows 10 Command prompt to check snorts working.
6. As you can see in the above figure that snort runs successfully
7. Check the wireless interface cards from which we will be using snort by using the command below.

```
snort -w
```

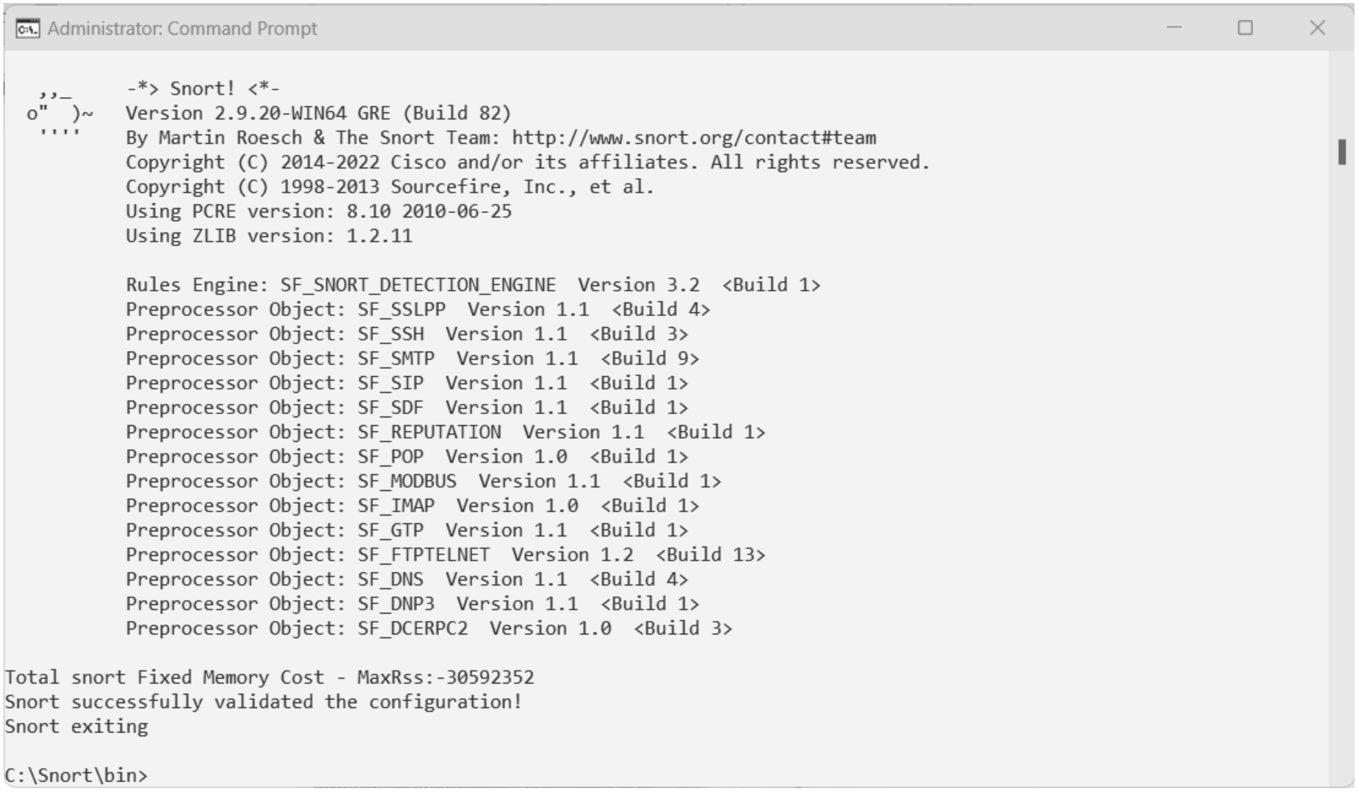


```
C:\Snort\bin>snort -V

   ,,_     -*> 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>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_Loopback    Adapter for loopback traffic capture

C:\Snort\bin>
```

8. To check the validation of snort’s configuration by choosing a specific wireless interface card (1) the rest of the command shows the config file path. The command is:
   snort -i 1 -c C:\Snort\etc\snort.conf -T

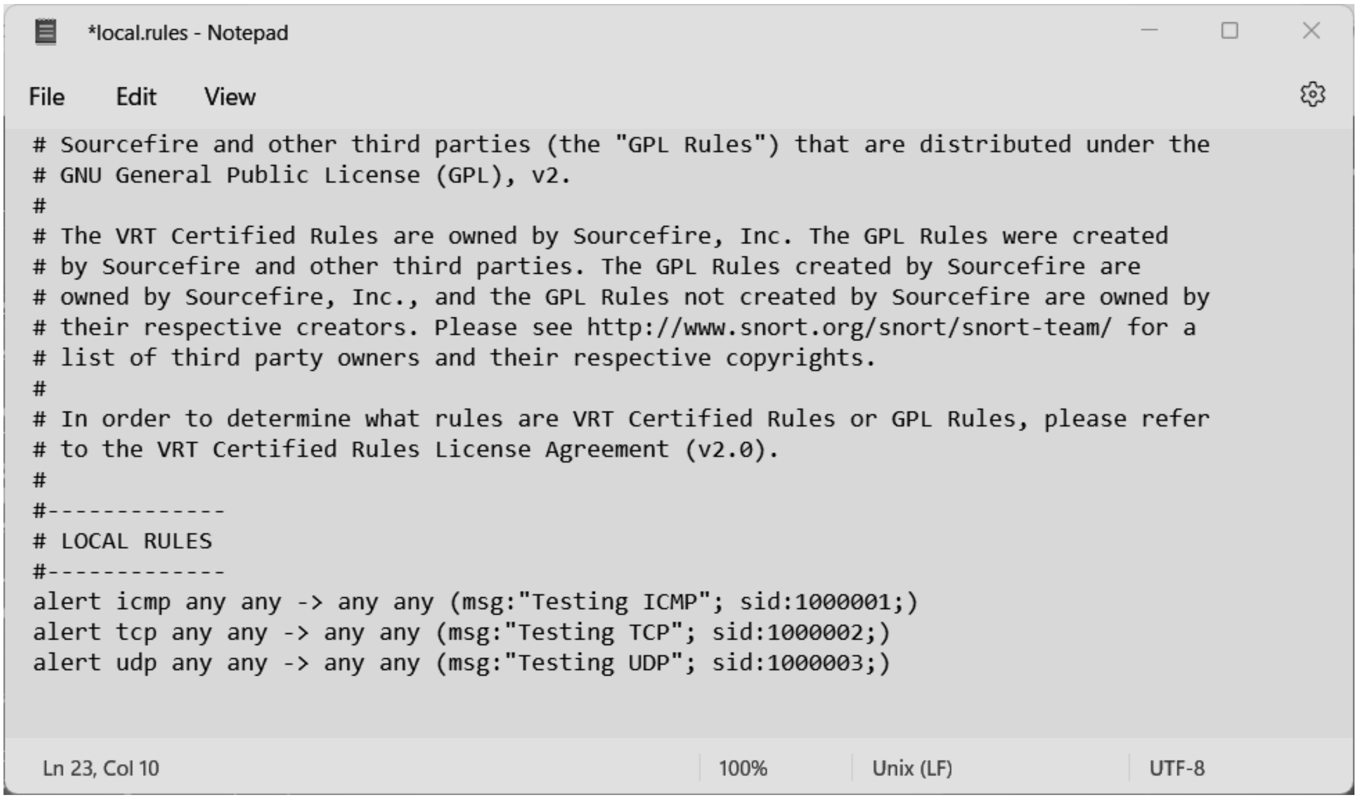


```
C:\Snort\bin>snort -i 1 -c C:\Snort\etc\snort.conf -T
Running in Test mode

        --== 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 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 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 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
Loading dynamic engine c:\snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library c:\snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
```



```
   ,,_     -*> 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:-30592352
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

Before we go and test the next command of snort, we are supposed to add few rules in the local.rules files. To access the local.rules file we need to go to c:\Snort\rules and search for local.rules file as shown in the image below.



```
# 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;)
```

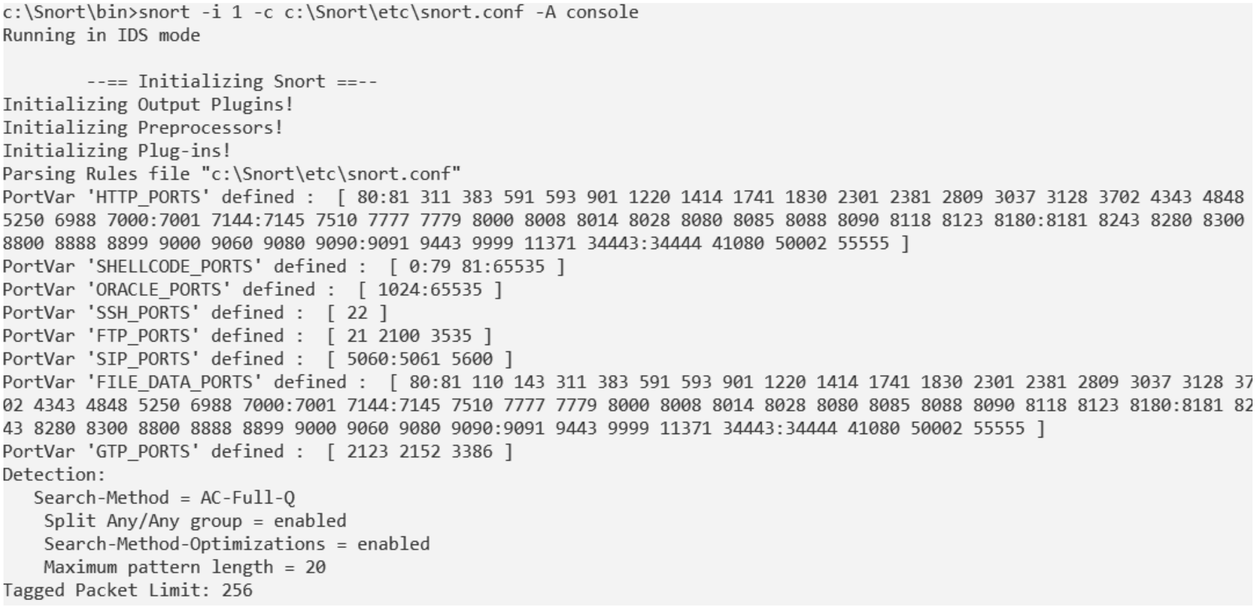
After adding the rules in the local.rules file the next thing is to run the following command **snort -i 3 -c c:\Snort\etc\snort.conf -A console**

1. I – stands for interface, here is where you tell snort what network interface it should sniff on
2. C – is where you tell snort the location of the file you want it to run

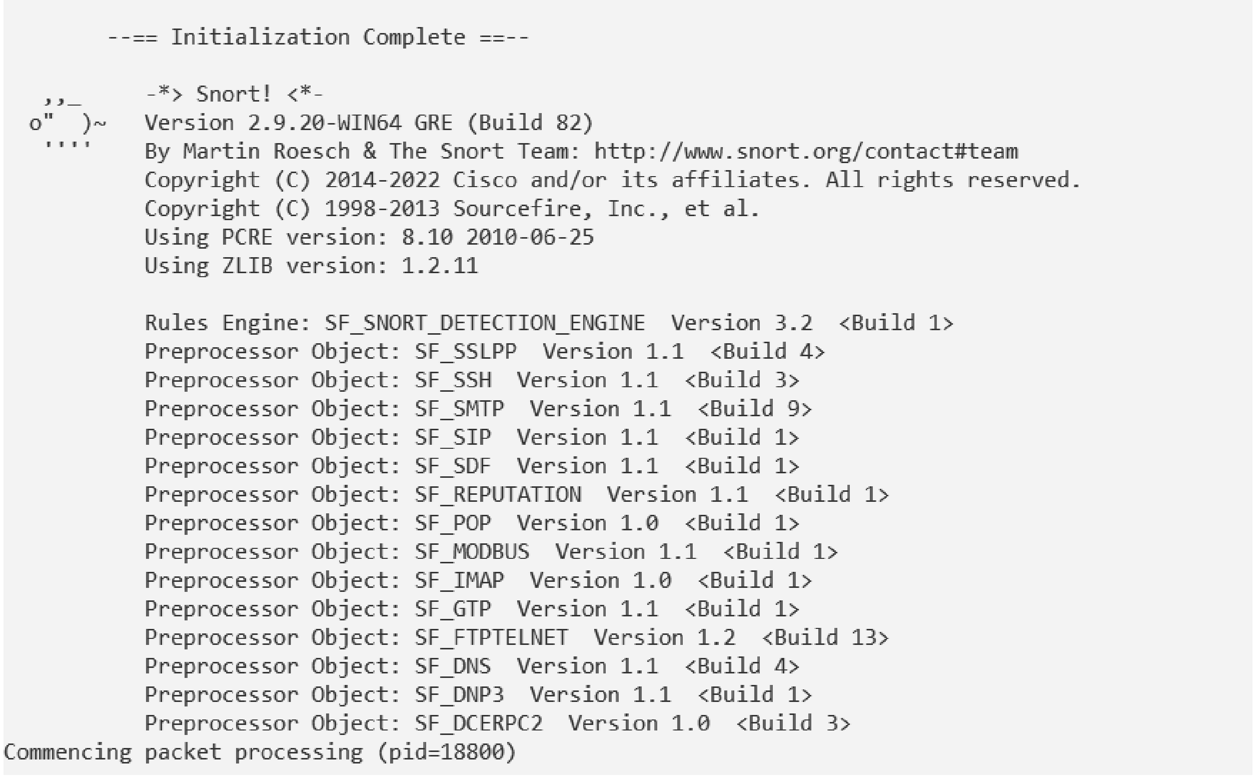
3. A – means print output in the terminal

Then press enter

Snort will start sniffing the network interface we have specified and all the traffic that is passing through our network whether tcp, udp or icmp based on the rules we had specified on the local.rules file.



```
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 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 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 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
```



```
        --== 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=18800)
```

Conclusion-

Snort has been set up and the study of logs has been successfully implemented.