Expt\_10\_D15B Internet Security Lab Roll No: 37



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 –

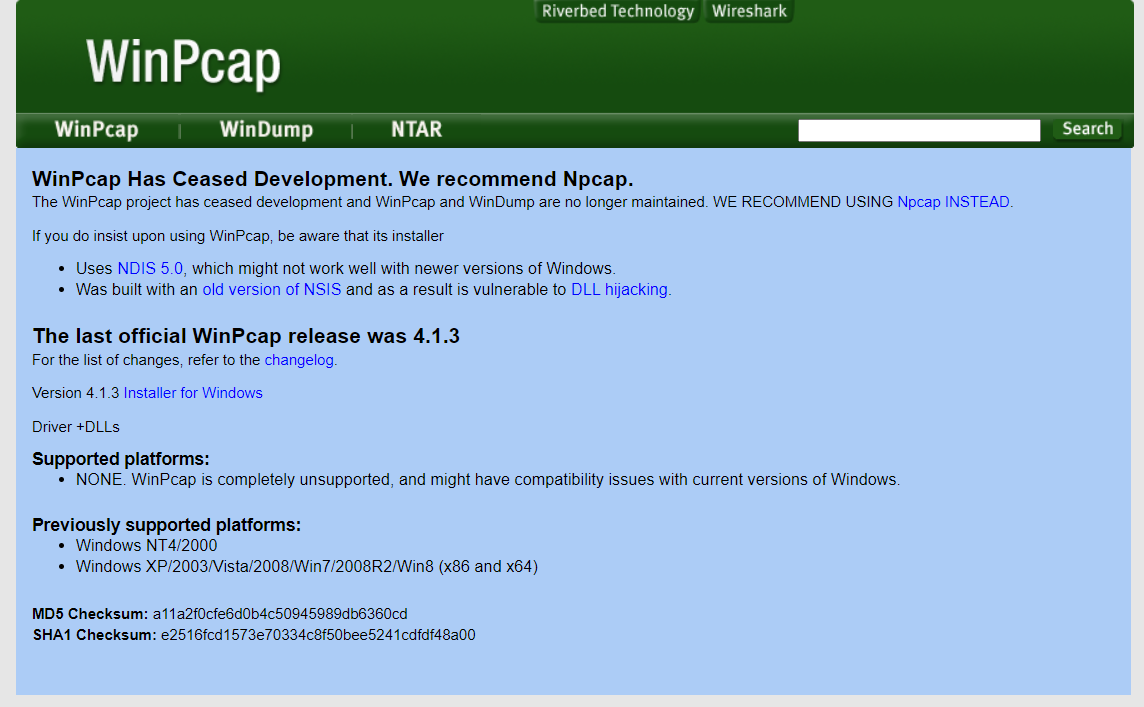
To store the packet in the disk you need to give the path where you want to store the logs. For this command is./snort -dev -l ./SnortLogs.

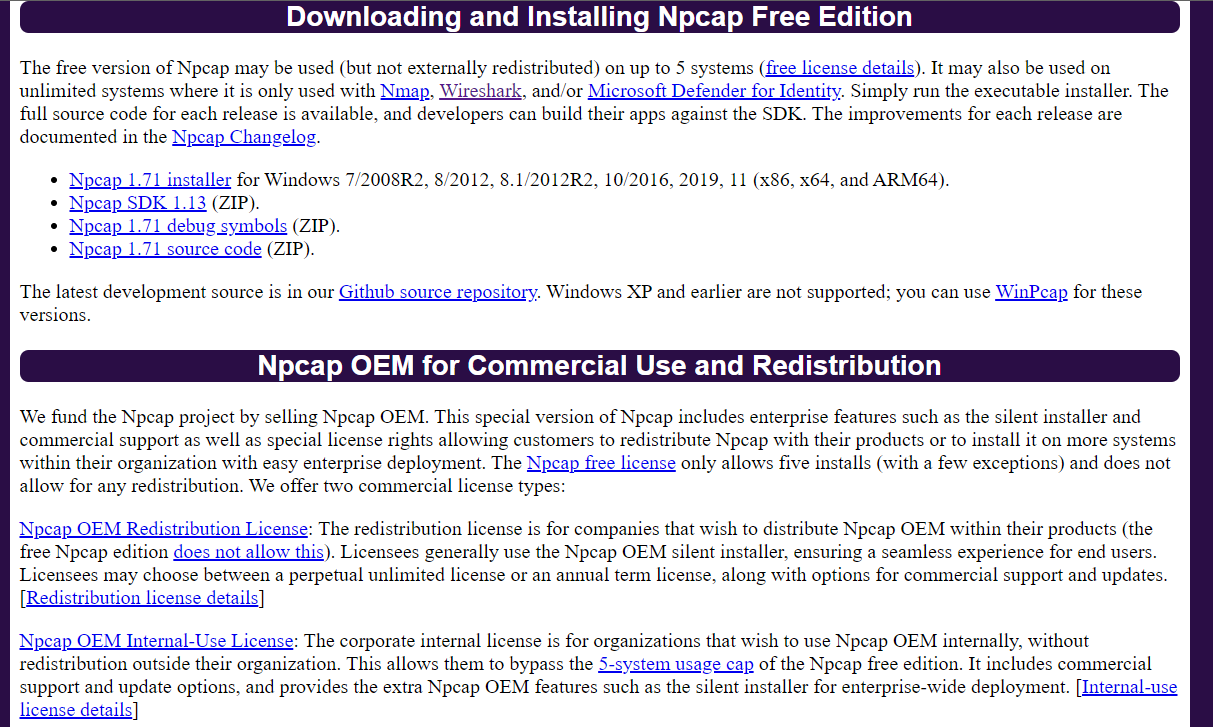
Activate network intrusion detection mode –

To start this mode use this command ./snort -dev -l ./SnortLogs -h 192.127.1.0/24 -c snort.conf

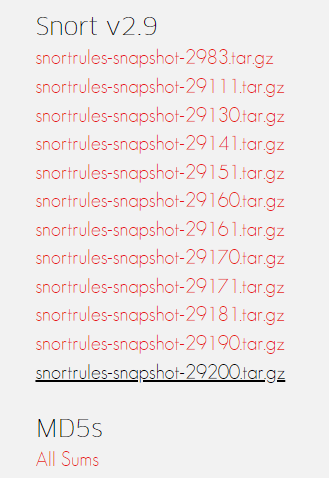
Procedure-

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

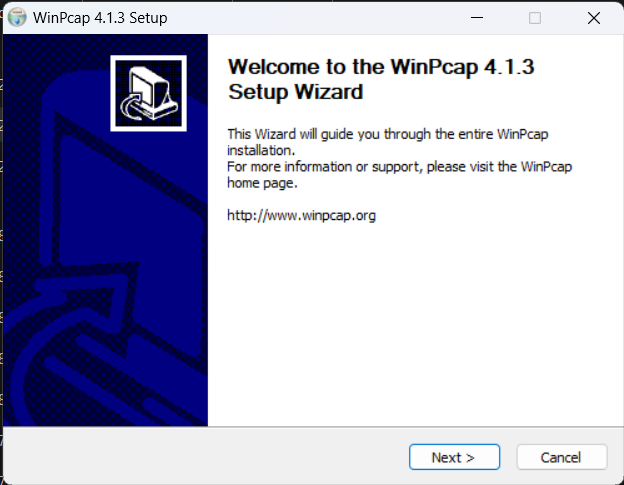


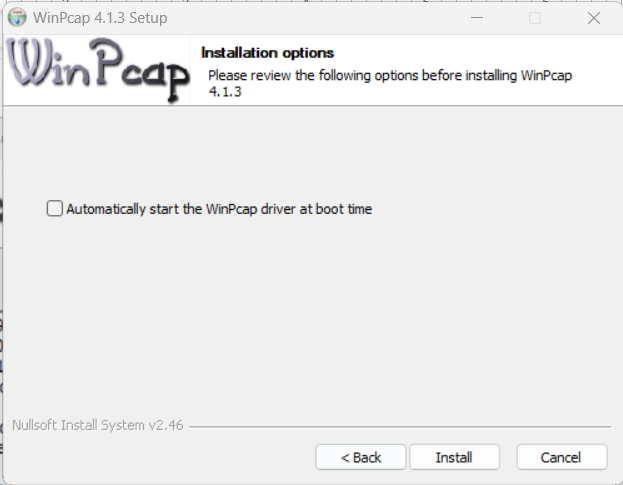
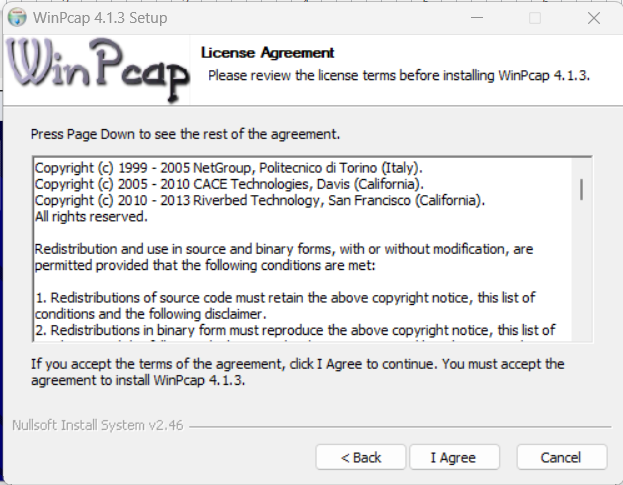


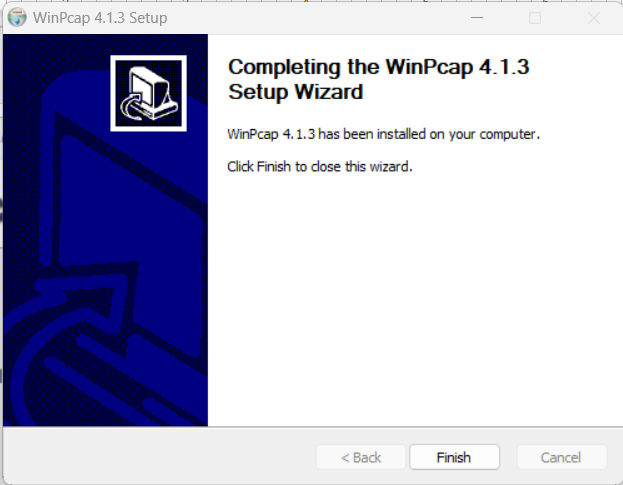


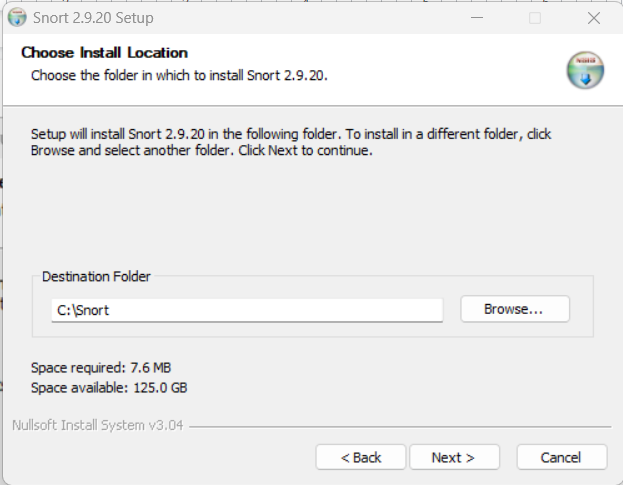
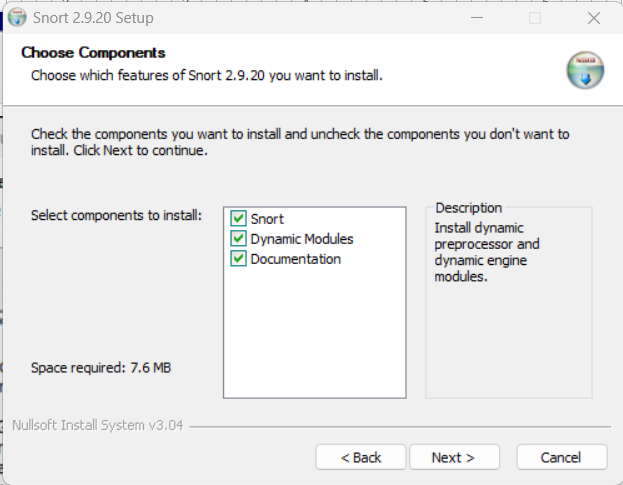
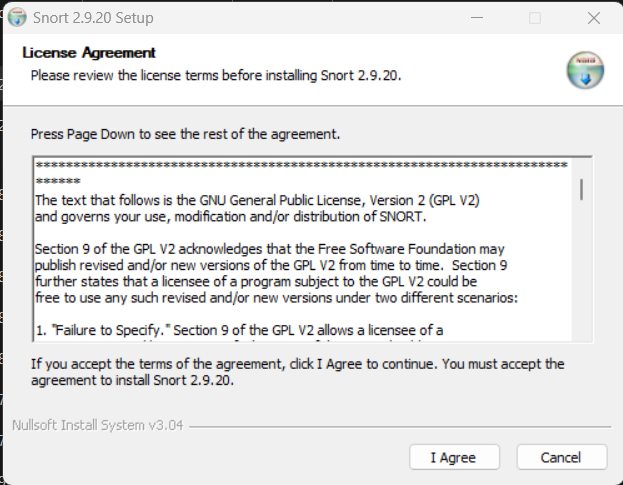


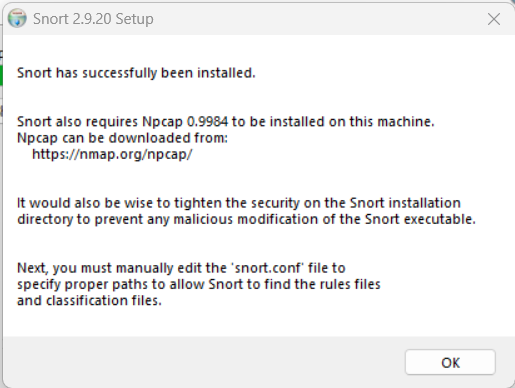
1. Install Snort, winpcap and npcap as shown below.



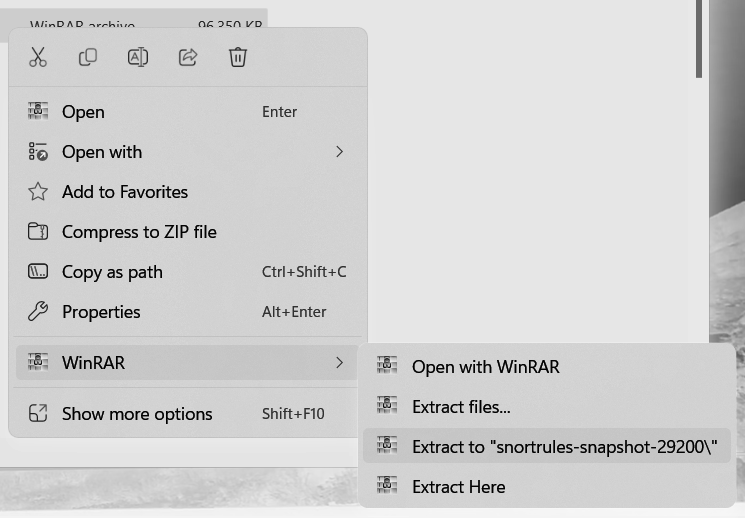


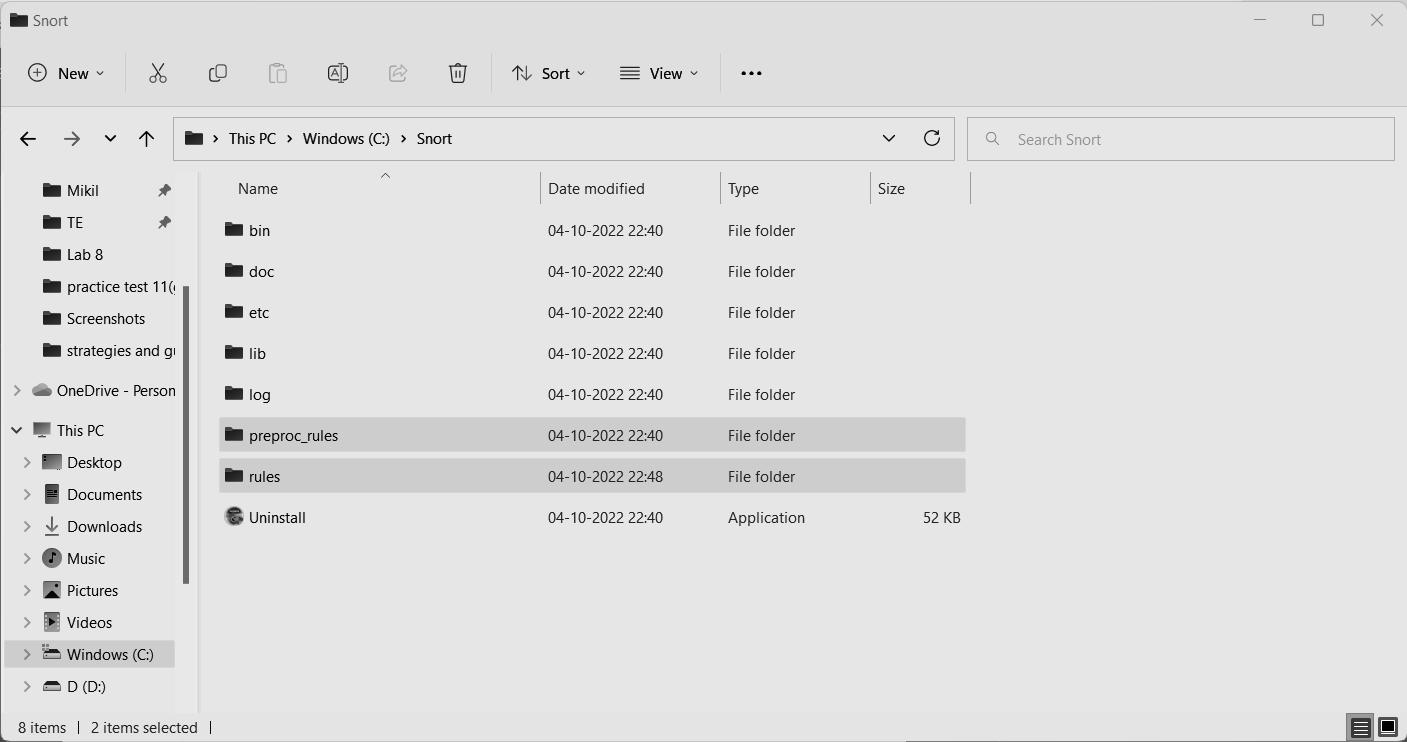
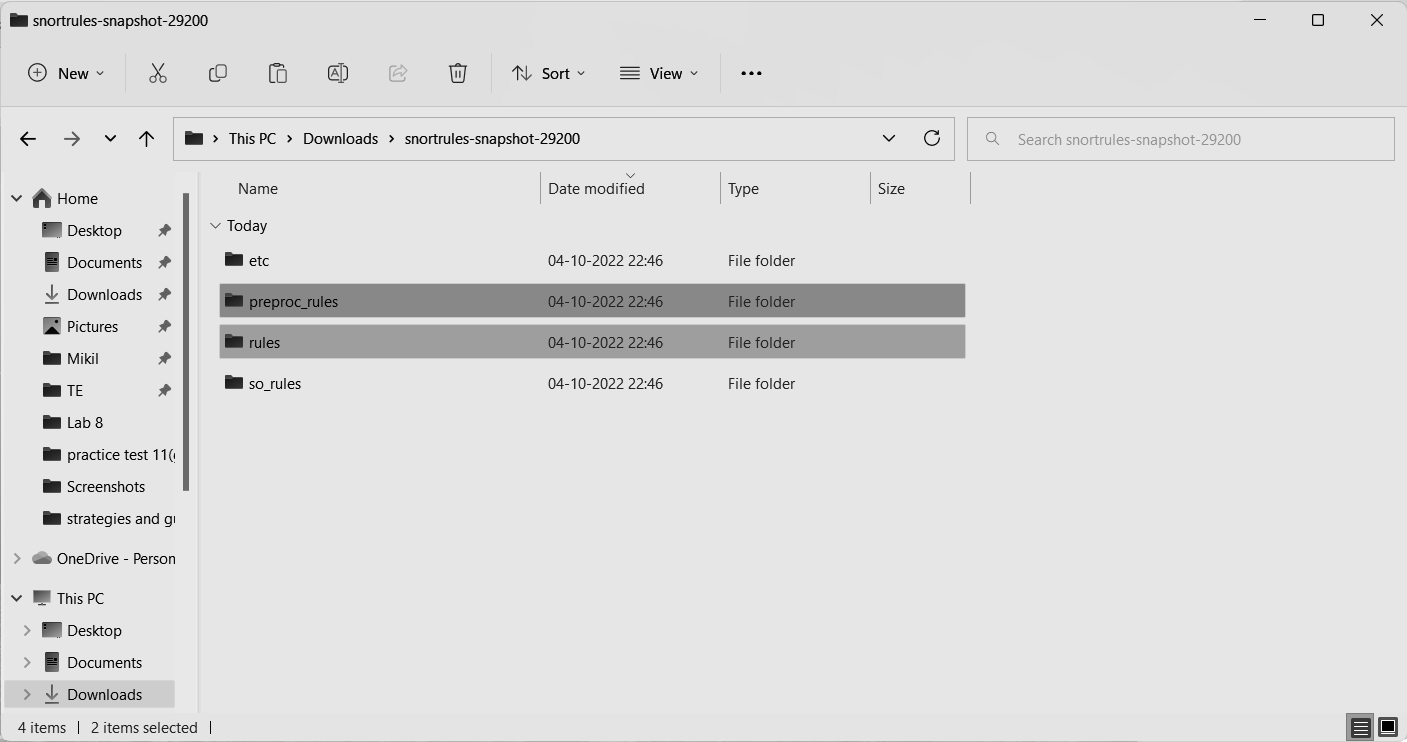




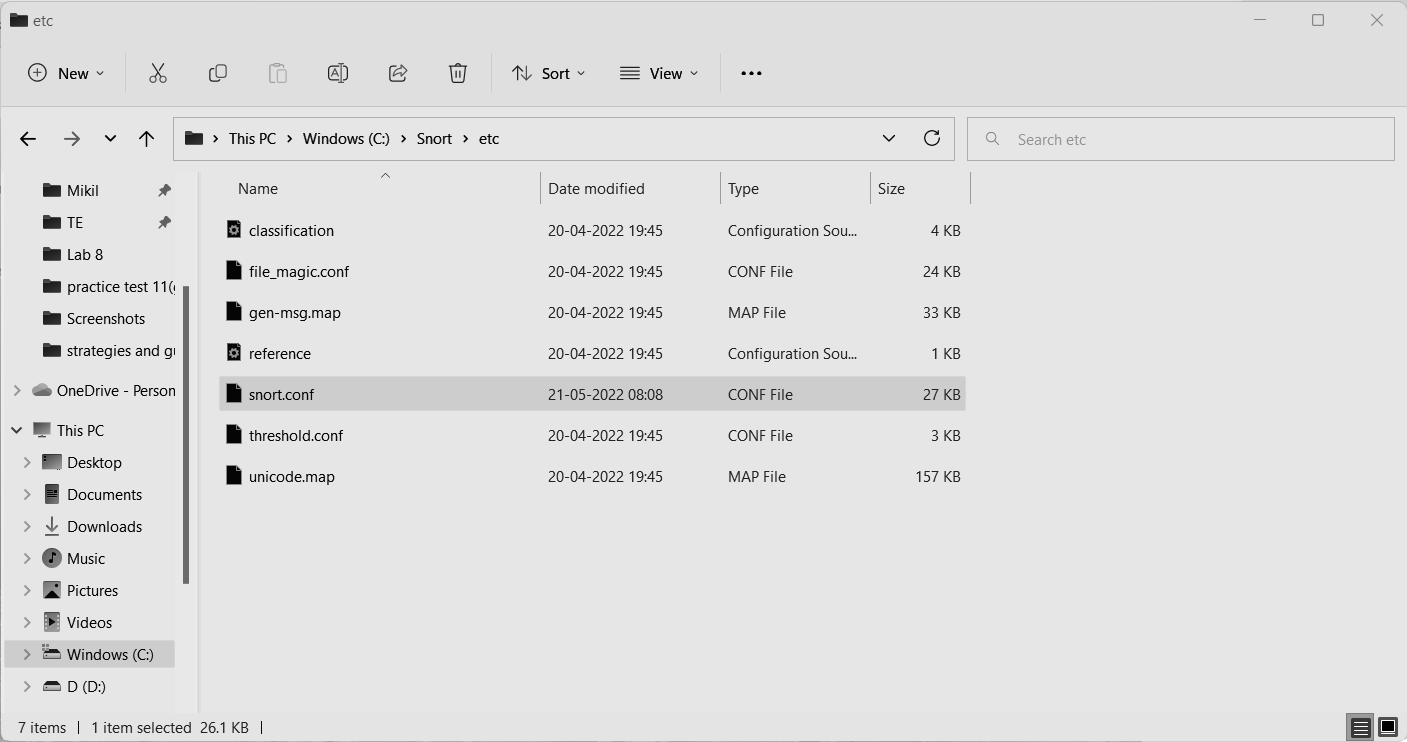


1. Extract snort rules and copy preproc\_rules and rules to C:/Snort/ .





1. Now we edit the config file.

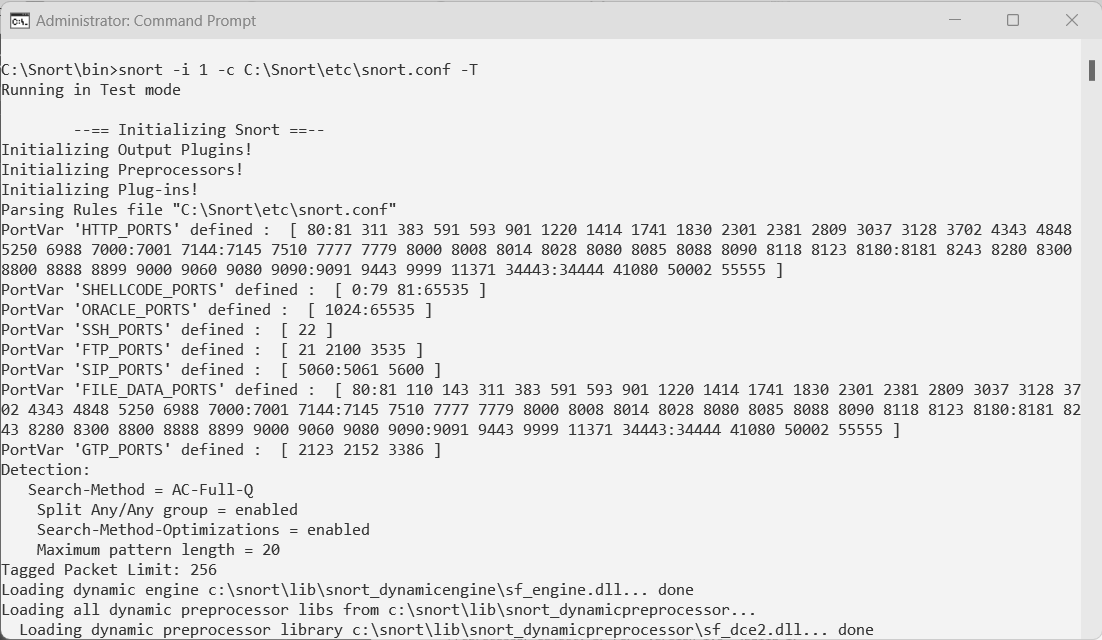


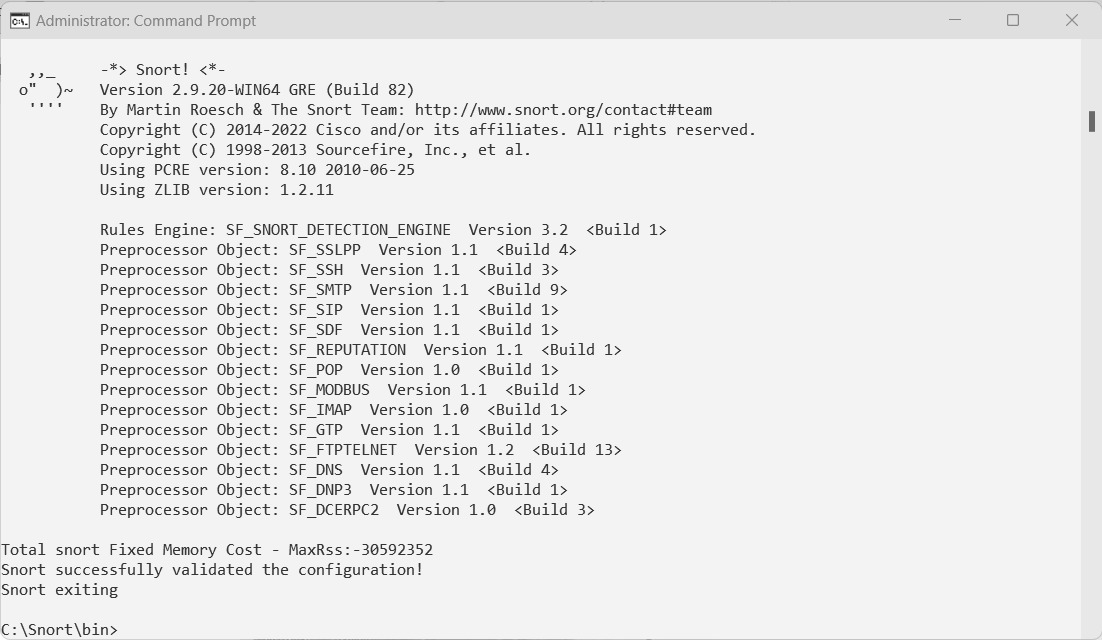
1. After installing Snort and Npcap enter these commands in the windows 10 Command prompt to check snorts working.
2. As you can see in the above figure that snort runs successfully
3. Check the wireless interface cards from which we will be using snort by using the command below.

snort -w

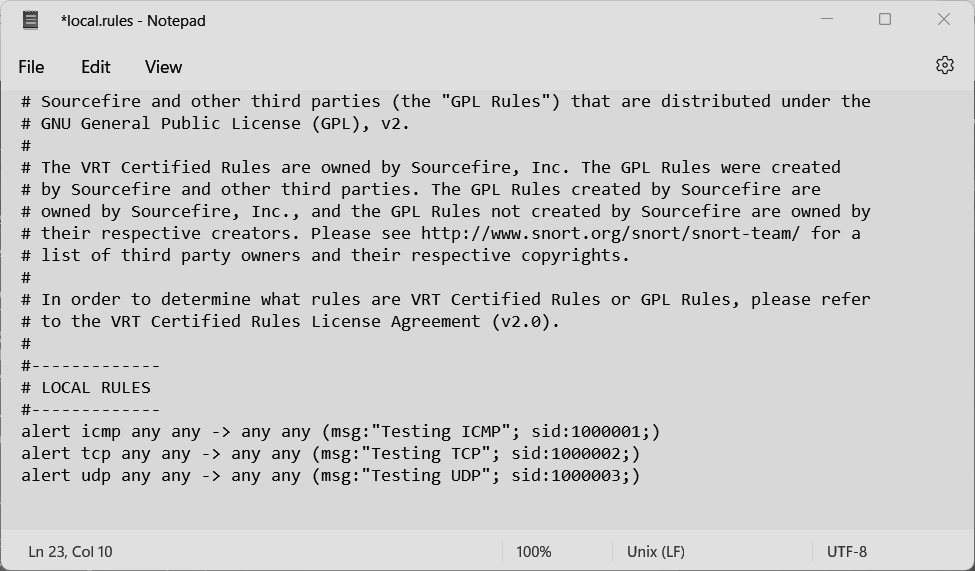
1. To check the validation of snort’s configuration by choosing a specific wireless interface card (1) the rest of the command shows the config file path. The command is:

snort -i 1 -c C:\Snort\etc\snort.conf -T





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.

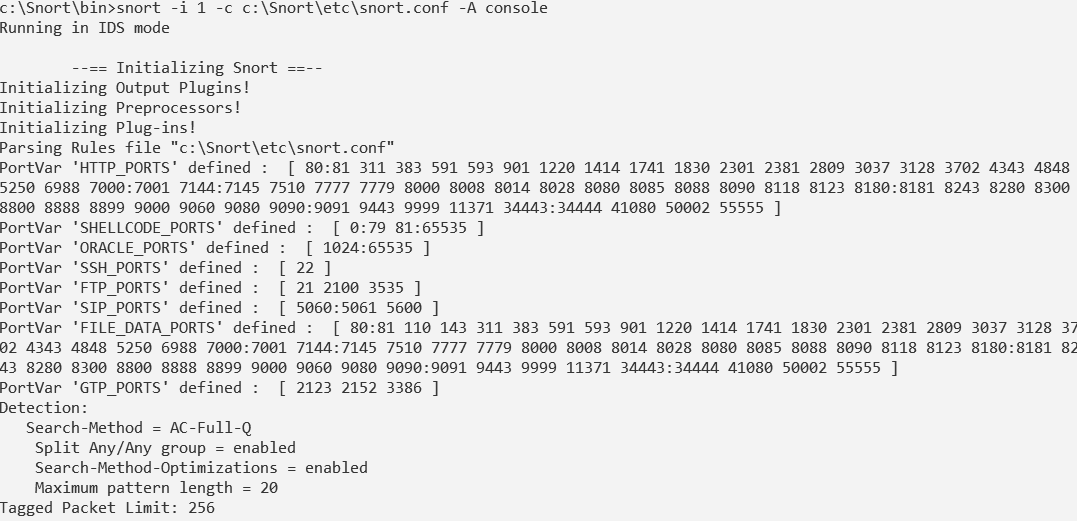


After adding the rules in the local.rules file the next thing is to run the following command **snort -i 3 -c c:\Snort\etc\snort.conf -A console**

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.





Conclusion-

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