NMAP

Step 1: Initial Port Discovery

The first part of your experiment was a basic port scan. The main goal here is to quickly identify which network "doors" (ports) are open on the target server, scanme.nmap.org.

- **Purpose:** To find all accessible TCP ports and their commonly associated services.
- **Command:** sudo nmap scanme.nmap.org
- **Key Findings:** The scan successfully identified several open ports, including:
  - **Port 22:** Running the SSH (Secure Shell) service.
  - **Port 80:** Running the HTTP service, indicating a live web server.
  - **Ports 9929 and 31337:** Two other non-standard open ports.

This initial step confirmed the target was online and mapped out the primary services available for further investigation.

Step 2: Detailed Service and Version Identification

The second phase of the experiment was a more in-depth probe to identify the exact software and version running on the open ports.

- **Purpose:** To go beyond just the service name (like "HTTP") and find the specific version (like "Apache 2.4.7"). This is a critical step, as vulnerabilities are almost always tied to specific software versions.
- **Command:** sudo nmap -p22 -A -sV -O scanme.nmap.org
- **Key Findings:**
  - The SSH service was identified as **OpenSSH version 6.6.1p1**.
  - The HTTP service was identified as **Apache web server version 2.4.7**.

This scan provided highly valuable intelligence, turning general information into specific, actionable data for vulnerability research.

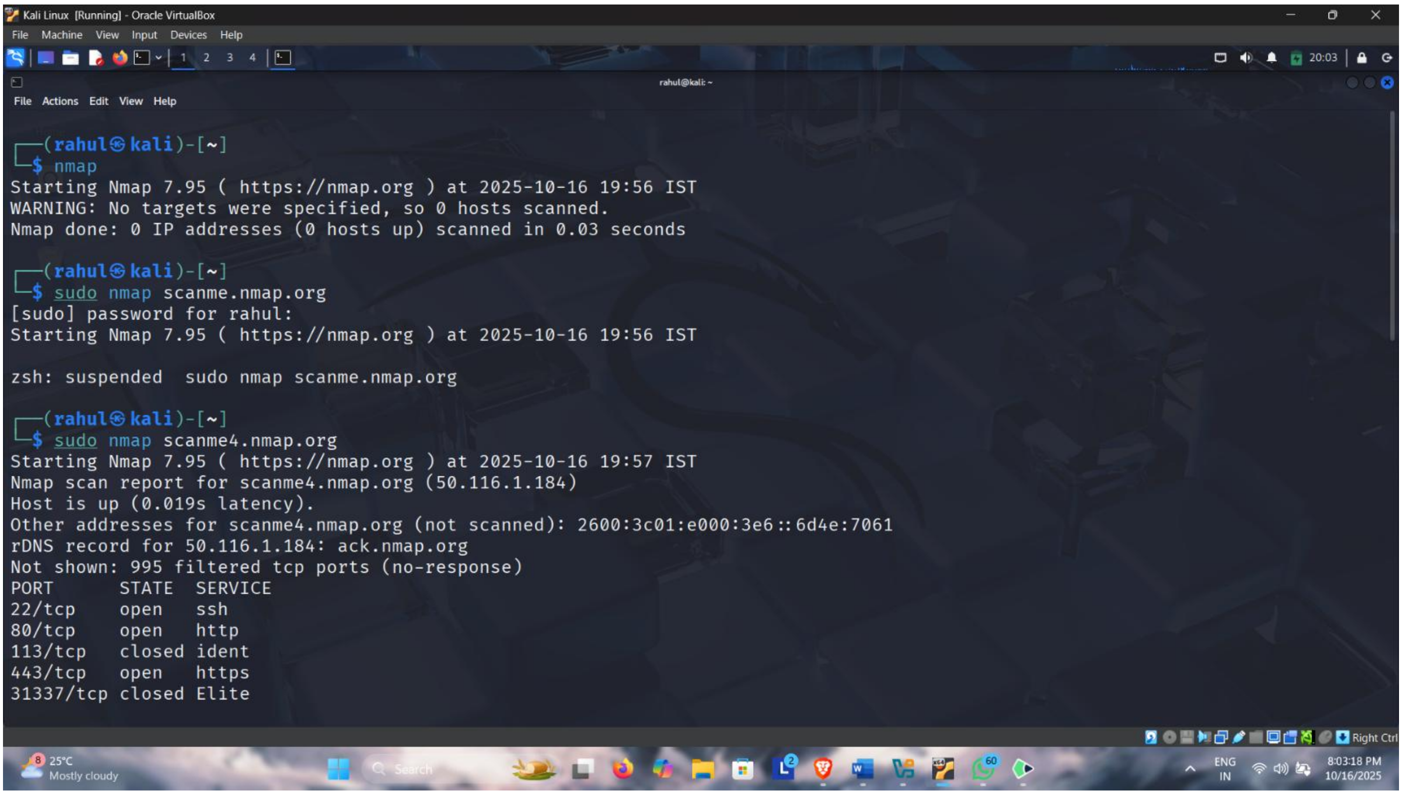
Step 3: Comprehensive System Profiling

The final part of the experiment involved an aggressive, all-in-one scan to gather a complete profile of the target machine.

- **Purpose:** To perform several advanced scans simultaneously, including **operating system (OS) detection**, script scanning, and network route tracing.
- **Command:** sudo nmap -A scanme.nmap.org
- **Key Findings:**

- **OS Detection:** Nmap analyzed the target's network behavior and made an educated guess that the server is running a **Linux** operating system.
- **Traceroute:** The scan mapped the network path from your location to the target server, showing the intermediate routers.

This concluding scan provided crucial context about the target's underlying operating system and its location on the network.

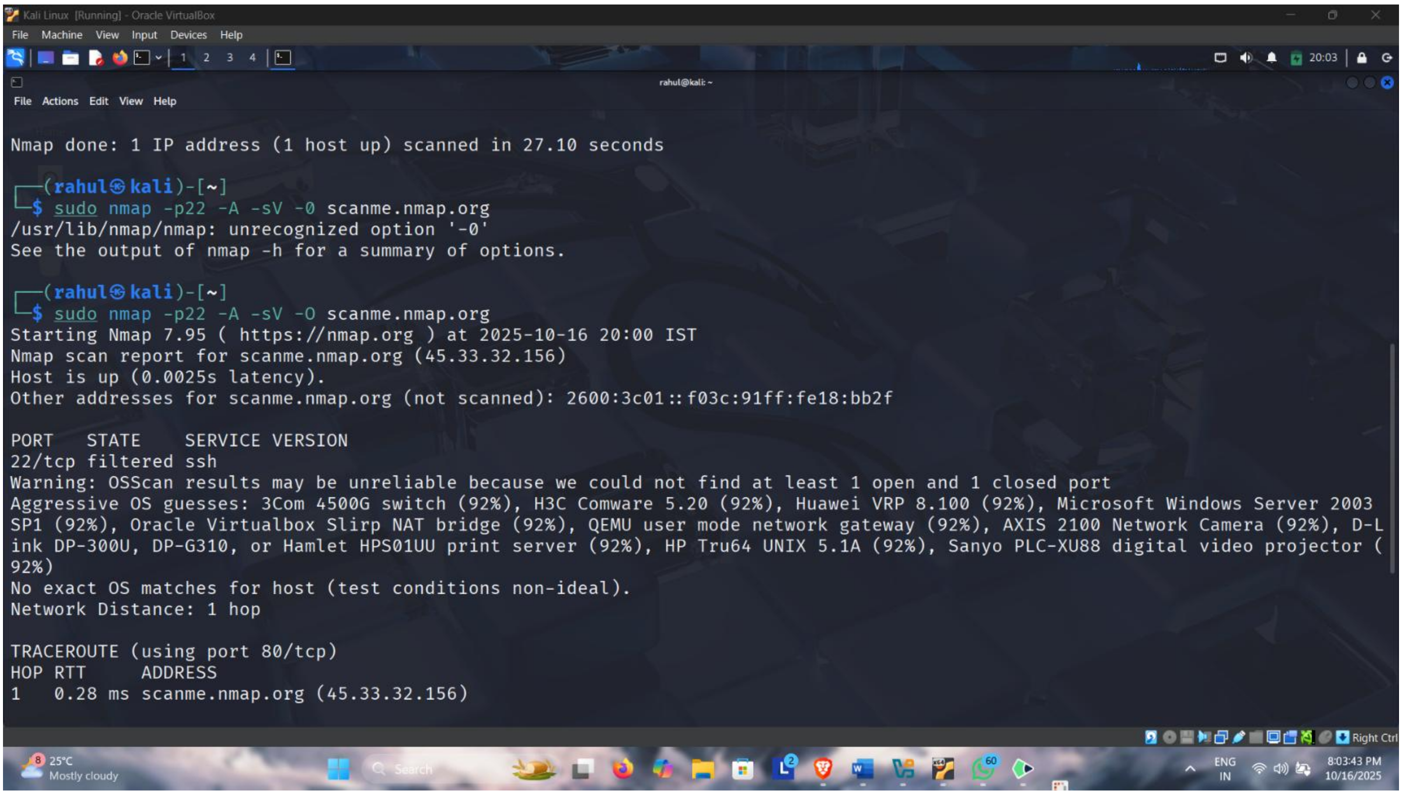

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
20:03
Right Ctrl
25°C
Mostly cloudy
Search
ENG
IN
8:03:18 PM
10/16/2025

```
┌──(rahul㉿kali)-[~]
└─$ nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 19:56 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds

┌──(rahul㉿kali)-[~]
└─$ sudo nmap scanme.nmap.org
[sudo] password for rahul:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 19:56 IST

zsh: suspended  sudo nmap scanme.nmap.org

┌──(rahul㉿kali)-[~]
└─$ sudo nmap scanme4.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 19:57 IST
Nmap scan report for scanme4.nmap.org (50.116.1.184)
Host is up (0.019s latency).
Other addresses for scanme4.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 50.116.1.184: ack.nmap.org
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite
```


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
20:03
Right Ctrl
25°C
Mostly cloudy
Search
ENG
IN
8:03:43 PM
10/16/2025

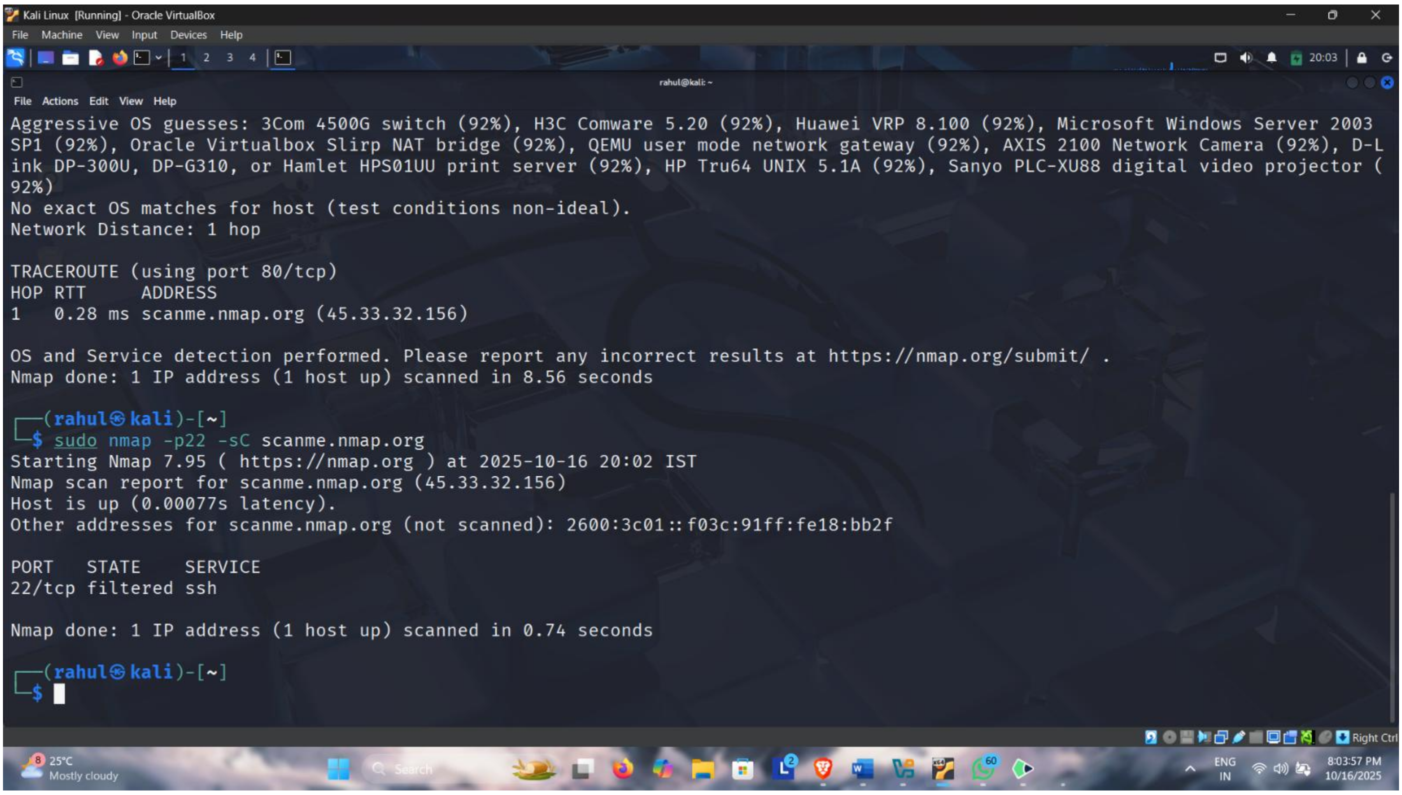
```
Nmap done: 1 IP address (1 host up) scanned in 27.10 seconds

┌──(rahul㉿kali)-[~]
└─$ sudo nmap -p22 -A -sV -0 scanme.nmap.org
/usr/lib/nmap/nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(rahul㉿kali)-[~]
└─$ sudo nmap -p22 -A -sV -O scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 20:00 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.0025s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003
SP1 (92%), Oracle Virtualbox Slirp NAT bridge (92%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-L
ink DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (
92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.28 ms scanme.nmap.org (45.33.32.156)
```



Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
rahul@kali: ~
File Actions Edit View Help
20:03
Right Ctrl
25°C
Mostly cloudy
ENG
IN
8:03:57 PM
10/16/2025

```
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003
SP1 (92%), Oracle Virtualbox Slirp NAT bridge (92%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-L
ink DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (
92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.28 ms scanme.nmap.org (45.33.32.156)

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 8.56 seconds

┌──(rahul㉿kali)-[~]
└─$ sudo nmap -p22 -sC scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-16 20:02 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.00077s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT   STATE    SERVICE
22/tcp filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds

┌──(rahul㉿kali)-[~]
└─$ 
```