

# **INSTITUTE OF AERONAUTICAL ENGINEERING**

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

#### **COURSE CONTENT**

	NETWORK SECU	RITY	Y LAP	BORAT	ORY			
V Semester: CSE (CS)								
Course Code	Category	Ho	urs / V	Week	Credits	М	aximum	n Marks
	Coro	L	Т	Р	С	CIA	SEE	Total
ACCCUO	Core	0	0	3	1.5	30	70	100
Contact Classes: Nil	Tutorial Classes: Nil	P	Practic	cal Clas	sses: 36	Т	otal Cla	sses: 36
Prerequisite: Python Progra	amming							

#### 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.

## **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=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:
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

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

input: pathping www.iare

#### 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
Нор
    RTT
            Lost/Sent = Pct Lost/Sent = Pct Address
                                              LAPTOP-QQKTCUSP [192.168.43.165]
  0
                                0/100 = 0\%
                                0/100 = 0\% 192.168.43.1
  1
      17ms
               0/100 = 0\%
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>system	info
Host Name:	LAPTOP-00KTCUSP
OS Name:	Microsoft Windows 11 Home Single Language
OS Version:	10.0.22621 N/A Build 22621
DS Manufacturer:	Microsoft Corporation
DS Configuration:	Standalone Workstation
DS Build Type:	Multiprocessor Free
Registered Owner:	SLIM 3
Registered Organization:	N/A
Product ID:	00356-24516-18291-AA0EM
Driginal 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
3IOS Version:	LENOVO GGCN51WW, 11/16/2022
Nindows 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
/irtual Memory: Max Size:	12,583 MB
/irtual Memory: Available:	2,617 MB
/irtual 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
Vetwork 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.

icense Agreement				
Please review the license terms before installing	g Wireshark 4.0.0 64	-bit.		4
Wireshark is distributed under the GNU Genera	l Public License.			
GNU GENERAL PUBLIC LICENSE Version 2, June 1991	E.			^
Copyright (C) 1989, 1991 Free Software Foun 51 Franklin Street, Fifth Floor, Boston, MA 02: Everyone is permitted to copy and distribute w of this license document, but changing it is no	dation, Inc., 110-1301 USA verbatim copies at allowed.			
Preamble				
The licenses for most software are designed t	to take away your	14		~
This is not an end user license agreement (EUL purposes only,	A). It is provided her	re for inform	ational	

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.

Choose which features of Wire	shark 4.0.0 64-bit you want to install.
The following components are	available for installation.
Select components to install:	<sup>₩</sup> Wireshark <sup>™</sup> TShark <sup>™</sup> Plugins & Extensions <sup>™</sup> Tools <sup>™</sup> Documentation
Space required: 228.2 MB	Description Position your mouse over a component to see its description.

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

Wireshark 4.0.0 64-bit Setup		_		$\times$
Additional Tasks				
Create shortcuts and associate file extens	ions.			
Create Shortcuts				
Wireshark Start Menu Item				
Wireshark Desktop Icon				
Wireshark Quick Launch Icon				
Associate File Extensions				
Associate trace file extensions will	th Wireshark			
Extensions include 5vw, acp, apc, at mplog, ntar, out, pcap, pcapng, pklg vwr, wpc, and wpz.	c, bfr, cap, enc, erf, fdc, ipfix J, pkt, rf5, snoop, syc, tpc, tr	, Icap, 1, trace, tro	÷	
Ninebaha) Installer				

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.

Choose Install Location					
Choose the folder in which to install Wiresha	rk 4.0.0 64-bit.				4
Choose a directory in which to install Wireshi	ark.				
Destination Folder C:\Program Files\Wireshark			Bro	wse	
Destination Folder C:\Program Files\Wireshark			Bro	wse	
Destination Folder [C:\Program Files\Wireshark] Space required: 228.2 MB			Bro	wse	
Destination Folder [C:\Program Files\Wireshark] Space required: 228.2 MB Space available: 37.5 GB		(	Bro	wse	
Destination Folder C:\Program Files\Wireshark Space required: 228.2 MB Space available: 37.5 GB redark@ Installer			Bro	wse	

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.

Wireshark 4.0.0 64-bit Setup			
Packet Capture			
Wireshark requires either Npcap or WinPca	p to capture live netwo	rk data.	
Currently installed Npcap or WinPcap ver	sion		
Neither of these are installed			
Install			
Install Npcap 1.71			
(Use Add/Remove Programs first to	uninstall any undetecte	ed old Npcap or	WinPcap
Important notice			
If your system has crashed during a Wi 'net stop npcap' as Administrator before	reshark installation, yo e upgrading Npcap, so	u must run the that it doesn't o	command rash again
Get WinPcap			
Learn more about Npcap and WinPcap			
resherk@ Installer			
	< Back	Next >	Cance
sherk@ Installer	< Back	Next >	Cano

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.

USBPcap is required to capture USB traffic. (experimental)?	Should USBPcap be	installed	-	2
Currently installed USBPcap version				
Lobecap is currency not instated				
Install				
Install USBPcap 1.5.4.0				
(Use Add/Remove Programs first to u	ninstall any undeter	ted old USBPcap	versions)	
Important notice				
In case of issue after installation, please https://github.com/desowin/usbpcap/iss	use the system resto ues/3	ore point created	or read	
I contract of the second second				
Learn more about USBPcap				

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

Extract: li	bwireshark.dll	62%		
Output f Extract: Extract: Extract:	older: C:\Prog uninstall-wires libwiretap.dll libwireshark.d	pram Files\Wiresh shark.exe II 62%	nark	

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.

Npcap 1.71 Setup	Installing	
NMAP, ORG	Please wait while Npcap 1.71 is being installed.	
Installing NDIS filter driv	ver	
Show details		

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

cup nus compreses successionly.		4
omplated		
Extract: x-capture-stop.png		
Extract: x-colorize-packets.png		
Extract: x-resize-columns.png		
Extract: x-stay-last.png		
Extract: zoom-in.png		
Extract: zoom-original.png		
Extract: zoom-out.png		
Output folder: C:\Program Files\Wire	shark\Wireshark User's Guide	
Output folder: C:\Program Hies\Wire	Isnark	
Extract: raq.ntmi		
Completed		

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

	Completing Wireshark 4.0.0 64-bit Setup
	Wireshark 4.0.0 64-bit has been installed on your computer. Click Finish to close Setup.
	Show News
Et.	

## 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.

The Wireshark Network Analyzer		1	- 1	
File Edit View Go Capture Analyze Statistic	Fielephony Wireless Tools	Help		
Apply a display filter				
A STATE OF A DAMAGE AND A STATE OF A STATE O			_	
Welcome to Wireshark				
Capture				
cupture				
using this filter:	ter	<ul> <li>All interfaces show</li> </ul>	vn *	
Wi-Fi	A		~	
Local Area Connection* 9	0.00		111	
Local Area Connection* 8				
Local Area Connection* 7				
Bluetooth Network Connection				
Local Area Connection* 10				
Local Area Connection* 1				
VirtualBox Host-Only Network				
vEthernet (WSL)				
Adapter for loopback traffic captu	ire			
Local Area Connection			~	
-mornar				
Learn				
User's Guide Wiki Questions a	nd Answers · Mailing Lists			
You are running Wireshark 4.0.0 (v4.0.0-	0-g0cbe09cd796b). You receive au	tomatic updates.		
and the second se			Hornson	

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.

	C.E. 1944 C. C.	and a finite Telebook	. Married		-	200	222								
rite -	Edit View Go Caj	pture Analyze Statistics telephon	iy wite	ess	100	5	neip								
11		N	a a	. 9	21								-	_	
Ipa	pty a distalay taker <ch< td=""><td>(1-7-5</td><td></td><td>_</td><td></td><td></td><td></td><td>15.17</td><td></td><td></td><td></td><td>-</td><td>- Con</td><td></td><td>13</td></ch<>	(1-7-5		_				15.17				-	- Con		13
10.	Time	Source D	estination					Pr	otuci	h	Lengt	h 1	nto		
	555 6.496336	192,168.0.103 1	72.217	.166	. 10	16		TL	Svi	.,2	2	32.1	Appl	ica	It:
	556 6.497688	142.250.195.74 1	92.168	.0.1	.03			т	P			:4 4	143	+ 5	14.
	557 6.502495	31.47.196.154 1	92.168	.0.1	.03			Т	P		14	34 4	443	+ 5	18
	558 6,502546	192.168.0.103 3	1.47.1	96.1	54			TO	P			i4 5	6051	0 -	1
	559 6.502866	31.47.196.154 1	92.168	.0.1	EQ			TO	P		14	34 4	143	+ 5	IE!
	560 6.503195	31.47.196.154 1	92.168	.0.1	03			TO	P		14	34 4	143	+ 5	0
	561 6.503223	192.168.0.103 3	1.47.19	96.1	54			т	P			54 3	5051	8 -	1
	562 6,504245	172.217.165.106 1	92.168	.0.1	.03			TO	P			54 4	43	+ 5	4
-	563 6,5//43/	31.47.196.154 1	92.168	.0.1	.03			23	LV4		14:	94 1	encr	ypt	e
															-
Fr	ame 1: 1494 byte	es on wire (11952 bits),	8609	48	56	d8	32	31	f9	c4	бе	1f	49	44	7
Et	hernet II, Src:	Tp-LinkT_49:44:7a (c4:6e	8019	05	c8	fe	15	40	60	32	96	aØ	21	1f	2
In	ternet Protocol	Version 4, Src: 31.47.19	9020	00	67	01	bb	c5	4e	ae	fd	3a	6a	6d	4
Tr	ansmission Contr	rol Protocol, Src Port: 4	9639	01	f5	65	29	90	60	Øf	d7	e5	49	f2	b
Tr	ansport Layer Se	ecurity	8848	77	9b	d1	06	88	54	87	81	a3	d4	21	b
			9626	c7	99	cf	68	60	c9	84	d8	<b>e</b> 9	81	f6	5
			8699	a3	f9	ca	f5	1a	e3	Øb	d6	50	c4	3d	a
			8678	79	e7	57	3c	e6	84	34	c5	c5	d7	03	f
			9989	20	94	63	83	65	53	53	5e	52	26	f6	8
			9098	a3	38	b9	64	e5	51	fő	35	86	a8	d9	2
		>													3

## 2.3 Analyze Packet Header format

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

<u>F</u> ile	<u>E</u> dit <u>V</u> i	ew <u>G</u> o	<u>C</u> apture	<u>A</u> nalyze g	<u>S</u> tatistics Telep	ohon <u>y W</u> ireless <u>T</u> ools <u>H</u>	elp	
📕 Ар	ply a displa	y filter ·	<ctrl-></ctrl->					
No.		Time				Source	Destination	Protocol
	4574	11 202	3-09-05	16:20:	40.062374	Dell_5f:0b:63	Broadcast	ARP
	4574	12 202	3-09-05	16:20:	40.076445	10.1.1.33	10.255.255.255	BROW
	4574	13 202	3-09-05	16:20:	40.085585	0e:4c:a2:2a:60:	Broadcast	ARP
	4574	14 202	3-09-05	16:20:	40.094478	Dell_aa:13:c8	Broadcast	ARP
	4574	15 202	3-09-05	16:20:	40.124737	20.20.19.146	77.74.181.38	ТСР
	4574	16 202	3-09-05	16:20:	40.124890	20.20.19.146	180.87.4.157	ТСР
	4574	17 202	3-09-05	16:20:	40.126687	Dell_aa:13:c8	Broadcast	ARP
	4574	18 202	3-09-05	16:20:	40.128428	Dell_aa:13:c8	Broadcast	ARP
	4574	19 202	3-09-05	16:20:	40.128428	Dell_aa:13:c8	Broadcast	ARP
	4575	50 202	3-09-05	16:20:	40.128428	Dell_aa:13:c8	Broadcast	ARP
	4575	51 202	3-09-05	16:20:	40.128637	Sophos_06:1c:1d	Broadcast	ARP
	4575	52 202	3-09-05	16:20:	40.133700	20.20.21.225	224.0.0.251	MDNS
	4575	53 202	3-09-05	16:20:	40.133700	fe80::c9c:8b51:	ff02::fb	MDNS
	4575	54 202	3-09-05	16:20:	40.133700	HonHaiPr_f7:4d:	Broadcast	ARP
	4575	55 202	3-09-05	16:20:	40.143685	Dell_aa:13:c8	Broadcast	ARP
	4575	56 202	3-09-05	16:20:	40.156462	Hangzhou_bd:50:	Broadcast	ARP
	4575	57 202	3-09-05	16:20:	40.165425	HewlettP_ce:fc:	Broadcast	ARP
	4575	58 202	3-09-05	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 captured
    Section number: 1
  v 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 secon
    [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)
    reasons de manieras estas
```

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.

Choose Which features of Nma	p you want to install.	
Check the components you wa install. Click Next to continue.	nt to install and uncheck the com	ponents you don't want to
Select components to install:	Mmap Core Files     Register Nmap Path     Npcap 1.50     Check for newer Npca     Network Performance     V Zermap (GUI Fronten)	Description Position your mouse over a component to see its description.
Space required: 84.3 MB	VNdiff (Scan comparison Ncat (Modern Netcat r	
loft Install System v3.07		

**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.

Thingp occup	S-11-1
Choose Install Location	Gui
Choose the folder in which to install Nmap.	
Setup will install Nmap in the following folder. To install in a d select another folder. Click Install to start the installation.	ifferent folder, dick Browse and
Destination Folder C: Program Files (x86)Wmap	Browse
Destination Folder C: Program Files (x86)(Winap Space required: 94.3 MB	Browse
Destination Folder C.:Program Files (x86) (Winap Space required: 84.3 MB Space available: 57.8 GB	Browse
Destination Folder C:Program Files (x86)(Wnap Space required: 84,3 MB Space available: 57,8 GB	Browse

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.

🕞 Npcap 1.50 Setup	_		
NMAP: ORG			
Completed			
Show details			
Nullsoft Install System v3.06.1		_	- 2
< Back Next >		Can	cel 📄

**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.

Setup was completed successfully.		
Completed		
Output folder: C: (Program Files (x86)) Output folder: C: (Program Files (x86)) Extract: gtlrc Output folder: C: (Program Files (x86)) Output folder: C: (Program Files (x86)) Extract: ncat.exe Extract: ca-bundle.crt Output folder: C: (Program Files (x86)) Extract: nping.exe Completed	Imap   py 2exe \share \themes WS-Wir Imap   py 2exe \share \themes WS-Wir Imap Imap	Idows A
lsoft Install System v3.07		

**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.

🕞 Nmap Setup		
Finished Thank you for installing Nmap		
Nmap has been installed on your compu	ter.	
Click Finish to close this wizard.		
Nullsoft Install System v3.07		ii
	< Back Finish	Cancel

**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

Zenmap		-
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile <u>H</u> elj	p	
Target: www.amazon.com	V Profile:	Regular scan
Command: nmap www.an	nazon.com	Intense scan
		Intense scan plus UDP
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	Intense scan, all TCP ports
OS 4 Host	nmap www.amazon.com	Intense scan, no ping
W www.amazon.com Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-08 10:54 India Standard Time		Ping scan
	Nmap Scan report for WWW.amazon.com (108.157.247.131) Host is up (0.017s latency).	Quick scan
	rDNS record for 108.157.247.131: server-108-157-247-131.hyd57.r.cloudfront.net	Quick scan plus
	PORT STATE SERVICE	Quick traceroute
	21/tcp open ftp 25/tcp open smtp	Regular scan
	80/tcp open http 110/tcp open pop3	Slow comprehensive scan
	143/tcp open imap	
	443/tcp open https 465/tcp closed smtps	
	587/tcp open submission	
	6346/tcp closed gnutella	
	Nmap done: 1 IP address (1 host up) scanned in 17.17 seconds	
	rDNS record for 108.157.247.131: server-108-157-247-131.hyd57.r.cloudfront.net Not shown: 991 filtered tcp ports (no-response) PORT STATE SERVICE 21/tcp open ftp 25/tcp open http 109/tcp open http 110/tcp open imap 443/tcp open imap 443/tcp open imap 443/tcp closed smtps 587/tcp open submission 6346/tcp closed gnutella Nmap done: 1 IP address (1 host up) scanned in 17.17 seconds	Quick scan plus Quick traceroute Regular scan Slow comprehensive scan

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

👁 Zenmap			
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> elp	lp		
Target: 108.157.247.131		<ul> <li>Profile:</li> </ul>	Regular scan
Command: nmap 108.157.	/.247.131		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans		
OS 4 Host	nmap 108.157.247.131		
3 www.amazon.com	<pre>Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-08 11:02 India Standard Nmap scan report for server-108-157-247-131.hyd57.r.cloudfront.net (108.15 Host is up (0.011s latency). Not shown: 991 filtered tcp ports (no-response) PORT STATE SERVICE 21/tcp open ftp 25/tcp open ftp 80/tcp open http 110/tcp open pop3 143/tcp open imap 443/tcp open imap 443/tcp closed smtps 587/tcp closed smtps 587/tcp closed gnutella Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds</pre>	d Time 57.247.131)	

#### 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.



The fallowing figure shows how the SYN Scan will working.

Figure 5.2. SYN sca	n of open port 22		
	krad# meap -p22,113,1	SYN (Request port 22 connection)	
	starting Nwap ( http: Interesting ports on PORT STATE SERV 22/tcp open ssh	SYN/ACK (It's open, go ahead)	
	113/tcp closed auth 139/tcp filtered netb	RST (No, forget it!)	
	krad		scanme

## 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.



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



### 5.2. TCP Connect Port Scan

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



## 5.3 UDP Port Scan

It scan only UDP ports. -sU: UDP Scan



## 5.4 TCP ACK Port Scan

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



## 5.5 TCP Window Port Scan

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



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



#### **Expected Output:**

```
1 Nmap scan report for 192.168.1.1
2 Nmap scan report for 192.168.1.2
3 Nmap scan report for 192.168.1.3
4 Nmap scan report for 192.168.1.4
5 Nmap done: 4 IP addresses (0 hosts up) scanned in 2.13 seconds
6
```

## 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





## 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



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



## 7.2 Range of Port Scanning

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

_	
1	C:\Users\Administrator>nmap 192.168.1.1 -p 21-30
Exp	pected Output:
1	Stats: 0:00:02 elapsed: 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
2	ARP Ping Scan Timing: About 100.00% done: FTC: 18:52 (0:00:00 remaining)
	Name scap report for 192,168.1.1
4	Host is up (0.0042s latency).
-	
6	PORT STATE SERVICE
- 7	21/tcn closed ftn
	22/tcp closed ssh
a a	23/tcp closed telnet
1.0	24/tcp closed privemail
11	25/tcp closed setp
12	26/tcp closed rsftp
13	27/tcp closed nsw-fe
14	ZB/tcp closed unknown
15	29/tcp closed msg-icp
16	30/tcp closed unknown
17	
18	Nmap done: 1 IP address (1 host up) scanned in 2.91 seconds
1.9	

# 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

12	C:\Users\Administrator>nmap 192.168.1.1 -p U:53,T:21-30,80
Exp	ected Output:
194	Nmap scan report for 192.168.1.1 Host is up (0.0086s latency).
	PORT STATE SERVICE
	22/tcp closed ssh
	24/tcp closed priv-mail
	26/tcp closed satp
	28/tcp closed inknown
	30/tcp closed msg-lcp 30/tcp closed unknown
	BU/ICP Closed HTTP
17	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.



## 7.5 Scanning by Using Service Name

It Scan by using service name.

-p [Service name] : Scanning using service name.



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



## 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)



### 8.3 Light Mode of Version Determine.

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



## 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)

1 C:\Users\Administrator>nmap 192.168.1.1 -sV --version-all 2 Expected Output: 1 Nmap scan report for 192.168.1.1 2 Host is up (0.0027s latency). 3 Not shown: 999 closed ports 4 PORT STATE SERVICE VERSION 5 53/tcp open domain dnsmasq 2.51 6 7 Nmap done: 1 IP address (1 host up) scanned in 15.84 seconds 8

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

2	ers\Adminis	trator>nmap 192.160.1.1 -0
Expecte	d Output	t:
1 Nemap 2 Host 3 Not 3 4 PORT 4 PORT 4 PORT 4 7 TCP/1 6 JJJ 6 JJJ 6 JJJ 7 TCP/1 1 0515C 0 0512 10 0515C 10 0505C 10 0515C 10 0515	scan report is up (0:00 Thomas 1.07 Thomas	<pre>row 193.1468.1.1 a latency). loses purits loses purits set row 193.1468.1.1 a latency). loses purits set row 104.144.144.144.144.144.144.144.144.144.</pre>

## 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

```
1 C:\Users\Administrator>nmap 192.168.1.1 -osscan-limit
2

Expected Output:

1 Nmap scan report for 192.168.1.1

2 Host is up (0.0027s latency).

3 Not shown: 999 closed ports

4 PORT STATE SERVICE

5 ### ###

6

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

8
```

## 9.3 Nmap Scanning More Aggressively

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



#### **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.



## 10.2 Nmap 192.168.1.1 -T1

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



Try:

T2 This is default speed of scanningT3

Τ4

Т5

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 – –scripthttp – titlescanme.nmap.org



### 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
1
<pre>[_ (Request type: HEAD)</pre>
_http-title: Go ahead and ScanMe!
646/tcp filtered ldp
9929/tcp open nping-echo

#### **11.3 Using Script Name**

nmap - -scripthttp - headersscanme.nmap.org



#### **11.4 Run all the scripts in the vuln category:**

nmap -sV -script vuln itarget;

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

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.



## 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.



## 12.3 Cloak a scan with decoys

. Nmap 192.168.1.1 Decoy1, Decoy2, Your IP Target IP.



#### 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

1000	fiva (1	1	oruñ 19511001001	103		lestination	1 host it	) adress
PING	192.	168.5	56.109 (192.168.	56.109) 56(8	84) byte	es of data.		
64 b	ytes	from	192.168.56.109:	icmp_req=1	ttl=64	time=1.45	ns	
64 b	ytes	from	192.168.56.109:	icmp_req=2	ttl=64	time=0.969	ms	
64 b	ytes	from	192.168.56.109:	icmp_req=3	ttl=64	time=1.52	ms	
64 b	ytes	from	192.168.56.109:	icmp req=4	ttl=64	time=1.12	ns	
64 b	ytes	from	192.168.56.109:	icmp req=5	ttl=64	time=0.633	ms	
^7				-				

## 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.

IP Range: 192.168.43.0	10 192.168.4	155 If flange - O					
Hostname: LAPTOP-QQ	KTCUSP IPt Netmas	R - P Start -					
P	Ping	Hostname	Ports (3+)				
192.168.43.1	10 104	[m/a]	(ryta)				
192.168.43.2	(m/a)	[m/n]	[n/5]				
192.168.43.3	04/40	01/10	[n/h]				
192.168.43.4	(n/a)	[n/s]	(ry/s)				
192.168.43.5	(m/a)	[n/s]	[m/s]				
9192.168.43.6	(9/4)	[mn]	[m/s]				
92.168.43.7	1×/41	Envisi	[m/s]				
92.168.43.8	34/A3	[rs/a]	[14/4]				
9192.168.43.9	In/al	Jrs/s0	6n/n2	Contraction Statistics	×		
92.168.43.10	(m/n)	10/50	0m/n2				
192.168.43.11	(m/m)	[m/s]	(m/s)	Scanning con	pleted		
192.168.43.32	[14/26]	10/10	[19/52	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0		
192.168.43.13	∃n/a]	En/sil	[m/s]	Total time 11.55 s	13.55 sec		
192.168.43.14	04/A1	in/si	19/91	www.age one per	101 023 MI		
9192.168.43.15	04/40	(pyn)	[m/s]	SP Range			
192.168.43.16	12.168.43.16 (n/a) (n/a)		(m/s)	192.168.43.0 - 192	168-43.55		
192.168.43.17	0%/40	[m/s]	Infit				
9192.168.43.18	(n/a)	(n/s)	[n/s]	Hosts scanned: 55			
192.168.43.19	(14/4)	10/10	(m/s)	Paints across 1			
192.168.43.20	(w/w)	[m/s]	[1/1]				
192.168.43.21	(m/a)	Invid	[1/1]		Close		
192.168.43.22	[14/W]	[15/3]	In/sl				
102 102 10 12 12	Sec. And	De fait	Includ				

#### 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, 5<sup>th</sup> 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