

Using the software tools/commands to perform the following, generate an analysis report:

## A. Port Scanning.

### Nmap Tool:

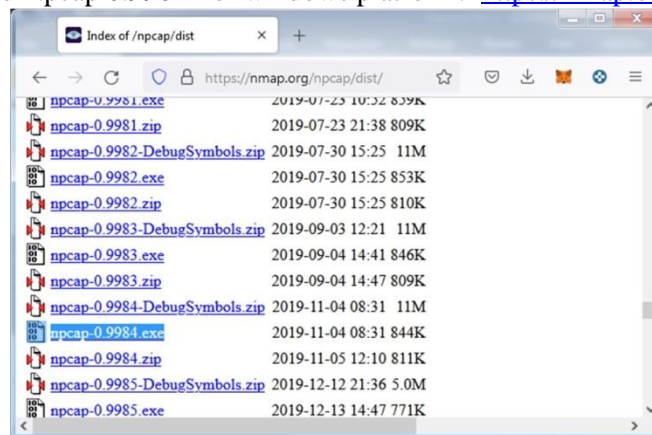
Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

Link to download nmap-7.92 for windows platform: <https://nmap.org/download.html>

The screenshot shows the 'nmap.org/download.html' page. It features a 'Subscribe to Nmap-hackers' button and a link to the 'Nmap-hackers list info page'. Below this, it mentions updates from Facebook and Twitter, and states that Nmap is distributed under the GNU General Public License. A section titled 'Microsoft Windows binaries' contains instructions for installing Nmap on Windows. It includes a note about the version of Npcap included in the installers and a link to the 'Latest Npcap release'. The page also provides links for the 'Latest stable release self-installer: nmap-7.92-setup.exe' and the 'Latest Npcap release self-installer: npcap-1.55.exe'. At the bottom, it mentions 'post-install usage instructions' and asks users to notify if they encounter any problems.

Nmap needs Npcap which is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

Link to download Npcap 0.9984 for windows platform: <https://nmap.org/npcap/dist/>



Note: We can use more command to display one screen of output at a time. Here use /E option and pass the other command output to more command using | (pipe) symbol.

Example: C:> dir | more/E

### Questions:

1. Display the following for ip address 127.0.0.1 or any other ip address

a. Scan open ports (syntax: nmap -open ip\_address / url )

```
C:\Users\Dell>nmap -open scanme.nmap.org | more /E
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 10:58 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)Host is up (0.25s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
```

b. Scan single port (syntax: nmap -p 80 ip\_address)

```
C:\Users\Dell>nmap -p 80 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:00 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds
```

c. Scan specified range of ports (syntax: nmap -p 1-200 ip\_address)

```
C:\Users\Dell>nmap -p 1-200 scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:02 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 198 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 8.28 seconds
```

d. Scan entire port range (syntax: nmap -p 1-65535 ip\_address)

```

C:\>nmap -p 1-65535 scanme.nmap.org ! more /E
Starting Nmap 7.92 ( https://nmap.org ) at 2021-10-03 16:21 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Nmap done: 1 IP address (1 host up) scanned in 1112.15 seconds

```

- e. Scan top 100 ports (fast scan) (syntax: nmap -F ip\_address )

```

C:\Users\Dell>nmap -F scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:13 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 98 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 8.08 seconds

```

## B. Network Scanning Tools

### Nmap Tool:

Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

### Questions:

- a. Demonstrate how to scan networks. Explain the steps and attach output.

1. **Ping Scan** – It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further. Syntax: nmap -sP

```

C:\Users\Dell>nmap -sP www.techpanda.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:14 India Standard Time
Nmap scan report for www.techpanda.org (72.52.251.71)
Host is up (0.22s latency).
rDNS record for 72.52.251.71: host.moneyboats.com
Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds

```

2. **Host Scan** – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network. Syntax: `nmap -sP`

```
C:\Users\Dell>nmap -sP 72.52.251.71
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:15 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Host is up (0.21s latency).
Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
```

3. If you see anything unusual in this list, you can then run a DNS query on a specific host, by using: Syntax: `nmap -sL`

```
C:\Users\Dell>nmap -sL 72.52.251.71
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:16 India Standard Time
Nmap scan report for host.moneyboats.com (72.52.251.71)
Nmap done: 1 IP address (0 hosts up) scanned in 6.59 seconds
```

This returns a list of names associated with the scanned IP. This description provides information on what the IP is actually for.

4. **OS Scan** – This command return information on the OS (and version) of a host. Syntax: `nmap -O`

```
C:\Users\Dell>nmap -O scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-10 11:18 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (96%), OpenWrt White Russian 0.9 (Linux 2.4.30) (96%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (96%), DD-WRT v24-sp1 (Linux 2.4.36) (96%), Asus RT-AC66U router (Linux 2.6) (94%), Asus RT-N16 WAP (Linux 2.6) (94%), Asus RT-N66U WAP (Linux 2.6) (94%), Tomato 1.28 (Linux 2.6.22) (94%), Linux 2.4.18 (94%), Linux 3.5 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 23 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.83 seconds
```

## C. IDS Tool

Snort IDS Tool:



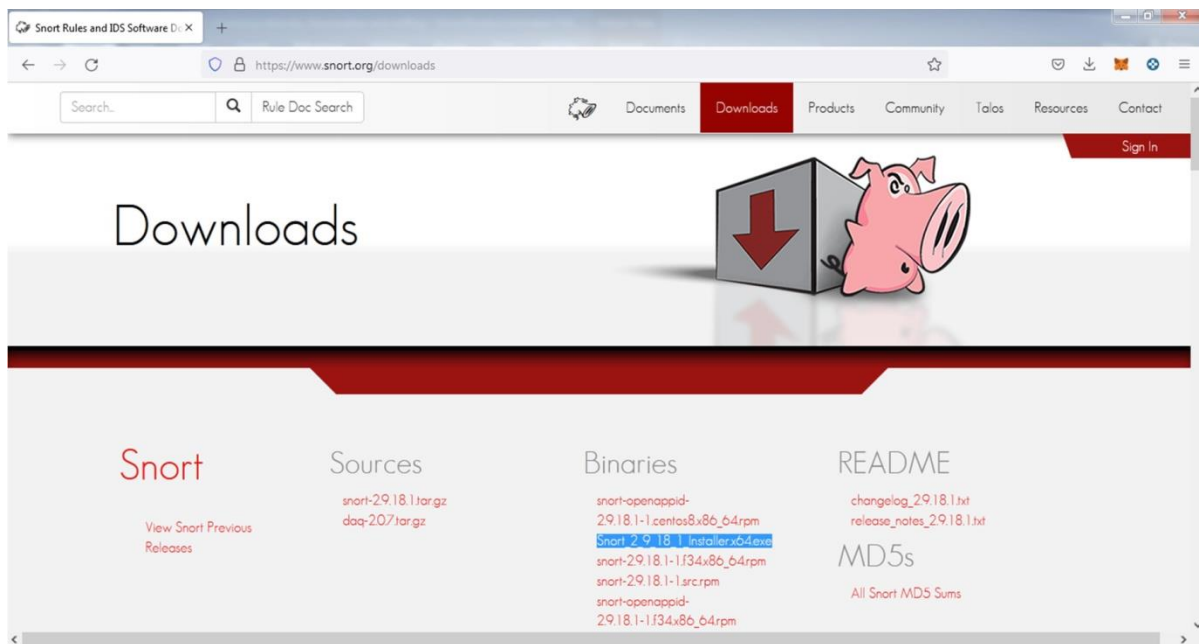
Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS). Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be configured in three main modes:

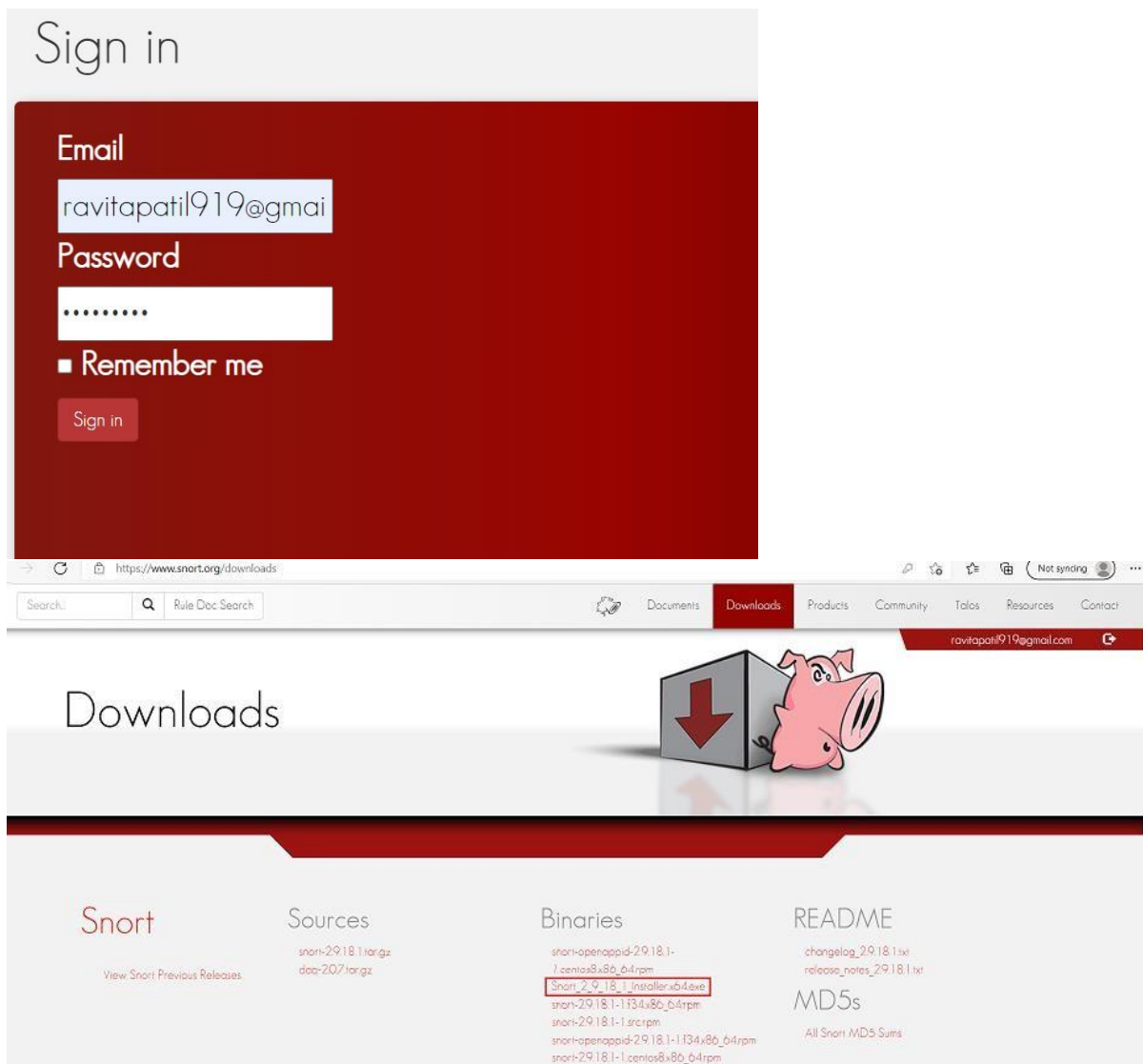
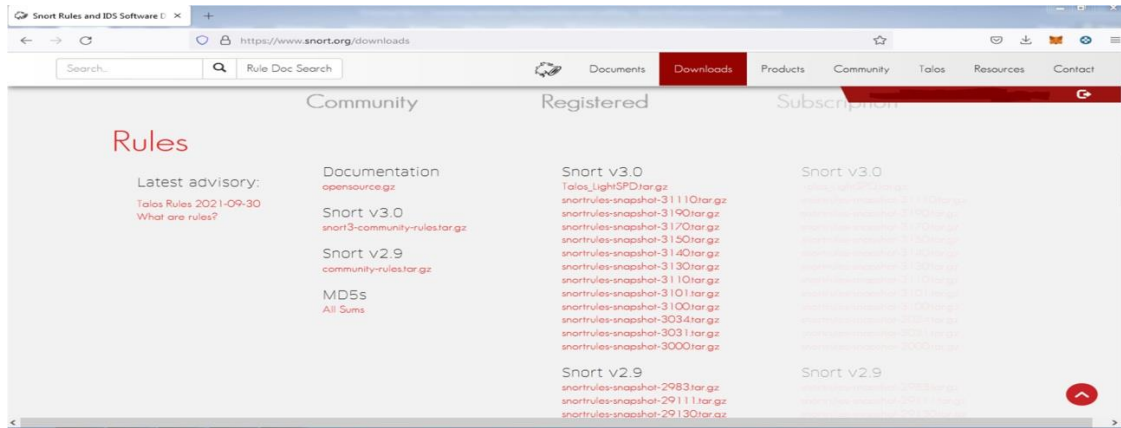
- 1. Sniffer Mode:** The program will read network packets and display them on the console.
- 2. Packet Logger Mode:** The program will log packets to the disk.
- 3. Network Intrusion Detection System Mode:** The program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Link to download Snort\_2.9.18.1\_Installer.x64.exe for Windows Platform:

<https://www.snort.org/download>

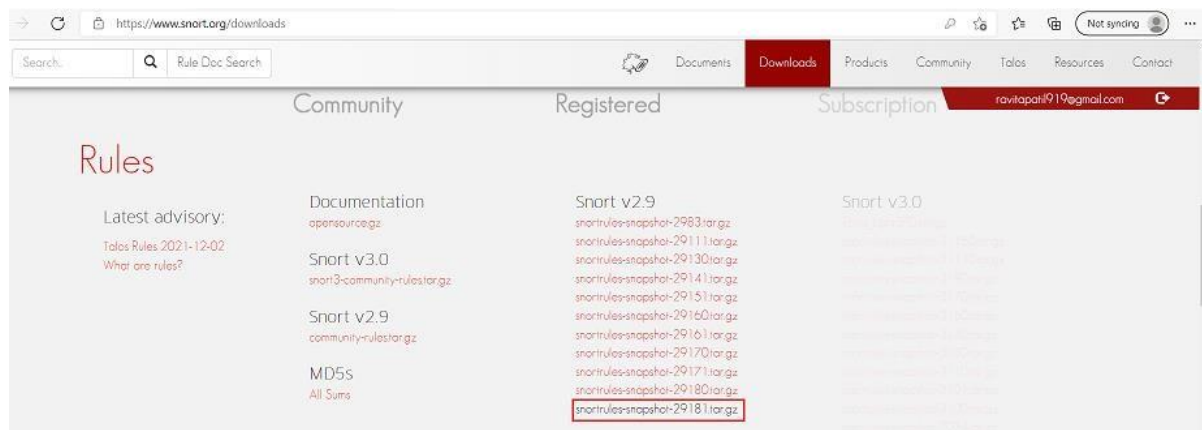


Link to download the rules for snort: <https://www.snort.org/download> You can Sign up to snort to get more detailed rules.



**Link to download the rules for snort:**

<https://www.snort.org/download>



You can Sign up to snort to get more detailed rules.

#### Questions:

a. How snort works. Explain with steps and demonstrate various modes of snort.

Steps to defend your network with Snort for Windows:

Snort should be a dedicated computer in your network. This computer's logs should be reviewed often to see malicious activities on your network.

1. Download Snort from the Snort.org website.
2. Download Rules from Snort.org website. You must register to get the rules. (You should download these often) <https://snort.org/downloads>
3. Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder.

It is important to have npcap or WinPcap installed

4. Extract the Rules file. You will need WinRAR for the .gz file.

snortrules-snapshot-29181.tar.gz (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan

↑ snortrules-snapshot-29181.tar.gz - TAR+GZIP archive, unpacked size 671,286,887 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
etc	8,280,595	?	File folder	02-12-2021 01:...	
preproc_rules	75,143	?	File folder	02-12-2021 01:...	
rules	31,244,942	?	File folder	02-12-2021 01:...	
so_rules	631,686,207	?	File folder	30-11-2021 01:...	

↑ snortrules-snapshot-29181.tar.gz\rules - TAR+GZIP archive, unpacked size 671,286,887 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
app-detect.rules	67,532	?	RULES File	02-12-2021 01:...	
attack-responses...	1,061	?	RULES File	02-12-2021 01:...	
backdoor.rules	1,037	?	RULES File	02-12-2021 01:...	
bad-traffic.rules	1,046	?	RULES File	02-12-2021 01:...	
blacklist.rules	1,040	?	RULES File	02-12-2021 01:...	
botnet-cnc.rules	1,043	?	RULES File	02-12-2021 01:...	
browser-chrome....	68,791	?	RULES File	02-12-2021 01:...	
browser-firefox.r...	158,317	?	RULES File	02-12-2021 01:...	
browser-ie.rules	1,690,295	?	RULES File	02-12-2021 01:...	
browser-other.ru...	42,428	?	RULES File	02-12-2021 01:...	
browser-plugins....	1,563,552	?	RULES File	02-12-2021 01:...	

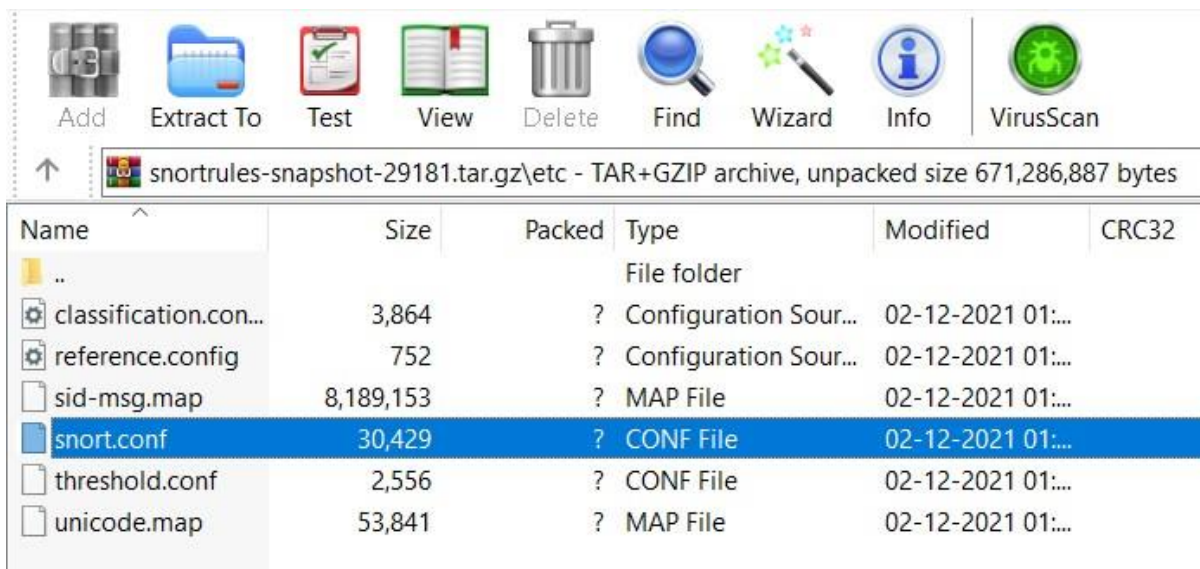
5. Copy all files from the “rules” folder of the extracted folder. Now paste the rules into “C:\Snort\rules” folder.

This PC > Local Disk (C:) > Snort > rules

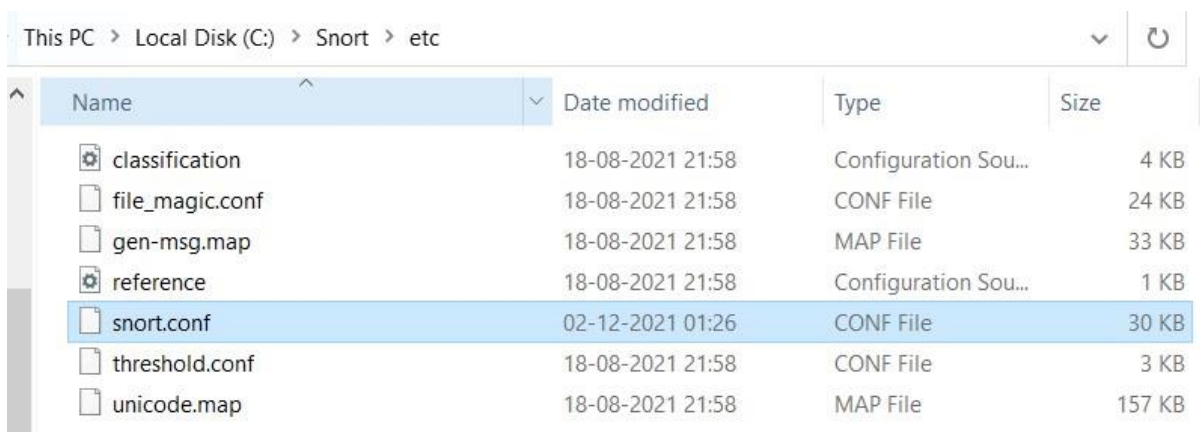
Name	Date modified	Type	Size
app-detect.rules	02-12-2021 01:28	RULES File	66 KB
attack-responses.rules	02-12-2021 01:28	RULES File	2 KB
backdoor.rules	02-12-2021 01:28	RULES File	2 KB
bad-traffic.rules	02-12-2021 01:28	RULES File	2 KB
blacklist.rules	02-12-2021 01:28	RULES File	2 KB
botnet-cnc.rules	02-12-2021 01:28	RULES File	2 KB

6. Copy “snort.conf” file from the “etc” folder of the extracted folder. You must paste it

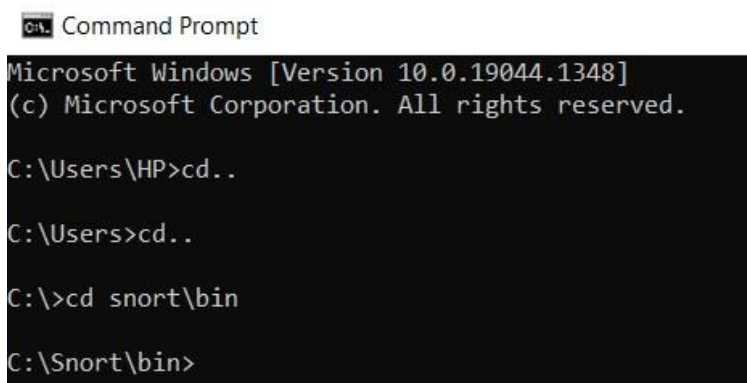




into “C:\Snort\etc” folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.



7. Open a command prompt (cmd.exe) and navigate to folder “C:\Snort\bin” folder. ( at the Prompt, type cd\snort\bin)



8. To start (execute) snort in sniffer mode use following command:  
snort -dev -i 3

-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.

-dev is used to run snort to capture packets on your network.

```

C:\Snort\bin>snort -dev -i 3
Running in packet dump mode

    === Initializing Snort ===
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{E11E5DD0-AABE-4023-A7F2-C4C20D797A64}".
Decoding Ethernet

    === Initialization Complete ===

    ,,-
    o" )~
    ' ' '
    -*> Snort! <*-
      Version 2.9.18.1-WIN64 GRE (Build 1005)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2021 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

Commencing packet processing (pid=15384)
```

Command Prompt

Commencing packet processing (pid=15384)

\*\*\* Caught Int-Signal

Run time for packet processing was 116.925000 seconds

Snort processed 0 packets.

Snort ran for 0 days 0 hours 1 minutes 56 seconds

Pkts/min: 0

Pkts/sec: 0

Packet I/O Totals:

Received: 0

Analyzed: 0 ( 0.000%)

Dropped: 0 ( 0.000%)

Filtered: 0 ( 0.000%)

Outstanding: 0 ( 0.000%)

Injected: 0

Breakdown by protocol (includes rebuilt packets):

Eth: 0 ( 0.000%)

VLAN: 0 ( 0.000%)

IP4: 0 ( 0.000%)

Frag: 0 ( 0.000%)

ICMP: 0 ( 0.000%)

UDP: 0 ( 0.000%)

TCP: 0 ( 0.000%)

Command Prompt

All Discard: 0 ( 0.000%)

Other: 0 ( 0.000%)

Bad Chk Sum: 0 ( 0.000%)

Bad TTL: 0 ( 0.000%)

S5 G 1: 0 ( 0.000%)

S5 G 2: 0 ( 0.000%)

Total: 0

Memory Statistics for File at: Fri Dec 3 11:17:42 2021

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: 0 bytes

No of allocs: 0

No of frees: 0

Snort exiting

9. To check the interface list, use following command:

**snort -W**

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

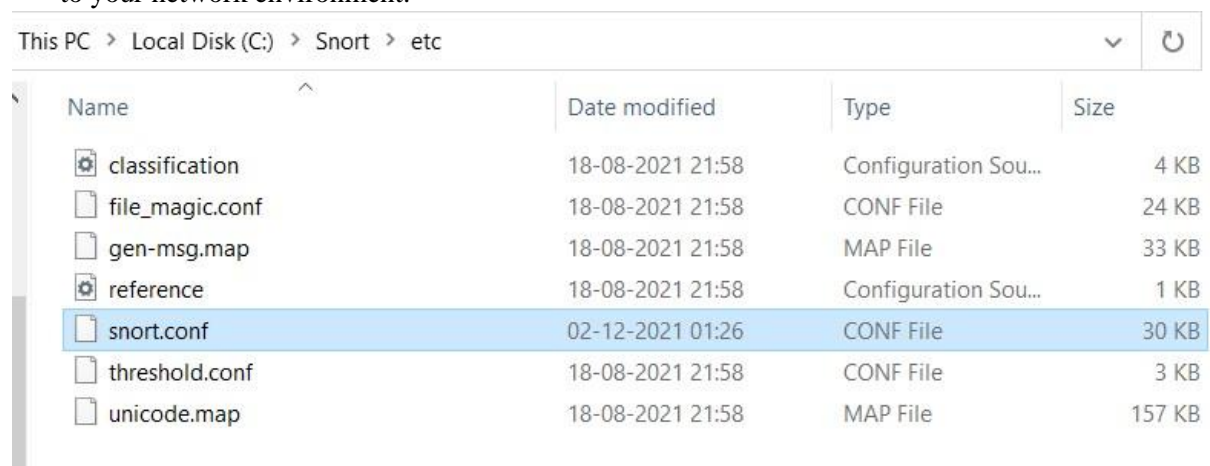
--_
o" )~
'---

-*> Snort! <*-
Version 2.9.18.1-WIN64 GRE (Build 1005)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2021 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_{D52B3C98-1CD2-4DFB-A6E0-0CA2D4BC5C76}      WAN Miniport (Ne
network Monitor)
2  00:00:00:00:00:00      disabled      \Device\NPF_{B567E815-69FC-4341-8531-56D598EBF2F6}      WAN Miniport (IP
v6)
3  00:00:00:00:00:00      disabled      \Device\NPF_{E11E5DD0-AABE-4023-A7F2-C4C20D797A64}      WAN Miniport (IP
)
4  80:91:33:65:60:3B      0000:0000:fe80:0000:0000:0000:2cc4:a4d0 \Device\NPF_{9C3D8143-4EE9-483F-ADDF-8821D660AFC}      Realtek RTL8723DE 802.11b/g/n PCIe Adapter
5  80:91:33:65:60:3B      0000:0000:fe80:0000:0000:0000:85a7:7f45 \Device\NPF_{67F038A2-5ACC-4414-8B81-B0DA0523A42}      Microsoft Wi-Fi Direct Virtual Adapter #2
6  82:91:33:65:60:3B      0000:0000:fe80:0000:0000:0000:319e:936f \Device\NPF_{A4373AD9-B39E-49AC-B01E-8BC4FBA7035}      Microsoft Wi-Fi Direct Virtual Adapter
7  02:00:4C:4F:4F:50      0000:0000:fe80:0000:0000:0000:59ea:aed5 \Device\NPF_{06A57EC8-F10F-4A1D-BF91-13D32B152A1}      Npcap Loopback Adapter
1}
```

10. 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 for VMWare. My interface is 3.

11. To run snort in IDS mode, you will need to configure the file “snort.conf” according to your network environment.



12. 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)





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

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24 |
```

13. You may also want to set the addresses of DNS\_SERVERS, if you have some on your network. Example:

```
File Edit Format View Help
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24

# 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 192.168.1.1

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

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

14. Change the RULE\_PATH variable to the path of rules folder. **var RULE\_PATH**  
**c:\snort\rules**





snort.conf - Notepad

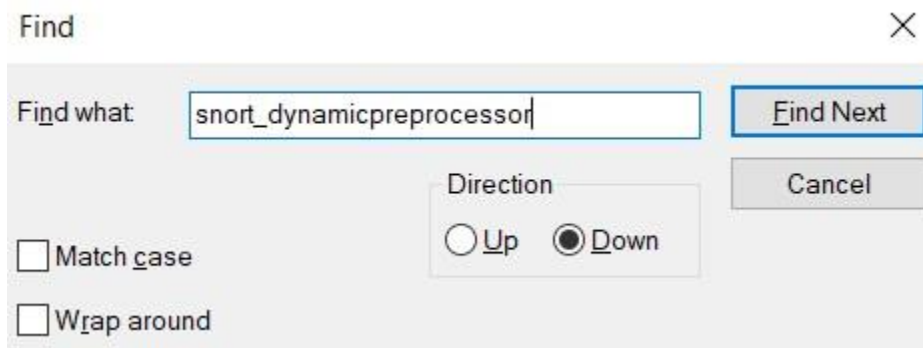
File Edit Format View Help

```
# 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.

# 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 ../preproc_rules
```

15. Change the path of all library files with the name and path on your system. and you must change the path of snort\_dynamicpreprocessor variable.

**C:\Snort\lib\snort\_dynamicpreprocessor**



File Edit Format View Help

```
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
#####

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



# path to base preprocessor engine
dynamicengine /usr/local/lib/snort_dynamicengine/libsfc_engine.so

# path to dynamic rules libraries (Shared Object (SO) Rules)
# Set this path to where the compiled *.so binaries are installed
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

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


This PC > Local Disk (C:) > Snort > lib > snort\_dynamicpreprocessor

Name	Date modified	Type	Size
 sf_dce2.dll	19-08-2021 04:37	Application extens...	203 KB
 sf_dnp3.dll	19-08-2021 04:37	Application extens...	33 KB

16. Change the path of the “dynamicengine” variable value in the “snort.conf” file..

Example: dynamicengine C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll

This PC > Local Disk (C:) > Snort > lib > snort\_dynamicengine

Name	Date modified	Type	Size
 sf_engine.dll	19-08-2021 04:38	Application extens...	77 KB

Find

Find what:

Direction: ☐ Up ☒ Down

☐ Match case

☐ Wrap around

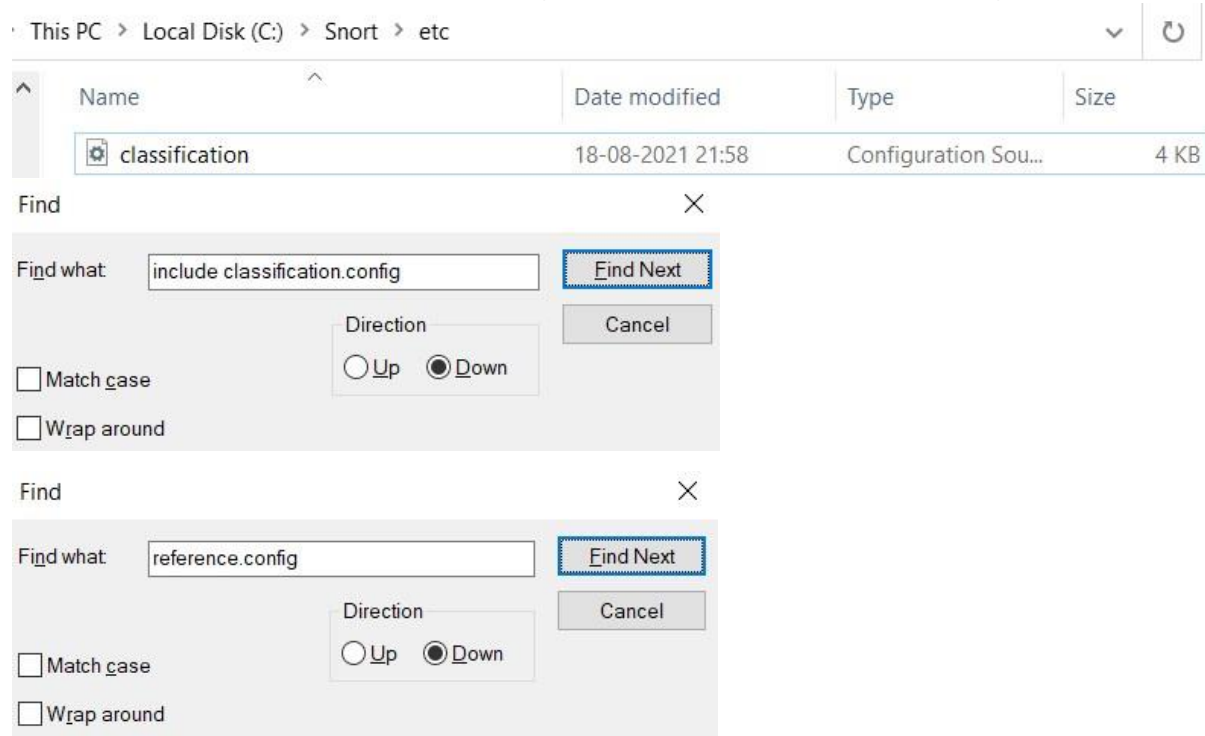
```
File Edit Format View Help
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
#####

# 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 (Shared Object (SO) Rules)
# Set this path to where the compiled *.so binaries are installed
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
```

17. Add the paths for “include classification.config” and “include reference.config” files.  
include c:\Snort\etc\classification.config include c:\Snort\etc\reference.config



```
File Edit Format View Help
# metadata reference data. do not modify these lines
include C:\Snort\etc\classification.config
include C:\Snort\etc\reference.config
```

18. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.  
include \$RULE\_PATH/icmp.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-scan.rules
```

19. You can also remove the comment of ICMP-info rules comment, if it is commented.

**include \$RULE\_PATH/icmp-info.rules**



snort.conf - Notepad

File Edit Format View Help

```
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
```

20. 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**

```
snort.conf - Notepad
File Edit Format View Help
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
# output alert_syslog: LOG_AUTH LOG_ALERT
output alert_fast: snort-alerts.ids

# pcap
# output log_tcpdump: tcpdump.log
```

21. Comment (add a #) the whitelist \$WHITE\_LIST\_PATH/white\_list.rules and the blacklist **Change the nested\_ip inner , \ to nested\_ip inner #, \**

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

22. Comment out (#) following lines:

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

```
snort.conf - Notepad
File Edit Format View Help

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

23. Save the “snort.conf” file.



24. To start snort in IDS mode, run the following command: **snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3**

```
Administrator: Command Prompt
C:\Snort\bin>snort -c c:\snort\etc\snort.conf -l c:\snort\log -i 3
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 : [ 36 80:90 311 383 443 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 1741 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3443 3702 4000 4343 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 6080 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082 8085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8694 8787 8800 8852 8880 8888 8899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9700 9710 9788 9830 9850 9999:10000 10080 10100 10250 10255 10297 10443 11371 12601 13014 14592 15489 16000 16992:16995 17000 18081 19980 29991 30007 30018 30888 33300 34412 34443:34444 36099 40007 41080 44449 49152:49153 50000 50002 50452 51423 53331 54444 55252 55555 56712 ]
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 : [ 36 80:90 110 143 311 383 443 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 1741 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3443 3702 4000 4343 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 6080 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082 8085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8694 8787 8800 8852 8880 8888 8899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9700 9710 9788 9830 9850 9999:10000 10080 10100 10250 10255 10297 10443 11371 12601 13014 14592 15489 16000 16992:16995 17000 18081 19980 ]
```

(Note: 3 is used for my interface card)

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

```
snort - Notepad
File Edit Format View Help
#-----
# VRT Rule Packages Snort.conf
#
# For more information visit us at:
# http://www.snort.org Snort Website
# http://vrt-blog.snort.org/ Sourcefire VRT Blog
**
```

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**

```
Administrator: Command Prompt

C:\Snort\bin>snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
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 : [ 36 80:90 311 383 443 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1
533 1581 1719:1720 1741 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3443 3702 4
000 4343 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 6080 6173 6988 7
000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082 8
085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8694 8787 8800 8
852 8880 8888 8899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9700 9710 9788 9830 9850 9999:1
0000 10080 10100 10250 10255 10297 10443 11371 12601 13014 14592 15489 16000 16992:16995 17000 18081 19980 29991 30007 3
0018 30888 33300 34412 34443:34444 36099 40007 41080 44449 49152:49153 50000 50002 50452 51423 53331 54444 55252 55555 5
6712 ]
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 : [ 36 80:90 110 143 311 383 443 555 591 593 623 631 664 801 808 818 901 972 1158 122
0 1270 1414 1533 1581 1719:1720 1741 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 312
8 3443 3702 4000 4343 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 608
0 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 804
0 8080:8082 8085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 869
4 8787 8800 8852 8880 8888 8899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9700 9710 9788 983
0 9850 9999:10000 10080 10100 10250 10255 10297 10443 11371 12601 13014 14592 15489 16000 16992:16995 17000 18081 19980 ]
```

25. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Note: if it gives an error message add comment (#) for following lines in snort.config file.

```
decompress_swf { deflate lzma } \
```

```
decompress_pdf { deflate }
```

```
File Edit Format View Help
webroot no \
#decompress_swf { deflate lzma} \
#decompress_pdf { deflate }
```

Snort monitoring traffic – Snort’s detailed report when scanning has stopped – Log files – We can also view log files.

```
Command Prompt
C:\Snort\bin>snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
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 : [ 36 80:90 311 383 443 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1
533 1581 1719:1720 1741 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2980 3000 3029 3037 3057 3128 3443 3702 4
000 4343 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 6080 6173 6988 7
000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7770 7777:7779 8000:8001 8008 8014:8015 8020 8028 8040 8080:8082 8
085 8088 8090 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8694 8787 8800 8
852 8880 8888 8899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9700 9710 9788 9830 9850 9999:1
0000 10080 10100 10250 10255 10297 10443 11371 12601 13014 14592 15489 16000 16992:16995 17000 18081 19980 29991 30007 3
```

## D. Sniffing Tool Generate Reports

### Wireshark:

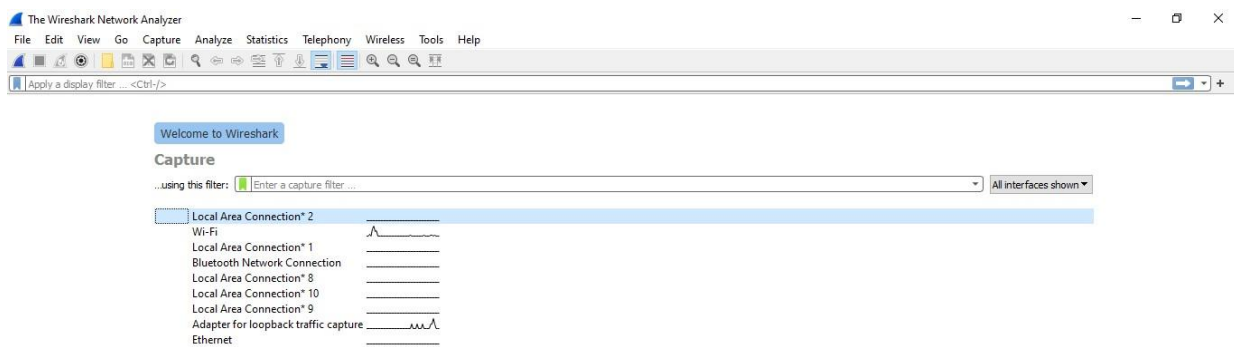
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.

There is also a terminal-based (non-GUI) version called TShark. Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

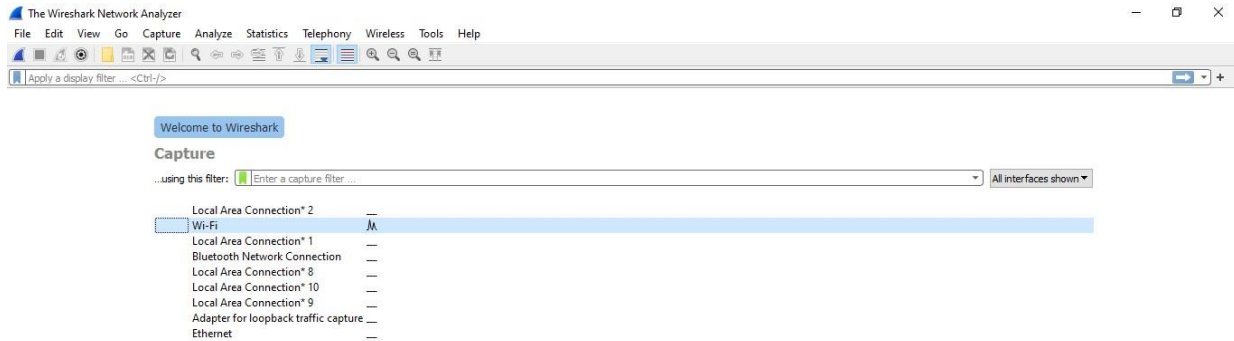
### Questions:

a. How Wireshark works? Explain with steps to

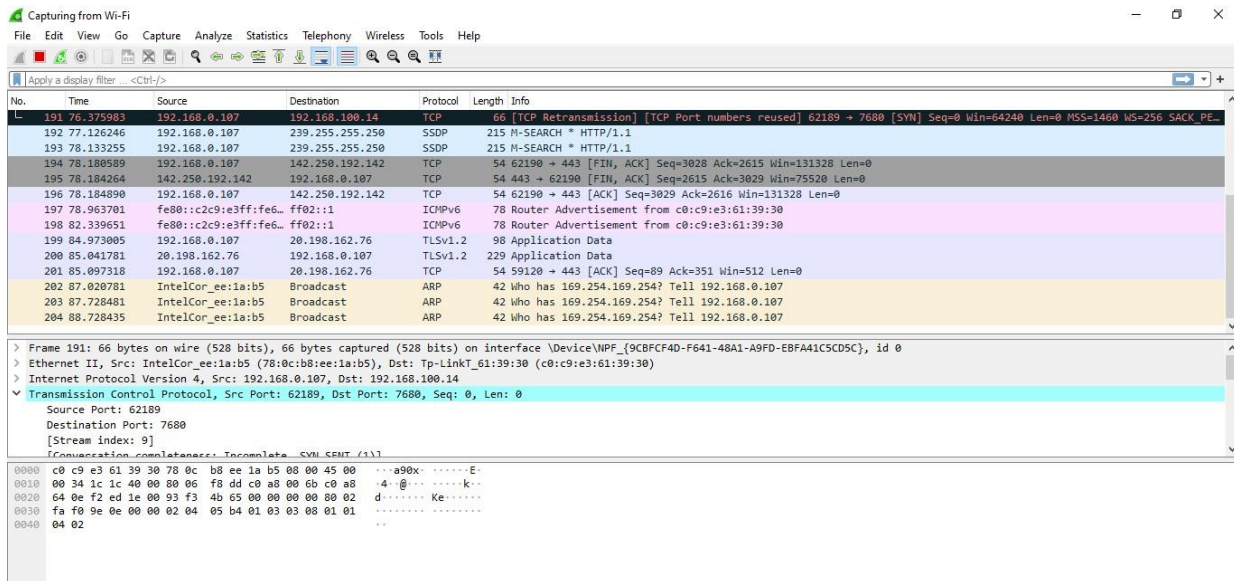
1. capture and analyse packets,
2. Apply filters and analyse packets
- 4.1 Wireshark User Interface



## 4.2 Capturing Live Network Data

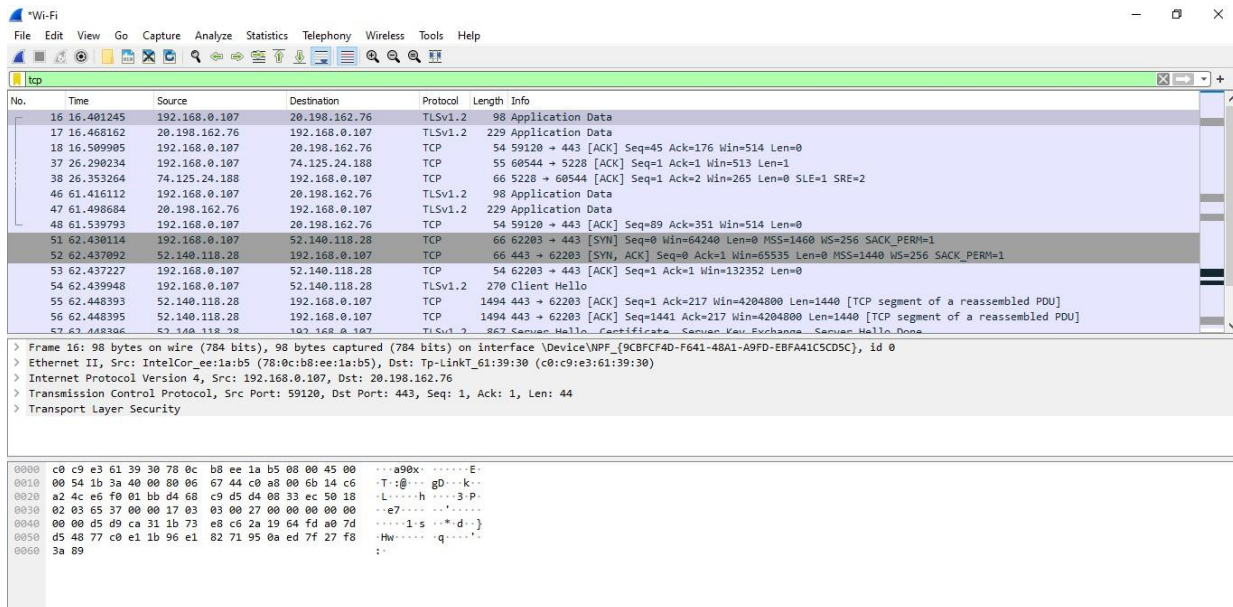


### 4.3 Viewing Captured Packets



## 4.4 Filtering Packets While Viewing





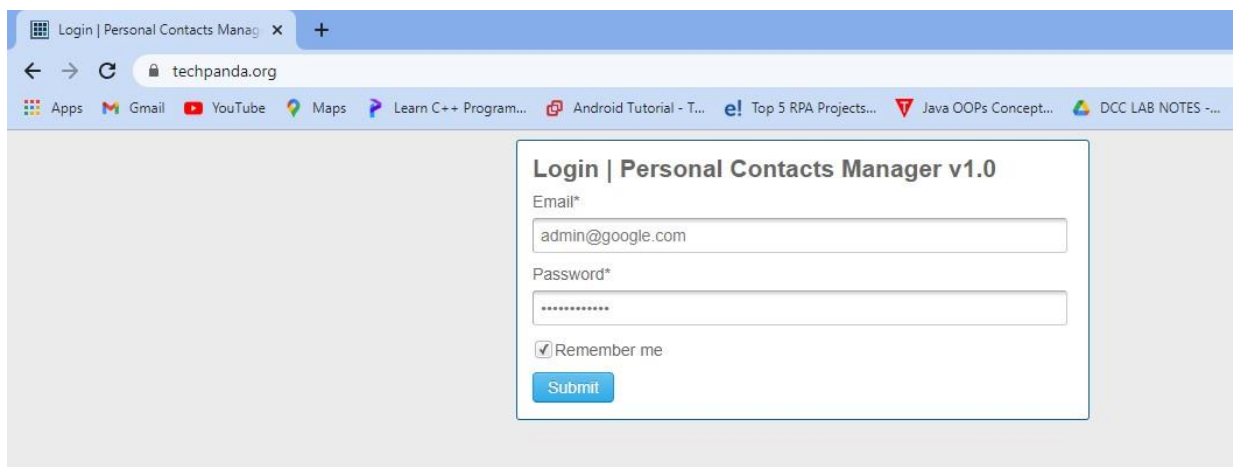
## b) How to sniff the network using Wireshark?

we are going to use Wireshark to sniff data packets as they are transmitted over HTTP protocol. For example

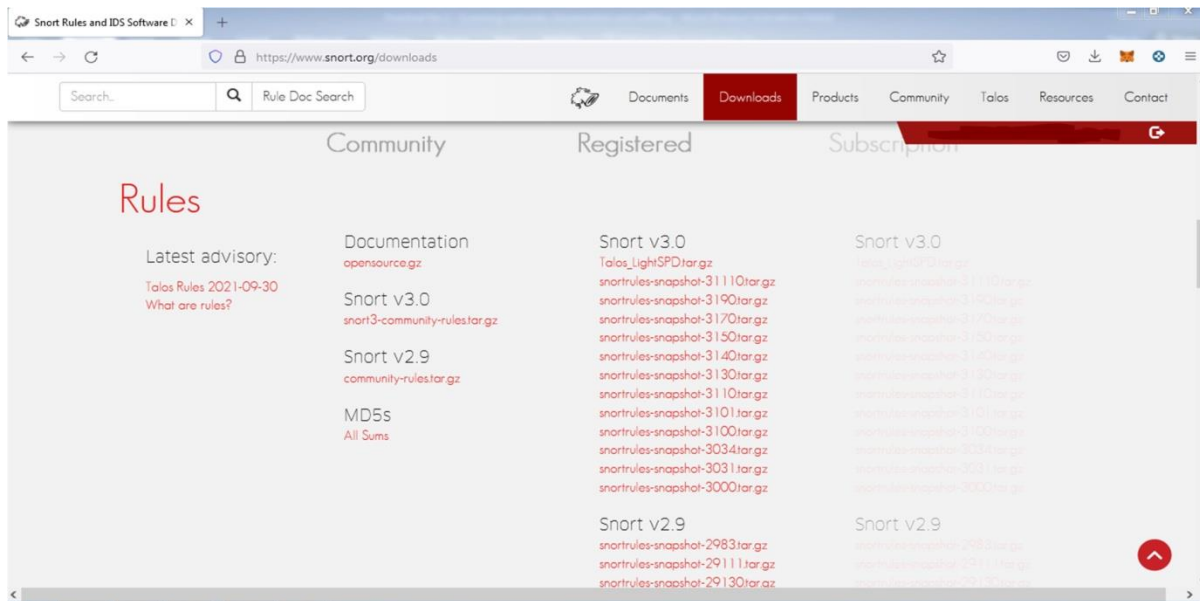
**Step 1** start Wireshark and start capturing network

**Step 2** Login to a web application that does not use secure communication. We will login to a web application on <http://www.techpanda.org/> address with the login name is admin@google.com, and the password is Password2010.

Note: we will login to the web app for demonstration purposes only.







**Step 3** Go back to wireshark and stop the live capture

**Step 4** Enter filter for HTTP protocol results only using the filter textbox and press enter key

**Step 5** select frame form packet list with POST /index.php

**Step 6** Look for the summary that says Line-based text data: application/x-www-form-urlencoded

