**Scanning networks, Enumeration and sniffing:**

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

1. Port scanning
2. Network scanning
3. IDS
4. Network Sniffing
5. **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>

Graphical user interface, text

Description automatically generated

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/**](https://nmap.org/npcap/dist/)

A screenshot of a computer

Description automatically generated

**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
   1. Scan open ports (syntax: nmap –open ip\_address / url )

A screenshot of a computer screen

Description automatically generated

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

A screenshot of a computer program

Description automatically generated

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

A screen shot of a computer

Description automatically generated

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

A computer screen with white text

Description automatically generated

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

A screen shot of a computer

Description automatically generated

**References:**

* + 1. <https://techtalk.gfi.com/scanning-open-ports-in-windows-part-3-nmap/>
    2. <https://www.youtube.com/watch?v=MoGxY3yCySk>

1. **Network scanning:**

**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:**

* 1. **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 <ip\_address>

A computer screen with white text

Description automatically generated

* + - 1. **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 <target IP range>

A computer screen with white text

Description automatically generated

* + - 1. If you see anything unusual in this list, you can then run a DNS query on a specific host, by using:

Syntax: namp -sL <IP address>

A computer screen with white text

Description automatically generated

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

* + - 1. **OS Scan** – This command return information on the OS (and version) of a host.

Syntax: nmap -O <target IP>

A screenshot of a computer screen

Description automatically generated

**More options to try:**

1. Scan ip address which passes from text file (syntax : nmap –iL <filename.txt>)
2. Aggressive scanning (syntax : nmap –A <ip\_address>)
3. To trace the route of destination address (syntax : nmap - - traceroute <ip\_address>)

**References:**

1. <https://www.varonis.com/blog/nmap-commands/>
2. <https://www.youtube.com/watch?v=IoIsTrKrl-0>
3. **Intrusion Detection:**

**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>

A screenshot of a computer

Description automatically generated

**Link to download the rules for snort:** <https://www.snort.org/download>

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

A screenshot of a computer

Description automatically generated

Snort needs **Npcap**.

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

**Questions:**

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

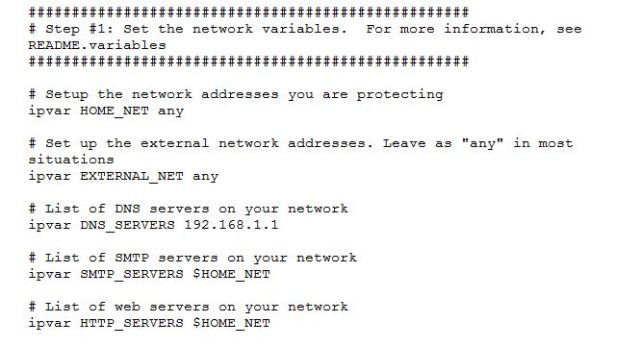
**Steps to defend your network with Snort for Windows:**

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** WinPcapinstalled
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 start (execute) snort in sniffer mode use following command:  
    **snort -dev -i 3**

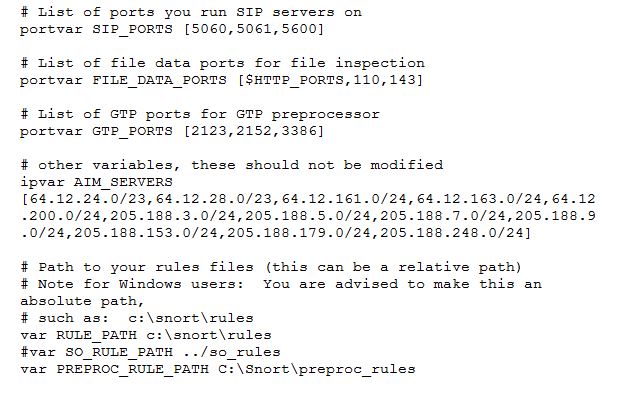
-i indicates the interface number.  You must pick the correct interface number.  In my case, it is 3.  
  -dev is used to run snort to capture packets on your network.

1. To check the interface list,  use following command:  
   **snort   -W**
2. 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.
3. To run snort in IDS mode, you will need to configure the file “**snort.conf**” according to your network environment.
4. 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)**
5. You may also want to set the addresses of DNS\_SERVERS, if you have some on your network. Example:

[](https://ttcshelbyville.files.wordpress.com/2014/03/example-snort.jpg)

1. Change the RULE\_PATH variable to the path of rules folder.

var RULE\_PATH c:\snort\rules

[](https://ttcshelbyville.files.wordpress.com/2014/03/path-to-rules.jpg)

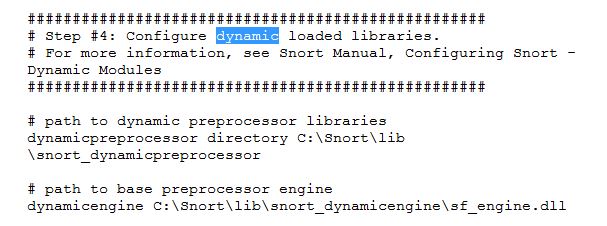
15. Change the path of all library files with the name and path on your system. and you must change the path of snort\_dynamicpreprocessorvariable.

**C:\Snort\lib\snort\_dynamiccpreprocessor**

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**

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

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

[](https://ttcshelbyville.files.wordpress.com/2014/03/libraries.jpg)

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**

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

19. You can also remove the comment of ICMP-info rules comment, if it is commented.  
  **include $RULE\_PATH/icmp-info.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**

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

22. Comment out (#) following lines:  
#preprocessor normalize\_ip4  
#preprocessor normalize\_tcp: 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**

(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**

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 }

**Snort monitoring traffic –**

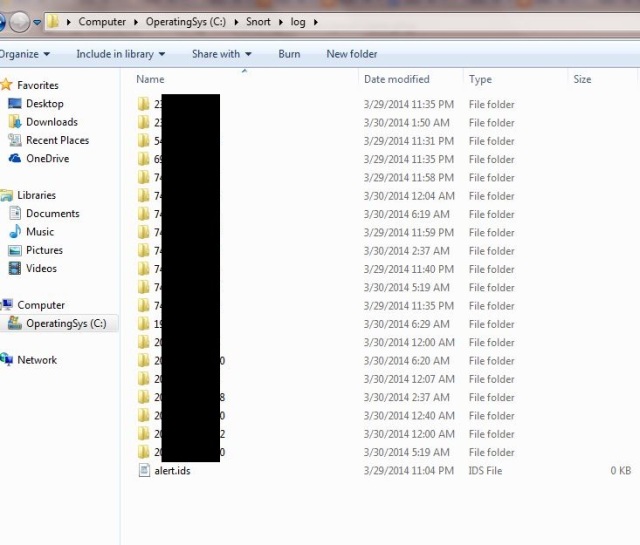
[](https://ttcshelbyville.files.wordpress.com/2014/03/traffic.jpg)

**Snort’s detailed report when scanning has stopped –**

A screenshot of a computer

Description automatically generated

**Log files – We can also view log files.**



**Note:** Read the setup and configuration of Snort from Snort.org. While this is a demo, Snort can be configured thousands of ways to detect and alert you in the event you have malicious activity on your network. Downloading signatures often is extremely important.

**References:**

* + 1. <https://www.snort.org/>
    2. <https://en.wikipedia.org/wiki/Snort_(software)>
    3. <https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/>
    4. <https://www.youtube.com/watch?v=W1pb9DFCXLw>
    5. <https://youtu.be/X64-0ogjoP4>

1. **Network Sniffing:**

**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.

**Link to download Wireshark 3.4.8 for windows platform:** <https://www.wireshark.org/download.html>

Wireshark needs **Npcap.**

**Link to download Npcap 0.9984 for windows platform:** [**https://nmap.org/npcap/dist/**](https://nmap.org/npcap/dist/)

A screenshot of a computer

Description automatically generated

**Questions:**

* 1. **How Wireshark works? Explain with steps to**

**1. capture and analyse packets,**

**2. Apply filters and analyse packets**

**4.1 Wireshark User Interface**

A screenshot of a computer

Description automatically generated

**4.2 Capturing Live Network Data**

A screenshot of a computer

Description automatically generated

**4.3 Viewing Captured Packets**

A screenshot of a computer

Description automatically generated

**4.4 Filtering Packets While Viewing**

A screenshot of a computer

Description automatically generated

**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**/](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.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**References:**

1. <https://en.wikipedia.org/wiki/Wireshark>
2. <https://www.guru99.com/wireshark-passwords-sniffer.html>
3. <https://www.youtube.com/watch?v=lb1Dw0elw0Q>