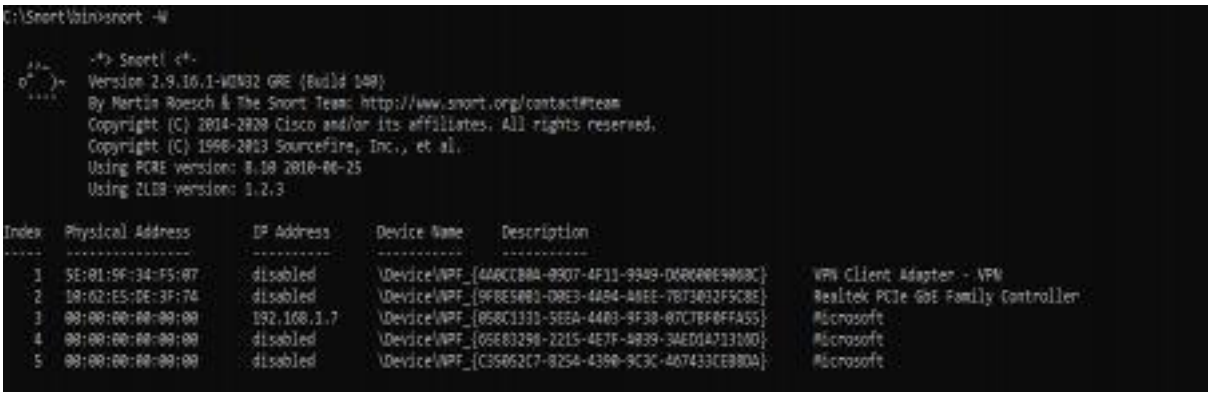
Ex. No : 9 Date:20/10/2020	Demonstration of Intrusion Detection System(IDS)

STEPS :

1. Download Snort from the Snort.org website. (http://www.snort.org/snort downloads)
2. Download Rules(https://www.snort.org/snort-rules). You must register to get the rules.
3. Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder.It is important to have WinPcap (https://www.winpcap.org/install/) installed
4. Extract the Rules file. You will need WinRAR for the .gz file. **5**. Copy all files from the "rules" folder of the extracted folder. Now paste the rules into *"C:\Snort\rules"* folder.
6. Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc" folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.
7. Open a command prompt (cmd.exe) and navigate to folder "C:\Snort\bin" folder. (at the Prompt, type cd\snort\bin)
8. To check the interface list, use following command:

```
snort -W
```

Finding an interface



You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are disabled. My interface is 3.

9. To run snort in IDS mode, you will need to configure the file "snort.conf" according to your network environment.
10. To specify the network address that you want to protect in snort.conf file, look for the following line.
var HOME_NET 192.168.1.0/24 (You will normally see any here)

11. Change the RULE_PATH variable to the path of rules folder.
var RULE_PATH c:\snort\rules
path to rules
12. Change the path of all library files with the name and path on your system. And you must change the path of **snort_dynamicpreprocessorvariable**.

C:\Snort\lib\snort_dynamiccpreprocessor
13. You need to do this to all library files in the "C:\Snort\lib" folder. The old path might be: "/usr/local/lib/…". you will need to replace that path with your system path. Using C:\Snort\lib
14. Change the path of the "**dynamicengine"** variable value in the "snort.conf" file..
Example:
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
15 Add the paths for "include classification.config" and "include reference.config" files.

include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
16. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.
include $RULE_PATH/icmp.rules
17. You can also remove the comment of ICMP-info rules comment, if it is

commented.
include $RULE_PATH/icmp-info.rules

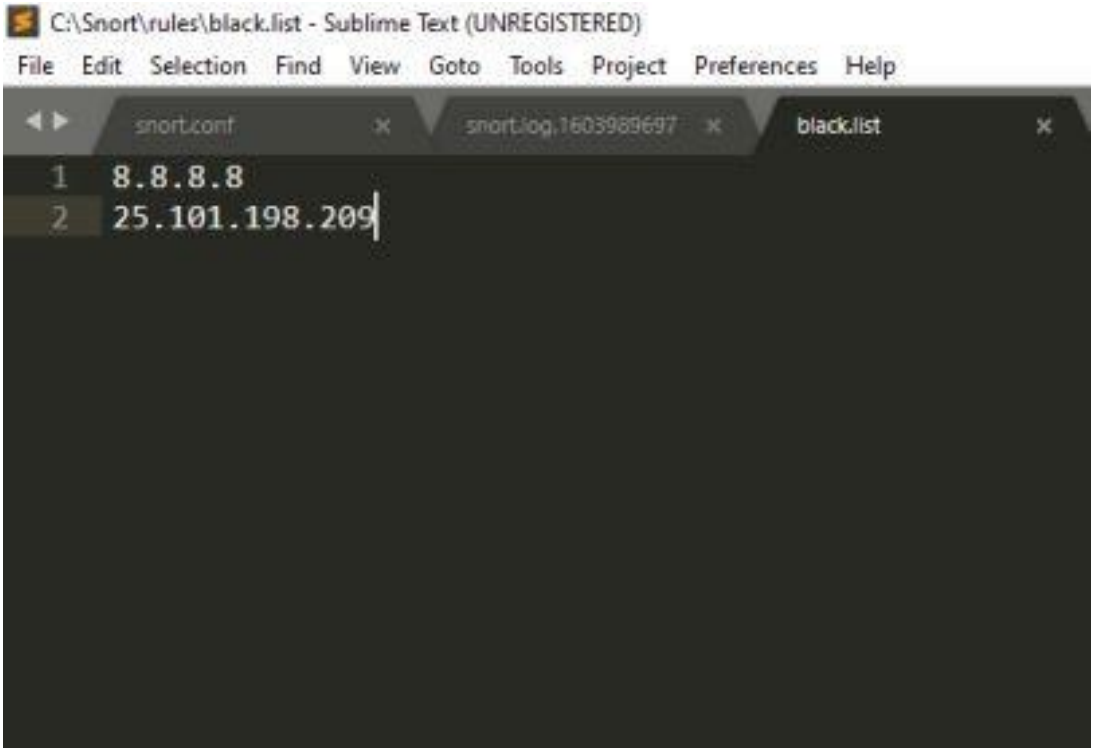
18. To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:

output alert_fast: snort-alerts.ids

19. Find $WHITE_LIST_PATH/white_list.rules and change it to white.list and similarly black_list.rules to black.list

Create white.list and black.list file in C:\Snort\rules.

Add the ip address that needs to be blacklisted in black.list file.



20. Comment out (#) following lines:

#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6

21. Save the “snort.conf” file.

22. To start snort in IDS mode, run the following command:

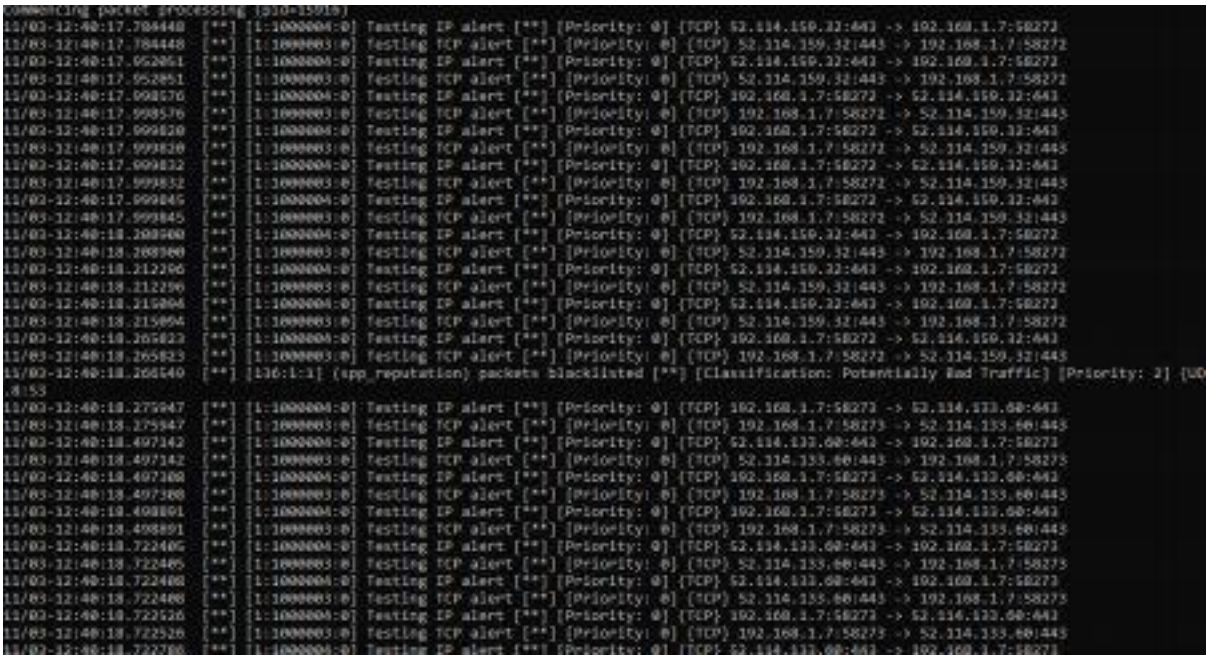
snort -i 3 -c C:\Snort\etc\snort.conf -A console

(Note: 3 is used for my interface card)

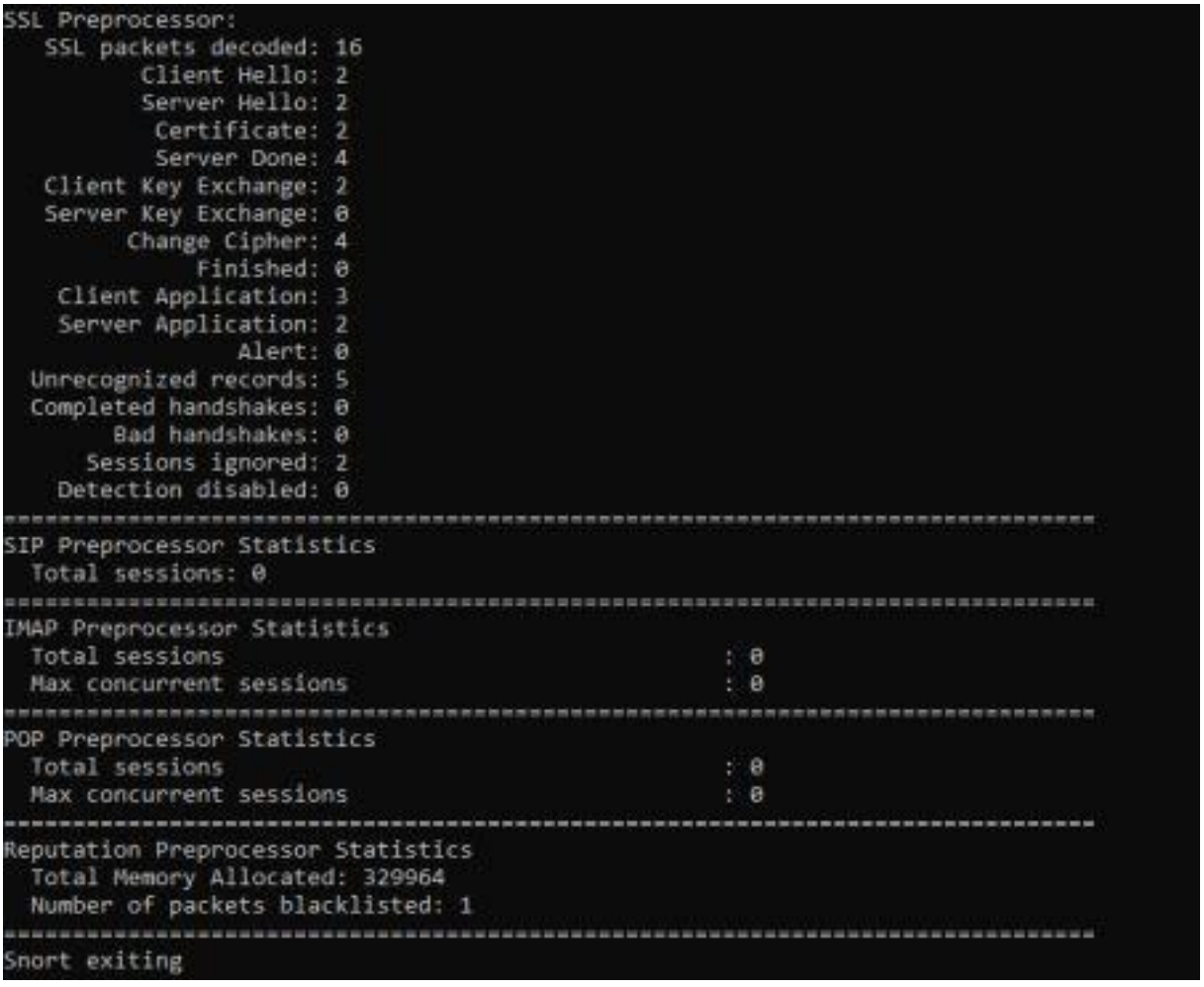
If a log is created, select the appropriate program to open it. You can use WordPard or NotePad++ to read the file.

To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

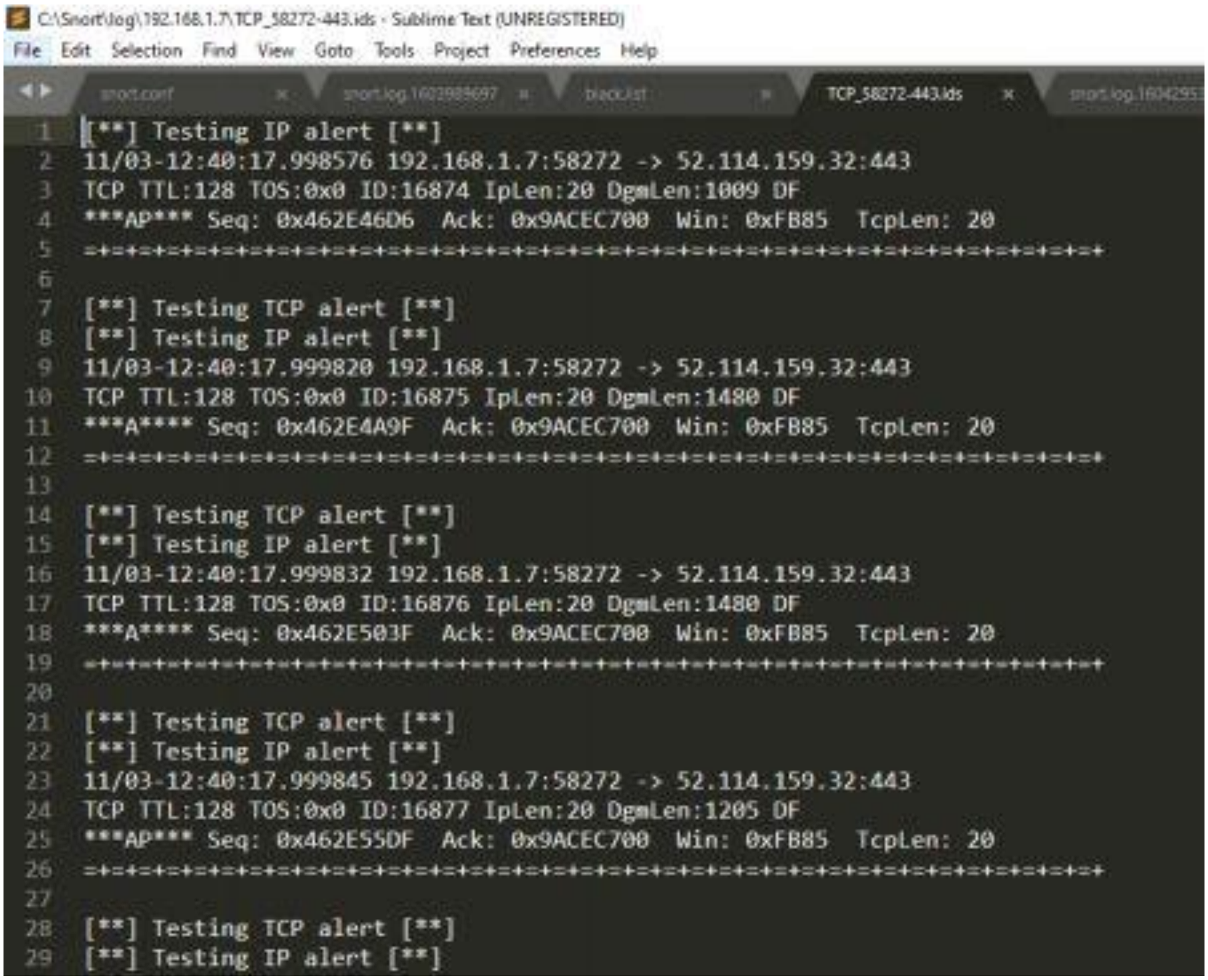
snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii



Snort monitoring traffic –



Log files--




```
[**] Testing IP alert [**]
11/03-12:40:17.998576 192.168.1.7:58272 -> 52.114.159.32:443
TCP TTL:128 TOS:0x0 ID:16874 IpLen:20 DgmLen:1009 DF
***AP*** Seq: 0x462E46D6  Ack: 0x9ACEC700  Win: 0xFB85  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] Testing TCP alert [**]
[**] Testing IP alert [**]
11/03-12:40:17.999820 192.168.1.7:58272 -> 52.114.159.32:443
TCP TTL:128 TOS:0x0 ID:16875 IpLen:20 DgmLen:1480 DF
***A**** Seq: 0x462E4A9F  Ack: 0x9ACEC700  Win: 0xFB85  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] Testing TCP alert [**]
[**] Testing IP alert [**]
11/03-12:40:17.999832 192.168.1.7:58272 -> 52.114.159.32:443
TCP TTL:128 TOS:0x0 ID:16876 IpLen:20 DgmLen:1480 DF
***A**** Seq: 0x462E503F  Ack: 0x9ACEC700  Win: 0xFB85  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] Testing TCP alert [**]
[**] Testing IP alert [**]
11/03-12:40:17.999845 192.168.1.7:58272 -> 52.114.159.32:443
TCP TTL:128 TOS:0x0 ID:16877 IpLen:20 DgmLen:1205 DF
***AP*** Seq: 0x462E55DF  Ack: 0x9ACEC700  Win: 0xFB85  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] Testing TCP alert [**]
[**] Testing IP alert [**]
```