

Real Time Cyber Threat Detection and Mitigation Practical Manual





Chikitsak Samuha's

Sir Sitaram and Lady Shantabai Patkar College of Arts and Science

and V.P. Varde College of Commerce and Economics



Chapter 1. Advanced Network Security

Lab1: Create a basic network monitoring environment for realtime threat detection using NMAP and ZENMAP.

1. NMAP

Nmap (Network Mapper) is an open-source tool used for network discovery and security auditing. It allows to Discover Hosts, Port Scanning, Service Detection, Operating System Detection, Network Inventory. Nmap is widely used by network administrators and security professionals for monitoring network security and conducting vulnerability assessments.

Task 1: Installation of Nmap on Ubuntu

- 1. What command should you run to update the package list on Ubuntu?
- 2. What command do you use to install Nmap?
- 3. How can you verify that Nmap has been installed successfully?

Task 2: Network Scanning

- 4. 4. What command will you use to scan the network and identify which servers and devices are up and running in the subnet 192.168.1.0/24?
- 5. 5. Any types of Nmap scans that you are aware of?

Step 1: installation of Nmap on Ubuntu

command \rightarrow sudo apt update

root@comp413:~# sudo apt update
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1854 kB]
Get:5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [300 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [13.3 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2451 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [422 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 c-n-f Metadata [584 B]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [910 kB]

command → sudo apt install nmap

root@comp413:~# sudo apt install nmap Reading package lists... Done Building dependency tree... Done Reading state information... Done The following additional packages will be installed: liblias3 liblinear4 liblua5.3-0 lua-lpeg nmap-common Suggested packages: liblinear-tools liblinear-dev ncat ndiff zenmap The following NEW packages will be installed: liblias3 liblinear4 liblua5.3-0 lua-lpeg nmap-common 0 upgraded, 6 newly installed, 0 to remove and 134 not upgraded. Need to get 6113 kB of archives. After this operation, 268 MB of additional disk space will be used. Do you want to continue? [Y/n] y Get:1 http://archive.ubuntu.com/ubuntu jammy/main amd64 liblas3 amd64 3.10.0-2ubuntu1 [228 kB] Get:2 http://archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB] Get:4 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]

command \rightarrow nmap --version



root@comp413:~# nmap --version Nmap version 7.80 (https://nmap.org) Platform: x86_64-pc-linux-gnu Compiled with: liblua-5.3.6 openssl-3.0.2 nmap-libs:

Step 2: Scan a network and find out which servers and devices are up and running:

command \rightarrow nmap 192.168.1.0/24

🔤 Adminis	trator: Comma	and Prompt	-	o >	<		
Microsof	t Windows	[Version 10.0.22000.856]					
(c) Micro	osoft Corp	poration. All rights reserved.					
					11		
C:\Users\Administrator>nmap 192.168.1.0/24							
Starting	Nmap 7.95	5 (http://nmap.org) at 2024-10-14 10:55 India Standard Time					
Nmap scar	n report f	For 192.168.1.10					
Host is u	up (0.019s	s latency).					
Not show	n: 976 clo	osed top ports (reset)					
PORT	STATE	SERVICE					
100/tcp	open	newacct					
135/tcp	open	msrpc					
139/tcp	open	netbios-ssn					
445/tcp	open	microsoft-ds					
1025/tcp	open	NFS-or-IIS					
1026/tcp	open	LSA-or-nterm					
1027/tcp	open	IIS					
1028/tcp	open	unknown					
1029/tcp	open	ms-lsa					
1030/tcp	open	iad1					
1067/tcp	open	instl_boots					
1073/tcp	open	bridgecontrol					
1533/tcp	filtered	virtual-places					
1801/tcp	open	msmq					
2103/tcp	open	zephyr-clt					
2105/tcp	open	eklogin					
2107/tcp	open	msmq-mgmt					
2222/tcp	open	EtherNetIP-1					
3389/tcp	open	ms-wbt-server					
3814/tcp	filtered	neto-dcs					
5357/tcp	open	wsdapi					
5985/tcp	open	wsman					
7070/tcp	open	realserver					
8080/tcp	open	http-proxy					
MAC Addr	ess: 30:90	C:23:74:6D:C2 (Micro-Star Intl)					
Nmap scar	n report f	For 192.168.1.20					
Host is I	up (0.011s	s latency).					
Not show	n: 983 clo	osed top ports (reset)					
PORT	STATE	SERVICE					
80/tcp	open	http					
135/tcp	open	msrpc					
139/tcp	open	netbios-ssn					
443/tcp	open	https					



Zenmap is the graphical user interface (GUI) for Nmap, designed to make network scanning easier and more accessible. It allows users to visualize and interact with Nmap's powerful features without needing to use command-line instructions. Key functionalities include User-Friendly Interface, Profile Selection, Target Specification, Visual Outputs. Zenmap is a valuable tool for network administrators and security professionals, facilitating effective network monitoring and vulnerability assessments.

Task 1: Download and Installation

- 1. Where can you download Zenmap?
- 2. What steps must you follow to install Zenmap on your system?

Task 2: Basic Network Scan

- 3. Which profile should you select for a quick scan?
- 4. What types of output will you receive after performing the scan? (List them.)

Task 3: Scanning Techniques

- 5. How can you scan multiple IP addresses or subnets using Zenmap?
- 6. What command can you use to scan the subnet while excluding a specific host (e.g., 192.168.1.101)?
- 7. What command would you use for a fast scan on the network range 192.168.1.10/24?
- 8. How can you observe packets sent and received during a scan?

Task 4: Single Host Scan

9. How do you scan a single host in Zenmap?

Task 5: Saving Scan Results

10. What steps do you follow to save your scan results in Zenmap?



Step 1: Download Zenmap from https://nmap.org

$\leftrightarrow \rightarrow$	G	🔓 https	://nmap.org					\$	🌲 🖸 🗊 🚯 🗄
				b		Npcap.co	m Seclists.org Sect	tools.org Insecure.org)
			NMAP. ORG	Site Search				[Q	
			Download	Reference Guide	Book	Docs	Zenmap GUI	In the Movies	
					<u>Get Nmaj</u> Ne	<u>p 7.95 here</u>			
 Nmap org has been redesigned! Our new mobile-friendly layout is also on Npcap com, Seclists org, Insecure.org, and Sectools.org. Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Amouncement] [Download page] After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Amouncement] [Download page] Nmap 7.80 was released for DEFCON 27! [release notes download] Nmap 7.80 was released for DEFCON 27! [release notes download] Nmap 7.50 is now available! [release notes download] We're pleased to release our new and Improved Iccons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet! Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to Jaunch nuclear missiles in G.I. Joe: Retaintion! We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new QS and yersion detection, and more! Activate Windows fautores! [Announcement/Details], [Download Site] We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! Announcement/Details]. [Download Site] Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.0!! Nmap 6 is now available! [release notes download] 								Windows ngs to activate Windows.	

← → C 🔄 https://nmap.org/download ☆ 🏨 🖸 | 🕶 📵 🗄 Npcap.com Seclists.org Sectools.org Insecure.org 0 Q Site Search NMAP. ORG Reference Guide Download Book Docs Zenmap GUI In the Movies **Downloading Nmap** Get the latest Nmap for your system: <u>Windows</u> <u>macOS</u> Linux (RPM) . Any other OS (source code) Older versions (and sometimes newer test releases) are available from the <u>Nmap release archive</u> (and really old ones are in <u>dist-old</u>). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the <u>sigs directory</u> (<u>verification instructions</u>). Before downloading, be sure to read the relevant sections for your platform from the <u>Nmap Install Guide</u>. The most important changes (features), bugfixes, etc) in each Nmap version are described in the <u>changelog</u>. Using Nmap is covered in the <u>Reference</u> <u>Guide</u>, and don't forget to read the other <u>available documentation</u>, particularly the official book <u>Nmap Network Scanning</u>! Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address bare. by submitting your email address here: Subscribe to Nmap-hackers (or subscribe with custom options from the <u>Nmap-hackers list info page</u>) Activate Windows Go to Settings to activate Window You can also get updates by liking Nmap on Facebook or following us @nmap on Twitter.





→ C 25 https://nmap.org/download#windows ←



coporate	a organize		open	Server			
← → × ↑ 🕹 × T	his PC > Downloads >				✓ ひ Search Downloads		٩
🗸 🖈 Quick access	Name	Date modified	Туре	Size		^	
📃 Desktop 🛛 🖈	✓ Ioday (2)						
👆 Downloads 🛛 🖈	. 🔞 nmap-7.95-setup	10/13/2024 9:28 PM	Application	33,174 KB			
	1-4						

Step 2: After downloading the application, install it in the system.

💮 Nmap Setup —	×			
License Agreement	NUIS			
Please review the license terms before installing Nmap.	J			
Press Page Down to see the rest of the agreement.				
For more information on this license, see <u>https://nmap.org/npsl/</u> 0. Preamble	^			
The intent of this license is to establish freedom to share and change the software regulated by this license under the open source model. It also includes a Contributor Agreement and disclaims any warranty on Covered Software. Companies wishing to use or incorporate Covered Software within their own products may find that our Nmap OEM product (<u>https://nmap.org/oem/</u>) better suits their needs. Open source developers who wish to incorporate parts of Covered Software into free software with conflicting licenses may write Licensor to request a waiver of terms.				
If you accept the terms of the agreement, dick I Agree to continue. You must accept the agreement to install Nmap.				
I Agree Can	el			



🕞 Nmap Setup		_	\times				
Choose Components Choose which features of Nma	p you want to install.	C					
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.							
Select components to install:	 Nmap Core Files Register Nmap Path Npcap 1.79 Check online for newe Network Performance Zenmap (GUI Fronteni Ndiff (Scan comparison 	Description Position your mouse over a component to see its description.					
Space required: 80.5 MB	< Ncat (Modern Netcat r v						
Nullsoft Install System v3.08							
	< Back	Next > Cancel					

😚 Nmap Setup	_		×
Choose Install Location Choose the folder in which to install Nmap.			
Setup will install Nmap in the following folder. To install in a different fold select another folder. Click Install to start the installation.	der, dick	Browse	and
Destination Folder C:\Program Files (x86)\VImap	Brov	vse	
Space required: 80.5 MB Space available: 93.7 GB			
Nullsoft Install System v3.08	all	Car	ncel



🌐 Nmap Setup		—		\times
Installing Please wait while Nmap is being installed.				
Extract: Uninstall.exe 100%				
Show details				
Nullsoft Install System v3.08				
	< Back	Next >	Can	cel

🌍 Npcap 1.79 Setup		_		×			
NMAP. ORG	License Agreement Please review the license terms before	e installing N	pcap 1.79	l.			
Press Page Down to see th	Press Page Down to see the rest of the agreement.						
NPCAP COPYRIGHT / END	USER LICENSE AGREEMENT			^			
Npcap (<u>https://npcap.com</u> library and is copyright (c) Project"). All rights reserv) is a Windows packet sniffing driver and 2013-2023 by Nmap Software LLC ("The red.	Nmap					
Even though Npcap source not open source software software without special p standard (free) version is	e code is publicly available for review, it is and may not be redistributed or used in o ermission from the Nmap Project. The usually limited to installation on five	; other		¥			
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.79.							
Nullsoft Install System v3.07 -		A	6				
		Agree	Cano	lei			

	o-funded by le European Union					
🌍 Npcap 1.79 Se	tup			_		>
NMAP. OR	G Installation	on Optio	ns following optior	ns before installi	ing Npcap	1.79
□ Restrict M ☑ Support r ☑ Install Np Nullsoft Install Syst	lpcap driver's access to aw 802.11 traffic (and cap in WinPcap API-con :em v3.07	o Administ monitor n mpatible N	ators only node) for wirele node	ss adapters		
		[< Back	Install	Can	icel

💮 Npcap 1.79 Setup		_		\times
NMAP. ORG	Installation Complete Setup was completed successfully.			
Completed				
Show details				
Nullcoft Toctall System v3:07				
Truisore inscall bystelli vo, 07 -	< Back N	ext >	Cano	el

 \times



i Npcap 1.79 Setup		—		\times
MMAP.ORG	Finished Thank you for installing Npcap			
Npcap has been installe	d on your computer.			
Click Finish to close this	wizard.			
Nullsoft Install System v3.07				
	< Back	Finish	Cano	cel

💮 Nmap Setup		_		×
Installation Complete Setup was completed successfully.				
Completed				
Output folder: C:\Program Files (x86)\Wmap Extract: ndiff.py Extract: ndiff.bat Extract: NDIFF_README Output folder: C:\Program Files (x86)\Wmap Extract: ncat.exe Extract: ca-bundle.crt Output folder: C:\Program Files (x86)\Wmap Extract: nping.exe Completed				*
Nullsoft Install System v3.08	< Back	Next >	Ca	ncel



🌍 Nmap Setup		—		×
Create Shortcuts				
☑ Start Menu Folder ☑ Desktop Icon				
Nullsoft Install System v3,08	< Back	Next >	Car	ncel

词 Nmap Setup	_		\times
Finished Thank you for installing Nmap			
Nmap has been installed on your computer.			
Click Finish to close this wizard.			
Nullsoft Install System v3.08 – Kack F	inish	Ca	ncel



Step 3: The Zenmap has been installed

📑 Zenmap			_	\Box ×
Scan Tools Profile He	elp			
Target:	Profile: Intense sca	an 💌	Scan	Cancel
Command: nmap -T4 -A	-v			
Hosts Services	Nmap Output Ports / Hosts	Topology Host Details	Scans	
OS Host 🔺			-	Details
			Act	ivate Win
Filter Hosts			Go ti	o Settings to

Step 4: Scan a network and find out which servers and devices are up and running:

In Target give 192.168.1.0/24, Profile give Quick Scan

a. The following output will give for Nmap Output





b. The following output will give for Ports/Hosts Output

📴 Ze	nmap														-	
Scan	Tools	Profile	Hel	lp												
Target	192	2.168.1.0/24	4							-	Profile:	Quick scan		•	Scan	
Comm	and:	nmap - T4	4 -F 19	92.168	.1.0/24											
Ho	sts	Services				ut Ports /	Hosts									
os	Hos	a a			Port	Protocol	State	Service	Version							
	192.	168.1.0			22	tcp	open	ssh								
	192.	168.1.10			23	tcp	open	telnet								18
	192.	168.1.20			80	tcp	open	http								
	192.	168.1.82			443	tcp	open	https								18
	192.	168.1.86														
	192.	168.1.87														
	192.	168.1.88														
	192.	168.1.89														
	192.	168.1.90														
	192.	168.1.92														
	192.	168.1.93														
	192.	168.1.94														
	192.	168.1.95														
	192.	168.1.96														
	192.	168.1.97														
	192.	168.1.98														
	192.	168.1.99														
	192.	168.1.100														
	192.	168.1.101														
	192.	168.1.102														
	Filter	Hosts														

c. The following output will give for topology





d. The following output will give for Host details

🍠 Zenm	ар					- 0 ×
Scan T	ools Profile Hel	p				
Target:	192.168.1.0/24		•	Profile:	Quick scan	Scan Cancel
Comman	d: nmap - T4 - F 19	2.168.1.0/24				
Hosts	Services		igy Host Details Scans			
	Host 192168.1.0 192.168.1.0 192.168.1.20 192.168.1.82 192.168.1.82 192.168.1.85 192.168.1.85 192.168.1.90 192.168.1.90 192.168.1.90 192.168.1.93 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.95 192.168.1.01 192.168.1.101 192.168.1.102	▼ 192.168.1.0 State: up opt: 4 ports: 50 Closed 46 ports: 100 ports: 100 up time: Not available V Addresses IPv4: 192.168.1.0 IPv5: Not available MAC: 06DAD20F;C1:86 V Comments				
Fi	ter Hosts					

Step 5: Scan multiple IP addresses or subnets:

对 Zenmap						-	o x
Scan Too	ls Profile H	lp					
Target: 1	92.168.1.214 192	168.1.222 192.168.1.230	Profile:	Quick scan	•	Scan	
Command:	nmap - T4 - F	92.168.1.214 192.168.1.222 192.168.1.230					
Hosts	Services	Nmap Output Ports / Hosts Topology Host Details					
OS H	ost 🔺	nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230				•	Details
19	2.100.1.0	Starting Nmap 7.95 (https://nmap.org) at 2024-09-24 10	55 Indi a Star	ndard Time			
10 IS	2 168 1 20	Nmap scan report for 192.168.1.214 Host is up (0.00093s latency).					
	2 168 1 82	Not shown: 94 closed tcp ports (reset) PORT STATE SERVICE					
III 19	2.168.1.86	135/tcp open msrpc					
III 19	2.168.1.87	445/tcp open microsoft-ds					
I 9	2.168.1.88	3389/tcp open ms-wbt-server 5357/tcp open wsdapi					
📝 19	2.168.1.89	5900/tcp open vnc MAC Address: C8:52:CF:03:00:F1 (HP)					
F 19	2.168.1.90	INC Address. co.ok.cr.00.00.01 (hr)					
📝 19	2.168.1.92	Nmap scan report for 192.168.1.222 Host is up (0.00080s latency).					
📝 19	2.168.1.93	Not shown: 93 closed tcp ports (reset)					
🕑 19	2.168.1.94	135/tcp open msrpc					
🕑 19	2.168.1.95	139/tcp open netbios-ssn 445/tcp open microsoft-ds					
📝 19	2.168.1.96	3389/tcp open ms-wbt-server					
📝 19	2.168.1.97	5900/tcp open vnc					
📝 19	2.168.1.98	7070/tcp open realserver <u>MAC Address:</u> C8:5A:CF:03:01:3F (HP)					
📝 19	2.168.1.99	Name good second for 102 169 1 220					
📝 19	2.168.1.100	Host is up (0.00052s latency).					
🕑 19	2.168.1.101	Not shown: 96 filtered tcp ports (no-response) PORT STATE SERVICE					
🗾 19	2.168.1.102	135/tcp open msrpc					
🗾 19	2.168.1.104	445/tcp open microsoft-ds					
Filte	r Hosts	3389/tcp open ms-wbt-server MAC Address: B4:2E:99:0B:31:93 (Giga-byte Technology)					





🛃 Zenmap

D	iop.												
Scan	Tools Profile H	lelp											
Target:	192.168.1.214 192	2.168.1.22	2 192.168	.1.230				-	Profile:	Quick scan	•	Scan	
Comman	ommand: nmap -T4 -F 192.168.1.214 192.168.1.222 192.168.1.230												
Hosts	Services			it Ports /	Hosts								
OS	Host 🔺		Port	Protocol	State	Service	Version						
.W	192.168.1.0		22	tcp	open	ssh							
	192.168.1.10		23	tcp	open	telnet							
	192.168.1.20		80	tcp	open	http							
	192.168.1.82		443	tcp	open	https							
	192.168.1.86												
	192.168.1.87												
	192.168.1.88												
	192.168.1.89												
	192.168.1.90												
	192.168.1.92												
	192.168.1.93												
	192.168.1.94												
	192.168.1.95												
	192.168.1.96												
	192.168.1.97												
	192.168.1.98												
	192.168.1.99												
	192.168.1.100												
	192.168.1.101												
	192.168.1.102												
	192.168.1.104												
F	ilter Hosts												

🛃 Zen	map			- 0 ×
Scan	Tools Profile H	lp		
Target:	192.168.1.214 192	168.1.222 192.168.1.230	Profile: Quick scan	Scan Cancel
Comma	and: nmap -T4 -F	92.168.1.214 192.168.1.222 192.168.1.230		
Hos	ts Services	Nmap Output Ports / Hosts Topology Host Deta		
OS	Host 🔺	Hosts Viewer Fisheye Controls		Legend Save Graphic
	192.168.1.10			
	192.168.1.20			
	192.168.1.82		192 (193) (193) (193) (193)	
	192.168.1.86			
۲	192.168.1.87		192.168.1.20	
۲	192.168.1.88		192,168,1,10	
	192.168.1.89		192.168.1.151	
	192.168.1.90		192.168.1.213	
	192.168.1.92		492,168,194	
	192.168.1.93		192.168:1.214 (Oggalhös)	
	192.168.1.94		192 168 1 402	
	192.168.1.95		192.168.1.99	
	192.168.1.96			
	192.168.1.97		192 168 1 211	
	192.168.1.98			
	192.168.1.99		168.1.272	
	192.168.1.100			
	192.168.1.101			
	192.168.1.102			
	192.168.1.104			
	Filter Hosts	Fisheye on ring	with interest factor	and spread factor 0.50 — +



Step 6: Scan by excluding a host:

Command > nmap 192.168.1.0/24 --exclude 192.168.1.101

That will exclude the host while scanning.

🛃 Zenmap				_	ð X	
Scan Tools Profile H	lelp					
Target: nmap 192.168.1.)/24exclude 192.168.1.101	Profile:	Quick scan	▼ Scan		
Command: nmap -T4 -F	mmand: nmap -T4 - Fexclude 192.168.1.10 nmap 192.168.1.0/24exclude 192.168.1.101exclude 192.168.1.10exclude 192.168.1.10ex					
Hosts Services	Nmap Output Ports / Hosts Topology Host Details S					
OS Host 🔺	nmap -T4 -Fexclude 192.168.1.10 nmap 192.168.1.0/24			-	Details	
Image: 192,168,1,0 192,168,1,10 192,168,1,20 192,168,1,20 192,168,1,20 192,168,1,20 192,168,1,20 192,168,1,20 192,168,1,20 192,168,1,26 192,168,1,26 192,168,1,39 192,168,1,94 192,168,1,94 192,168,1,93 192,168,1,94 192,168,1,94 192,168,1,94 192,168,1,94 192,168,1,94 192,168,1,95 192,168,1,94 192,168,1,95 192,168,1,97 192,168,1,99 192,168,1,99 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,1,02 192,168,	Starting Namp 7-85 (https://mmap.org) at 2024-09-24 11: Talled to resolve "mmap" Not sendre "mmap" Not sendre "mmap" Not shown: 88 closed top ports (reset) PORT STATS SERVICE 80/top open mtps 133/top open mtnown 49153/top open mtnown 49153/top open mthown 141/top open ftp 80/top open ftp 133/top open ftp 133/top open mtrow-sen 133/top open mtps 133/top open mtps 133/top open mtps 133/top open mtps 133/top open ftp 80/top open ftp 80/top open ftp 80/top open mtrow-sen 133/top open mtrow-sen 133	02 India Stam	ndard Time			

Step 7: Fast nmap scanning for a network range:

nmap -F 192.168.1.10/24

🛃 Zenm	ар						_	o ×
Scan T	ools Profile H	elp						
Target:	192.168.1.10/24		-	Profile:	Quick scan	•	Scan	
Comman	d: nmap -T4 -F	192.168.1.10/24						
Hosts	Services	Nmap Output Ports / Hosts Topology Host Details S						
OS	Host 🔺	nmap -T4 -F 192.168.1.10/24					-	Details
	192.168.1.0 192.168.1.10 192.168.1.20 192.168.1.65 192.168.1.66 192.168.1.82 192.168.1.82 192.168.1.83 192.168.1.87 192.168.1.89 192.168.1.90 192.168.1.92	Starting Nmap 7.95 (https://nmap.org) at 2024-09-24 11: Nmap scan report for 192.168.1.10 Host is up (0.0118 latency). Not shown: 80 closed top ports (reset) PORT STATE SERVICE 135/top open methios-san 445/top open microsoft-ds 1025/top open NFS-or-ItS 1026/top open NFS-or-ItS 1026/top open ms-lsa 3389/top open ms-lsa 3090/top open http-proxy <u>MAC Addressi</u> 30:95:23:74:6D:C2 (Micro-Star Intl)	16 In	di a Stand	ard Time			
	192.168.1.92 192.168.1.93 192.168.1.94 192.168.1.95 192.168.1.96 192.168.1.97 192.168.1.99 192.168.1.99 192.168.1.100 192.168.1.100 192.168.1.101 192.168.1.101	Namp scan report for 192.168.1.20 Host is up (0.011s litency). Bort is up (0.011s litency). BOUTON STATS SERVICE 80/top open https 139/top open msrpc 139/top open msrpc 139/top open microsoft-ds 3306/top open msrgl 338/top open msrgl 33						



Step 8: To see packets sent and received r using nmap:

nmap --packet-trace 192.168.1.10

📑 Zenmap	- 0 ×
Scan Tools Profile H	elp
Target: nmappacket-t	ace 192.168.1.10 Profile: Quick scan Cancel
Command: nmap -T4 -F	packet-trace nmappacket-trace 192.168.1.10
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 🔺	nmap -T4 - Fpacket-trace nmap 192.168.1.10 💌 Details
192:163.10 192:168.120 192:168.120 192:168.120 192:168.120 192:168.120 192:168.122 192:168.122 192:168.122 192:168.122 192:168.122 192:168.122 192:168.128 192:168.139	Starting Bmap 7.55 (https://mmap.org) at 2024-09-24 11:19 India Standard Time Failed to resolve "mmap". SERT (2.3650) ARF reply 192.166.1.10 rell 192.166.1.23 (C) 2.35500 and C) and C connect_udp(). UDF connection requested to 8.6.8:55 (100 41) EID 8 NSOCK HIPO (2.35500) nock_connect_udp(). UDF connection requested to 4.2.2.2:53 (100 42) EID 24 NSOCK HIPO (2.35500) nock_connect_udp(). UDF connection requested to 4.2.2.2:53 (100 42) EID 24 NSOCK HIPO (2.4000) nock_read(): Read request from 100 41 (8.6.8.8:551) (timeout: -lmm) EID 18 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.2.2.2:53) (timeout: -lmm) EID 24 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.2.2.2:53) (timeout: -lmm) EID 34 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.2.2.2:53) (timeout: -lmm) EID 34 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.2.2.2:53) (timeout: -lmm) EID 34 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.2.2.2:53) (timeout: -lmm) EID 34 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.8.8.8:53) (timeout: -lmm) EID 34 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.4000) nock_read(): Read request from 100 42 (4.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 42 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 42 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 42 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 42 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 41 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read request from 100 41 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read Request from 100 41 (0.8.8.8:53) (timeout: -lmm) EID 50 NSOCK HIPO (2.40000 nock_read(): Read Request from 100 41 (0.8.8.8:53) (timeout: -lmm) EID 50 NSO
192.168.1.98 192.168.1.99	SENT (2.40909) TCP 192.168.1.213:46003 > 192.168.1.10:135 5 tul=50 1d=36545 1plen=44 seq=1323100590 vin=1024 cmss 1460> SENT (2.40909) TCP 192.168.1.213:46003 > 192.468.1.101050 5 tul=46108 1plen=44 seq=1323100590 vin=1024 cmss 1460>
192.168.1.100	RCVD (2.41008) TCP 192.168.1.101173 > 192.168.1.213.46003 RA tL=128 ind=5668 splem=40 seq=0 vin=0 RCVD (2.41008) TCP 192.168.1.101189 > 192.168.1.213.446003 RA tL=128 ind=566 splem=40 seq=0 vin=0 RCVD (2.41008) TCP 192.168.1.101189 > 192.168.1.213.44003 RA tL=128 ind=566 splem=40 seq=0 vin=0
Filter Hosts	<pre>RVUD (2.41009 10F 192.166.1.01350 > 192.166.1.213:46003 RA tL1=26 1d=8671 bjtem=40 seq=0 Min=40 RVUD (2.41008) TCP 192.168.1.0135 > 192.166.1.213:46003 RA tL1=26 1d=8671 bjtem=40 seq=0 Min=8192 (mss 1460) RCVD (2.41008) TCP 192.168.1.10:25 > 192.168.1.213:46003 RA tL1=28 1d=8672 bjtem=40 seq=0 Min=0</pre>

ican Tools Profile H	Help	
arget: nmappacket-	trace 192.168.1.10 Profile: Quick scan	Scan Cancel
ommand: nmap -T4 -F	F packet-trace nmap packet-trace 192.168.1.10	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
)S Host 🔺	nmap -T4 -Fpacket-trace nmap 192.168.1.10	▼ Details
192.168.1.0 192.168.1.0 192.168.1.20 192.168.1.65 192.168.1.65 192.168.1.65 192.168.1.82 192.168.1.82 192.168.1.82 192.168.1.82 192.168.1.87 192.168.1.87 192.168.1.89 192.168.1.89 192.168.1.90 192.168.1.93 192.168.1.93 192.168.1.93 192.168.1.94 192.168.1.95 192.168.1.96 192.168.1.96 192.168.1.94 192.168.1.95 192.168.1.96 192.168.1.96 192.168.1.96 192.168.1.96 192.168.1.96 192.168.1.96 192.168.1.97	RCVD [2.4150s] TCF 192.168.1.10:544 > 192.168.1.213:46003 RA ttl=128 id=8753 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:560 > 192.168.1.213:46003 RA ttl=128 id=8753 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:560 > 192.168.1.213:46003 RA ttl=128 id=8754 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:500 > 192.168.1.213:46003 RA ttl=128 id=8754 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:500 > 192.168.1.213:46003 RA ttl=128 id=8758 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:644 > 192.168.1.213:46003 RA ttl=128 id=8758 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:443 > 192.168.1.213:46003 RA ttl=128 id=8758 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:443 > 192.168.1.213:46003 RA ttl=128 id=8758 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8750 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:419 > 192.168.1.213:46003 RA ttl=128 id=8761 iplen=40 seq=0 win=0 RCVD [2.4150s] TCF 192.168.1.10:410	
192.168.1.99	000/tcp open velagi 7070/tcp open realserver 8080/tcp open http-proxy	
 192.168.1.100 192.168.1.101 	MAC Address: 30:90:23:74:60:02 (Micro-Star Intl)	
Filter Hosts	Map done: 1 IP address (1 host up) scanned in 2.42 seconds	



Step 9:

Now let's Scan a single host:

Here we have added our systems IP address

Go to Nmap and add the respective IP address > From Profile select Intense Scan > Click on Scan

a. The following output will give for Nmap Output

📴 Zenmap		_	\Box \times
Scan Tools Profile Hel	p		
Target: 192.168.29.183	Profile: Intense scan	Scan	Cancel
Command: nmap -T4 -A -v	v 192.168.29.183		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details	Scans	
OS Host 🔺	nmap -T4 -A -v 192.168.29.183	-	Details
	<pre>NSE: Sourded 157 scripts for scanning. NSE: Sourpt Pre-scanning. Initiating NSE at 23:16 Completed NSE at 23:16, 0.00s elapsed Initiating NSE at 23:16, 0.00s elapsed Initiating NSE at 23:16 Outpeled NSE at 23:16 Initiating NSE at 23:16 Initiating Parallel DNS resolution of 1 host. at 23:16 Scanning 192.168.29.183 [1000 ports] Discovered open port 3306/tcp on 192.168.29.183 Discovered open port 3306/tcp on 192.168.29.183 Discovered open port 902/tcp on 192.168.29.183 Discovered open port 902/tcp on 192.168.29.183 Completed SYN Stealth Scan at 23:16 Scanning 7 services scan at 23:16 Scanning 7 services scan at 23:16 Completed Service scan at 23:17, 11.14s elapsed (7 set Initiating SE at 23:17, 14.30s elapsed Initiating NSE at 23:17, 0.15s elapsed</pre>	l6 5, 0.01s e 1000 tota: srvices or 183 Act	l ports) 1 l host) tivate Win
Filter Hosts	Initiating NSE at 23:17	Go.1	to Settings to

b. The following output will give for Ports/Hosts Output

📑 Zenn	map					- 🗆 ×
Scan T	Tools Profile Hel	lp				
Target:	192.168.29.183		•	Profile:	Intense scan	▼ Scan Cancel
Comman	id: nmap -T4 -A -	v 192.168.29.183				
Hosts	Services	Nmap Outpu	it Ports /	Hosts	Topology	Host Details Scans
OS	Host 🔺	Port	Protocol	State	Service	Version
- 5	192.168.29.183	25	tcp	filtered	smtp	
		9 110	tcp	filtered	рор3	
		9 135	tcp	open	msrpc	Microsoft Windows RPC
		9 139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
		6 445	tcp	open	microsoft-ds	
		548	tcp	filtered	afp	
		902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
		912	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
		3306	tcp	open	mysql	MySQL 5.5.16
		07070	tcp	open	realserver	
						Activate Windows
Fi	ilter Hosts					Go to Settings to activate Windows



📑 Zenmap \times _ Scan Tools Profile Help Target: 192.168.29.183 Profile: Intense scan • Scan Cancel Command: nmap -T4 -A -v 192.168.29.183 Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Host OS . Hosts Viewer Fisheye Controls Legend Save Graphic 192.168.29.183 192.168.29.183 localhost Activate Windows Filter Hosts

c. The following output will give for topology

d. The following output will give for Host details

🛃 Zenmap		- 🗆 X
Scan Tools Profile	Help	
Target: 192.168.29.183	Profile: Intense scan	▼ Scan Cancel
Command: nmap - T4	-A -v 192.168.29.183	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details	Scans
OS Host 🔺	▼ 192.168.29.183	
192.168.29.183	▼Host Status State: up	
	Open 7 Ports:	
	Filtered 3 ports:	
	Closed 990 ports:	
	Scanned 1000 ports:	
	Up time: Not available	
	Last Not boot: available	
	▼ Addresses IPv4: 192.168.29.183	
	IPv6: Not available	
	MAC: Not available	
	▼ Operating System	
Filter Hosts	Microsoft Windows 10 1809	Activate Windows Go to Settings to activate Windows



Step 10: The scan can be saved in system as follows

Go to Scan -> Save Scan and Save

Scan Tools Profile Help Target: 192.168.29.183 Command: nmap -T4 - A - v 192.168.29.183 Hosts Services OS Host Imap -T4 - A - v 192.168.29.183 Map Cutput Ports / Hosts Topology Host Details Scan Canse OS Host Map Scan report for 192.168.29.183 Numap scan report for 192.168.29.183 Host is up (0.00044s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 25/tcp filtered 135/tcp open 445/tcp open 912/tcp open 912/tcp open 912/tcp open 912/tcp open 912/tcp Gancel Save Intered ID: 11	Scan Tools Profile He Target: 192.168.29.183 Command: nmap -T4 - A - Hosts Services OS Host	-v 192.168.29.183	Profile: ts / Hosts	Intense scan	▼ Scan Car	
Target: 192.168.29.183 Profile: Intense scan Scan Can Command: nmap -T4 - A - v 192.168.29.183 Map Output Ports / Hosts Topology Host Details Scans Can OS Host nmap -T4 - A - v 192.168.29.183 map scan report for 192.168.29.183 Details Scans Map scan report for 192.168.29.183 Nmap scan report for 192.168.29.183 Details Details Details Most shown: 900 closed tcp ports (reset) PORT STATE SERVICE VERSION 25/ccp filtered smp Choose a scan to save X You have 6 scans loaded in the current view. Select the scan which you would like to save. Nmap -T4 - A - v 192.168.1.0 on Daemon 1.10 (Uses VNC, SCAP) Naemon 1.0 (Uses VNC, SCAP) 10 Version:: 5.5. Image -T4 - A - v 192.168.1.0 Image -T4	Target: 192.168.29.183 Command: nmap -T4 -A - Hosts Services OS Host	•v 192.168.29.183 Nmap Output Port	Profile: ts / Hosts	Intense scan	Car	
Command: nmap -T4 - A - v 192.168.29.183 Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS Host map -T4 - A - v 192.168.29.183 Map scan report for 192.168.29.183 Host is up (0.00044s latency). Not shown: 990 closed tcp ports (reset.) PORT STATE SERVICE VERSION 25/tcp filtered smtp 110/tcp filtered smtp 110/tcp filtered 135/tcp open 445/tcp open 902/tcp open 902/tcp open 912/tcp open	Command: nmap -T4 -A - Hosts Services OS Host	-v 192.168.29.183 Nmap Output Port	ts / Hosts			
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS Host Imap -T4 - A - v 192.168.29.183 Imap -T4 - A - v 192.168.29.183 Details Details Instruction Imap -T4 - A - v 192.168.29.183 Imap -T4 - A - v 192.168.29.183 Details Details Instruction Imap -T4 - A - v 192.168.29.183 Imap -T4 - A - v 192.168.29.183 Details Details Instruction Imap -T4 - A - v 192.168.29.183 Imap -T4 - A - v 192.168.20.183 Imap -T4 - A - v 192.168.20.183 Imap -T4 - A - v 192.168.20.103 Instruction Imap -T4 - A - v 192.168.10 Imap - T4 - A - v 192.168.10 <td< td=""><td>Hosts Services</td><td>Nmap Output Port</td><td>ts / Hosts</td><td></td><td></td><td></td></td<>	Hosts Services	Nmap Output Port	ts / Hosts			
OS Host mmap -T4 - A - v 192.168.29.183 Deta 192.168.29.183 Imap scan report for 192.168.29.183 Host is up (0.00044s latency). Not shown: 990 closed tcp ports (reset) PORT STATE SERVICE VERSION 25/tcp open 13/tcp open 13/tcp open 445/tcp open 902/tcp open 912/tcp open 91	OS Host 🔺	nman -T4 - A - y 192,168,2				
192.168.29.183 Nmap scan report for 192.168.29.183 Host is up (0.00044s latency). Not shown: 990 closed topy: PORT STATE SERVICE VERSION 25/tcp filtered smtp 110/tcp filtered 133/tcp open 445/tcp open 902/tcp open 902/tcp open 912/tcp open 1 mysql-info: Imap -T4-A -v 192.168.1.0 Image T4-A -v 192.168.1.0 Image T4-A -v 192.168.1.0 Image T4-A -v 192.168.1.0 Image T4-A -v 192.168.1.0	40 102 169 20 192		9.183		▼ Det	ails
<pre> Capabilities flags: 63487 Some Capabilities: SupportsTransactions, LongColumnFlag, FoundRows, Speaks41ProtocolOld, LongPassword, ConnectWithDatabase, SupportsLoadDataLocal, Support41Auth, SupportsCompression, IgnoreSigpipes, IgnoreSpaceBeforeParenthesis, InteractiveClient, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, ODBCClient, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins Status: Autocommit Salt: UWVbihN/<!--lqf-Kr}<00<br--> _ Auth Plugin Name: mysql_native_password 7070/tcp open ssl/realserver? _ssl-date: TLS randomness does not represent time _ssl-date: TLS randomness does not represent time _ssl-date: TLS randomness does not represent time</pre>		PORT STATE SE 25/tcp filtered sm 110/tcp filtered 135/tcp open 139/tcp open 445/tcp open 902/tcp open 902/tcp open 902/tcp open 912/tcp open 912/t	RVICE atp Choose a sca bu have 6 scans elect the scan w nmap -T4 - A ags: 63487 s: Supports LongPasswo rtsCompress Speaks41Prot its, Support its, Support	VERSION In to save PC loaded in the current view. hich you would like to save. /192.168.1.0 Cancel Save Transactions, LongColumni rd, ConnectWithDatabase, ion, IgnoreSigpipes, Ign ocolNew, DontAllowDataba tsMultipleStatments, Supj ive_password r? not represent time =AnyDesk Client ient	Dios-ssn Daemon 1.10 (Uses VNC, SDAP) Daemon 1.0 (Uses VNC, SDAP) Flag, FoundRows, SupportsLoadDataLocal, oreSpaceBeforeParenthesis, seTableColumn, ODBCClient, portsAuthPlugins	
Issuer: commonName=AnyDesk Client		Public Kev type: r	rsa		Activate windows	