INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

NETWORK SECURITY LABORATORY								
V Semester: CSE (CS)								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
ACCC08	Core	L	T	P	C	CIA	SEE	Total
		0	0	3	1.5	30	70	100
Contact Classes: Nil	Tutorial Classes: Nil	Practical Classes: 36				Total Classes: 36		
Prerequisite: Python Programming								

I. COURSE OVERVIEW:

The purpose of this course is to provide understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

II.COURSE OBJECTIVES:

The students will try to learn:

I. The different packet crafting techniques using different networking tools.
II. The different network Script programmes to measure the performance of network.
III. The understanding of different Protocols that measure the scope and lifetime of network.

III. COURSE OUTCOMES:

At the end of the course students will be able to:

CO1 : Apply Hping tool to implement packet crafting on TCP and UDP protocol.

CO2 : Identify appropriate tools to scan the network services and diagnostics.

CO3 : Make Use of Nmap and Zenmap tools to monitor the networking mechanism.

CO4 : Compare some NSE scripts to scan the network of the target.

CO5 : Analyze the concept of firewall and IDS spoofing to scan the network

CO6 : Apply Angry IP Scanner tool to scan the network of the target.

IV. COURSE CONTENT:

EXERCISES FOR NETWORK SECURITY LABORATORY

Note: Students are encouraged to bring their own laptops for laboratory practice sessions.

1. Getting Started with Applying Networking Commands

1.1 Ping

The Ping command allows you to test the reachability of a device on a network. Pinging a host should return four data packets, if the data packets are not returned you know there is a problem with your network connection.

Input: ping www.google.com

Output:

```
C:\Users\SLIM 3>ping google.com

Pinging google.com [2404:6800:4007:809::200e] with 32 bytes of data:
Reply from 2404:6800:4007:809::200e: time=62ms
Reply from 2404:6800:4007:809::200e: time=55ms
Reply from 2404:6800:4007:809::200e: time=88ms
Reply from 2404:6800:4007:809::200e: time=193ms

Ping statistics for 2404:6800:4007:809::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 193ms, Average = 99ms
```

Try

Students can use different top level and bottom level domains to test the reachability of the target.

Hint

Any other marketing websites, banking sites, university sites can test with above command

1.2 Ipconfig:

The Ipconfig command displays basic IP address configuration information for the Windows device you are working on. The general information includes IP Addresses for both IPv4 and IPv6, the Default Gateway, and the Subnet Mask.

Input: type “ipconfig” on any system

Output:

```
C:\Users\SLIM 3>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:4820:43fb:50f9:9de8:1354:a227
   Temporary IPv6 Address. . . . . . : 2401:4900:4820:43fb:e051:a6dc:9861:6e43
   Link-local IPv6 Address . . . . . : fe80::50f9:9de8:1354:a227%15
   IPv4 Address. . . . . . . . . . . : 192.168.43.165
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::106e:25ff:fe85:9405%15
                                       192.168.43.1
```

1.3 NSLookUp

The NSLookUp command displays information that you can use to diagnose Domain Name System (DNS) infrastructure.

Using NSLookUp without a parameter will show the DNS server your PC is currently using to resolve domain names into IP addresses Given a roman numeral, convert it to an integer.

Input: nslookup

Output:

```
C:\Users\SLIM 3>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> www.google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4007:828::2004
          142.250.195.228
```

1.4 Tracert

This command will trace the route a data packet takes before reaching its destination, displaying information on each hop along the route.

Each hop of the route will display the latency between your device and that particular hop and the IP address of the hop.

Input: tracert www.iare.ac.in

Output:

```
C:\Users\SLIM 3>tracert www.google.com

Tracing route to www.google.com [2404:6800:4007:822::2004]
over a maximum of 30 hops:

  1     3 ms    16 ms     3 ms  2401:4900:4820:43fb::f1
  2     *        *        *     Request timed out.
  3   228 ms    94 ms    47 ms  2401:4900:d0:4001::205
  4    84 ms    39 ms    26 ms  2401:4900:c0:1::99
  5    80 ms    51 ms    36 ms  2404:a800:3a00:2::39
  6   248 ms    80 ms    48 ms  2404:a800::92
  7   242 ms    57 ms    42 ms  2001:4860:1:1::674
  8    85 ms    55 ms    68 ms  2404:6800:80f7::1
  9    91 ms    52 ms    37 ms  2001:4860:0:1::4a22
 10    76 ms    47 ms    92 ms  2001:4860:0:1::55cd
 11   225 ms    73 ms    66 ms  maa03s37-in-x04.1e100.net [2404:6800:4007:822::2004]

Trace complete.
```

1.5 PathPing

PathPing combines the ping command with the tracert command, providing information about network latency and network loss at intermediate hops between a source and destination.

Input: pathping www.iare.ac.in

Output:

```
C:\Users\SLIM 3>pathping www.iare.com

Tracing route to www.iare.com [66.77.31.51]
over a maximum of 30 hops:
  0  LAPTOP-QQKTCUSP [192.168.43.165]
  1  192.168.43.1
  2     *        *        *
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-QQKTCUSP [192.168.43.165]
                                 0/ 100 =  0%   |
  1   17ms     0/ 100 =  0%     0/ 100 =  0%  192.168.43.1

Trace complete.
```

1.6 System Info:

The System Info command, which displays a detailed list of configuration information includes the installed version of Windows 10, the host name, the Product ID, the type and number of CPUs, RAM configuration, network card details and installed hotfixes.

Input: systeminfo
Output:

```
C:\Windows\System32>systeminfo

Host Name:                 LAPTOP-QQKTCUSP
OS Name:                   Microsoft Windows 11 Home Single Language
OS Version:                10.0.22621 N/A Build 22621
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          SLIM 3
Registered Organization:   N/A
Product ID:                00356-24516-18291-AAOEM
Original Install Date:     12/12/2022, 2:23:39 PM
System Boot Time:          8/28/2023, 11:19:05 AM
System Manufacturer:       LENOVO
System Model:              82H8
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 140 Stepping 1 GenuineIntel ~2995 Mhz
BIOS Version:              LENOVO GGCN51WW, 11/16/2022
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              00004009
Time Zone:                 (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory:     7,975 MB
Available Physical Memory: 1,453 MB
Virtual Memory: Max Size:  12,583 MB
Virtual Memory: Available: 2,617 MB
Virtual Memory: In Use:    9,966 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-QQKTCUSP
Hotfix(s):                 4 Hotfix(s) Installed.
                           [01]: KB5028948
                           [02]: KB5012170
                           [03]: KB5029263
                           [04]: KB5028756
Network Card(s):           2 NIC(s) Installed.
```

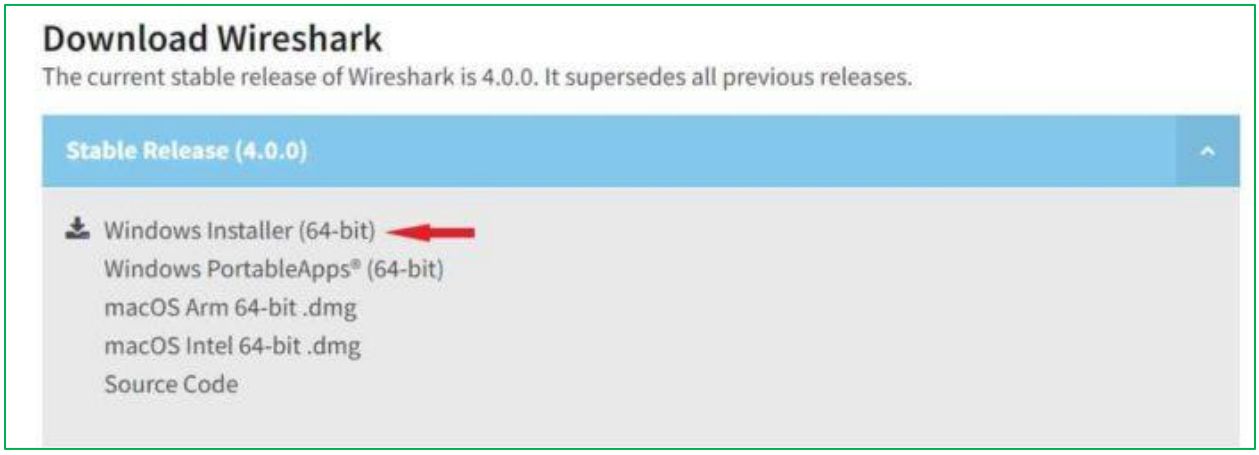
2. Tcp and Udp Packet Crafting using Wireshark tool

2.1 Install Wireshark tool

Software Requirements:

- Supported operating systems:
- Windows 10
- 64-bit OS X/macOS 10.6 or later
- Linux (check the Wireshark prerequisites for version compatibility)
- Wireshark v3.4.7 or later

We need to visit official website and download wireshark for 64-bit Windows system using below highlighted link.

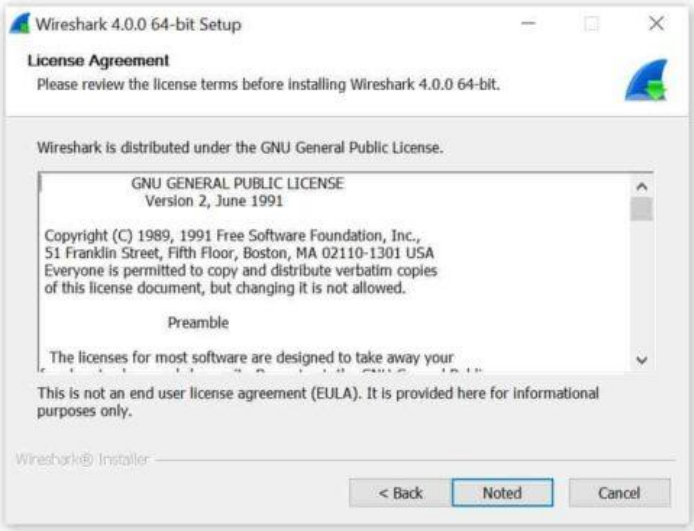


Once you click on the download link, it will start downloading in your local system as shown below.

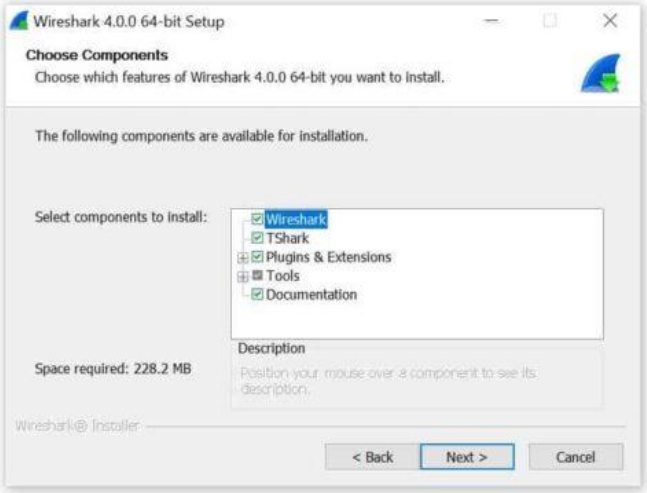
Installing Wireshark

Then double click on local downloaded installer to start the installation. It will first show you below setup wizard asking to make sure Wireshark is not running. Click Next to Continue.

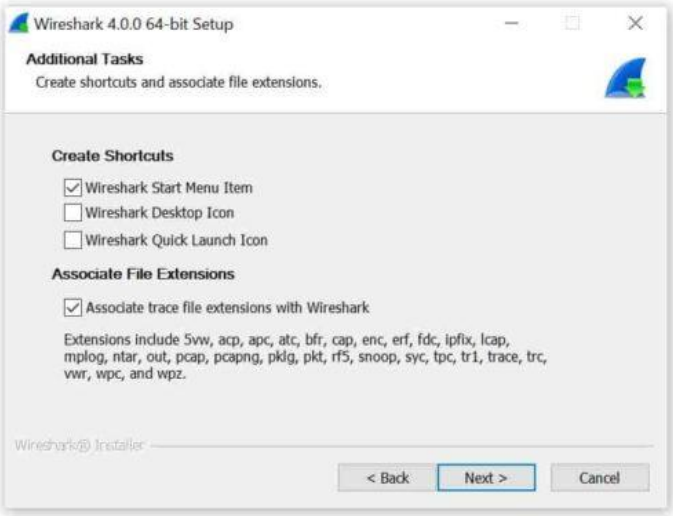
You will see below License Agreement. Please go through it and review all the License terms under this agreement before installing Wireshark. Click Noted to continue.



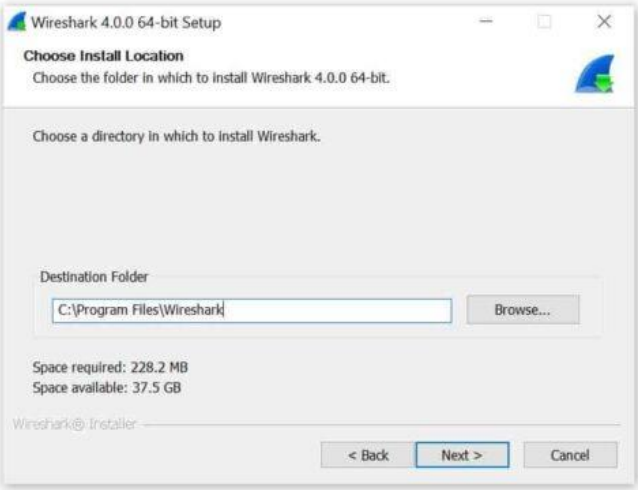
You can select all the Wireshark features to install. Below are the main features available to install. You can select all the required features and then click on Next to continue.



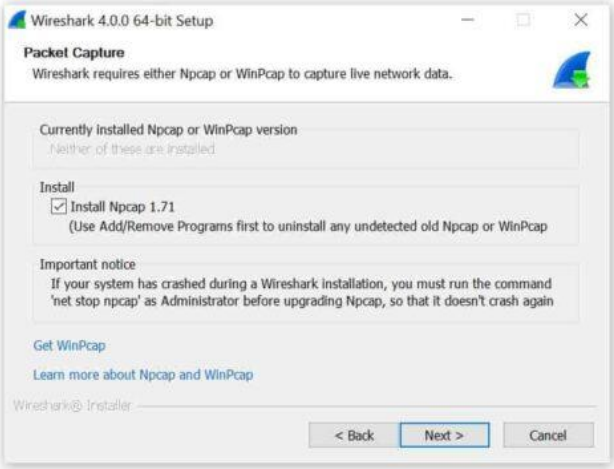
In additional tasks, you can choose to create shortcuts and associate file extensions from below. Once selected, Click Next to continue.



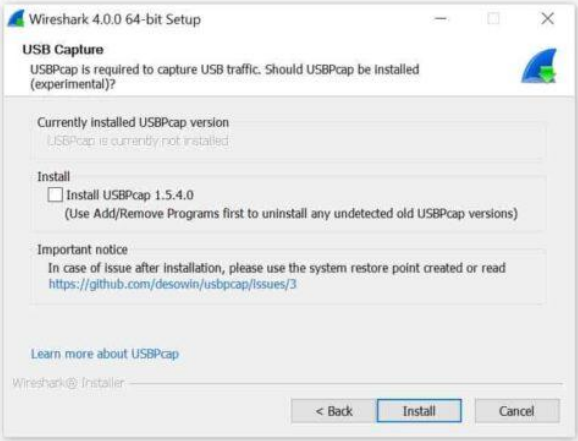
You need to choose the destination folder by browsing to the location where you need to install wireshark. By default, it will install under C:\Program Files\Wireshark folder as shown below. Once chosen, Click on Next to proceed.



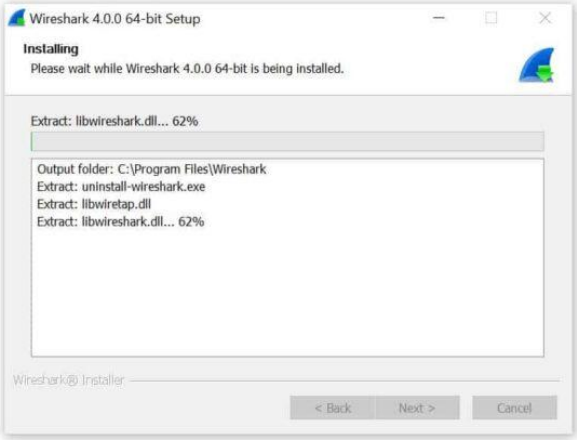
To capture live network data, Wireshark requires either Npcap or WinPcap to be installed or else by default it will install Npcap in your System. If you would like to install this program then just click on Next. Otherwise, you need to unselect and then click on Next.



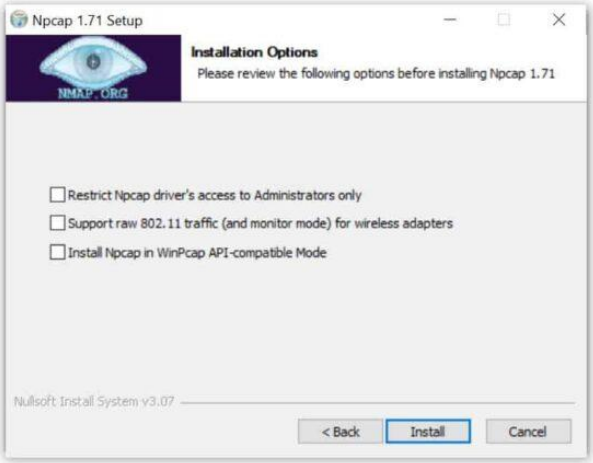
Similarly, for capturing USB traffic, wireshark needs to install USBPcap tool in your System. It won't be selected by default, so you need to select it manually in case you want to install this tool. Then Click on Install.



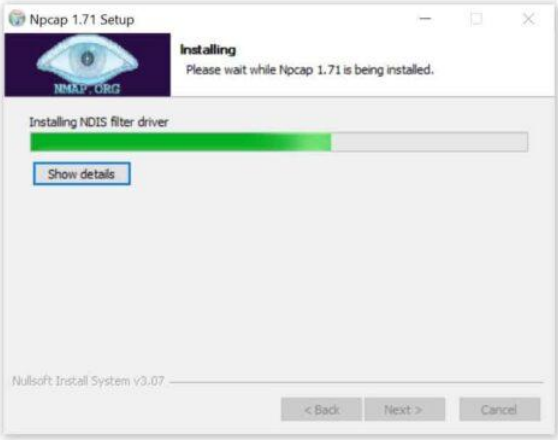
You can see that Wireshark installation will be started as shown below



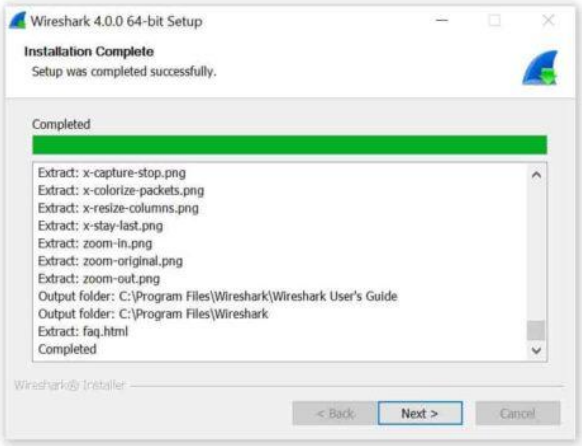
Once the installation started, you will see below Npcap screen popped up where you will be asked to select below option. Once done, click on Install to complete the installation of this tool first.



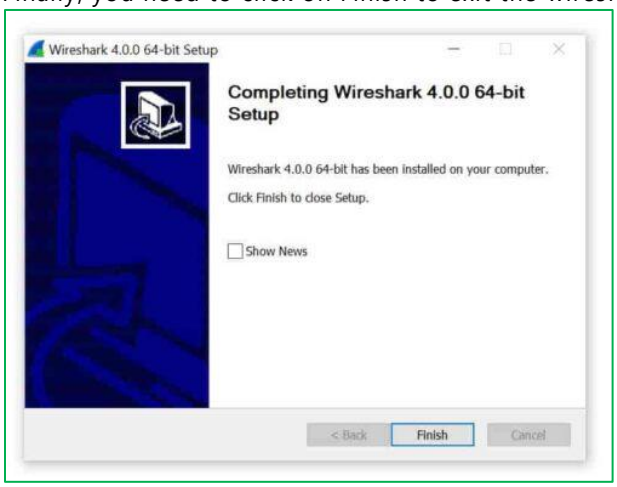
You can track the progress of Npcap installation from below wizard screen.



After a while you will see the installation of wireshark is completed as shown below. Click on Next to continue.

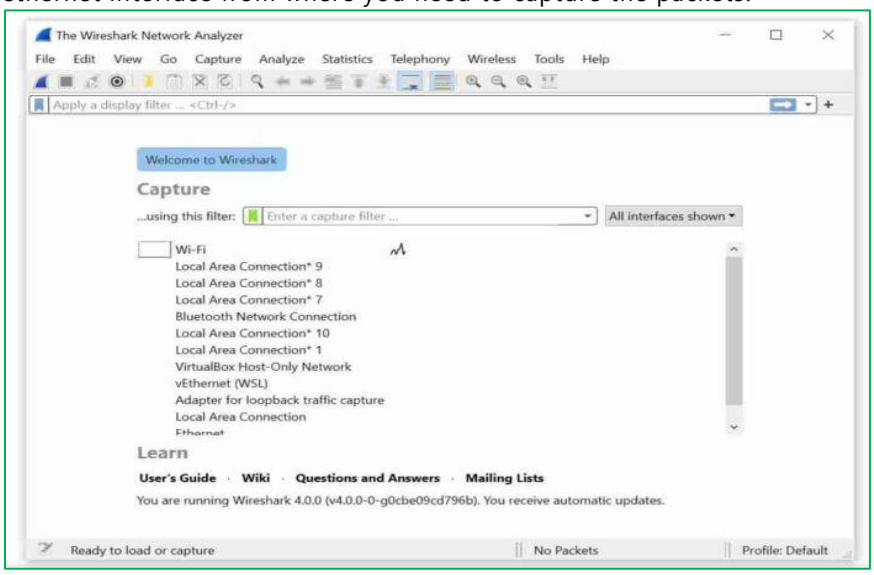


Finally, you need to click on Finish to exit the wireshark setup wizard.

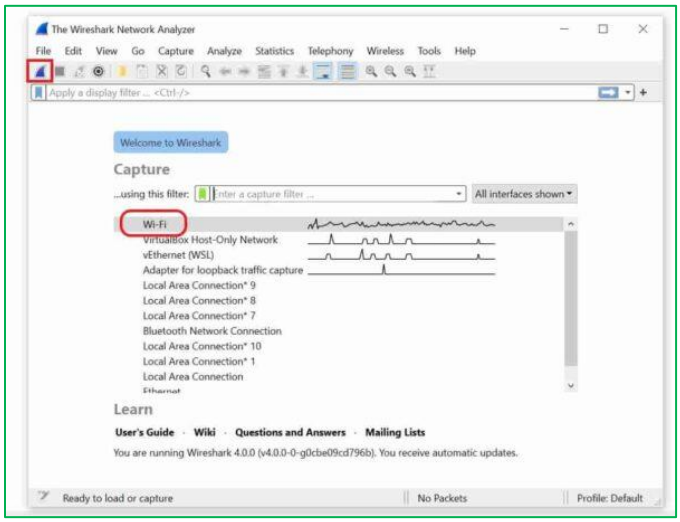


2.2 Capture packet transmission

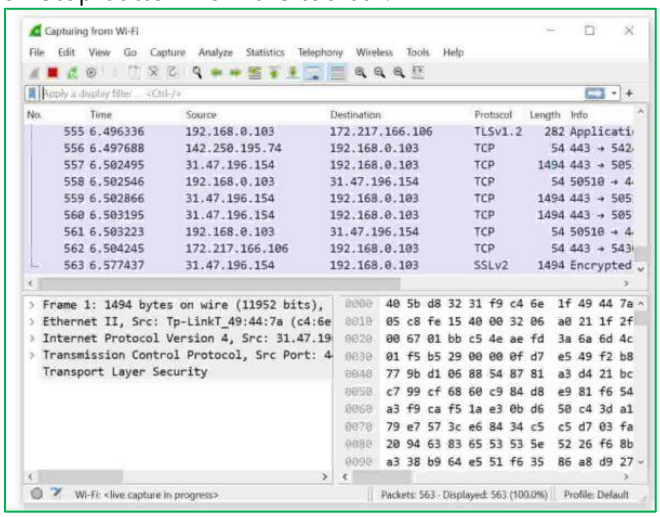
After successful installation, the first launch of Wireshark should look like below. You need to select the ethernet interface from where you need to capture the packets.



Here we are selecting wi-fi interface and then clicking on start capture to capture the packets from this interface as shown below.



you will see all the live packets getting captured as shown below. To stop the capture, you need to click on Stop button from the toolbar.



2.3 Analyze Packet Header format

From the below figure capturing all live packets select any of protocol such as TCP, UDP etc.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol
45741	2023-09-05 16:20:40.062374	Dell_5f:0b:63	Broadcast	ARP
45742	2023-09-05 16:20:40.076445	10.1.1.33	10.255.255.255	BROW…
45743	2023-09-05 16:20:40.085585	0e:4c:a2:2a:60:…	Broadcast	ARP
45744	2023-09-05 16:20:40.094478	Dell_aa:13:c8	Broadcast	ARP
45745	2023-09-05 16:20:40.124737	20.20.19.146	77.74.181.38	TCP
45746	2023-09-05 16:20:40.124890	20.20.19.146	180.87.4.157	TCP
45747	2023-09-05 16:20:40.126687	Dell_aa:13:c8	Broadcast	ARP
45748	2023-09-05 16:20:40.128428	Dell_aa:13:c8	Broadcast	ARP
45749	2023-09-05 16:20:40.128428	Dell_aa:13:c8	Broadcast	ARP
45750	2023-09-05 16:20:40.128428	Dell_aa:13:c8	Broadcast	ARP
45751	2023-09-05 16:20:40.128637	Sophos_06:1c:1d	Broadcast	ARP
45752	2023-09-05 16:20:40.133700	20.20.21.225	224.0.0.251	MDNS
45753	2023-09-05 16:20:40.133700	fe80::c9c:8b51:…	ff02::fb	MDNS
45754	2023-09-05 16:20:40.133700	HonHaiPr_f7:4d:…	Broadcast	ARP
45755	2023-09-05 16:20:40.143685	Dell_aa:13:c8	Broadcast	ARP
45756	2023-09-05 16:20:40.156462	Hangzhou_bd:50:…	Broadcast	ARP
45757	2023-09-05 16:20:40.165425	HewlettP_ce:fc:…	Broadcast	ARP
45758	2023-09-05 16:20:40.265399	20.20.21.221	239.255.255.250	SSDP

Select any of the Protocol to see header format

```
> Frame 1841: 666 bytes on wire (5328 bits), 666 bytes capturec
    Section number: 1
  > Interface id: 0 (\Device\NPF_{BCCE385D-818D-4CE8-8A61-4B33
      Interface name: \Device\NPF_{BCCE385D-818D-4CE8-8A61-4B3
      Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep  5, 2023 16:14:59.273489000 India Standa
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1693910699.273489000 seconds
    [Time delta from previous captured frame: 0.000000000 seco
    [Time delta from previous displayed frame: 0.000000000 sec
    [Time since reference or first frame: 12.601719000 seconds
    Frame Number: 1841
    Frame Length: 666 bytes (5328 bits)
    Capture Length: 666 bytes (5328 bits)
```

Explore each and every field in the header format fields

Try

Identify other protocols to check Frame formats and Header formats
Capture TCP / UDP Live streaming process

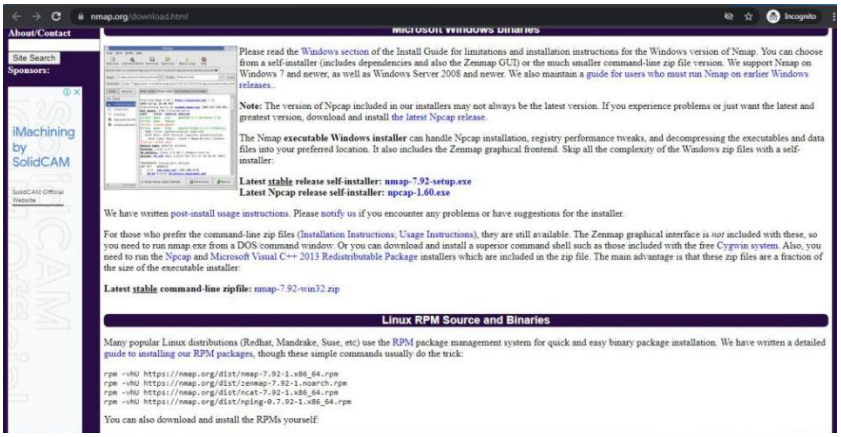
Hints

Related all network protocols that are transmitted during capturing process

3. Installing and apply different network scanning methods using NMAP / Zenmap tool

3.1 installing NMAP Tool

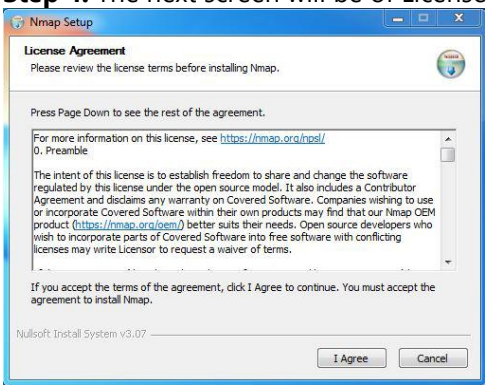
step 1: Visit the official website using the URL https://nmap.org/download.html on any web browser the click on nmap-7.92-setup.exe. Downloading of this executable file will start soon. It is a 21.8 MB file so it will take some minutes.



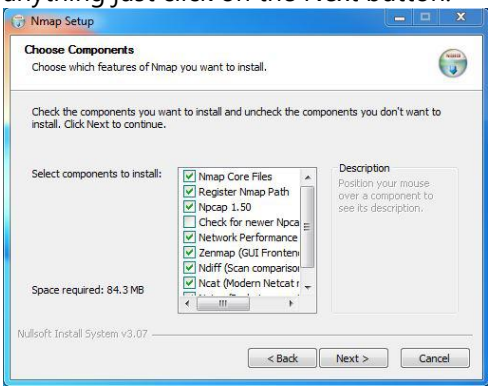
Step 2: Now check for the executable file in downloads in your system and run it.

Step 3: It will prompt confirmation to make changes to your system. Click on Yes.

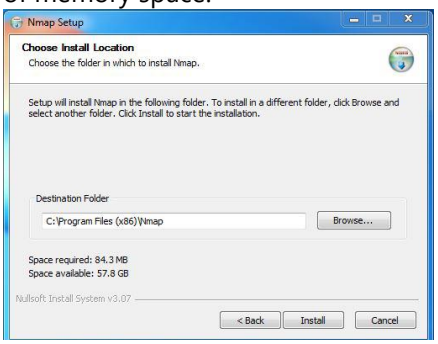
Step 4: The next screen will be of License Agreement click on I Agree.



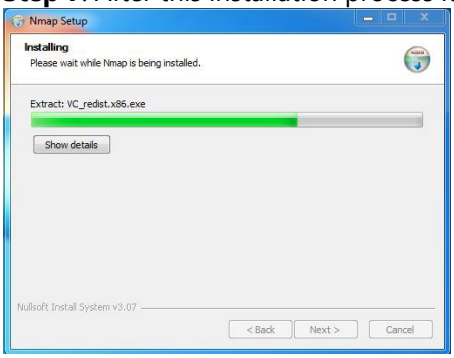
Step 5: Next screen is of choosing components, all components are already marked so don't change anything just click on the Next button.



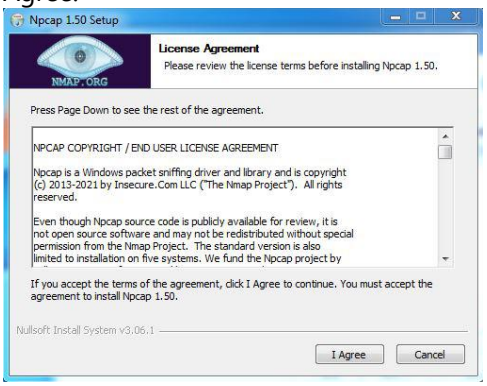
Step 6: In this step, we choose the installation location of Nmap. By default, it uses the C drive but you can change it into another drive that will have sufficient memory space for installation. It requires 84.3 MB of memory space.



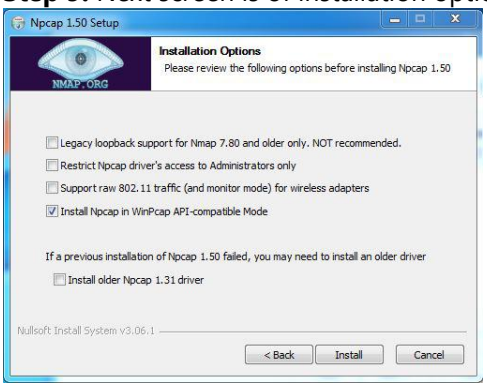
Step 7: After this installation process it will take a few minutes to complete the installation.



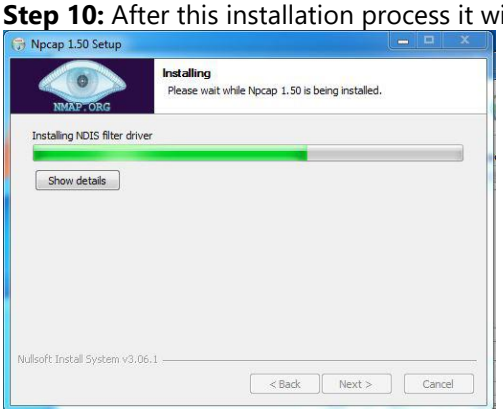
Step 8: Npcap installation will also occur with it, the screen of License Agreement will appear, click on I Agree.



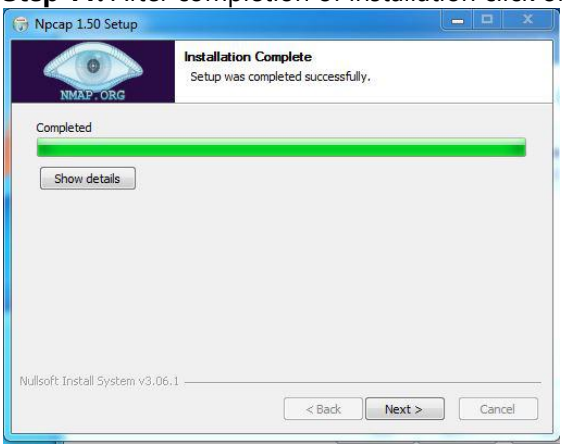
Step 9: Next screen is of installation options don't change anything and click on the Install button.



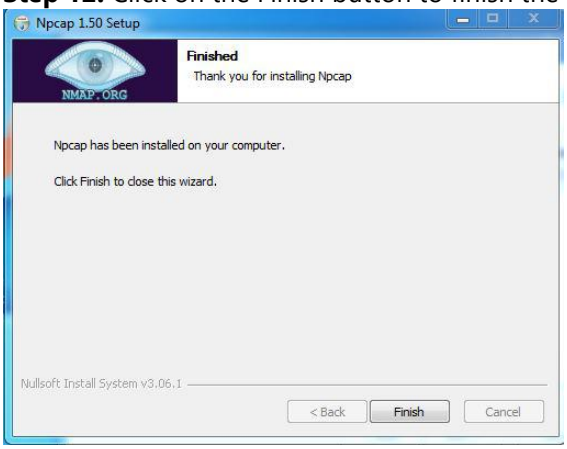
Step 10: After this installation process it will take a few minutes to complete the installation.



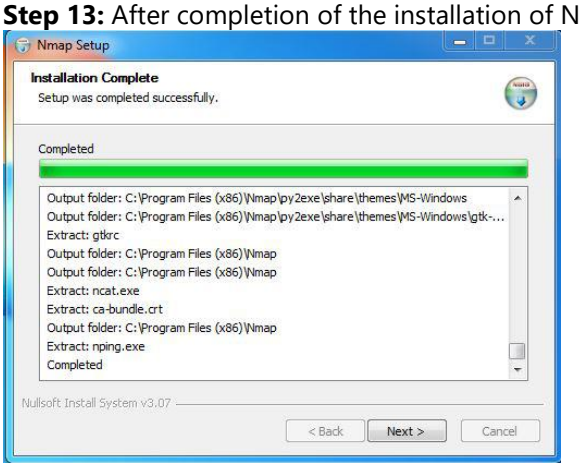
Step 11: After completion of installation click on the Next button.



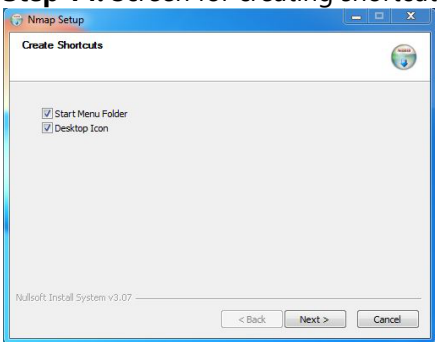
Step 12: Click on the Finish button to finish the installation of Npcap.



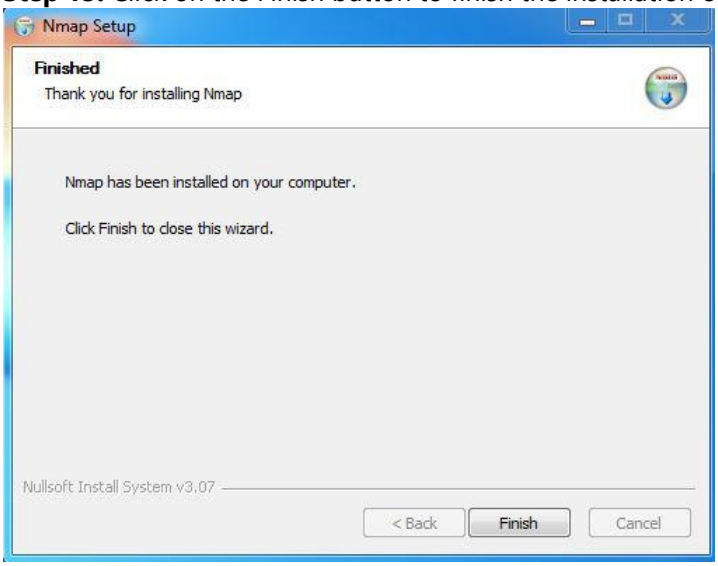
Step 13: After completion of the installation of Nmap click on Next button.



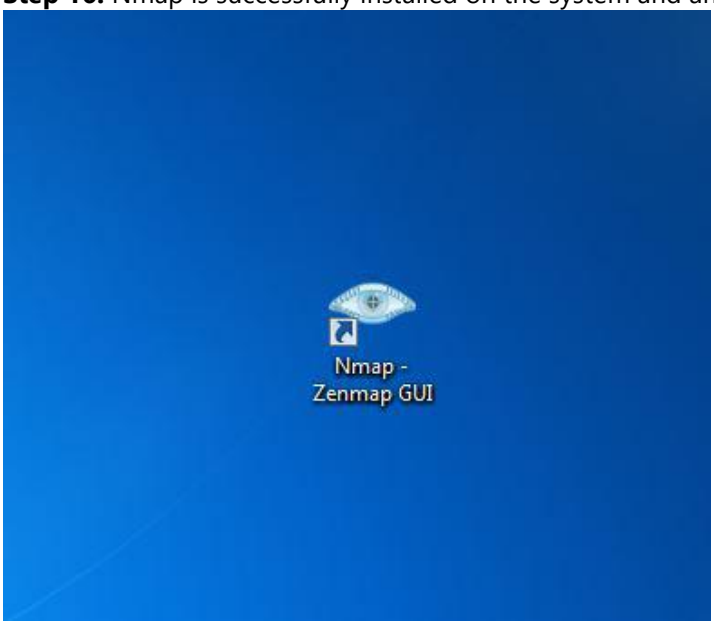
Step 14: Screen for creating shortcut will appear, click on Next button.



Step 15: Click on the Finish button to finish the installation of Nmap.



Step 16: Nmap is successfully installed on the system and an icon is created on the desktop.



Step 17: Run the software and see the interface.

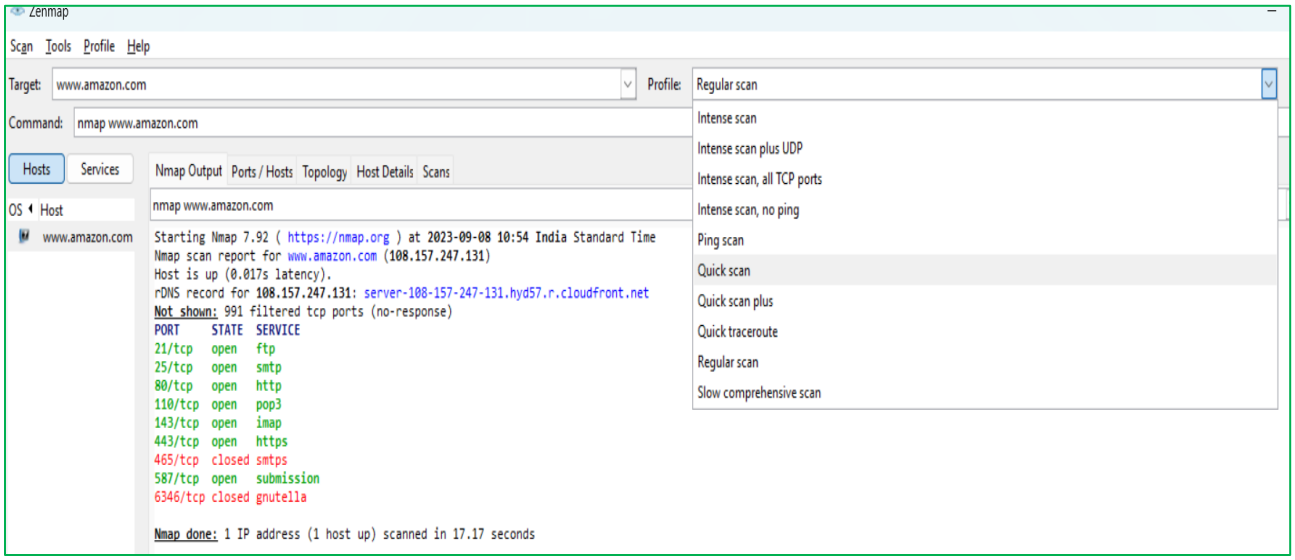
3.2 Scanning any of the target with domain name

To Perform Scanning of the target we need to understand all scanning types as shown in below
There are different types of scans available

Syntax: Nmap domain name

Example: nmap www.amazon.com

Type of scan: Regular



After performing scanning of the target it identifies different no of ports are open / closed and displays service available on that ports.

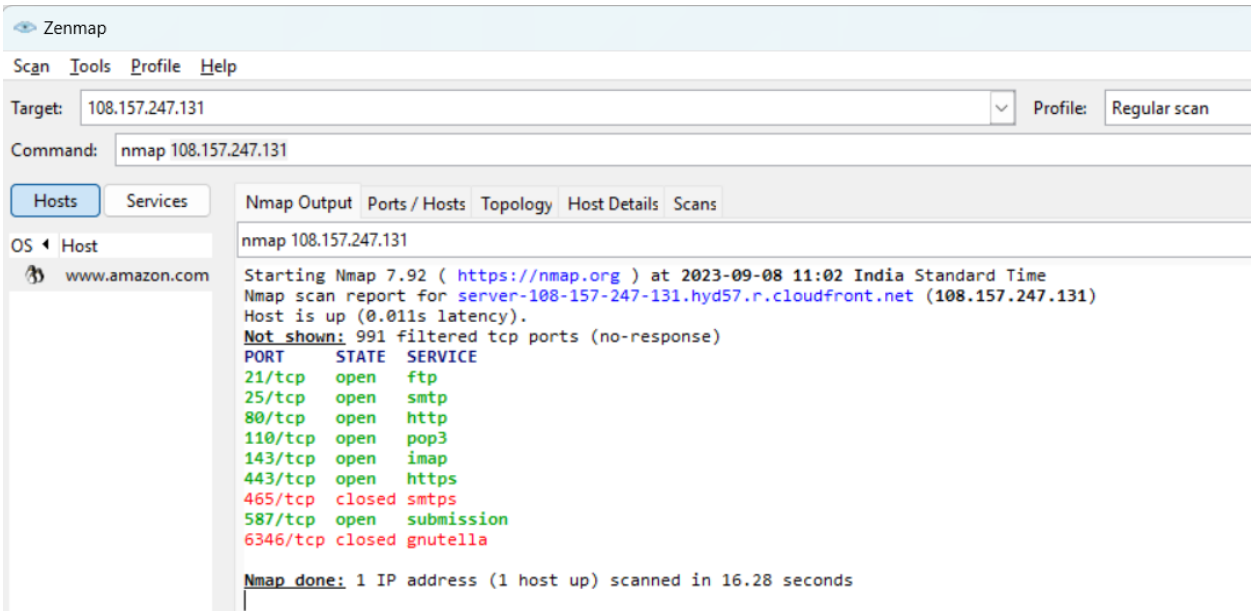
3.3 Scanning any of the target with IP Address

To Perform Scanning of the target we need to understand all scanning types as shown in below
There are different types of scans available

Syntax: Nmap IP Address

Example: nmap 108.157.247.131

Type of scan: Regular



Try

Students should perform scanning of the target with variety of scan types as shown in above
Hint:

Select the type of scan from dropdown window appeared on screen

4. Scanning network of the target about half open and full open scan

4.1 half open

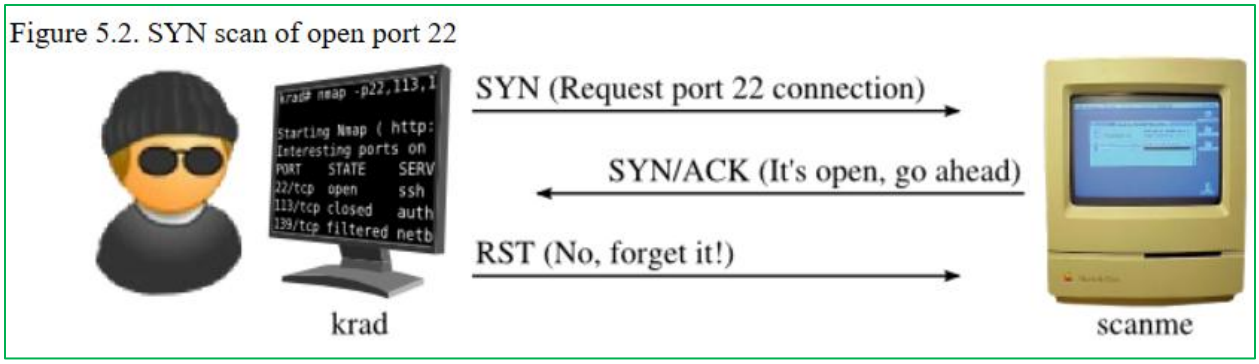
Half open scan also known as TCP Stealth scan

SYN scan may be requested by passing the -sS option to Nmap. It requires raw-packet privileges, and is the default

TCP scan when they are available.
So when running Nmap as root or Administrator, -sS is usually omitted.
which finds a port in each of the three major states.

```
krad# nmap -p22,113,139 scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
PORT     STATE    SERVICE
22/tcp   open     ssh
113/tcp  closed   auth
139/tcp  filtered netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

The fallowing figure shows how the SYN Scan will working.

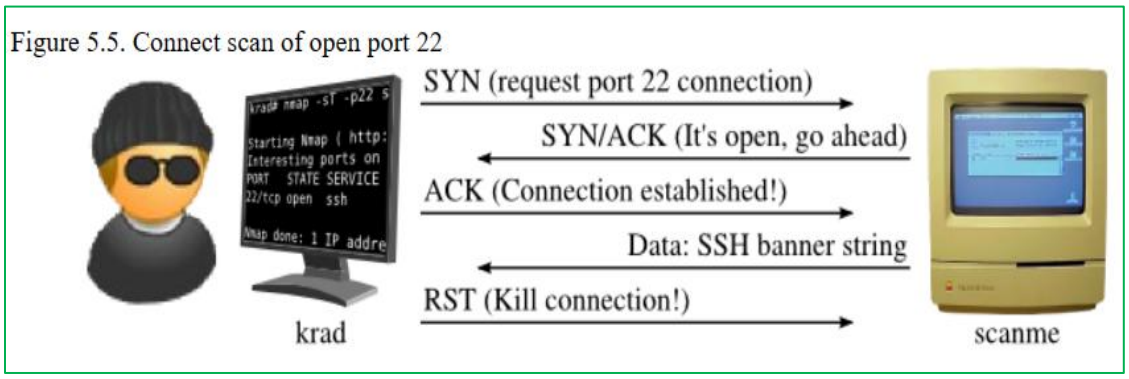


4.2 full open

TCP connect scan is the default TCP scan type when SYN scan is not an option
When SYN scan is available, it is usually a better choice. Nmap has less control over the high level connect call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does.

```
krad~> nmap -T4 -sT scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
25/tcp   closed smtp
53/tcp   open   domain
70/tcp   closed gopher
80/tcp   open   http
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```

The fallowing figure shows a connect scan in action against open port 22 of scanme.nmap.org.



5. Scanning network of the target using TCP scan techniques

5.1 TCP SYN Port Scan

It scans the TCP SYN ports.
-sS : TCP SYN scans
It scan the TCP SYN ports.
-sS : TCP SYN scans

```
C:\Users\Administrator>nmap 192.168.1.1 -sS

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###    ###

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

```

5.2. TCP Connect Port Scan

It scan only TCP ports.
-sT: TCP Connect() scan

```
C:\Users\Administrator>nmap 192.168.1.1 -sT

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###    ###

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

```

5.3 UDP Port Scan

It scan only UDP ports.
-sU: UDP Scan

```
C:\Users\Administrator>nmap 192.168.1.1 -sU

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###    ###

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

```

5.4 TCP ACK Port Scan

It scan TCP ACK ports.
-sA: TCP ACK scans

```
C:\Users\Administrator>nmap 192.168.1.1 -sA

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###     ###

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

```

5.5 TCP Window Port Scan

It scan TCP window ports.
-sW: TCP Window scans

```
C:\Users\Administrator>nmap 192.168.1.1 -sW

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###     ###

Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds

```

Try:
TCP Maimon Port Scan
Hint:
-sM: TCP maimon scans.

6. Scanning the network of the target using host discovery content

6.1 How to List Targets IP Addresses.

It doesn't scan a range of IP address. It just list out IP addresses.
-sL: List Scan - simply list targets to scan

```
C:\Users\Administrator>nmap 192.168.1.1-4 -sL

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap scan report for 192.168.1.4
Nmap done: 4 IP addresses (0 hosts up) scanned in 2.13 seconds

```

6.2 How to Scan Host by Disabling Port Scanning

It's scan host and check whether host is up or not by disabling port of host. It display only host is up or not.

-sn: Ping Scan - disable port scan

```
C:\Users\Administrator>nmap 192.168.1.1/24 -sn

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).

Nmap scan report for 192.168.1.2
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.99 seconds

```

6.3 How to Scan Port by Disabling Host Scanning

```
C:\Users\Administrator>nmap 192.168.1.1-254 -Pn

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###     ###

Nmap scan report for 192.168.1.212
Host is up (0.0023s latency).
Not shown: 991 closed ports
PORT     STATE     SERVICE
###      ###         ###

Nmap done: 254 IP addresses (2 hosts up) scanned in 14.55 seconds

```

6.4. How to Discover TCP SYN on Specific Port

It's scan TCP SYN port that is 80 by default. It display PORT, STATE and SERVICE on each host.

-PS[portlist]: TCP SYN discovery to given ports

```
C:\Users\Administrator>nmap 192.168.1.1-254 -PS22-25,80

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0038s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
###     ###     ###

Nmap scan report for 192.168.1.212
Host is up (0.0023s latency).
Not shown: 991 closed ports
PORT     STATE     SERVICE
###      ###         ###

Nmap done: 254 IP addresses (2 hosts up) scanned in 14.55 seconds
```

Try

Discover TCP ACK On Specific Port
Discover UDP On Specific Port
Discover ARP On Local Network
Hints
Use all protocols port, states, services to discover

7. Scanning the network of the target using the port specification

7.1 Single Specific Port Scanning

It scan a single specific port.
-p[port no.]: Only scan specified port

```
C:\Users\Administrator>nmap 192.168.1.1 -p 21

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds

```

7.2 Range of Port Scanning

It Scan range of ports.
-p[port range]: Only scan specified ports.

```
C:\Users\Administrator>nmap 192.168.1.1 -p 21-30

```

Expected Output:

```
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 18:52 (0:00:00 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0042s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
24/tcp closed priv-mail
25/tcp closed smtp
26/tcp closed rsftp
27/tcp closed nsw-fe
28/tcp closed unknown
29/tcp closed msg-icp
30/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds

```

7.3 Scanning Multiple TCP and UDP Ports

It scan multiple TCP and UDP ports.
-p U:[port no.],T:[port range],[port no.]: Only scan specified ports

```
C:\Users\Administrator>nmap 192.168.1.1 -p U:53,T:21-30,80
```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0086s latency).

PORT    STATE  SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
24/tcp closed priv-mail
25/tcp closed smtp
26/tcp closed rsftp
27/tcp closed nsw-fe
28/tcp closed unknown
29/tcp closed msg-icp
30/tcp closed unknown
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
```

7.4 Scanning All Ports

It Scan all the ports but only display open ports.
-p- : Scanning all ports.

```
C:\Users\Administrator>nmap 192.168.1.1 -p-
```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 65534 closed ports
PORT    STATE SERVICE
###     ###   ###

Nmap done: 1 IP address (1 host up) scanned in 37.85 seconds
```

7.5 Scanning by Using Service Name

It Scan by using service name.
-p [Service name] : Scanning using service name.

```
C:\Users\Administrator>nmap 192.168.1.1 -p http,https
```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.033s latency).

PORT      STATE  SERVICE
80/tcp    closed http
443/tcp   closed https
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds
```

Try:
Fast Port Scanning.
Top Ports Scanning
Scanning All Port Except Initial Port.
Scanning All Port Except End Port
Hints:
-F: Fast mode - Scan fewer ports than the default scan

–top-ports [number]: Scan [number] most common ports
-p-[Port number]: Scanning all port except initial port
-p0-: Scanning all port except end port

8. Scanning the network of the target using the Service and version detection.

8.1 Determine the Version of The Service Running on Port.

It's used to find service version.
-sV: Probe open ports to determine service/version info

```
C:\Users\Administrator>nmap 192.168.1.1 -sV

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds

```

8.2 Using Intensity Level to Get Correct Version.

Use intensity level to get correct version. Higher the number possibility of correctness but decrease the speed. –version-intensity [level]: Set from 0 (light) to 9 (try all probes)

```
C:\Users\Administrator>nmap 192.168.1.1 -sV --version-intensity 9

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds

```

8.3 Light Mode of Version Determine.

It is faster but lower possibility of correctness.
–version-light: Limit to most likely probes (intensity 2)

```
C:\Users\Administrator>nmap 192.168.1.1 -sV --version-light

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds

```

8.4 Using Intensity Level 9 For All Version.

Here intensity level 9 is used for all version.
–version-all: Try every single probe (intensity 9)

```
C:\Users\Administrator>nmap 192.168.1.1 -sV --version-all

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds

```

Try
Determine OS, Version, Traceroute and Script Scanning

Hint:
It's used to determine OS, Version, traceroute of packets send and received and script scanning.
-A : Determine OS, Version, traceroute and script scanning

9. Scanning the network of the target using OS detection

9.1 Remote OS Detection Using TCP/IP Stack Fingerprinting

It Enable OS detection.
-O: Enable OS detection

```
C:\Users\Administrator>nmap 192.168.1.1 -O

Expected Output:

Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE    SERVICE
###       ###      ###

TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/22%OT=135%CT=1%CU=44003%PV=Y%DS=0%DC=I%G=Y%TM=5EF8D7
OS:D9%P=i686-pc-windows-windows)SEQ(SP=106%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=
OS:S%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=M
OS:FFD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF
OS:70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=00%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)

Network Distance: 0 hops

OS detection performed.
Nmap done: 1 IP address (1 host up) scanned in 15.72 seconds
```

9.2 OS Scan Limit

Here at least one tcp open and closed port required for scanning.
–osscan-limit: Limit OS detection to promising targets

```
C:\Users\Administrator>nmap 192.168.1.1 -osscan-limit

Expected Output:

Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT    STATE   SERVICE
###     ###     ###

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds
```

9.3 Nmap Scanning More Aggressively

Here OS detection is done more aggressively.
–osscan-guess: Guess OS more aggressively

```
C:\Users\Administrator>nmap 192.168.1.1 -osscan-guess

Expected Output:

Nmap scan report for 192.168.1.1
Host is up (0.0027s latency).
Not shown: 999 closed ports
PORT    STATE   SERVICE
###     ###     ###

Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds
```

Try:
Scanning Number Of OS.
Determine OS, Version, Traceroute And Script Scanning.
Hint:
–max-os-tries : Scanning number of OS
-A : Determine OS, Version, traceroute and script scanning.

10. Scanning the network of the target using the Timing and Performance

10.1 Nmap 192.168.1.1 -T0

nmap Timing and Performance: -T[number]: Used 0 to 5 for speed of scanning. Increase number 0 to 5 speed of scanning also increase.

```
C:\Users\Administrator>nmap 192.168.1.1 -T0

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE     SERVICE
###       ###       ###

Network Distance: 0 hops

OS detection performed.
Nmap done: 1 IP address (1 host up) scanned in 55.72 seconds

```

10.2 Nmap 192.168.1.1 -T1

The T1 Time scan performs more speed up than T0 scan as shown in below speed

```
C:\Users\Administrator>nmap 192.168.1.1 -T1

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE     SERVICE
###       ###       ###

Network Distance: 0 hops

OS detection performed.
Nmap done: 1 IP address (1 host up) scanned in 40.72 seconds

```

Try:
T2 This is default speed of scanning
T3
T4
T5

Hint
Nmap 192.168.1.1 -T2
Like the way apply for T3,T4,T5 also

11. Scanning the network of the target using the Nmap Script Engine (NSE) scripts

11.1 Running NSE scripts:

nmap – sV – –scriptthttp – titlescanme.nmap.org

```
cldrn@cldrn:~$ nmap -sV --script http-title scanme.nmap.org

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-10-29 18:22 PDT
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.092s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
25/tcp   filtered smtp
80/tcp   open     http       Apache httpd 2.2.14 ((Ubuntu))
| http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
9929/tcp open     nping-echo Nping echo
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.39 seconds
cldrn@cldrn:~$
```

11.2 run multiple scripts at once

nmap –script http-headers,http-title scanme.nmap.or

```
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.096s latency).
Not shown: 995 closed ports
PORT      STATE     SERVICE
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
| http-headers:
|    Date: Mon, 24 Oct 2011 07:12:09 GMT
|    Server: Apache/2.2.14 (Ubuntu)
|    Accept-Ranges: bytes
|    Vary: Accept-Encoding
|    Connection: close
|    Content-Type: text/html
|
|_   (Request type: HEAD)
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldp
9929/tcp open      nping-echo
```

.

11.3 Using Script Name

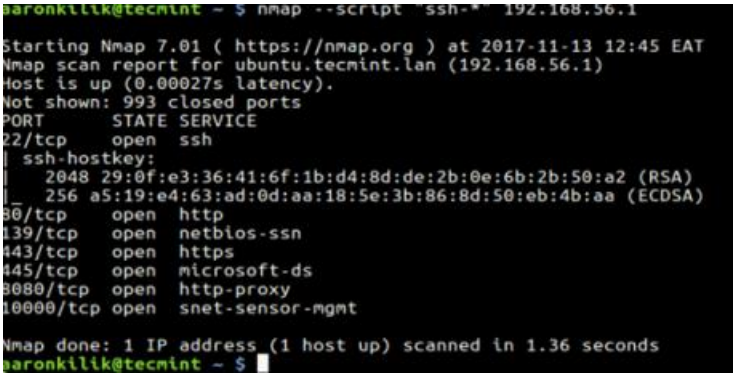
nmap – –scriptthttp – headersscanme.nmap.org

```
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-15 10:39 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Not shown: 996 closed ports
PORT      STATE     SERVICE
22/tcp    open      ssh
80/tcp    open      http
| http-headers:
|    Date: Wed, 15 Nov 2017 05:10:04 GMT
|    Server: Apache/2.4.7 (Ubuntu)
|    Accept-Ranges: bytes
|    Vary: Accept-Encoding
|    Connection: close
|    Content-Type: text/html
|
|_   (Request type: HEAD)
179/tcp   filtered bgp
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 20.96 seconds
```

11.4 Run all the scripts in the vuln category:

nmap -sV –script vuln ¡target¿

Run the scripts in the categories version or discovery:
nmap -sV –script=”version,discovery” ¡target¿
Run all the scripts except for the ones in the exploit category:
nmap -sV –script ”not exploit” ¡target¿
Run all HTTP scripts except http-brute and http-slowloris:
nmap -sV –script ”(http-*) and not(http-slowloris or http-brute)” ¡target¿ Using Categories:
nmap –script default,broadcast 192.168.56.1
Using * Wildcard:
nmap –script ”ssh-*” 192.168.56.1



Try:
Using Boolean Expressions
Not vuln category
Not ssh category
Hint:
For Boolean apply default or broadcast
Apply not vuln
Apply (default or broadcast) and not ssh-

12. Scanning the network of the target using Firewall/IDS evasion and spoofing.

12.1 bypassing Firewall and other IDS

1. Nmap 192.168.1.1 -F
-f: fragment packets
Used small header packets for scanning.
It is harder for Firewall and IDS to filter the packets.

```
C:\Users\Administrator>nmap 192.168.1.1 -f

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE     SERVICE
25/tcp    filtered smtp
110/tcp   filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds

```

12.2 offset size for scanning

Nmap 192.168.1.1 –Mtu 32
–mtu [val]: fragment packets (optionally w/given MTU)
Used offset size for scanning. It is harder for Firewall and IDS to filter the packets.

```
C:\Users\Administrator>nmap 192.168.1.1 --mtu 32

```

Expected Output:

```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE     SERVICE
25/tcp    filtered smtp
110/tcp   filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds

```

12.3 Cloak a scan with decoys

. Nmap 192.168.1.1 Decoy1, Decoy2, Your IP Target IP.
-D [decoy1,decoy2[,ME],...]: Cloak a scan with decoys.

```
C:\Users\Administrator>nmap -D 192.168.1.1 192.168.53.4 192.168.49.5 192.168.1.1

```

Expected Output:

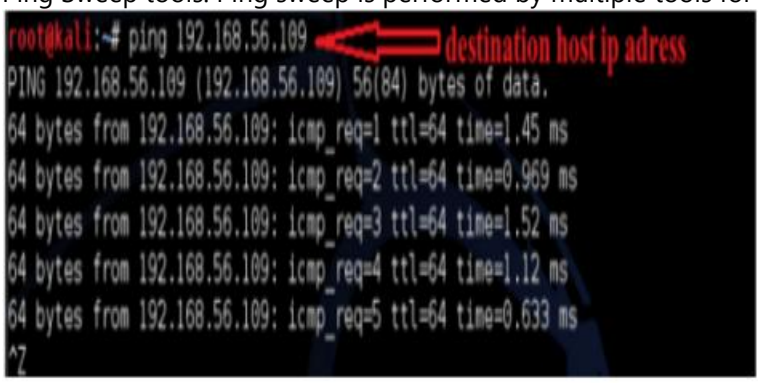
```
Nmap scan report for 192.168.1.1
Host is up (0.00s latency).
Not shown: 991 closed ports
PORT      STATE     SERVICE
25/tcp    filtered smtp
110/tcp   filtered pop3

Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds

```

Try:
specific port no. to scan
Used proxies to scan the IP
Hint:
Use given port number Used specific port no. to scan.
Use Target IP –proxies [url1,[url2],...]: Relay connections through HTTP/SOCKS4 proxies Used proxies to scan the IP. Used target IP at the end.

13. Checking for the live systems using Angry IP scanner tool

13.1 Scanning for Live System in Network by Ping and Ping sweep tools.

Free IP scanner Network Utility Ping:
Ping checks live system with the help of ICMP scanning.
Ping scan sends ICMP ECHO request to a host.
If the host is live, it will return an ICMP ECHO reply.
No reply means host is dead.
Sometimes firewall discards ICMP ECHO request so We cant identify host is live or dead.
Ping Sweep tools: Ping sweep is performed by multiple tools for windows as well as for

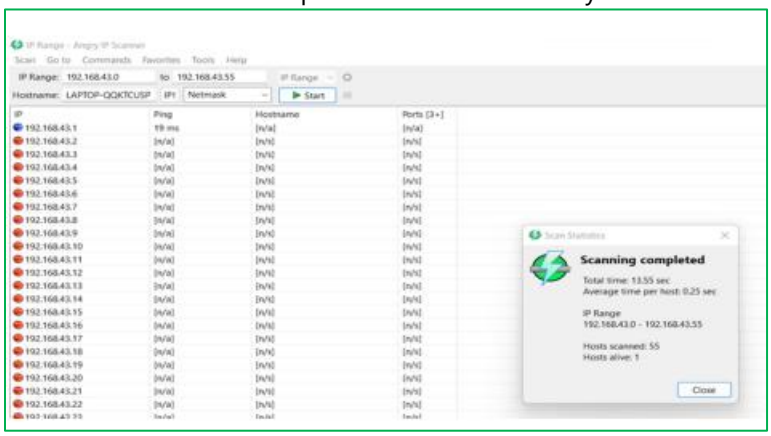


13.2 Zenmap a GUI for Nmap for Ip scanning

Zenmap is a free graphical interface for the very popular port scanner nmap comes with the 10 different scan type ping scan is one of them

Using Angry IP Scanner tool: Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use.

It scans IP addresses and ports as well as has many other features.



Try:

Ip scanning with other tools to display all parameters

Hint:

Use Advanced IP Scanner

Use My Lan Viewer

V. REFERENCE BOOKS:

1. W. Stallings, "Cryptography and Network Security: Principles and Practice", Boston: Prentice Hall, 5th Edition, 2010.
2. A.Das and C.Veni Madhavan, "Public-key Cryptography: Theory and Practice", New Delhi, India: Pearson Education India, 2009.

VI. MATERIAL ONLINE:

1. Course Descriptor
2. Lab Manual