Experiment No. 3

Title: Active Reconnaissance

Batch:SY-IT(B3) **Roll No.:16010423076** **Experiment No.: 3**

Aim: To understand and perform Active Reconnaissance with tools

Resources needed: Internet access

Theory:

Reconnaissance is the act of collecting information. It can be said as act of military observation of a region to locate an enemy or ascertain strategic features.
In Cyber Security, Reconnaissance (or recon. In short) refers to act of collecting information about the target system and looking for weaknesses to exploit
There are 2 types of Recon,

- Active Recon
- Passive Recon

Today, we will only discuss about Active Reconnaissance

Active Recon is a type of attack in which an attacker engages with the target system to gather information about possible vulnerabilities. The attacker often uses port scanning, for example, to discover any vulnerable ports. After a port scan, attacker can then exploit the known vulnerabilities of those services associated with open ports

Active Reconnaissance is also done by ethical hackers as it is also necessary for a pen tester to understand and observe the system before launching any valid attack.
Let's look at tools to perform the attack
-nmap
-netcat (nc)

NMAP

The Network Mapper is a network scanner created by Gordon Lyon. It is an open source tool used for network discovery and auditing. The tool searches for directories and services in a network by sending packets and analyzing their responses.

Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules and monitoring host or service uptime.

Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what OS (and their versions) they are running, what type of packet filters/firewalls are in use and dozens of other characteristics

It was primarily designed to scan large networks, but works well against single hosts. Nmap runs on all major computer operating systems and official binary packages are available for linux, Windows and MacOS X.

Characteristics of NMAP:

-Flexible

Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers and other obstacles (includes port scanning w/ TCP and UDP, OS detection, version detection, ping sweeps and more.
-Powerful

Allows you to scan large networks
-Portable

Open source software that can be used on Most Oss

-Easy

Even though it provides a wide range of features, beginners can start with simply nmap -v -A <target_hostname_or_IPaddress>

-Free

Primary goal being to make internet a safer place, giving admins, auditors and hackers a tool to assess the network. It is free to download and opensourced.

-Well Documented

A lot of effort has been put in the whitepapers, tutorials, up to date manual pages, etc

---

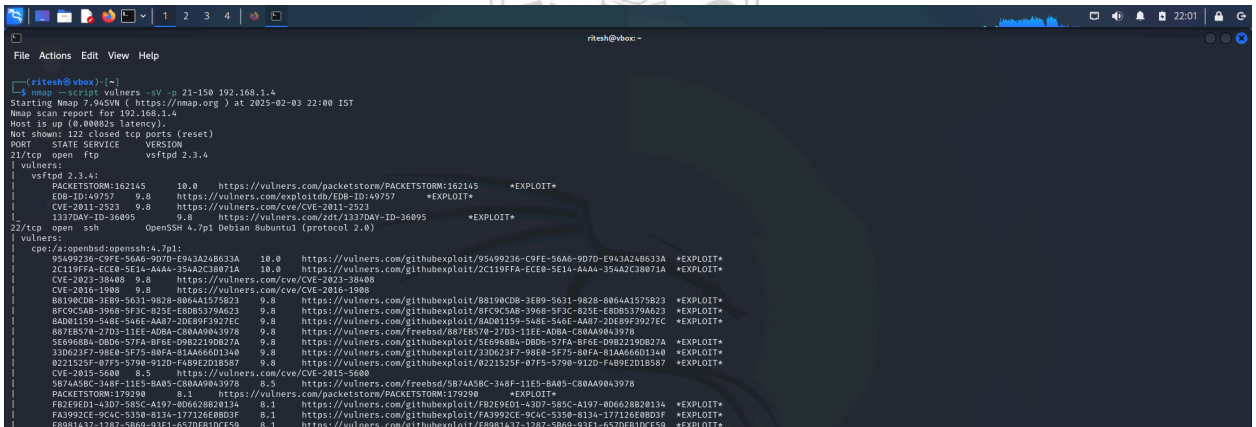
Procedure

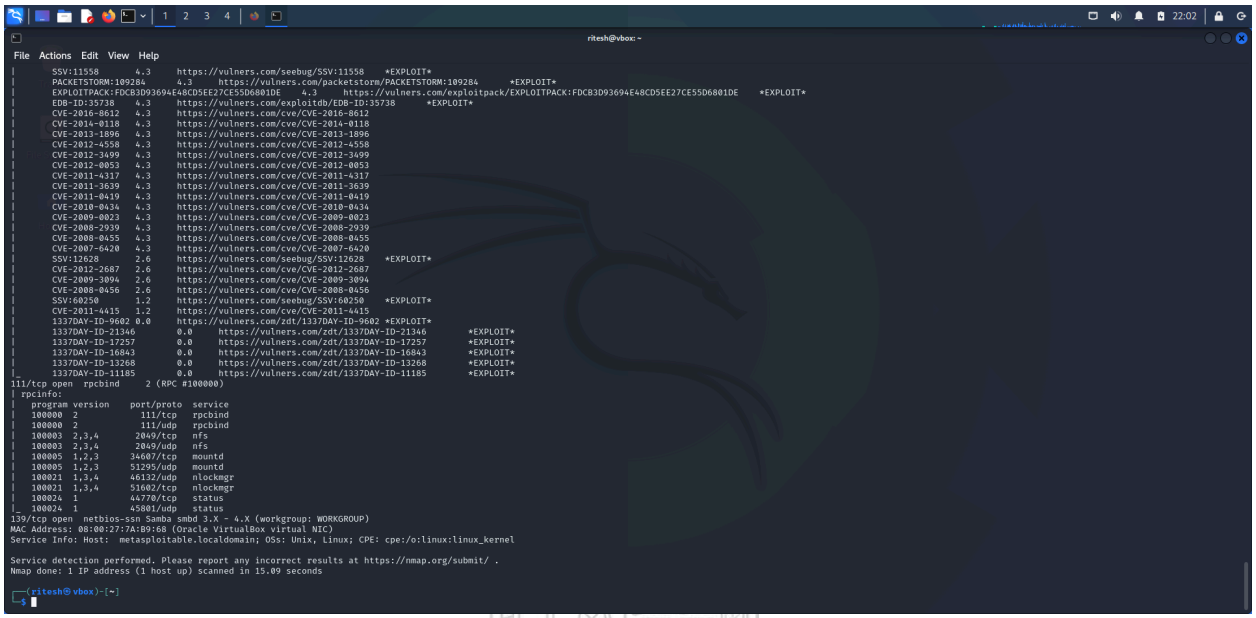
Working with NMAP

1) **Nmap 1**

   1. Vulners Script

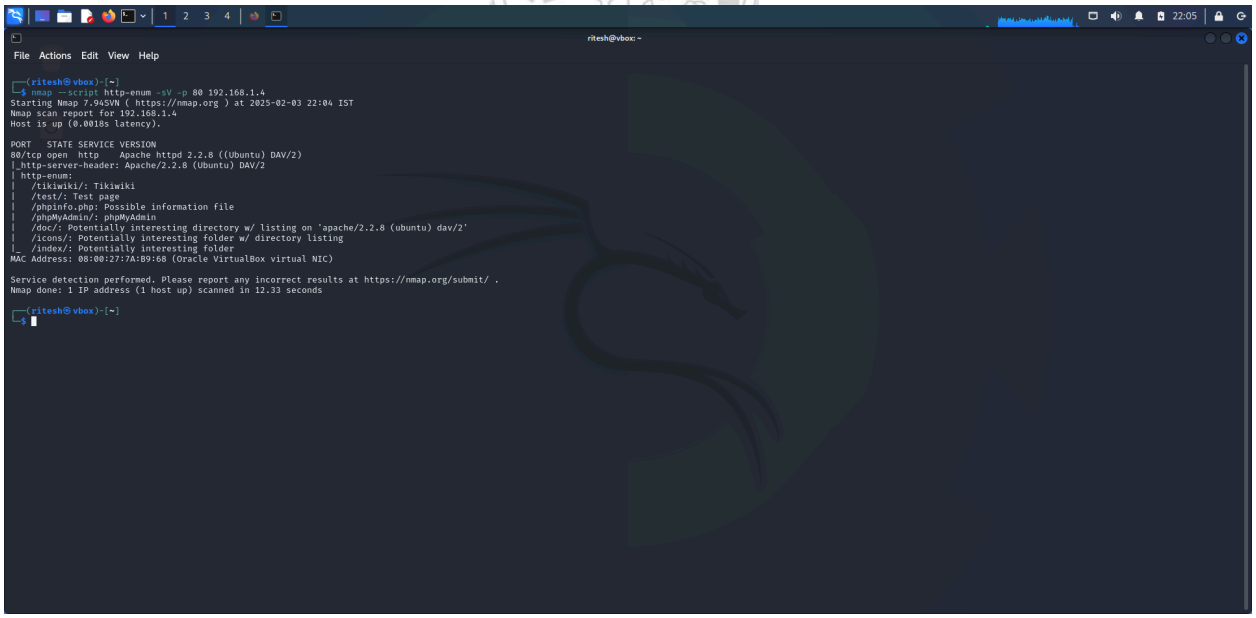
   nmap --script vulners -sV -p 21-150 192.168.1.4





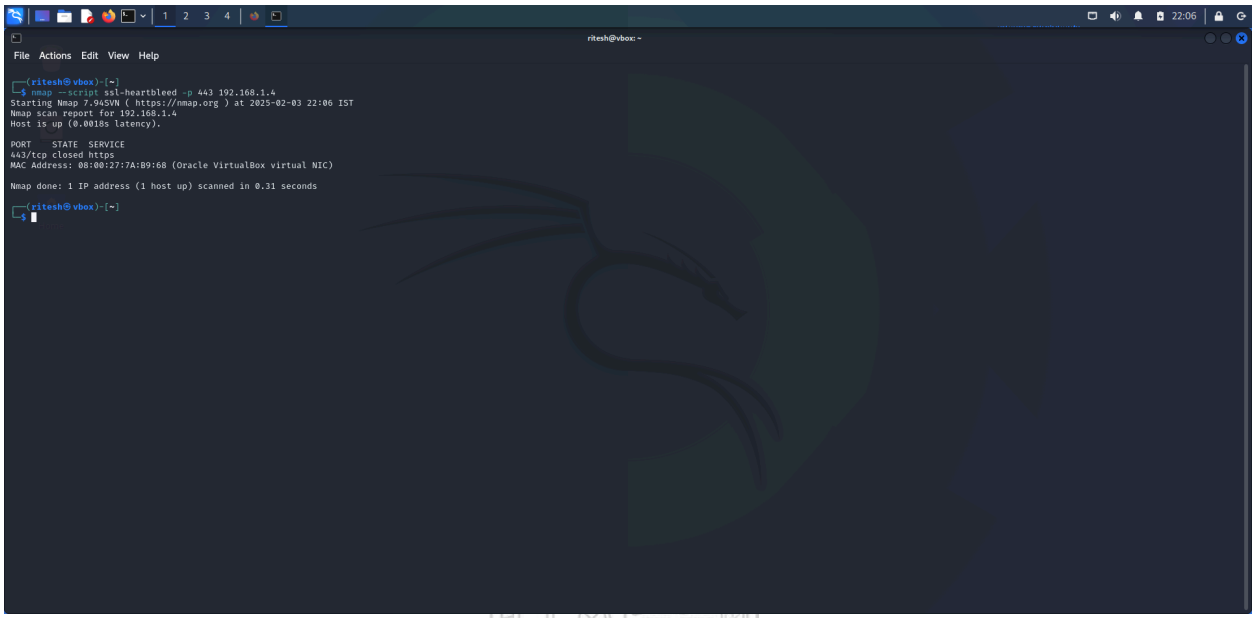
2. HTTP Enum Script

nmap --script http-enum -sV -p 80 192.168.1.4



3. Heartbleed Script

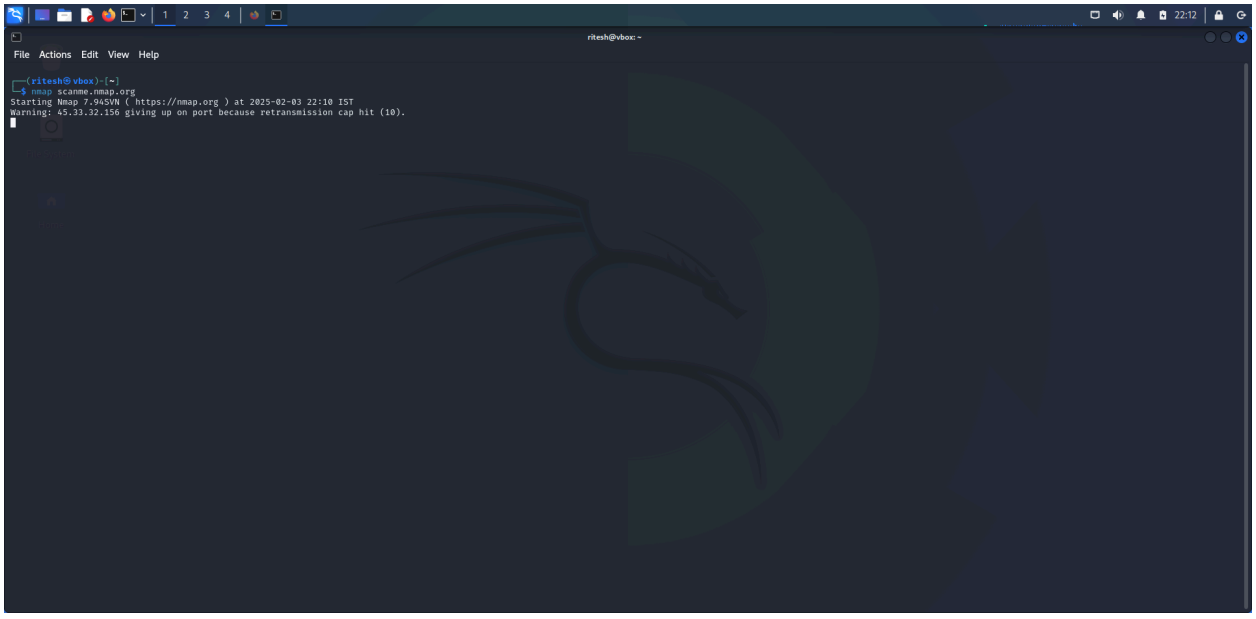
nmap --script ssl-heartbleed -p 443 192.168.1.4



2) Nmap 2

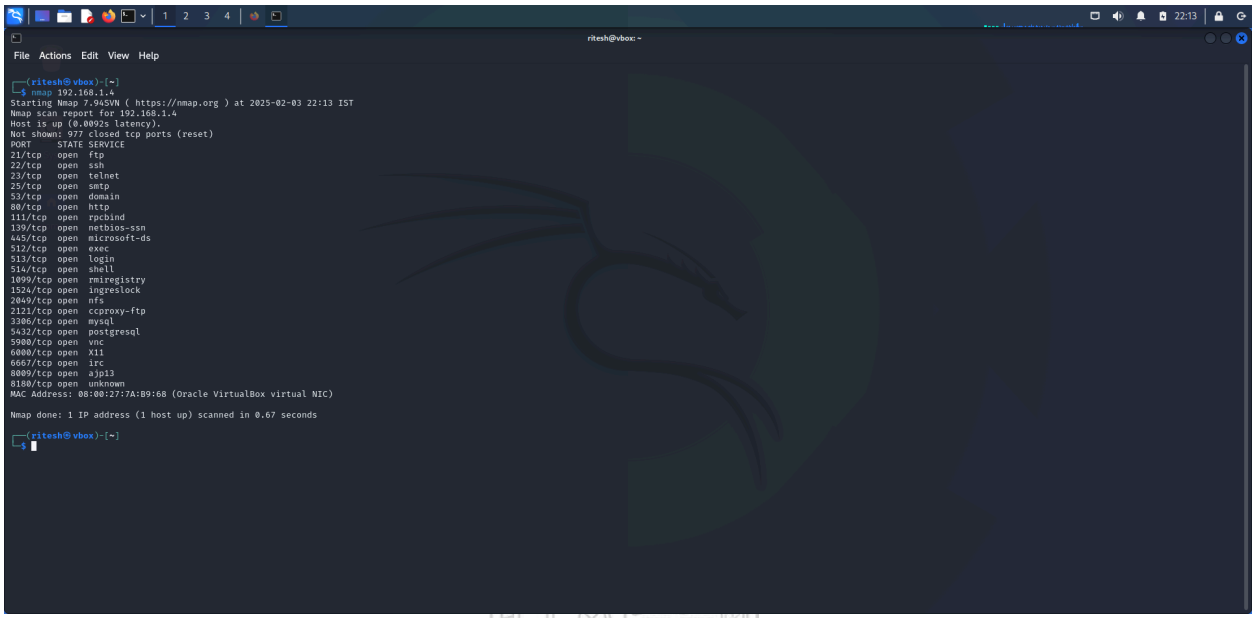
 # 1. Basic Nmap scan (targeting a website)

nmap scanme.nmap.org

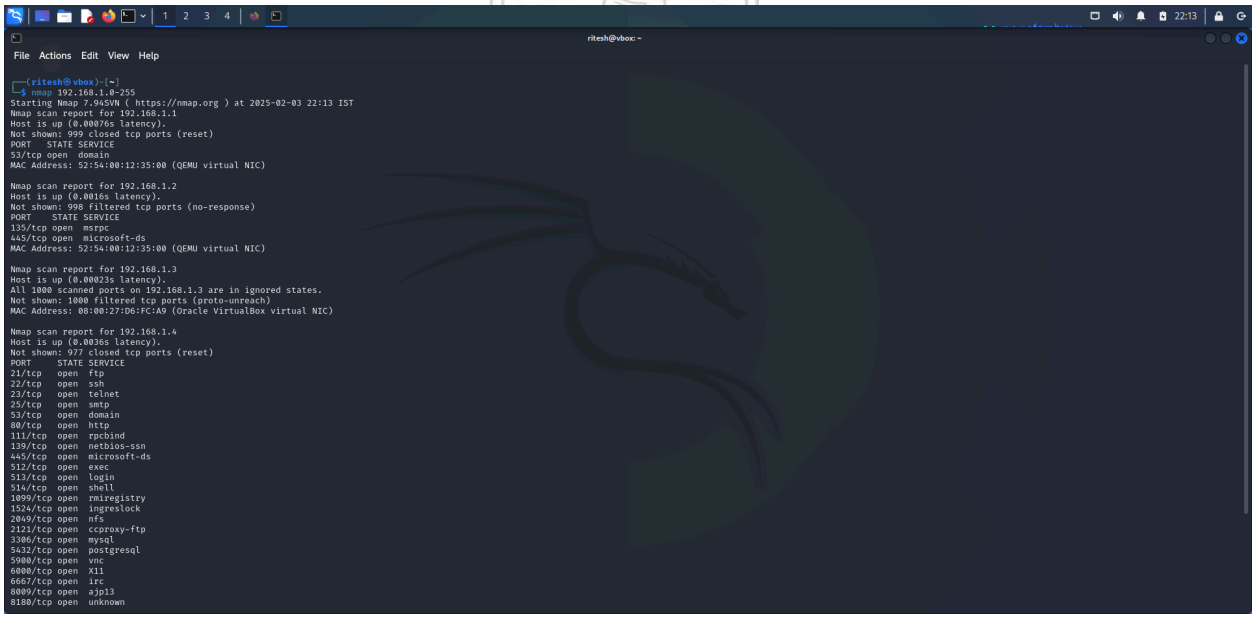


 # 2. Gathering IP Addresses

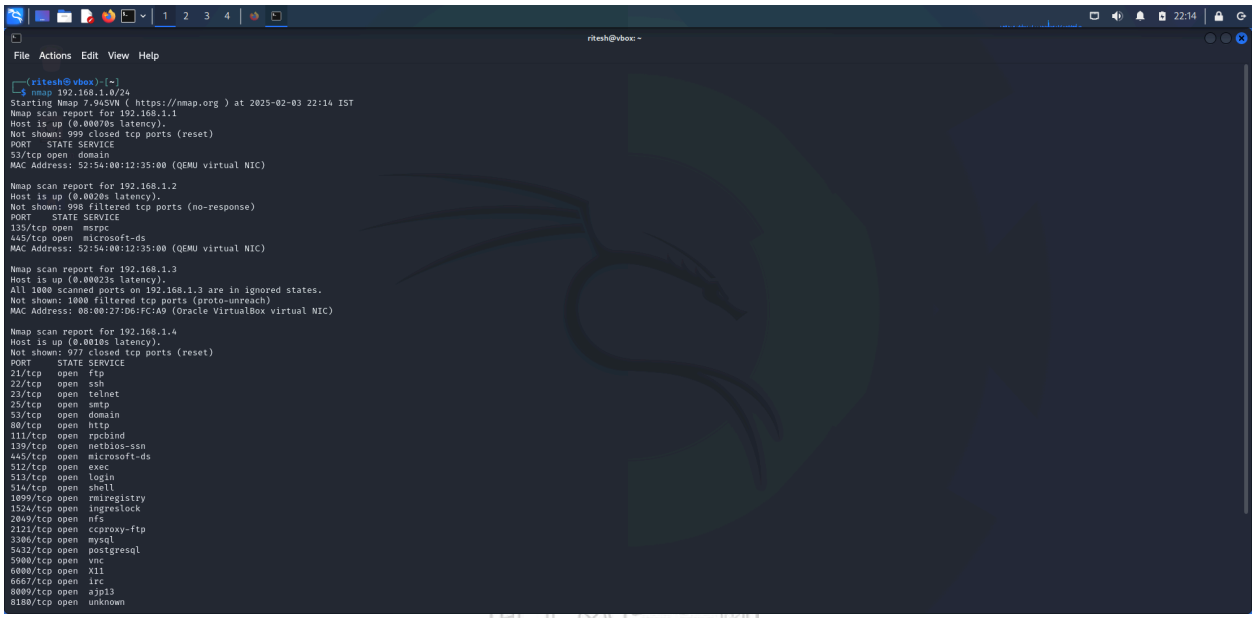
nmap 192.168.1.4

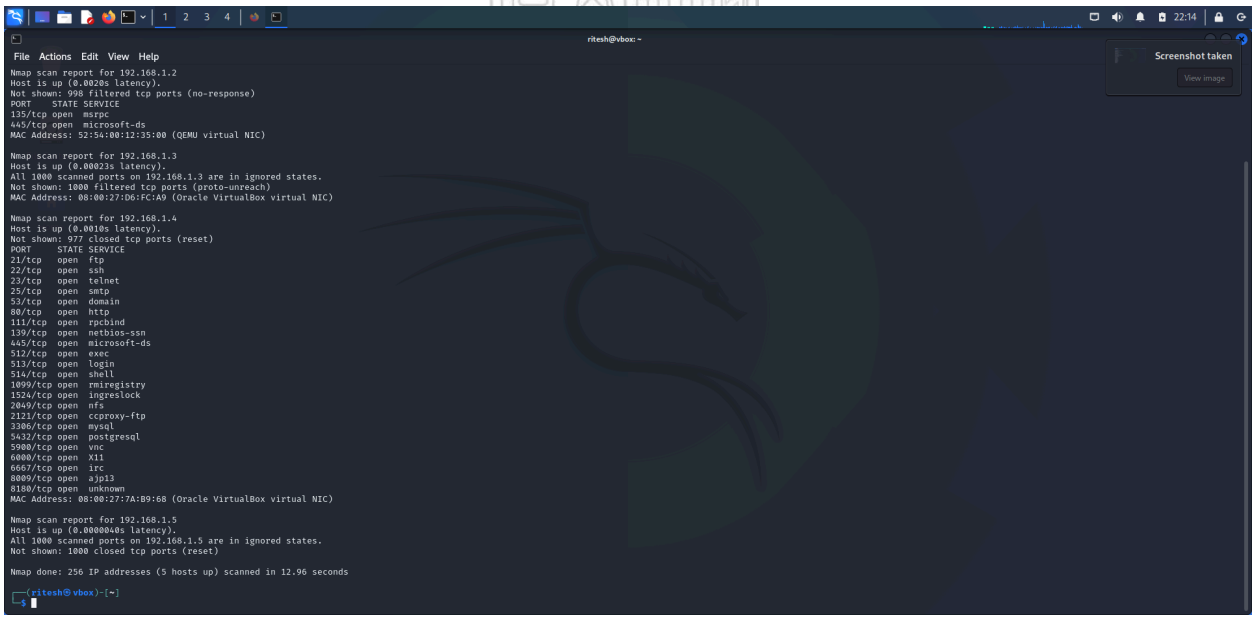


nmap 192.168.1.0-255

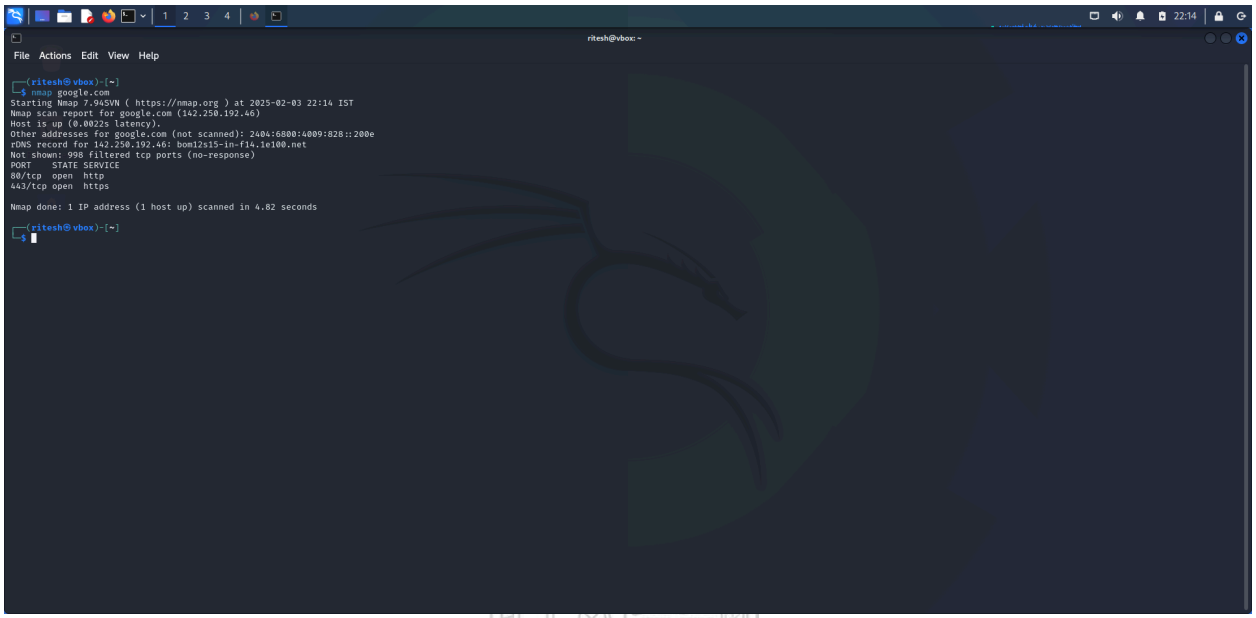


nmap 192.168.1.0/24





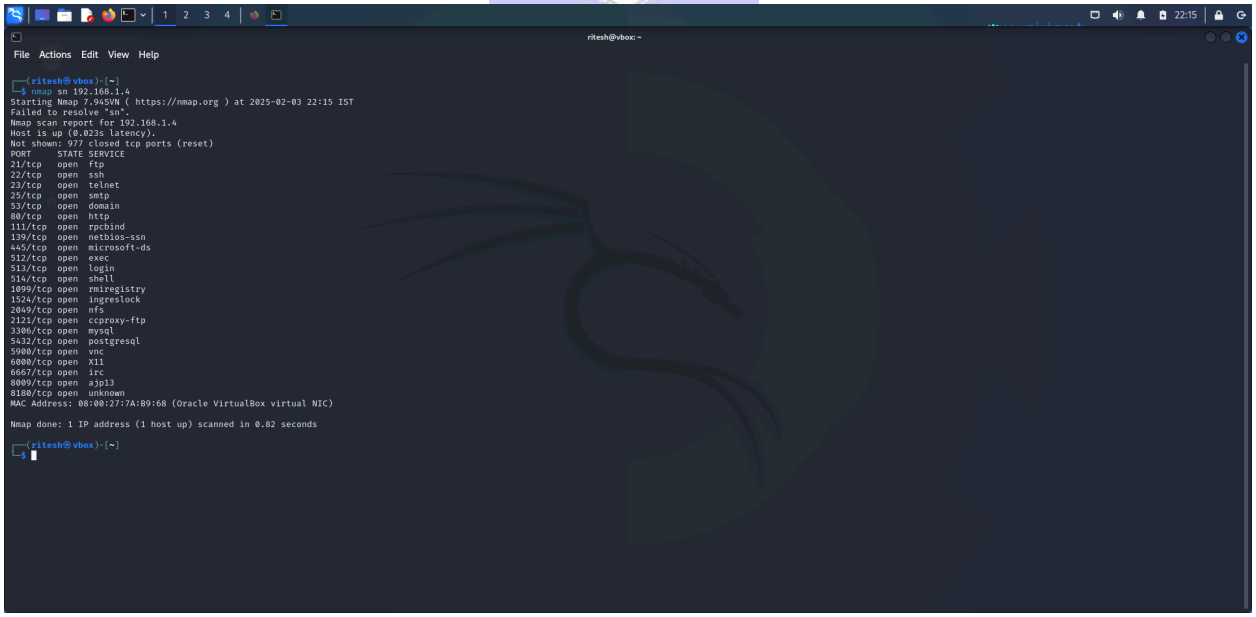
nmap google.com



 # 3. Running Different Scan Types

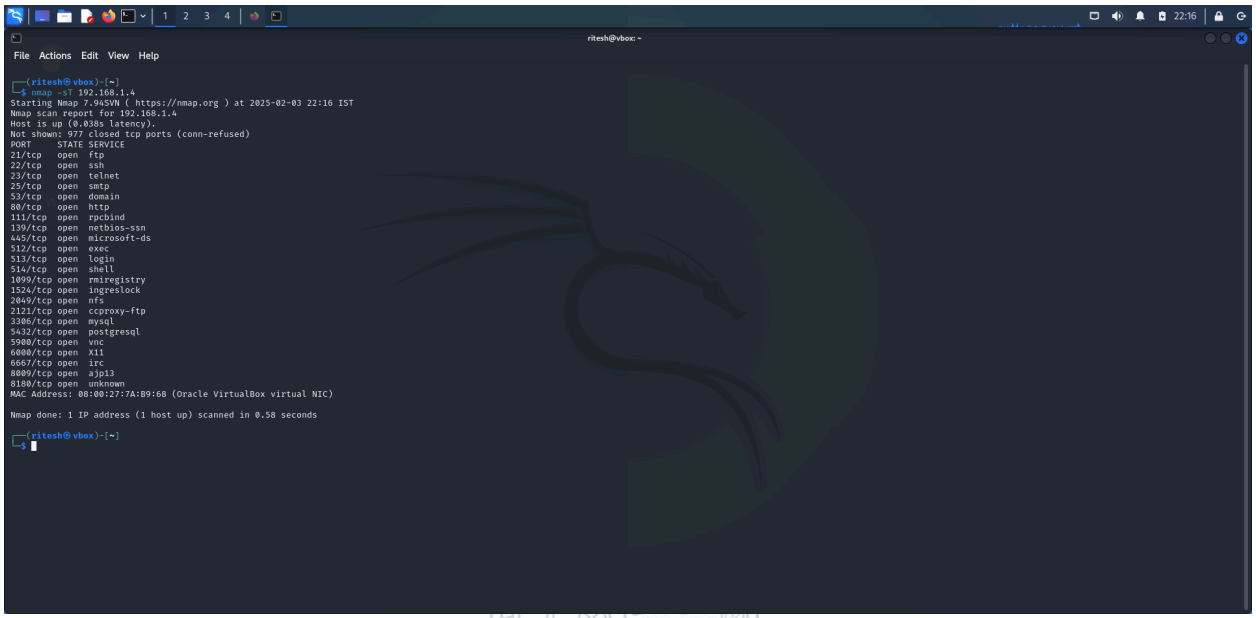
Ping Scan (detects which hosts are up)

nmap -sn 192.168.1.4

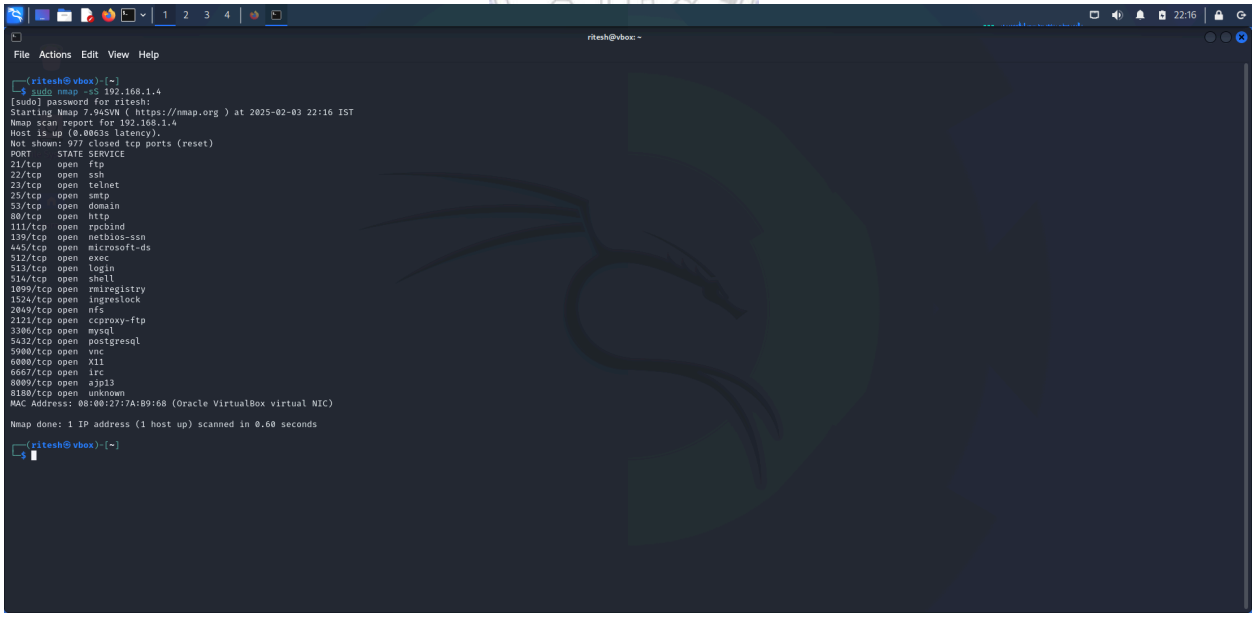


TCP Connect Scan (3-way handshake)

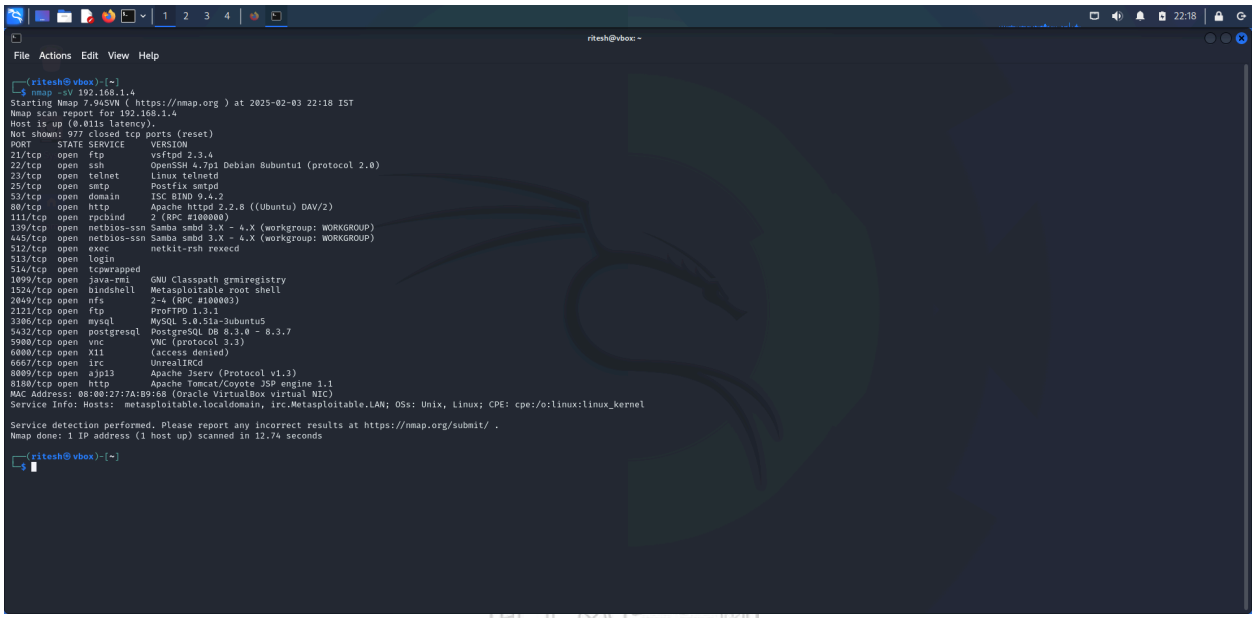
nmap -sT 192.168.1.4



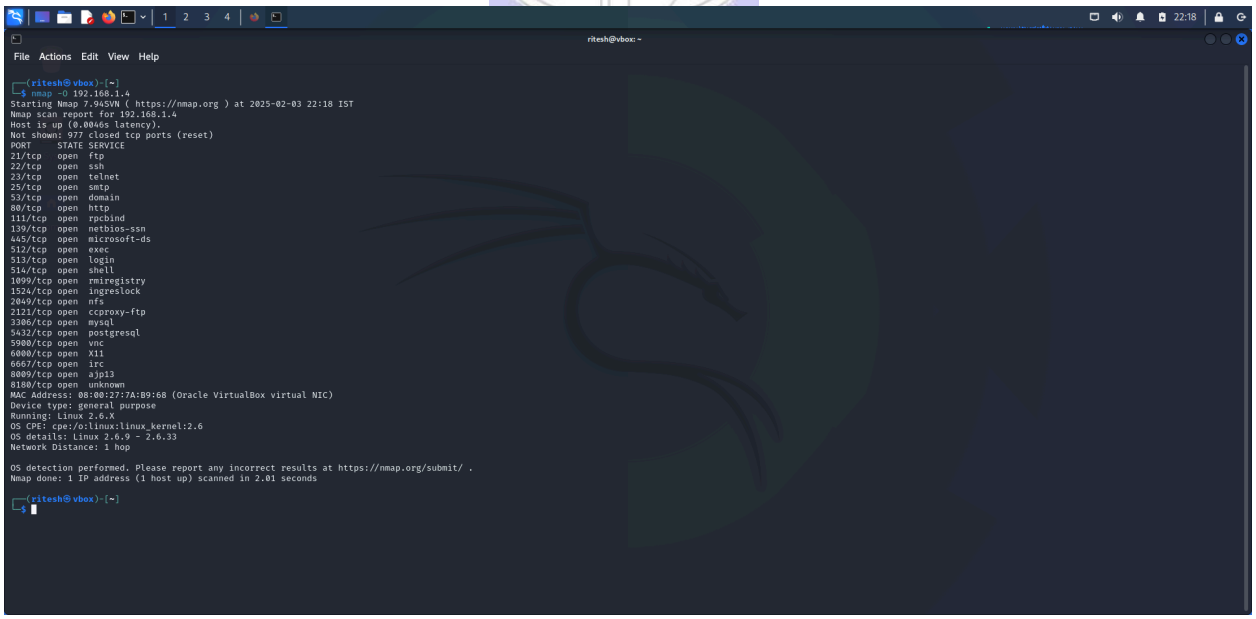
# SYN Scan (stealth scan)
sudo nmap -sS 192.168.1.4



Service Version Detection
nmap -sV 192.168.1.4

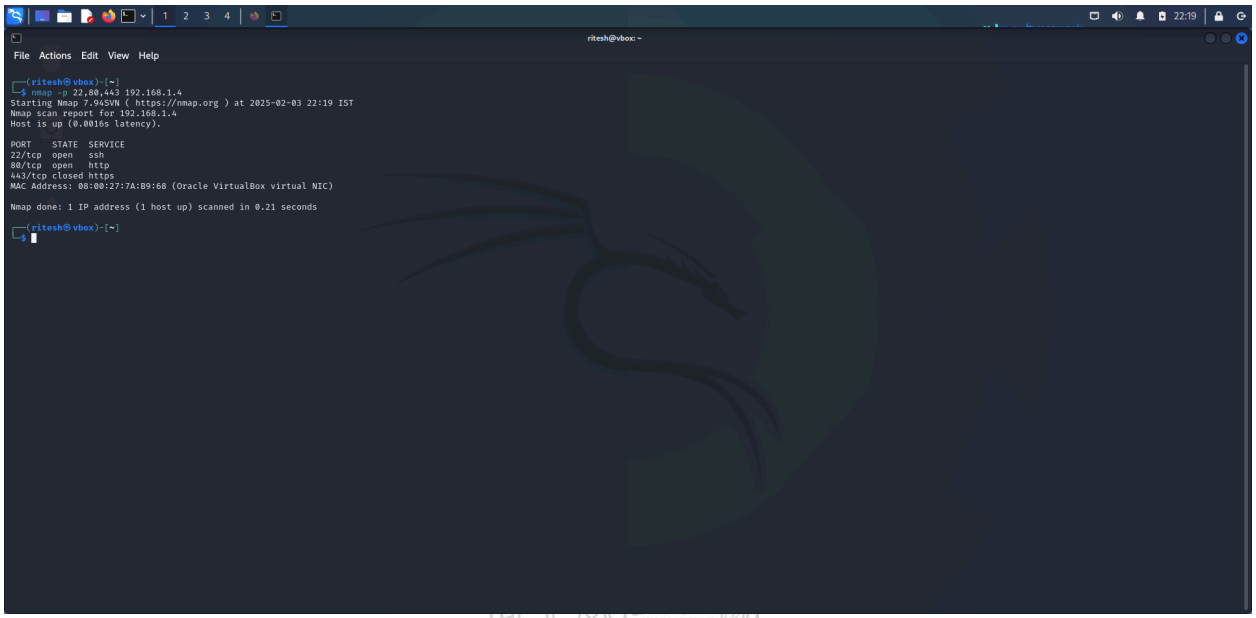


OS Detection
nmap -O 192.168.1.4

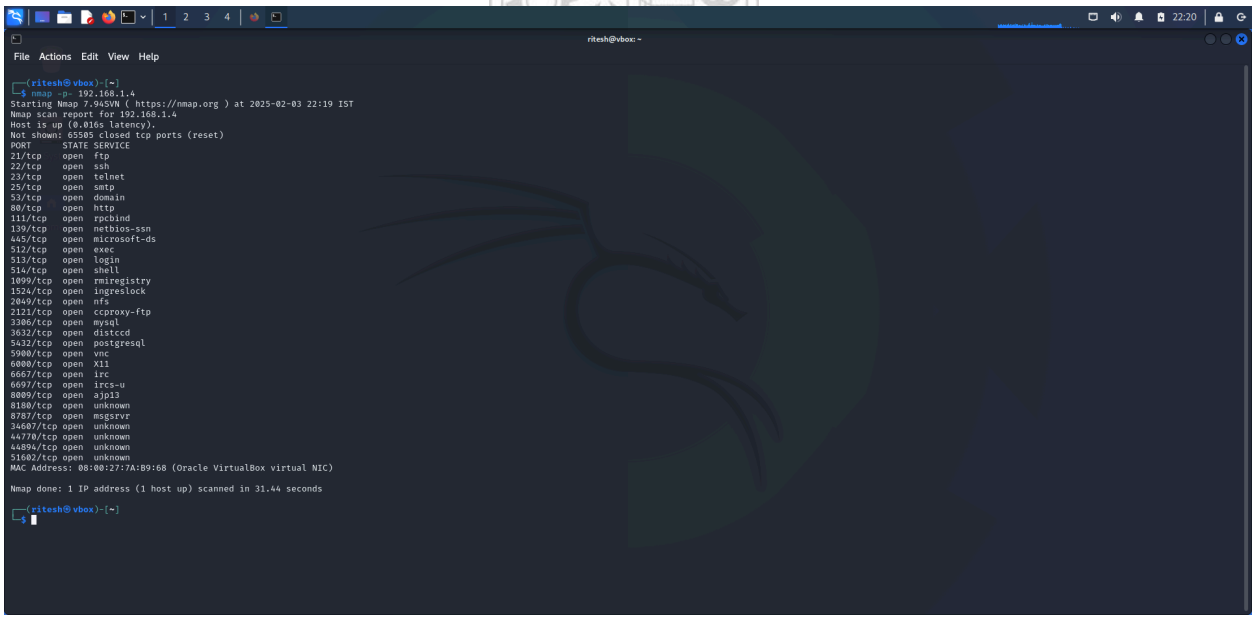


 # 4. Different Types of Port Scans

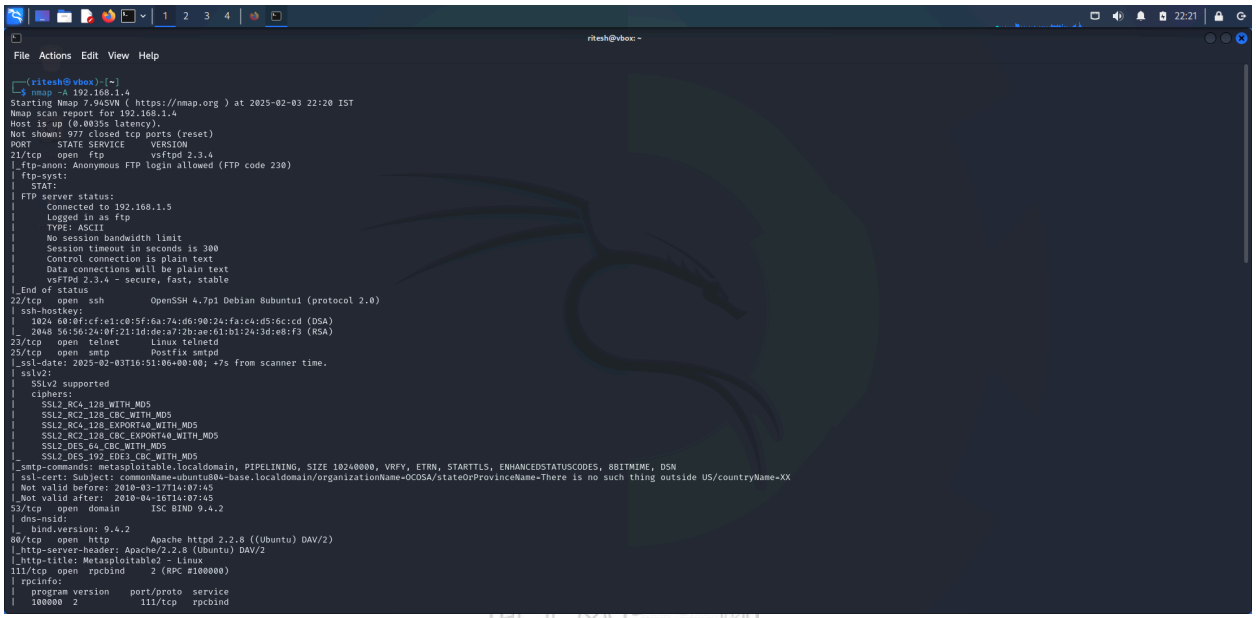
Port Range Scan (scans specific range of ports)
nmap -p 1-100 192.168.1.4

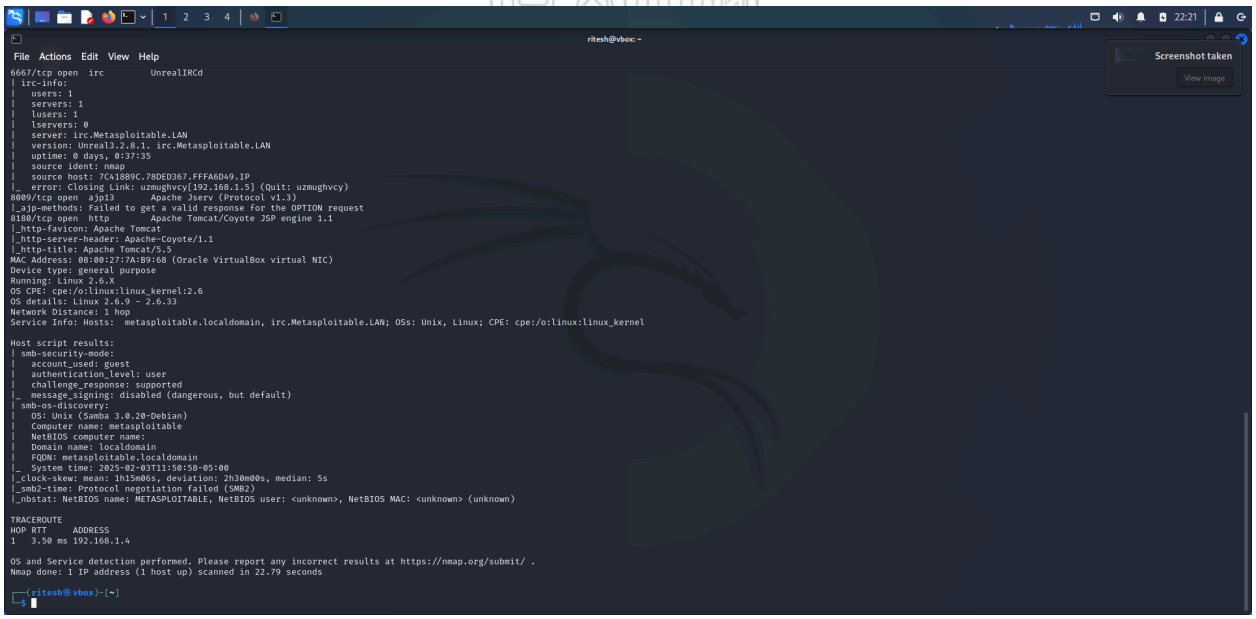


Specific Ports Scan (scans selected ports)
nmap -p 22,80,443 192.168.1.4

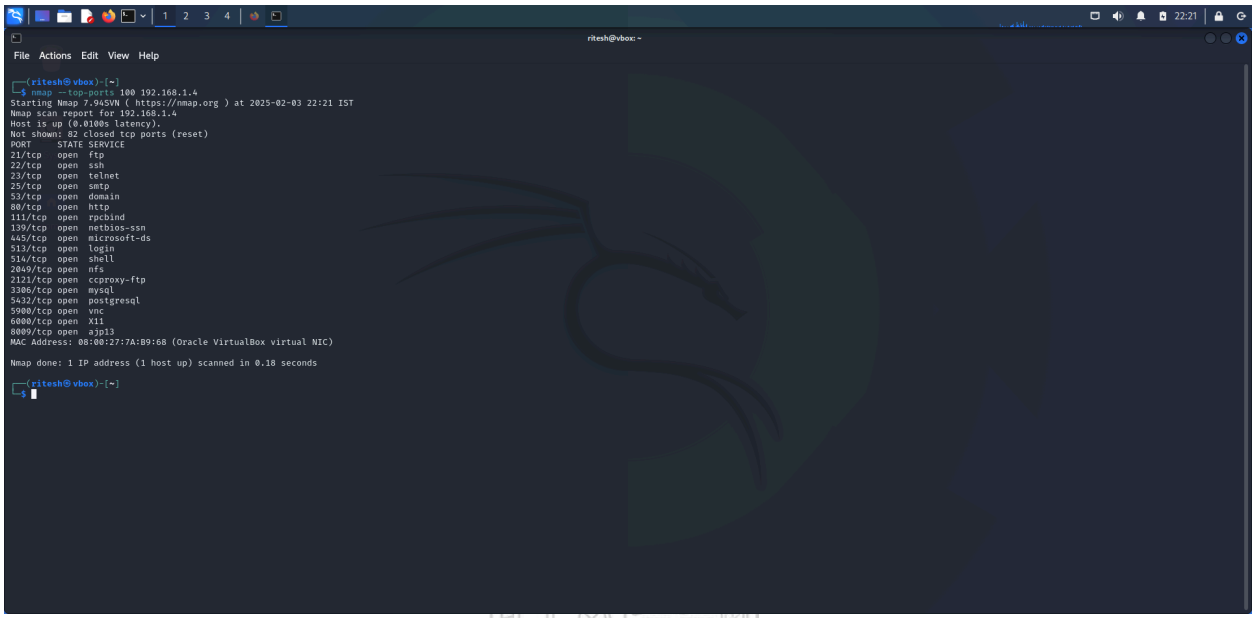


All Ports Scan
nmap -p- 192.168.1.4

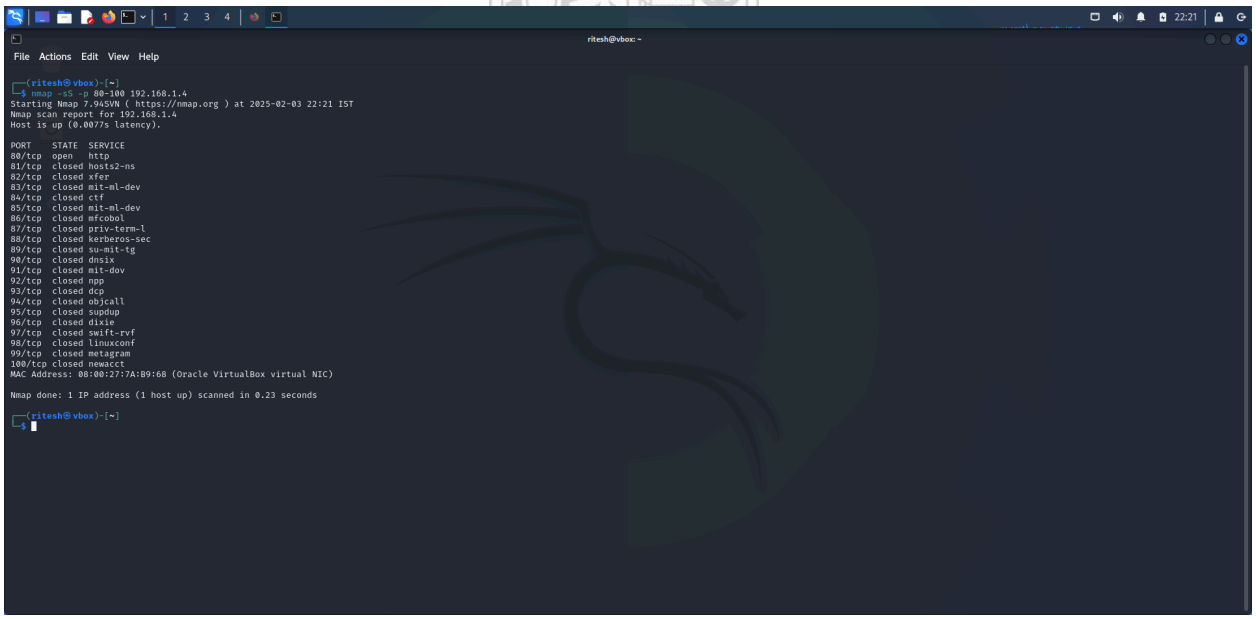




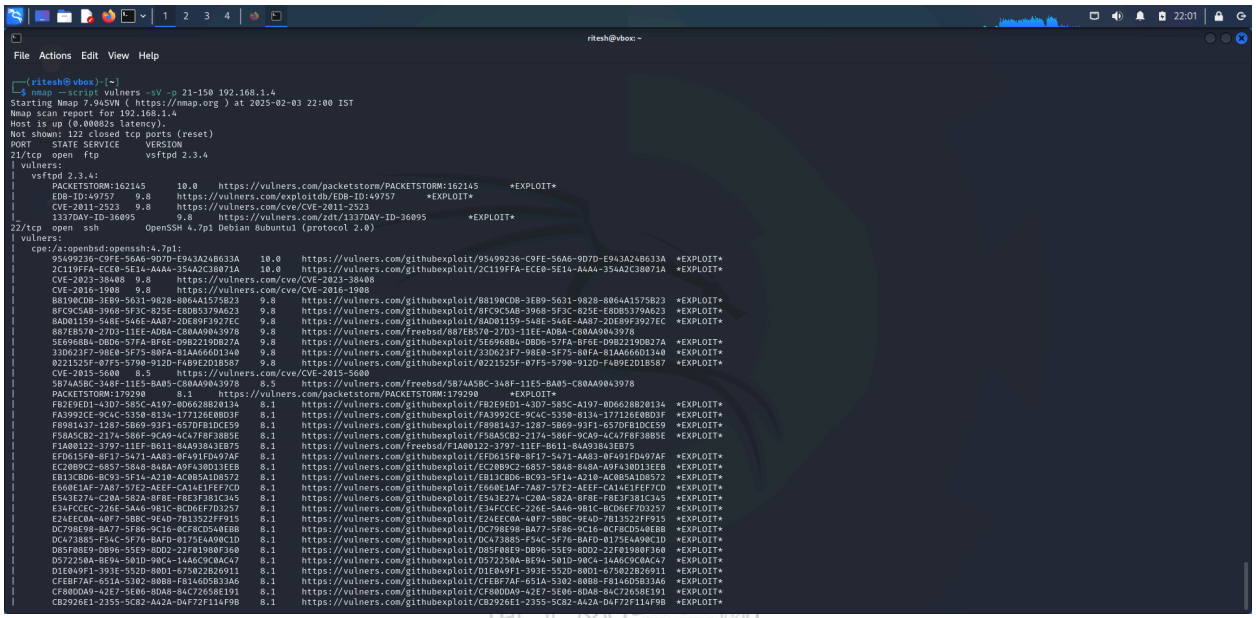
Aggressive Scan (includes OS, version, and script scanning)
nmap -A 192.168.1.4

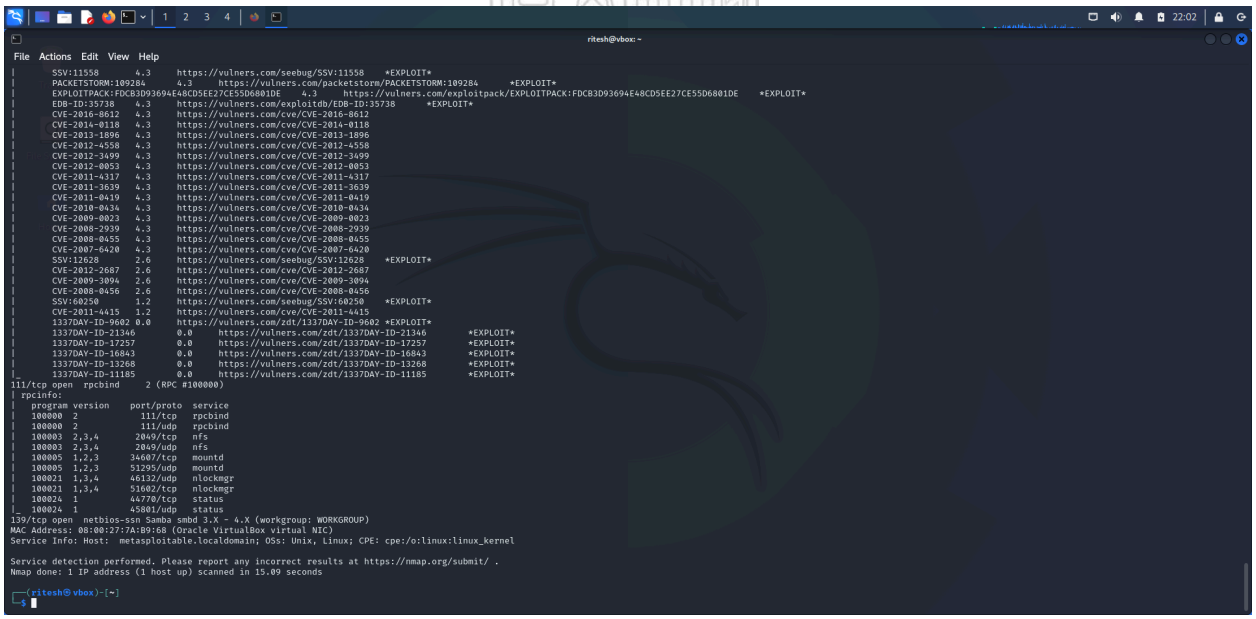


Top Ports Scan
nmap --top-ports 100 192.168.1.4



 # 5. Combining Different Scan and Port Scan Types
SYN scan with specific port range
nmap -sS -p 80-100 192.168.1.4


ritesh@vbox: ~
File Actions Edit View Help
┌──(ritesh㉿vbox)-[~]
└─$ nmap --script vulners -sV -p 21-150 192.168.1.4
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-03 22:00 IST
Nmap scan report for 192.168.1.4
Host is up (0.00082s latency).
Not shown: 122 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| vulners:
| vsftpd 2.3.4:
| PACKETSTORM:162145 10.0 https://vulners.com/packetstorm/PACKETSTORM:162145 *EXPLOIT*
| EDB-ID:49757 9.8 https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
| CVE-2011-2523 9.8 https://vulners.com/cve/CVE-2011-2523
|_ 1337DAY-ID-36095 9.8 https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| 95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
| 2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
| CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
| CVE-2016-1908 9.8 https://vulners.com/cve/CVE-2016-1908
| B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
| 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623 *EXPLOIT*
| 8AD01159-548E-546E-AA87-2DE89F3927EC 9.8 https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC *EXPLOIT*
| 887E8570-27D3-11EE-ADBA-C80AA9043978 9.8 https://vulners.com/freebsd/887E8570-27D3-11EE-ADBA-C80AA9043978
| 5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A 9.8 https://vulners.com/githubexploit/5E6968B4-DBD6-57FA-BF6E-D9B2219DB27A *EXPLOIT*
| 33D623F7-98E0-5F75-80FA-81AA666D1340 9.8 https://vulners.com/githubexploit/33D623F7-98E0-5F75-80FA-81AA666D1340 *EXPLOIT*
| 0221525F-07F5-5790-912D-F4B9E2D1B587 9.8 https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587 *EXPLOIT*
| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600
| 5874A5BC-348F-11E5-BA05-C80AA9043978 8.5 https://vulners.com/freebsd/5874A5BC-348F-11E5-BA05-C80AA9043978
| PACKETSTORM:179290 8.1 https://vulners.com/packetstorm/PACKETSTORM:179290 *EXPLOIT*
| FB2E9ED1-43D7-585C-A197-0D6628B20134 8.1 https://vulners.com/githubexploit/FB2E9ED1-43D7-585C-A197-0D6628B20134 *EXPLOIT*
| FA3992CE-9C4C-5350-8134-177126E0BD3F 8.1 https://vulners.com/githubexploit/FA3992CE-9C4C-5350-8134-177126E0BD3F *EXPLOIT*
| F8981437-1287-5B69-93F1-657DFB1DCE59 8.1 https://vulners.com/githubexploit/F8981437-1287-5B69-93F1-657DFB1DCE59 *EXPLOIT*
| F58A5CB2-2174-586F-9CA9-4C47F8F38B5E 8.1 https://vulners.com/githubexploit/F58A5CB2-2174-586F-9CA9-4C47F8F38B5E *EXPLOIT*
| F1A00122-3797-11EF-B611-8A93843E8E75 8.1 https://vulners.com/freebsd/F1A00122-3797-11EF-B611-8A93843E8E75
| EFD615F0-8F17-5471-AA83-0F491FD497AF 8.1 https://vulners.com/githubexploit/EFD615F0-8F17-5471-AA83-0F491FD497AF *EXPLOIT*
| EC20B9C2-6857-5848-848A-A9F430D13EEB 8.1 https://vulners.com/githubexploit/EC20B9C2-6857-5848-848A-A9F430D13EEB *EXPLOIT*
| EB13CBD6-BC93-5F14-A210-AC0B5A1D8572 8.1 https://vulners.com/githubexploit/EB13CBD6-BC93-5F14-A210-AC0B5A1D8572 *EXPLOIT*
| E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD 8.1 https://vulners.com/githubexploit/E660E1AF-7A87-57E2-AEEF-CA14E1FEF7CD *EXPLOIT*
| E543E274-C20A-582A-8F8E-F8E3F381C345 8.1 https://vulners.com/githubexploit/E543E274-C20A-582A-8F8E-F8E3F381C345 *EXPLOIT*
| E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257 8.1 https://vulners.com/githubexploit/E34FCCEC-226E-5A46-9B1C-BCD6EF7D3257 *EXPLOIT*
| E24EEC0A-40F7-5BBC-9E4D-7B13522FF915 8.1 https://vulners.com/githubexploit/E24EEC0A-40F7-5BBC-9E4D-7B13522FF915 *EXPLOIT*
| DC798E98-BA77-5F86-9C16-0CF8CD540E8B 8.1 https://vulners.com/githubexploit/DC798E98-BA77-5F86-9C16-0CF8CD540E8B *EXPLOIT*
| DC473885-F54C-5F76-BAFD-0175E4A90C1D 8.1 https://vulners.com/githubexploit/DC473885-F54C-5F76-BAFD-0175E4A90C1D *EXPLOIT*
| D85F08E9-DB96-55E9-8DD2-22F01980F360 8.1 https://vulners.com/githubexploit/D85F08E9-DB96-55E9-8DD2-22F01980F360 *EXPLOIT*
| D572250A-BE94-501D-90C4-14A6C9C0AC47 8.1 https://vulners.com/githubexploit/D572250A-BE94-501D-90C4-14A6C9C0AC47 *EXPLOIT*
| D1E049F1-393E-552D-80D1-675022B26911 8.1 https://vulners.com/githubexploit/D1E049F1-393E-552D-80D1-675022B26911 *EXPLOIT*
| CFEBF7AF-651A-5302-80B8-F8146D5B33A6 8.1 https://vulners.com/githubexploit/CFEBF7AF-651A-5302-80B8-F8146D5B33A6 *EXPLOIT*
| CF80DDA9-42E7-5E06-8DA8-84C72658E191 8.1 https://vulners.com/githubexploit/CF80DDA9-42E7-5E06-8DA8-84C72658E191 *EXPLOIT*
| CB2926E1-2355-5C82-A42A-D4F72F114F9B 8.1 https://vulners.com/githubexploit/CB2926E1-2355-5C82-A42A-D4F72F114F9B *EXPLOIT*


ritesh@vbox: ~
File Actions Edit View Help
| SSV:11558 4.3 https://vulners.com/seebug/SSV:11558 *EXPLOIT*
| PACKETSTORM:109284 4.3 https://vulners.com/packetstorm/PACKETSTORM:109284 *EXPLOIT*
| EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE 4.3 https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE *EXPLOIT*
| EDB-ID:35738 4.3 https://vulners.com/exploitdb/EDB-ID:35738 *EXPLOIT*
| CVE-2016-8612 4.3 https://vulners.com/cve/CVE-2016-8612
| CVE-2014-0118 4.3 https://vulners.com/cve/CVE-2014-0118
| CVE-2013-1896 4.3 https://vulners.com/cve/CVE-2013-1896
| CVE-2012-4558 4.3 https://vulners.com/cve/CVE-2012-4558
| CVE-2012-3499 4.3 https://vulners.com/cve/CVE-2012-3499
| CVE-2012-0053 4.3 https://vulners.com/cve/CVE-2012-0053
| CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317
| CVE-2011-3639 4.3 https://vulners.com/cve/CVE-2011-3639
| CVE-2011-0419 4.3 https://vulners.com/cve/CVE-2011-0419
| CVE-2010-0434 4.3 https://vulners.com/cve/CVE-2010-0434
| CVE-2009-0023 4.3 https://vulners.com/cve/CVE-2009-0023
| CVE-2008-2939 4.3 https://vulners.com/cve/CVE-2008-2939
| CVE-2008-0455 4.3 https://vulners.com/cve/CVE-2008-0455
| CVE-2007-6420 4.3 https://vulners.com/cve/CVE-2007-6420
| SSV:12628 2.6 https://vulners.com/seebug/SSV:12628 *EXPLOIT*
| CVE-2012-2687 2.6 https://vulners.com/cve/CVE-2012-2687
| CVE-2009-3094 2.6 https://vulners.com/cve/CVE-2009-3094
| CVE-2008-0456 2.6 https://vulners.com/cve/CVE-2008-0456
| SSV:60250 1.2 https://vulners.com/seebug/SSV:60250 *EXPLOIT*
| CVE-2011-4415 1.2 https://vulners.com/cve/CVE-2011-4415
| 1337DAY-ID-9602 0.0 https://vulners.com/zdt/1337DAY-ID-9602 *EXPLOIT*
| 1337DAY-ID-21346 0.0 https://vulners.com/zdt/1337DAY-ID-21346 *EXPLOIT*
| 1337DAY-ID-17257 0.0 https://vulners.com/zdt/1337DAY-ID-17257 *EXPLOIT*
| 1337DAY-ID-16843 0.0 https://vulners.com/zdt/1337DAY-ID-16843 *EXPLOIT*
| 1337DAY-ID-13268 0.0 https://vulners.com/zdt/1337DAY-ID-13268 *EXPLOIT*
|_ 1337DAY-ID-11185 0.0 https://vulners.com/zdt/1337DAY-ID-11185 *EXPLOIT*
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 34607/tcp mountd
| 100005 1,2,3 51295/udp mountd
| 100021 1,3,4 46132/udp nlockmgr
| 100021 1,3,4 51602/tcp nlockmgr
| 100024 1 44770/tcp status
|_ 100024 1 45801/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:7A:B9:68 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.09 seconds
┌──(ritesh㉿vbox)-[~]
└─$

Outcomes:

CO2: Comprehend purpose of Anonymity and Foot printing.

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how to perform Active Reconnaissance using tools like Nmap and Netcat. I understood the importance of gathering information about a target system to identify potential vulnerabilities. Using Nmap, I was able to explore various scanning techniques such as port scanning, service version detection, and OS detection, which are crucial for ethical hacking and penetration testing. Active Reconnaissance helps in identifying weaknesses in a system that can later be exploited, but it also emphasizes the need for ethical usage of these tools. Overall, this experiment enhanced my knowledge of network security and reinforced the significance of recon in cybersecurity.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

References:

https://nmap.org/book/
https://nmap.org/book/nse.html
https://www.geeksforgeeks.org/introduction-to-nmap/
https://www.tutorialspoint.com/netcat