Nmap Lab Assignment Report

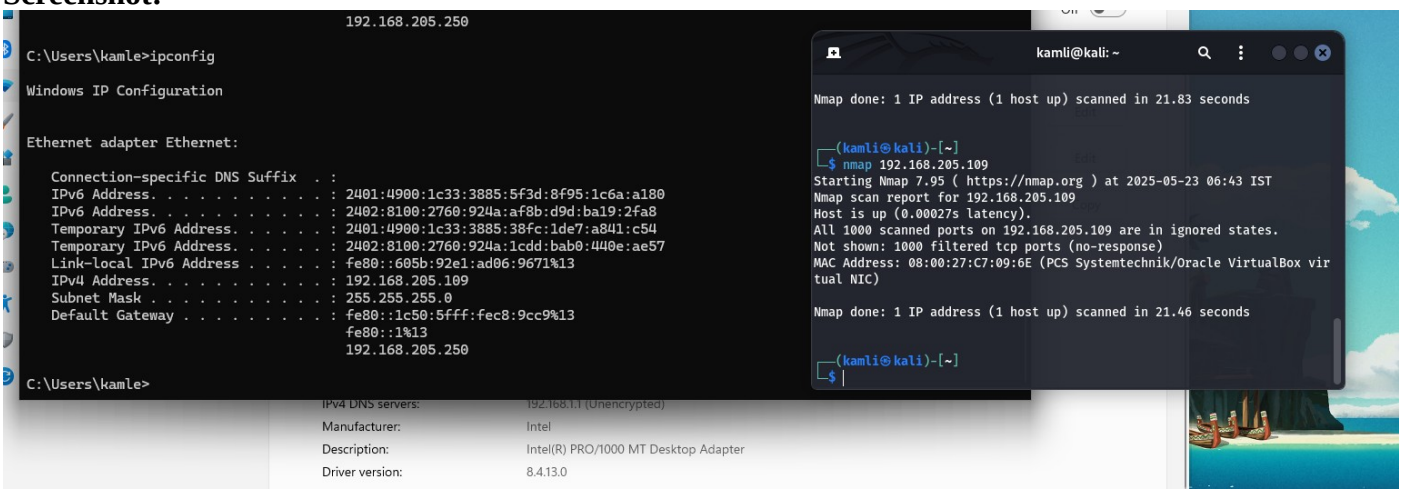
Introduction

This report documents the results of the Network Scanning using Nmap lab, as outlined in the "Network Scanning using Nmap" lab manual. The objective is to use Nmap to perform various network scanning tasks, including host discovery, port scanning, service detection, vulnerability scanning, and DNS enumeration. Below are the tasks performed, the commands used, their purpose, and placeholders for screenshots.

Lab Tasks and Results

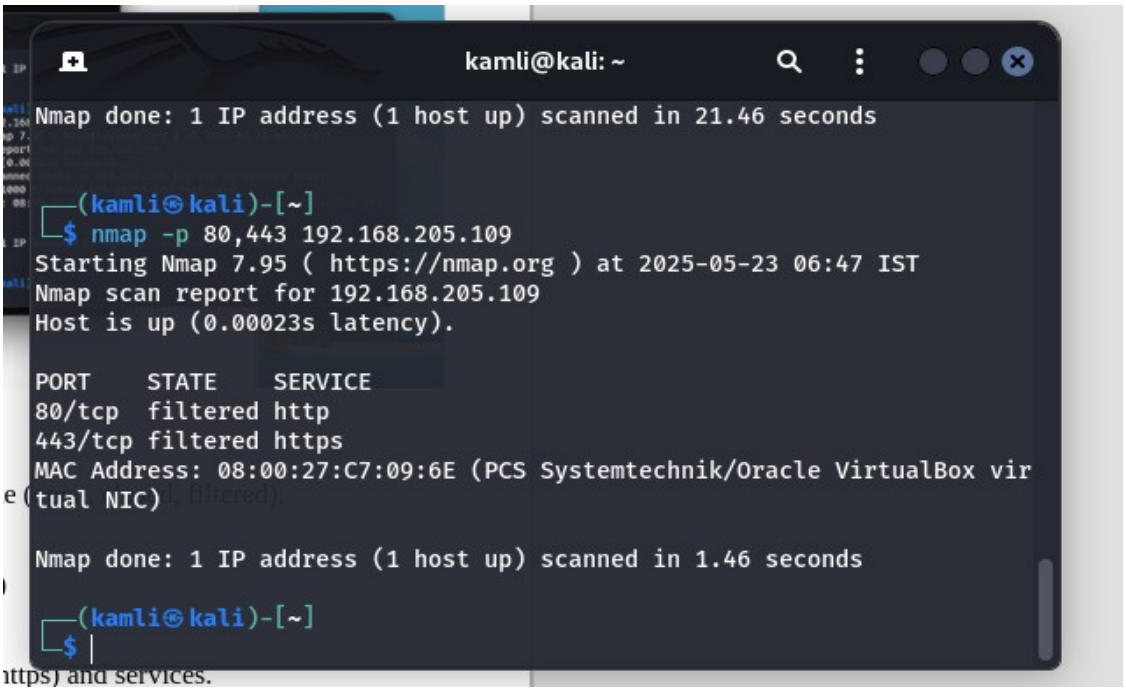
1. Basic Nmap Scan

Purpose: Perform a basic scan on a single IP or hostname to identify live hosts and open ports.
Command: nmap 192.168.205.109
Expected Output: List of open ports, services running, and host status (up/down).
Screenshot:



2. Port Scanning

Purpose: Scan specific ports or a range of ports to determine their state (open, closed, filtered).
Commands: nmap -p 80,443 192.168.45.130 Scan specific ports (HTTP, HTTPS)
nmap -p 1-65535 localhost Scan all ports
Expected Output: Port states (e.g., 80/tcp closed http, 443/tcp closed https) and services.
Screenshot:



3. Scanning Multiple IPs or IP Ranges

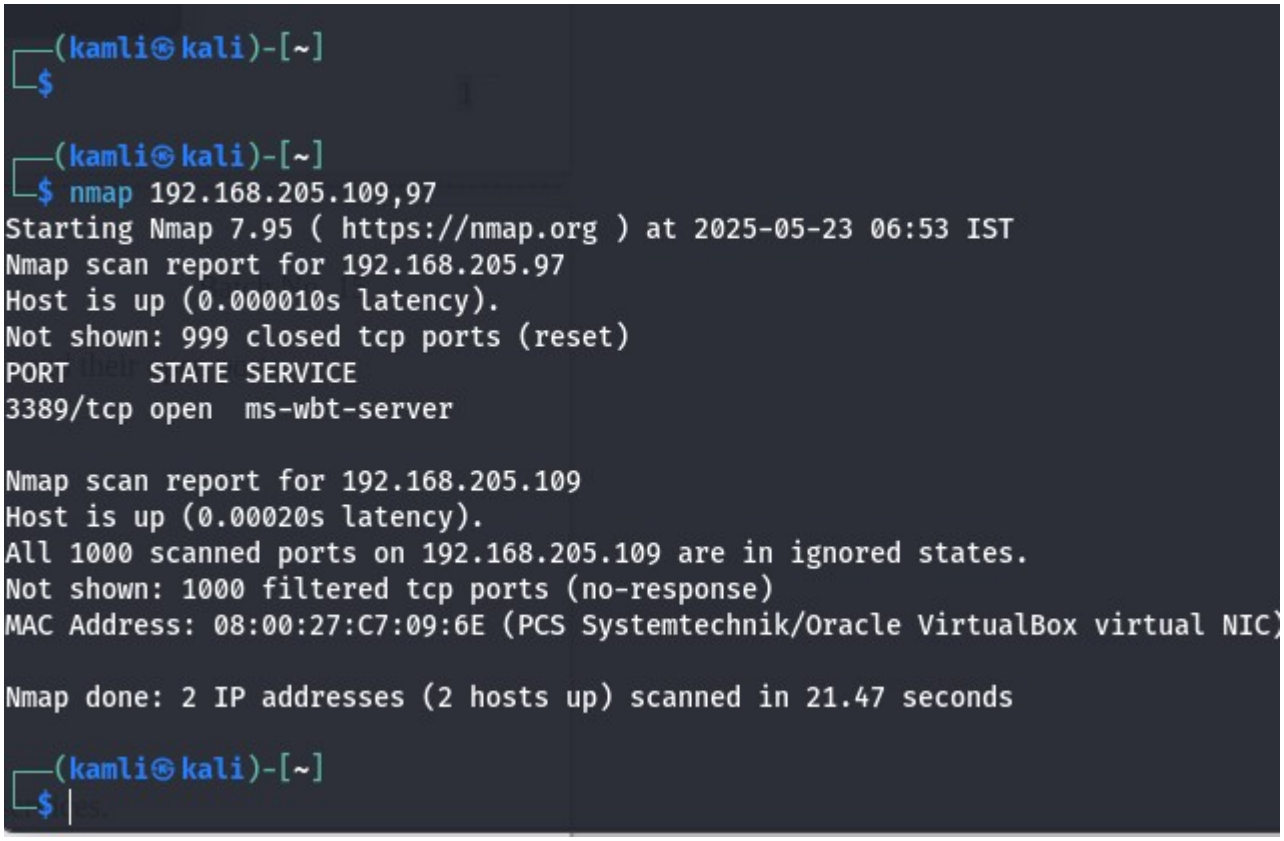
Purpose: Scan multiple IP addresses or an IP range to discover live hosts and their open ports.

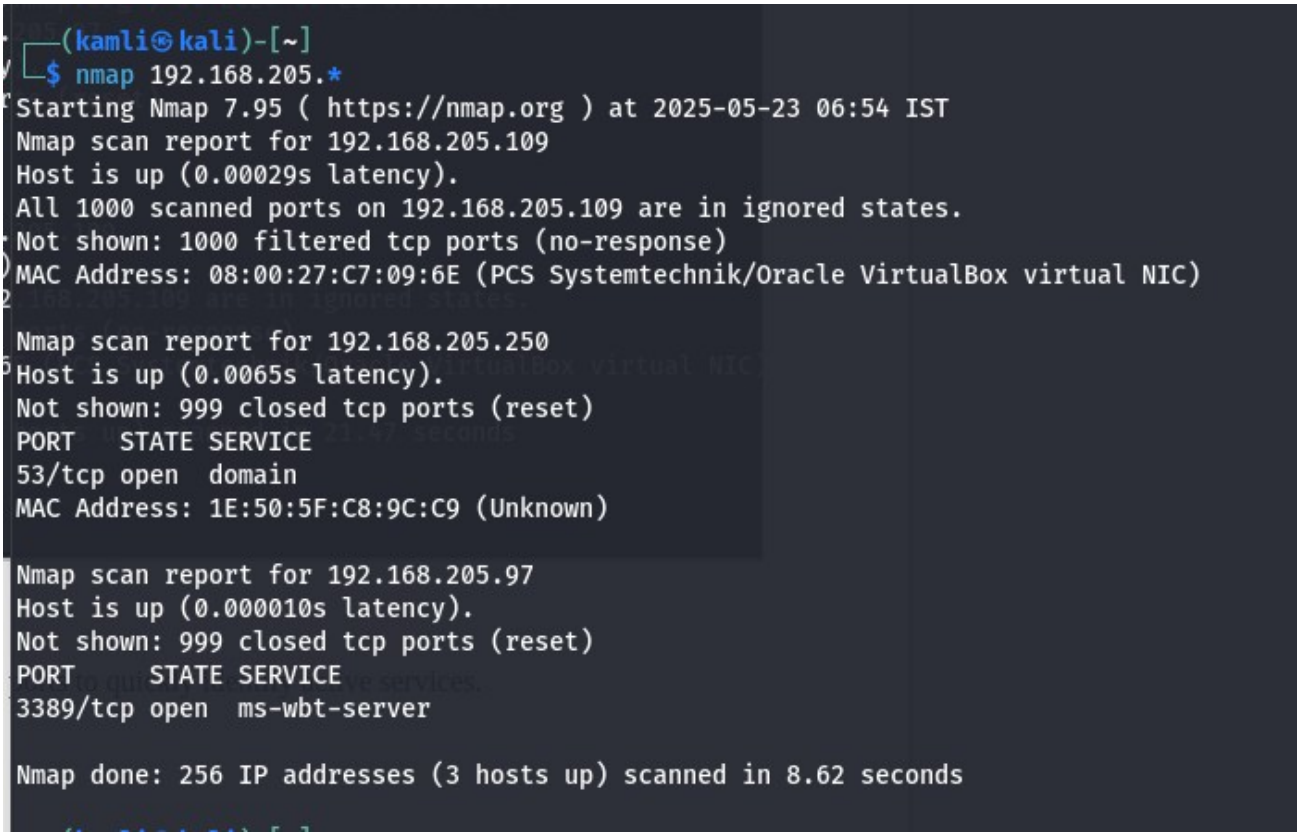
Commands:

nmap 192.168.45.130,138 Multiple IPs
nmap 192.168.45.0/24 CIDR range
nmap 192.168.45.* Wildcard range
nmap 192.168.45.* --exclude 192.168.45.138 Exclude specific IP

Expected Output: List of live hosts, their open ports, and services.

Screenshot:





4. Scanning Top Ports
Purpose: Scan the most commonly used ports to quickly identify active services.
Command: nmap --top-ports 20 192.168.45.130
Expected Output: Status of the top 20 ports (e.g., 80/tcp open http).
Screenshot:

```
┌──(kamli㉿kali)-[~]
└─$ nmap --top-ports 20 192.168.205.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 06:57 IST
Nmap scan report for 192.168.205.109
Host is up (0.00023s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

5. Saving Scan Results to a File
Purpose: Save scan results to a text file for documentation.
Command: nmap -oN output.txt 192.168.205.109
Expected Output: A text file (`output.txt`) containing scan results.
Screenshot:

```
┌──(kamli㉿kali)-[~]
└─$ nmap -oN output.txt 192.168.205.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 06:59 IST
Nmap scan report for 192.168.205.109
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.205.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.67 seconds

┌──(kamli㉿kali)-[~]
└─$ cat output.txt
# Nmap 7.95 scan initiated Fri May 23 06:59:41 2025 as: /usr/lib/nmap/nmap --privileged -oN output.txt 19
2.168.205.109
Nmap scan report for 192.168.205.109
Host is up (0.00031s latency).
All 1000 scanned ports on 192.168.205.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

# Nmap done at Fri May 23 07:00:03 2025 -- 1 IP address (1 host up) scanned in 21.67 seconds

┌──(kamli㉿kali)-[~]
└─$
```

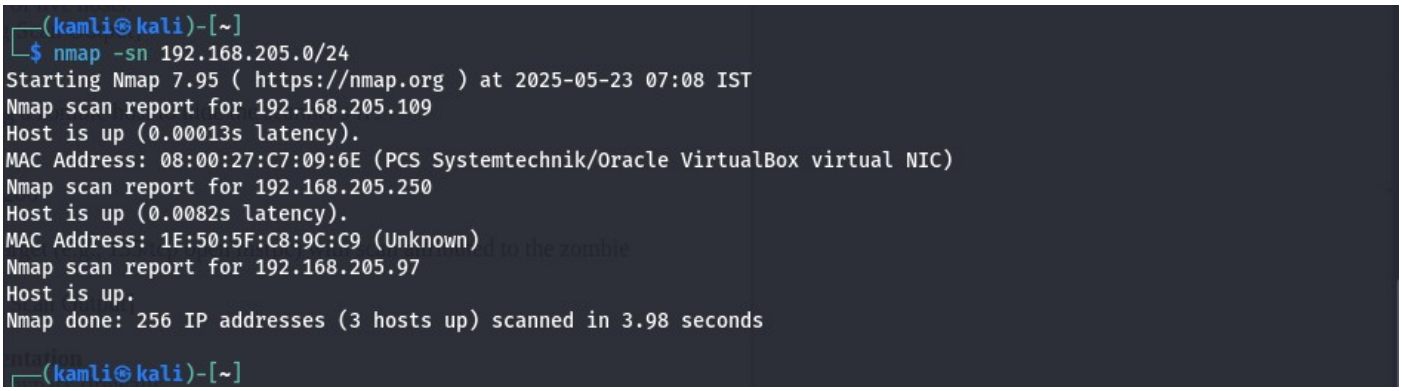
6. OS and Service Detection
Purpose: Identify the operating system and service versions running on the target.
Command: nmap -A -T4 192.168.205.109,97
Expected Output: OS details (e.g., Linux), service versions (e.g., Apache 2.4.7), and open ports.
Screenshot:

```
┌──(kamli㉿kali)-[~]
└─$ nmap -A -T4 192.168.205.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:01 IST
Nmap scan report for 192.168.205.109
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.205.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms 192.168.205.109

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 29.23 seconds

┌──(kamli㉿kali)-[~]
└─$ nmap -A -T4 192.168.205.97
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:02 IST
Nmap scan report for 192.168.205.97
Host is up (0.000057s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server GNOME remote desktop
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
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 7.86 seconds

┌──(kamli㉿kali)-[~]
```

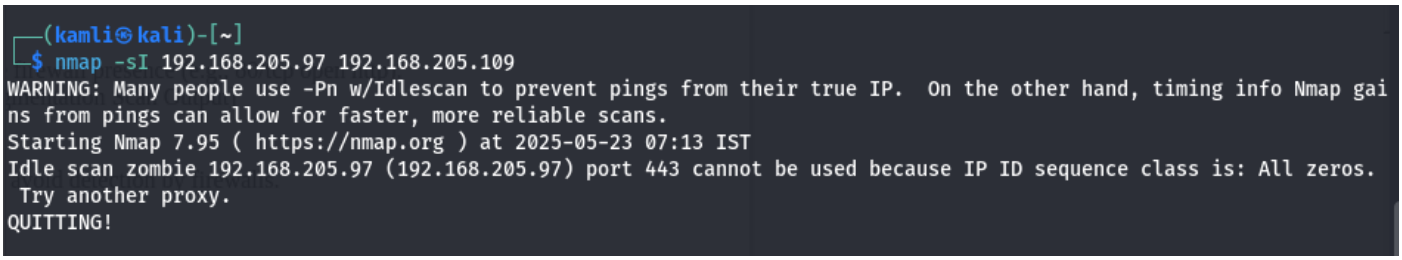
7. TCP and UDP Scanning
Purpose: Perform scans using TCP or UDP protocols to identify open ports.
Commands:
nmap -sT 1192.168.205.109 TCP scan
nmap -sU 1192.168.205.109 UDP scan
Expected Output: Open TCP/UDP ports (e.g., 53/tcp open domain, 53/udp open domain).
Screenshot:

```
┌──(kamli㉿kali)-[~]
└─$ nmap -sT 192.168.205.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:11 IST
Nmap scan report for 192.168.205.109
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.205.109 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.15 seconds

┌──(kamli㉿kali)-[~]
└─$ nmap -sU 192.168.205.109
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-23 07:11 IST
Nmap scan report for 192.168.205.109
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.205.109 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 08:00:27:C7:09:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.35 seconds
```

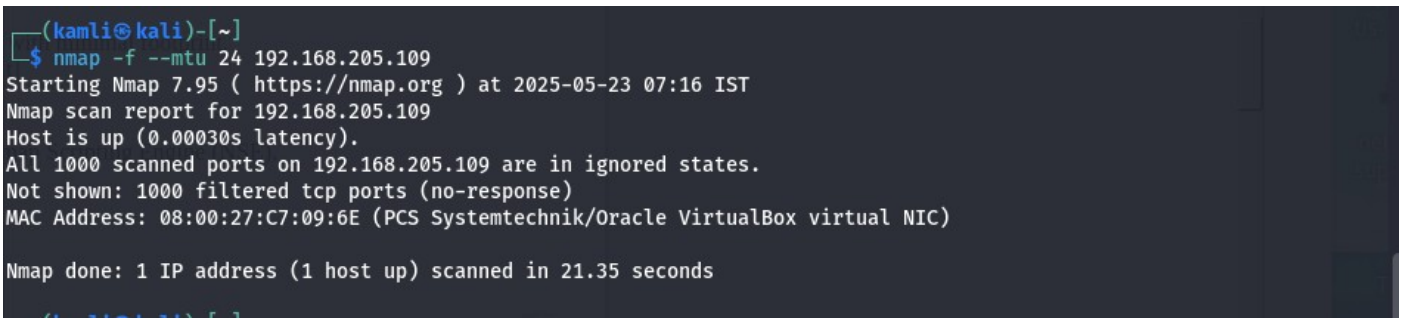
8. Live Hosts Discovery
Purpose: Identify live hosts in the network using a ping scan.
Command: nmap -sn 192.168.205.0/24
Expected Output: List of IP addresses of live hosts.
Screenshot:



9. Idle (Zombie) Scanning
Purpose: Perform a stealthy scan using a zombie host to hide the scanner's IP.
Command: nmap -sI 192.168.205.97 172.31.101.206
Expected Output: Open ports on the target (e.g., 135/tcp open msrpc) with scan attributed to the zombie host.
Screenshot:



10. Firewall Bypassing with Fragmentation
Purpose: Use packet fragmentation to bypass firewalls.
Command: nmap -f --mtu 24 192.168.205.109
Expected Output: Scan results despite firewall presence (e.g., 80/tcp open http).
Screenshot:



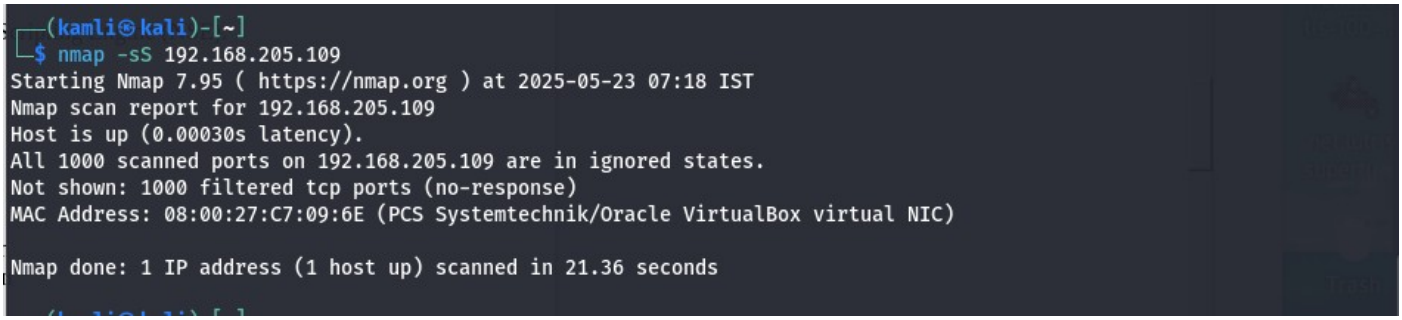
11. Stealth Scan

Purpose: Perform a TCP SYN scan to avoid detection by firewalls.

Command: nmap -sS 192.168.205.109

Expected Output: Open ports (e.g., 80/tcp open http) with minimal footprint.

Screenshot:



13. DNS Enumeration

Purpose: Discover DNS-related services and enumerate subdomains.

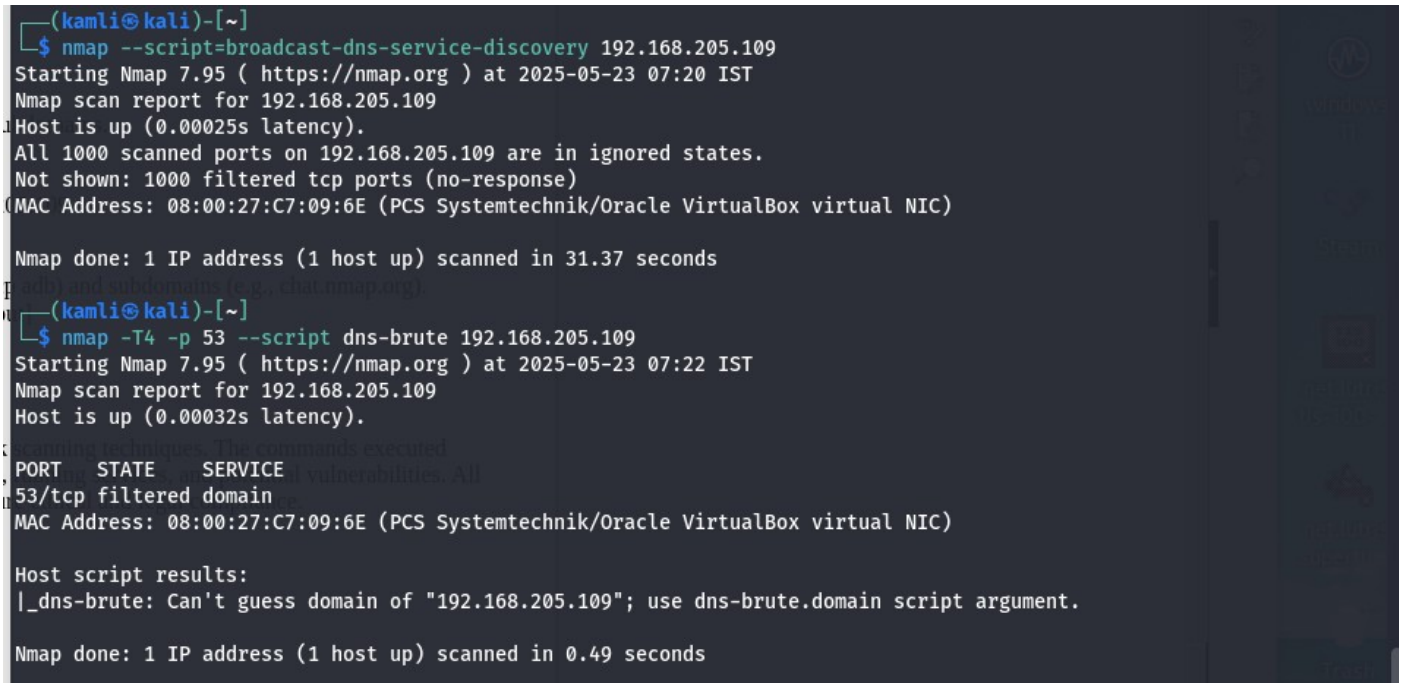
Commands:

nmap --script=broadcast-dns-service-discovery 192.168.205.109

nmap -T4 -p 53 --script dns-brute 192.168.205.109

Expected Output: Discovered DNS services (e.g., 5555/tcp adb) and subdomains (e.g., chat.nmap.org).

Screenshot:



Conclusion

The Nmap lab successfully demonstrated various network scanning techniques. The commands executed provided insights into network configurations, open ports, running services, and potential vulnerabilities. All scans were conducted in a controlled environment to ensure ethical and legal compliance.