CA -3 PROJECT REPORT

1.INTRODUCTION

The task that I have assigned was.

"Suppose you are an ethical hacker and you are asked to perform a scan on your simulated

network. Your task is to identify.

a) Live hosts,

b) Services running on live hosts,

c) Banner grabbing

d) OS fingerprinting

e) Conducting performance scans based on your current network bandwidth.

Use any open-source software to generate a report on the same."

1.1 Objective of the Project

The objective of the project is by using an open software we need to create a simulated network and to that network, we need to find the live hosts and what are the services that run on live hosts, perform banner grabbing to the network, OS fingerprinting and lastly conduct performance scans based on your current network bandwidth.

1.2 Description of the Project

- **Open-Source Software:**
  Open source software refers to software whose source code is available for anyone to view, modify, and distribute. This allows users to collaborate and contribute to the software, making it more versatile and customizable.
  I'm using the open source software Linux operating system using Ubuntu to perform the assigned task.

  Examples of Open Source Software: Git, Linux Operating system, GIMP, etc.

- **Live hosts:**
  In Ubuntu, live hosts refer to devices that are currently active and responsive on a network. These devices can be running Ubuntu or any other operating system and are connected to the same network as the Ubuntu machine. Ubuntu provides various tools and commands to identify live hosts on a network, including Nmap, arp-scan, and ping. These tools allow network administrators to scan the network and identify active devices, as well as gather information about their IP addresses, MAC addresses, and other network parameters. Knowing the live hosts on a network is important for managing network resources, troubleshooting network issues, and maintaining network security. It helps administrators ensure that all devices are properly configured, up-to-date, and secured against potential threats, and that only authorized devices are allowed to access the network.
  Command: nmap -sn <IP Adress> -vv

- **Services Running on live hosts:**
  It shows the services which are running on live hosts.
  Command: nmap -sV <IP Adress>

- **Banner grabbing:**
  Banner grabbing is a technique used by hackers to gather information about a web server or other networked device. It involves sending requests to the server and analyzing the responses to identify the server software, version, and other details that can be used to exploit vulnerabilities.
  The name "banner grabbing" comes from the fact that many servers include a "banner" or identifying information in their response headers. For example, an HTTP response from an Apache web server might include a banner like "Server: Apache/2.4.18 (Ubuntu)". By analyzing this banner, an attacker can determine that the server is running Apache version 2.4.18 on an Ubuntu system.
  Banner grabbing can be performed manually using tools like Telnet or Netcat, or automated using specialized tools like Nmap or BannerGrab. While banner grabbing is often used by attackers to identify vulnerabilities and plan attacks, it can also be used by security professionals to identify and patch vulnerabilities before they can be exploited.
  Command: sudo nmap - -script banner <IP Adress>

- **OS Fingerprinting:**
  OS fingerprinting is a technique used to determine the operating system (OS) running on a remote target host in a network. This is typically done by sending specific packets or probes to the target host and analyzing the responses received to identify the operating system running on the host.

  The process of OS fingerprinting usually involves analyzing various parameters, such as the packet sequence number, the time to live (TTL) value, the type of TCP/IP stack being used, and other such details that are unique to specific operating systems.

  There are several tools available that can be used to perform OS fingerprinting, such as Nmap, p0f, and Xprobe2. These tools use different techniques to identify the operating system running on a target host, and can be used to gather additional information about the host, such as the services running on it, the ports that are open, and more.

  While OS fingerprinting can be useful for network administrators to identify devices and systems running on their networks, it can also be used by attackers to gain information about the target hosts and launch attacks. Therefore, it is important to be aware of the potential risks associated with OS fingerprinting and take necessary security measures to protect against it.
  Command: sudo nmap -O <IP Address>

- **Performance Scan:**
  Performance scan gives a representative complete scan and performance of the ip address or network. T4 represents the timing template with range 1 to 5 the higher is faster.
  Example: sudo nmap -A -T4 <IP Address>

1.3 Scope of the Project

The scope of the project is we can get the live hosts and list of services running with the live hosts of a simulated network and also how to perform banner grabbing and the detection of Operating system with using very verbose we can get the detail analysis.

2. System Description

2.1 Target System Description

Banner grabbing and OS fingerprinting are techniques used by hackers and security professionals to gather information about a target system. Banner grabbing is the process of retrieving information about a remote system by analyzing the response from a network service or application running on that system. This technique is commonly used to determine the type of web server, the version of software, and other details such as the operating system and available services. Banner grabbing can be accomplished using tools such as Telnet or Netcat, or specialized tools such as Nmap.

OS fingerprinting, on the other hand, is the process of identifying the operating system running on a target system. This can be accomplished by analyzing the network packets and responses generated by the target system. OS fingerprinting techniques involve examining a variety of factors such as the TCP/IP stack behavior, the way the system responds to specific packets, and the way the system generates and handles network traffic.

Both banner grabbing and OS fingerprinting can be used for legitimate purposes, such as network administration and security auditing. However, they can also be used by malicious actors to gather information for potential attacks. As a result, it is important for organizations to be aware of these techniques and take steps to secure their systems against them. This can include implementing firewalls, disabling unnecessary services, and keeping software up-to-date with the latest security patches.

3. Analysis Report

3.1 System Snap Shots and full analysis of the Report

- Firstly, I am using the Ubuntu open-source software using the Oracle virtual box.
- To get started, firstly we need to know about the nmap command where all our task were related to the above command. I had learnt about the nmap by manual directory of nmap.
  Command : man nmap

Nmap :

Name: nmap - Network exploration tool and security / port scanner

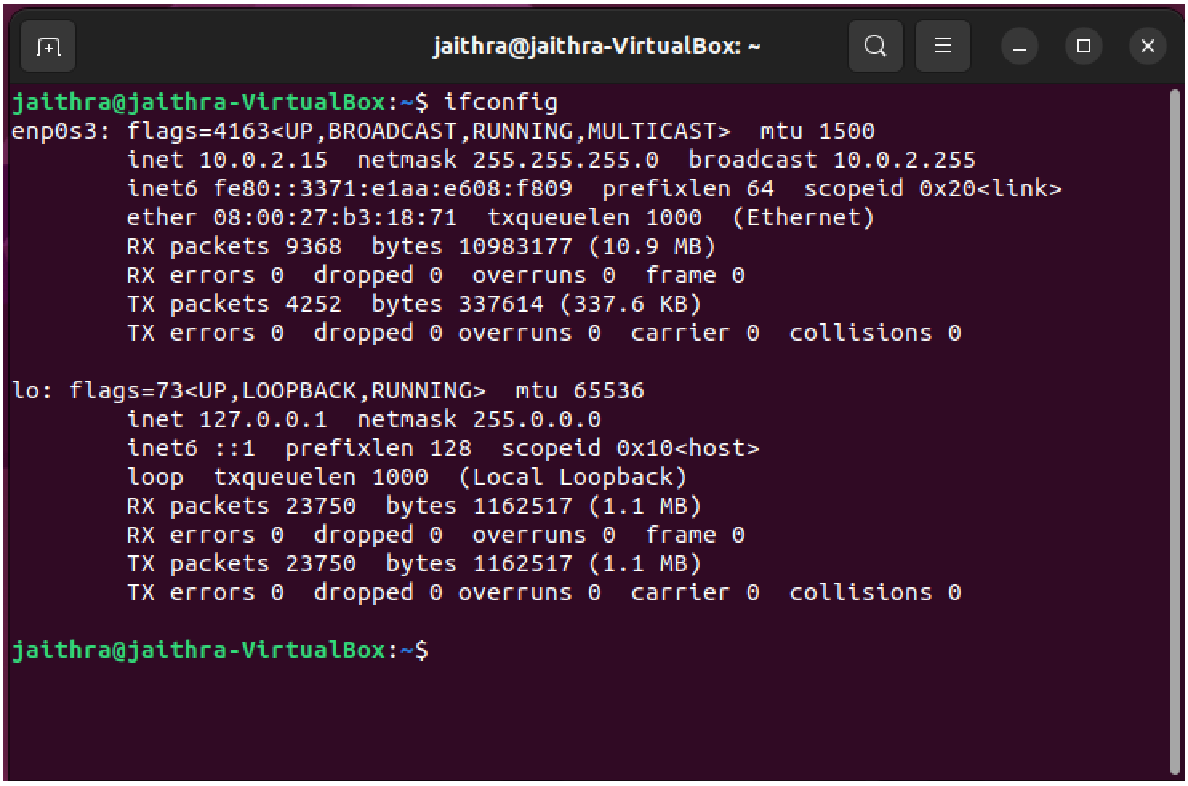
Synopsis: nmap [Scan Type...] [Options] {target specification}

Description

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

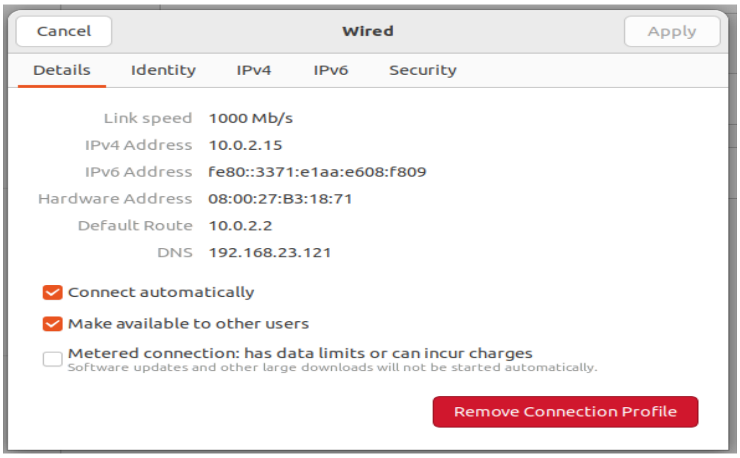
To do the above tasks, we need to know our IPV4 Address using the ifconfig. In general, in our windows operating system in command prompt to get ip address we need to use ipconfig. But in ubuntu we need to use ifconifg.

- To install the nmap we need to enter the command.
  Command : sudo apt install nmap
- To know the ip address
  Command : ifconfig



```
jaithra@jaithra-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3371:e1aa:e608:f809  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b3:18:71  txqueuelen 1000  (Ethernet)
        RX packets 9368  bytes 10983177 (10.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4252  bytes 337614 (337.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 23750  bytes 1162517 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23750  bytes 1162517 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

jaithra@jaithra-VirtualBox:~$
```

Fig 3.1



Link speed 1000 Mb/s
IPv4 Address 10.0.2.15
IPv6 Address fe80::3371:e1aa:e608:f809
Hardware Address 08:00:27:B3:18:71
Default Route 10.0.2.2
DNS 192.168.23.121

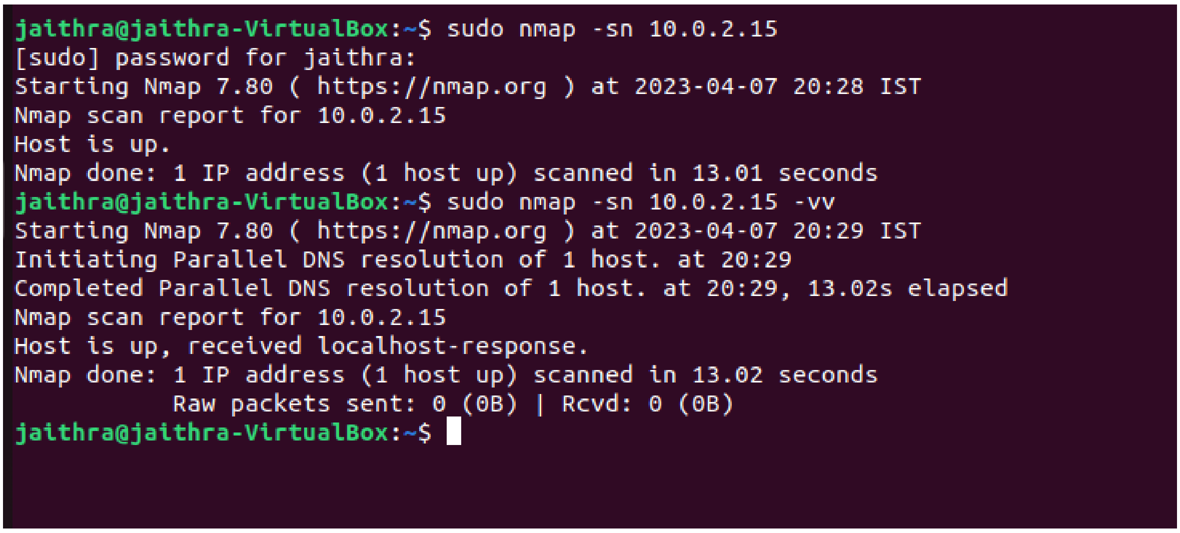
☑ Connect automatically
☑ Make available to other users
□ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Fig 3.2 Alternative method to find the ip address.

We need to note down the inet address which the IPV4 Address or the local area network (LAN) local ip address of our computer. In the above figures 3.1,3.2 , we need to take the enp0s3 which is the wired connection with our pc. I took that ip address for the assigned task therefore**;**

inet 10.0.2.15.

a) **Identify the Live hosts:**
To identify the live hosts, we have the command as mentioned above.
Command: nmap -sn <IP Adress>
we sometimes use "-vv" option at the end of the command which shows that the "vv" option specifies the level of verbosity for the output of the Nmap command. The "vv" option stands for "very verbose", which means that Nmap will provide more detailed information about the scanning process and results than it would with a single "v" (verbose) option or no verbosity option specified. This can be useful for troubleshooting or for obtaining a more comprehensive understanding of the scan results.



```
jaithra@jaithra-VirtualBox:~$ sudo nmap -sn 10.0.2.15
[sudo] password for jaithra:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 20:28 IST
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
jaithra@jaithra-VirtualBox:~$ sudo nmap -sn 10.0.2.15 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 20:29 IST
Initiating Parallel DNS resolution of 1 host. at 20:29
Completed Parallel DNS resolution of 1 host. at 20:29, 13.02s elapsed
Nmap scan report for 10.0.2.15
Host is up, received localhost-response.
Nmap done: 1 IP address (1 host up) scanned in 13.02 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
jaithra@jaithra-VirtualBox:~$
```

Fig 3.3

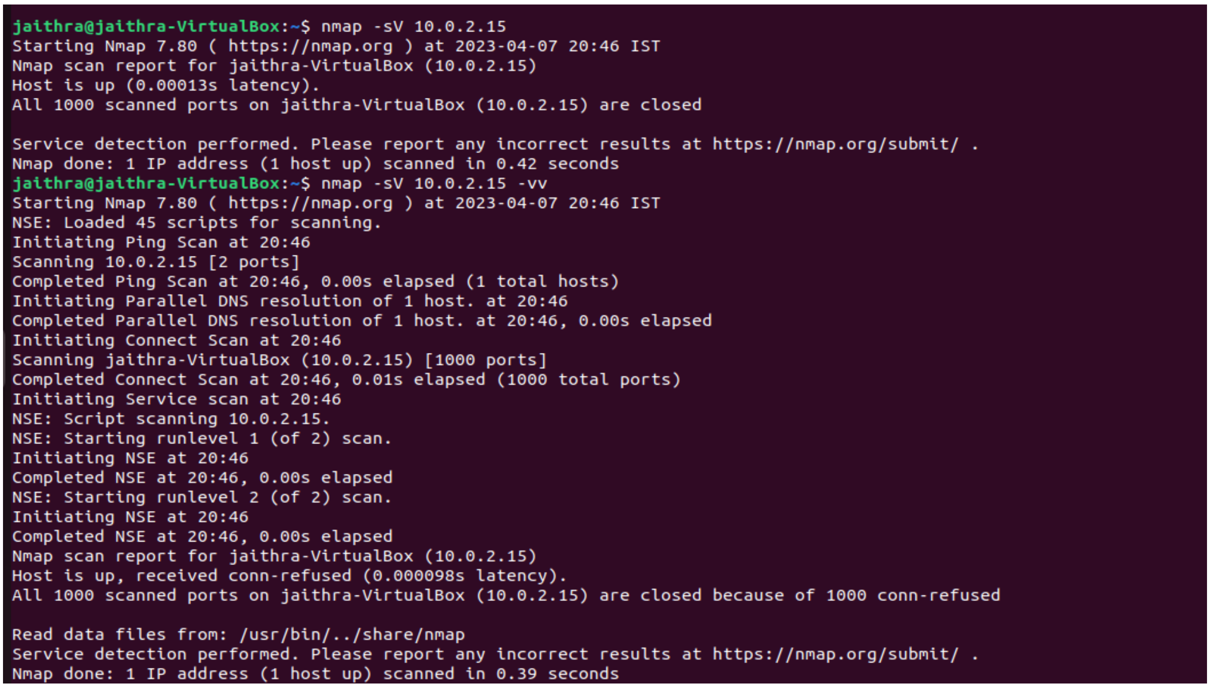
-sn (No port scan) .
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the scan. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run. This is by default one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list provided by list scan of every single IP and host name.
Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep, and is more reliable than pinging the broadcast address because many hosts do not reply to broadcast queries.

Both commands in fig 3.3, depict the same the only difference was the output information with "-vv" give more detailed information. And from fig 3.3, we can say that after the nmap scan report there is only one live host for my ip address.

b) Services that are running on live hosts:

To see the services that are running on live hosts use the following command.

Command: nmap -sV <IP Address>

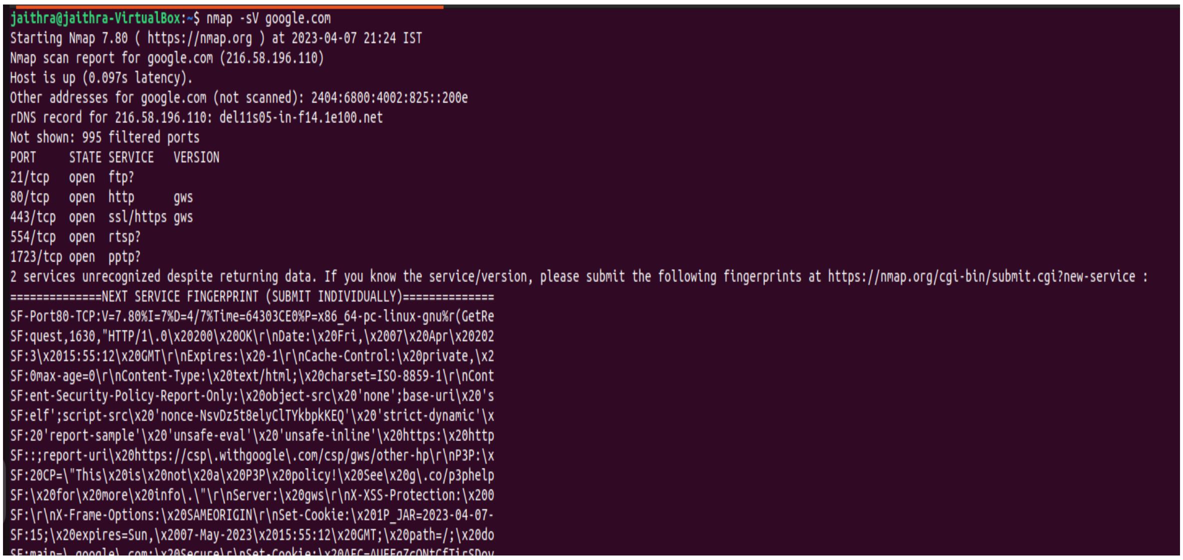


```
jaithra@jaithra-VirtualBox:~$ nmap -sV 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 20:46 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.00013s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
jaithra@jaithra-VirtualBox:~$ nmap -sV 10.0.2.15 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 20:46 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 20:46
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 20:46, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:46
Completed Parallel DNS resolution of 1 host. at 20:46, 0.00s elapsed
Initiating Connect Scan at 20:46
Scanning jaithra-VirtualBox (10.0.2.15) [1000 ports]
Completed Connect Scan at 20:46, 0.01s elapsed (1000 total ports)
Initiating Service scan at 20:46
NSE: Script scanning 10.0.2.15.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:46
Completed NSE at 20:46, 0.00s elapsed
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up, received conn-refused (0.000098s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed because of 1000 conn-refused

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Fig 3.4

-sV (version detection). Shows the services running on live hosts.

Here, just an experiment for more understanding with google.com

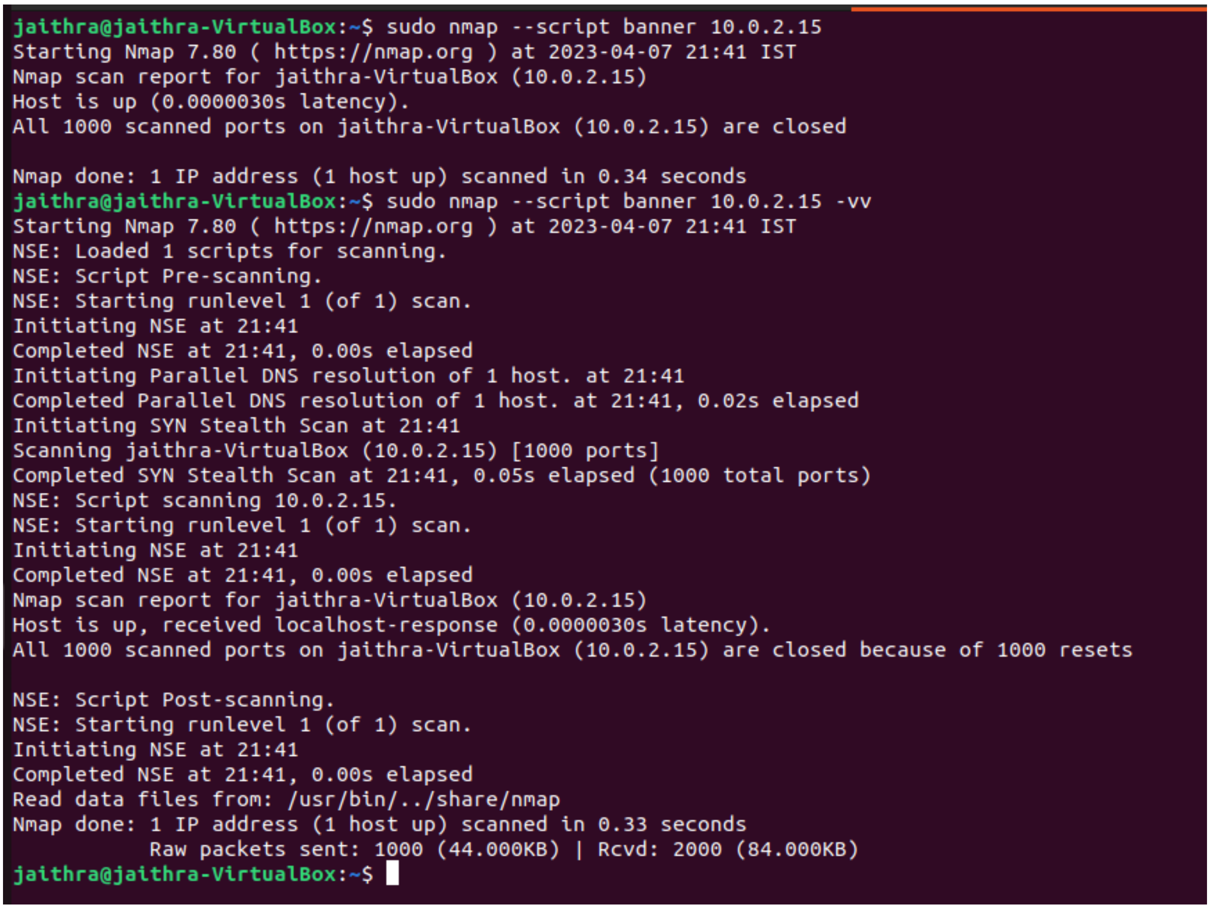


```
jaithra@jaithra-VirtualBox:~$ nmap -sV google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:24 IST
Nmap scan report for google.com (216.58.196.110)
Host is up (0.097s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:825::200e
rDNS record for 216.58.196.110: del11s05-in-f14.1e100.net
Not shown: 995 filtered ports
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp?
80/tcp   open  http      gws
443/tcp  open  ssl/https gws
554/tcp  open  rtsp?
1723/tcp open  pptp?
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.80%I=7%D=4/7%Time=64303CE0%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1630,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Fri,\x2007\x20Apr\x20202
SF:3\x2015:55:12\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20private,\x2
SF:0max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\nCont
SF:ent-Security-Policy-Report-Only:\x20object-src\x20'none';base-uri\x20's
SF:elf';script-src\x20'nonce-NsvDz5t8elyClTYkbpkKEQ'\x20'strict-dynamic'\x
SF:20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20https:\x20http
SF::;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-hp\r\nP3P:\x
SF:20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3phelp
SF:\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:\x200
SF:\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x201P_JAR=2023-04-07-
SF:15;\x20expires=Sun,\x2007-May-2023\x2015:55:12\x20GMT;\x20path=/;\x20do
SF:main=\.google\.com;\x20Secure\r\nSet-Cookie:\x20AEC=AUEFqZcONtCfTicSDov
```

Fig 3.5

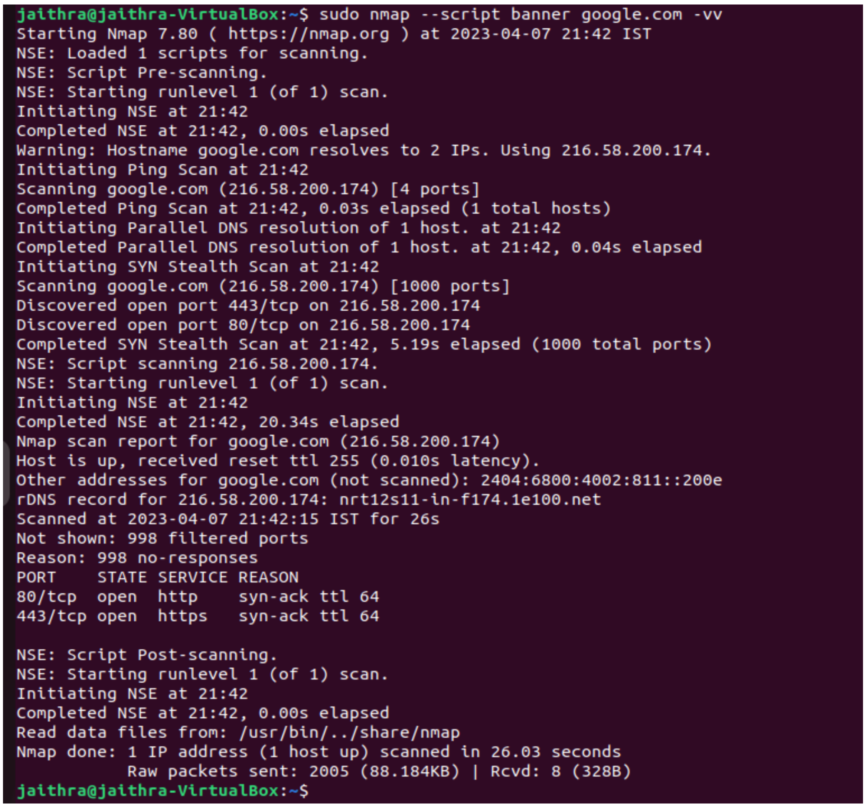
c) Banner Grabbing

The security purpose of banner grabbing is to gather information about a target system's software, operating system, and available services, to identify potential vulnerabilities and security weaknesses. This information can then be used to improve the security of the system by implementing appropriate security measures and patches to prevent attacks. Banner grabbing can also help security professionals to assess the level of risk posed by the system and to plan effective security strategies to protect against potential threats.



```
jaithra@jaithra-VirtualBox:~$ sudo nmap --script banner 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:41 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.0000030s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
jaithra@jaithra-VirtualBox:~$ sudo nmap --script banner 10.0.2.15 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:41 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:41
Completed NSE at 21:41, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:41
Completed Parallel DNS resolution of 1 host. at 21:41, 0.02s elapsed
Initiating SYN Stealth Scan at 21:41
Scanning jaithra-VirtualBox (10.0.2.15) [1000 ports]
Completed SYN Stealth Scan at 21:41, 0.05s elapsed (1000 total ports)
NSE: Script scanning 10.0.2.15.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:41
Completed NSE at 21:41, 0.00s elapsed
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up, received localhost-response (0.0000030s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed because of 1000 resets

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:41
Completed NSE at 21:41, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2000 (84.000KB)
jaithra@jaithra-VirtualBox:~$
```

Fig 3.6



```
jaithra@jaithra-VirtualBox:~$ sudo nmap --script banner google.com -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:42 IST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:42
Completed NSE at 21:42, 0.00s elapsed
Warning: Hostname google.com resolves to 2 IPs. Using 216.58.200.174.
Initiating Ping Scan at 21:42
Scanning google.com (216.58.200.174) [4 ports]
Completed Ping Scan at 21:42, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:42
Completed Parallel DNS resolution of 1 host. at 21:42, 0.04s elapsed
Initiating SYN Stealth Scan at 21:42
Scanning google.com (216.58.200.174) [1000 ports]
Discovered open port 443/tcp on 216.58.200.174
Discovered open port 80/tcp on 216.58.200.174
Completed SYN Stealth Scan at 21:42, 5.19s elapsed (1000 total ports)
NSE: Script scanning 216.58.200.174.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:42
Completed NSE at 21:42, 20.34s elapsed
Nmap scan report for google.com (216.58.200.174)
Host is up, received reset ttl 255 (0.010s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:811::200e
rDNS record for 216.58.200.174: nrt12s11-in-f174.1e100.net
Scanned at 2023-04-07 21:42:15 IST for 26s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack ttl 64
443/tcp open  https   syn-ack ttl 64

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 21:42
Completed NSE at 21:42, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 26.03 seconds
           Raw packets sent: 2005 (88.184KB) | Rcvd: 8 (328B)
jaithra@jaithra-VirtualBox:~$
```

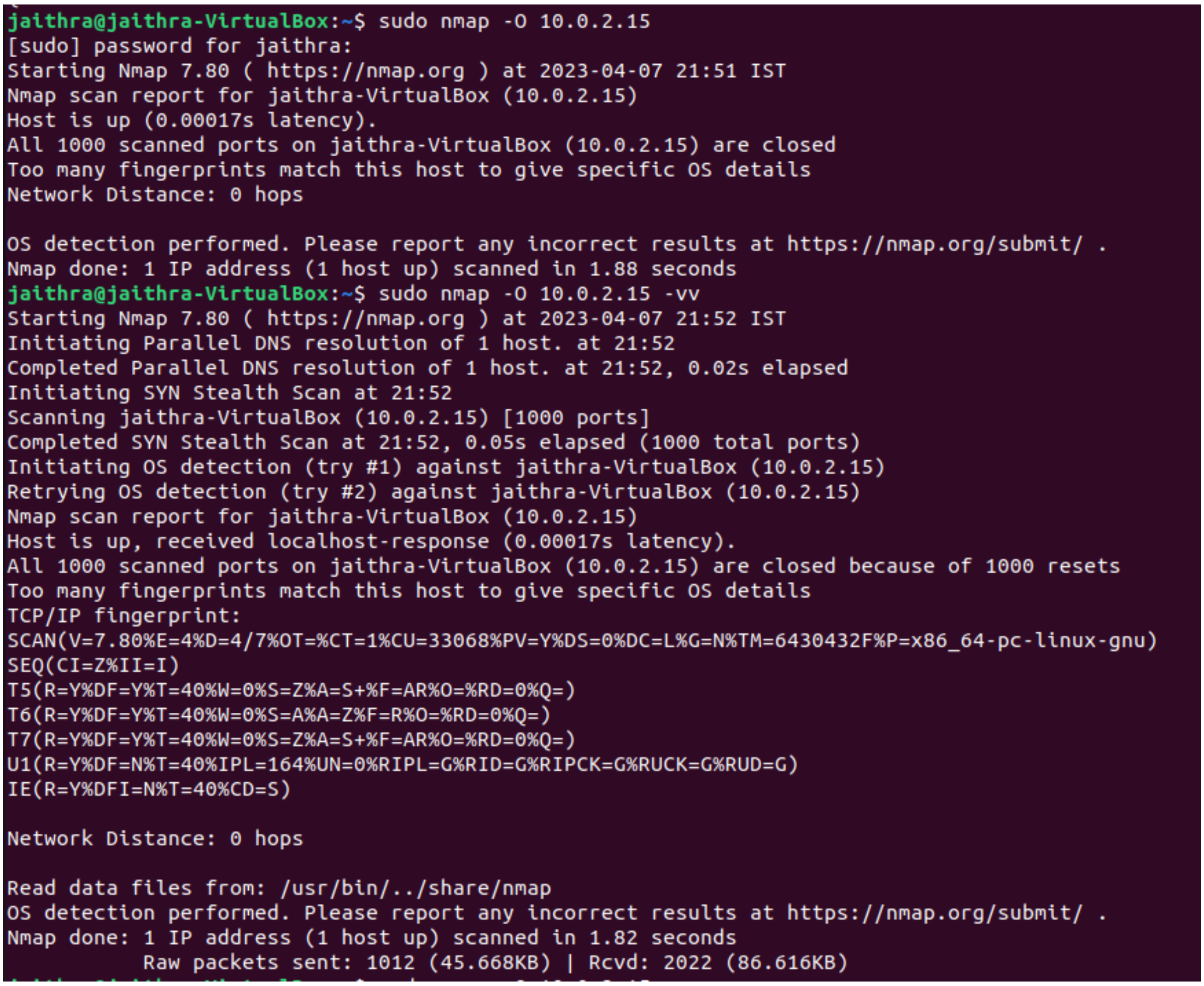
Fig 3.7 Detailing example

d) OS Fingerprinting

One of Nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit of the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares the results to its nmap-os-db. database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name (e.g. Sun), underlying OS (e.g. Solaris), OS generation (e.g. 10), and device type (general purpose, router, switch, game console, etc).

If Nmap is unable to guess the OS of a machine, and conditions are good (e.g. at least one open port and one closed port were found), Nmap will provide a URL you can use to submit the fingerprint if you know (for sure) the OS running on the machine. By doing this you contribute to the pool of operating systems known to Nmap and thus it will be more accurate for everyone.

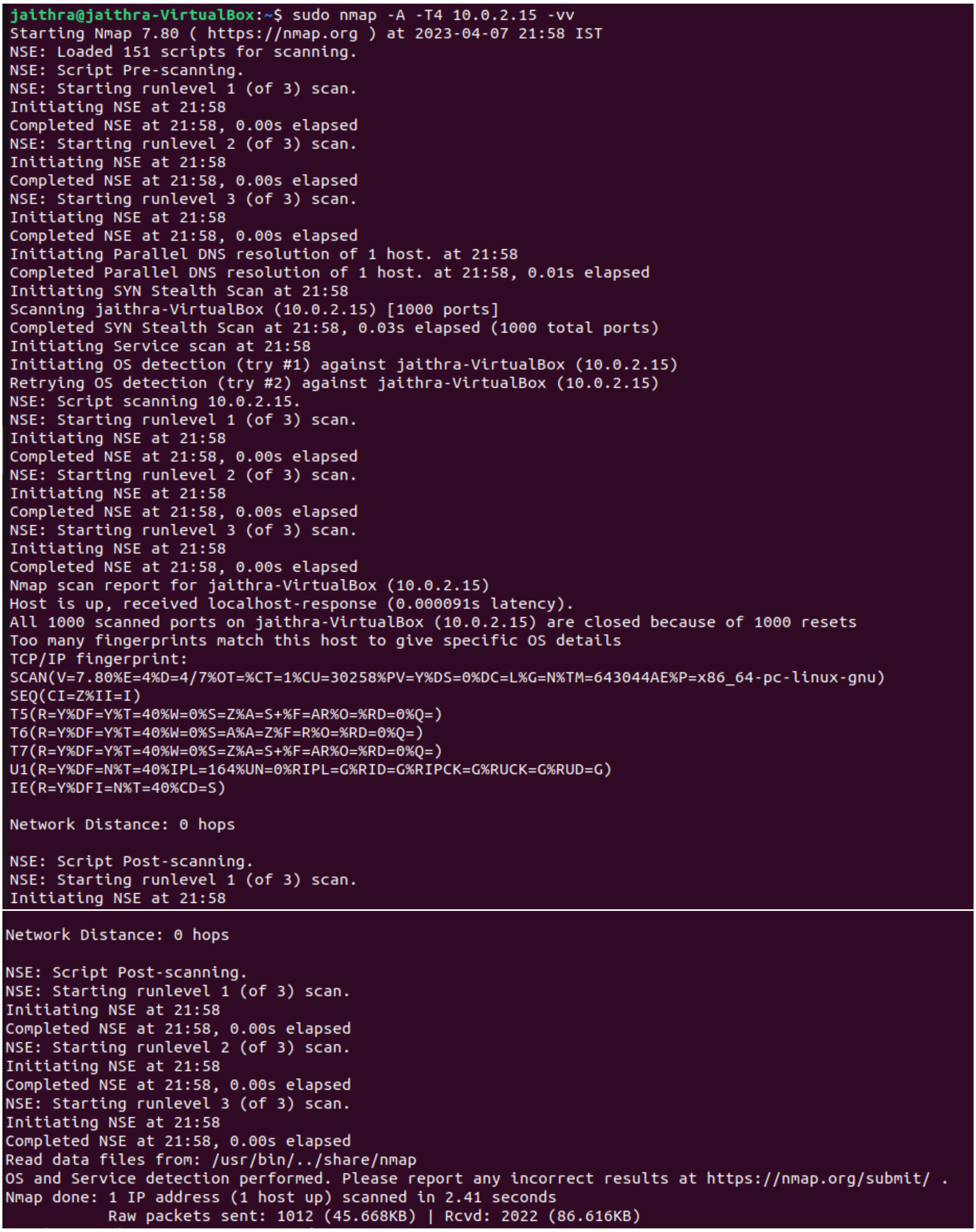
-O Enables OS detection,



```
jaithra@jaithra-VirtualBox:~$ sudo nmap -O 10.0.2.15
[sudo] password for jaithra:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:51 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.00017s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
jaithra@jaithra-VirtualBox:~$ sudo nmap -O 10.0.2.15 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:52 IST
Initiating Parallel DNS resolution of 1 host. at 21:52
Completed Parallel DNS resolution of 1 host. at 21:52, 0.02s elapsed
Initiating SYN Stealth Scan at 21:52
Scanning jaithra-VirtualBox (10.0.2.15) [1000 ports]
Completed SYN Stealth Scan at 21:52, 0.05s elapsed (1000 total ports)
Initiating OS detection (try #1) against jaithra-VirtualBox (10.0.2.15)
Retrying OS detection (try #2) against jaithra-VirtualBox (10.0.2.15)
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up, received localhost-response (0.00017s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed because of 1000 resets
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=4/7%OT=%CT=1%CU=33068%PV=Y%DS=0%DC=L%G=N%TM=6430432F%P=x86_64-pc-linux-gnu)
SEQ(CI=Z%II=I)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
           Raw packets sent: 1012 (45.668KB) | Rcvd: 2022 (86.616KB)
```

Fig 3.8

e) Conducting the performance scan based on the network.



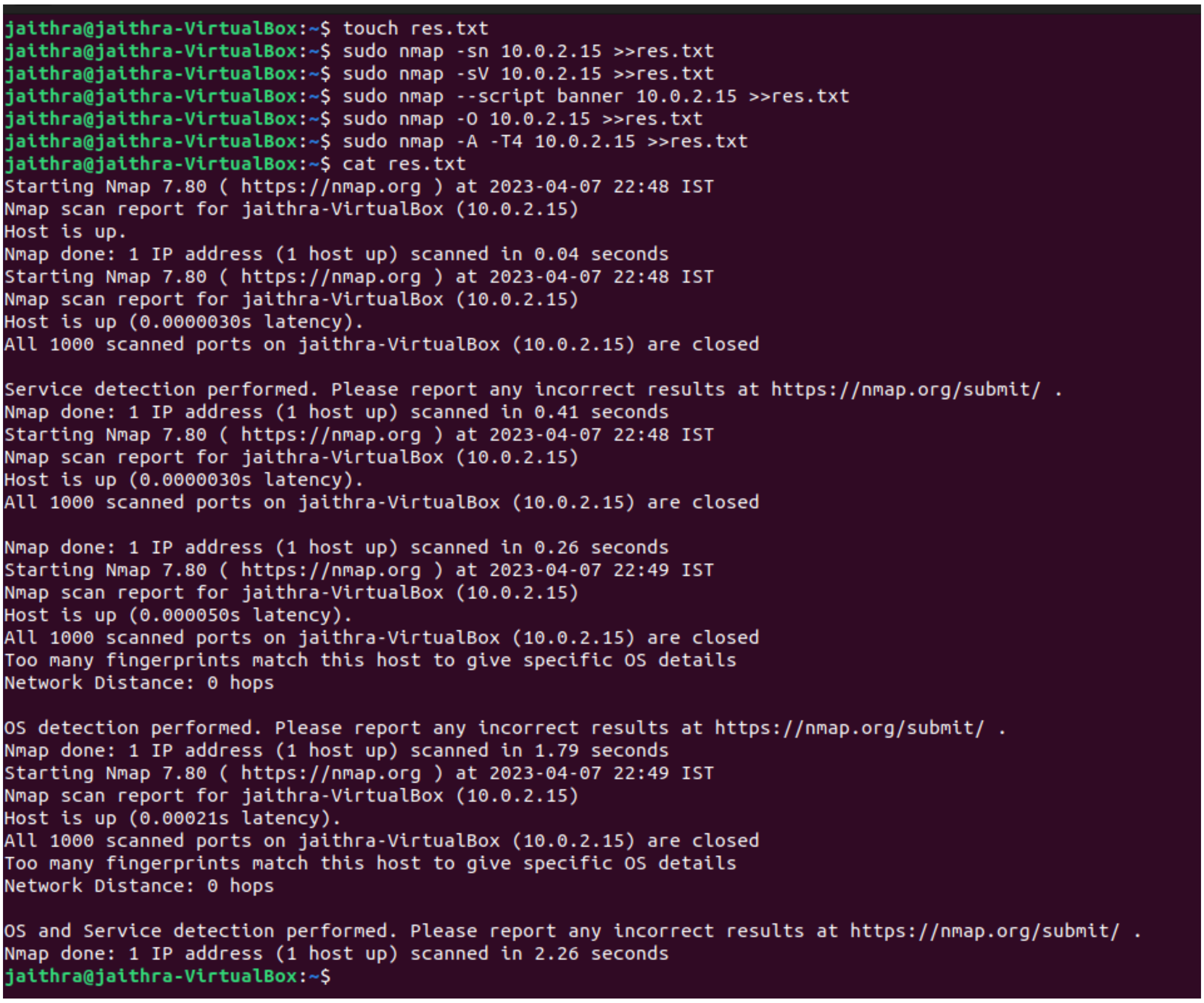
```
jaithra@jaithra-VirtualBox:~$ sudo nmap -A -T4 10.0.2.15 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 21:58 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 21:58
Completed Parallel DNS resolution of 1 host. at 21:58, 0.01s elapsed
Initiating SYN Stealth Scan at 21:58
Scanning jaithra-VirtualBox (10.0.2.15) [1000 ports]
Completed SYN Stealth Scan at 21:58, 0.03s elapsed (1000 total ports)
Initiating Service scan at 21:58
Initiating OS detection (try #1) against jaithra-VirtualBox (10.0.2.15)
Retrying OS detection (try #2) against jaithra-VirtualBox (10.0.2.15)
NSE: Script scanning 10.0.2.15.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up, received localhost-response (0.000091s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed because of 1000 resets
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.80%E=4%D=4/7%OT=%CT=1%CU=30258%PV=Y%DS=0%DC=L%G=N%TM=643044AE%P=x86_64-pc-linux-gnu)
SEQ(CI=Z%II=I)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 0 hops

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:58
```

```
Network Distance: 0 hops

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:58
Completed NSE at 21:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.41 seconds
           Raw packets sent: 1012 (45.668KB) | Rcvd: 2022 (86.616KB)
```

Fig 3.9

This gives a detailed scanning report for the performance of our ip address.

Lastly, I had added all the commands scanning report to a file called res.txt.



```
jaithra@jaithra-VirtualBox:~$ touch res.txt
jaithra@jaithra-VirtualBox:~$ sudo nmap -sn 10.0.2.15 >>res.txt
jaithra@jaithra-VirtualBox:~$ sudo nmap -sV 10.0.2.15 >>res.txt
jaithra@jaithra-VirtualBox:~$ sudo nmap --script banner 10.0.2.15 >>res.txt
jaithra@jaithra-VirtualBox:~$ sudo nmap -O 10.0.2.15 >>res.txt
jaithra@jaithra-VirtualBox:~$ sudo nmap -A -T4 10.0.2.15 >>res.txt
jaithra@jaithra-VirtualBox:~$ cat res.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 22:48 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 22:48 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.0000030s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 22:48 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.0000030s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 22:49 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.000050s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-07 22:49 IST
Nmap scan report for jaithra-VirtualBox (10.0.2.15)
Host is up (0.00021s latency).
All 1000 scanned ports on jaithra-VirtualBox (10.0.2.15) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
jaithra@jaithra-VirtualBox:~$
```

Fig 3.10 Scan Report

4. References

Manual directory – man nmap

https://linuxhint.com/nmap_banner_grab/

Git Repository: https://github.com/jaithramandavilli/CA-3-Open_Source.git