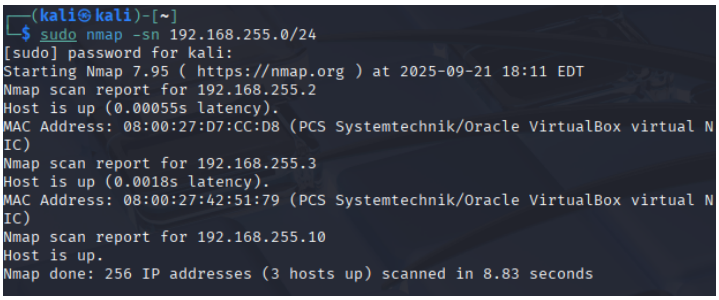
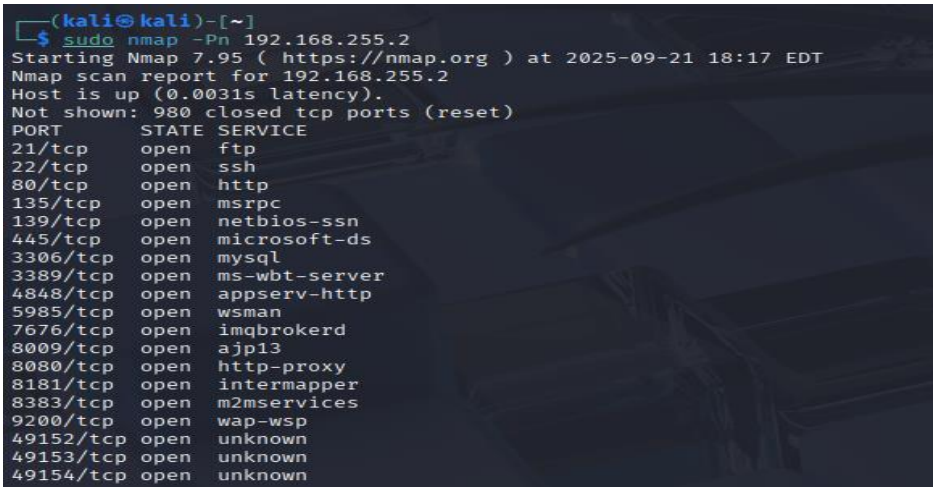
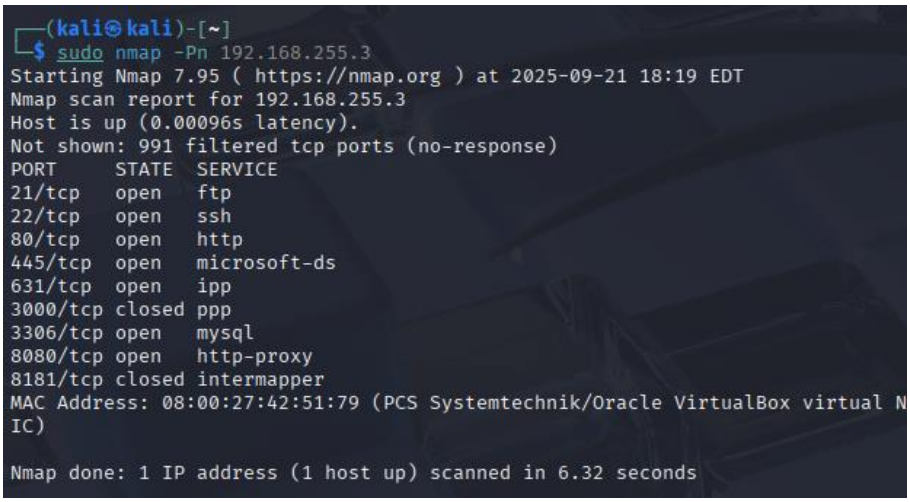
LAB 3 SCANNING AND ENUMERATION

1. -sn switch: Ping (host discovery) only and no port scan. It tells Nmap to skip the default port scan and only check which hosts are alive on the network.



2. The –Pn switch: Nmap will skip ping/host discovery and go straight to the port scan.





3. The –sS switch: Sends a TCP SYN to a port. If target replies SYN/ACK → port is open (Nmap usually sends an RST to avoid completing the handshake). If target replies RST → port is closed.

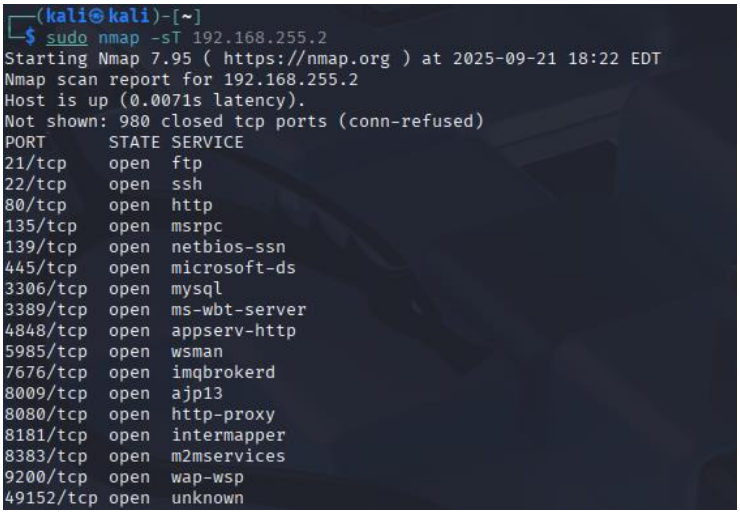
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.255.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 18:20 EDT
Nmap scan report for 192.168.255.2
Host is up (0.00064s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual
```

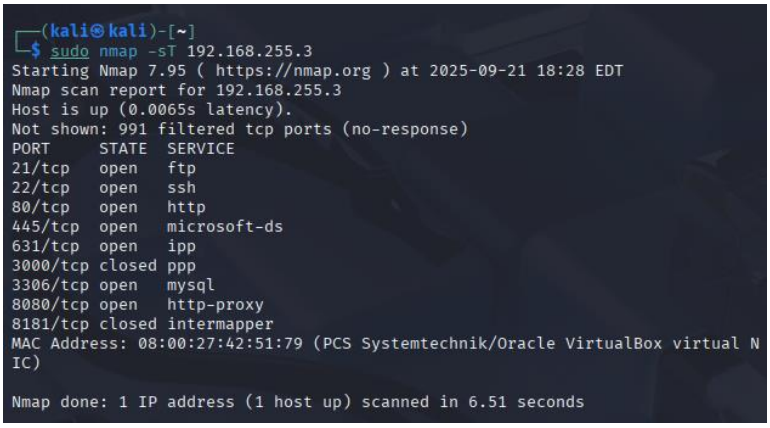
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.255.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 18:20 EDT
Nmap scan report for 192.168.255.3
Host is up (0.0011s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 5.09 seconds
```

4. -sT and –sU: Looks/scans for all TCP or UDP protocol-based ports respectively.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.255.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 18:33 EDT
Nmap scan report for 192.168.255.3
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.255.3 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 25.58 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.255.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 18:34 EDT
```





5. -O switch asks Nmap to fingerprint on fingerprint's OS system

```
└─$ sudo nmap -O 192.168.255.2
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 00:13 EDT
Nmap scan report for 192.168.255.2
Host is up (0.0017s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 08:00:27:D7:CC:D8 (PCS Systemtechnik/Oracle VirtualBox virtual N
```

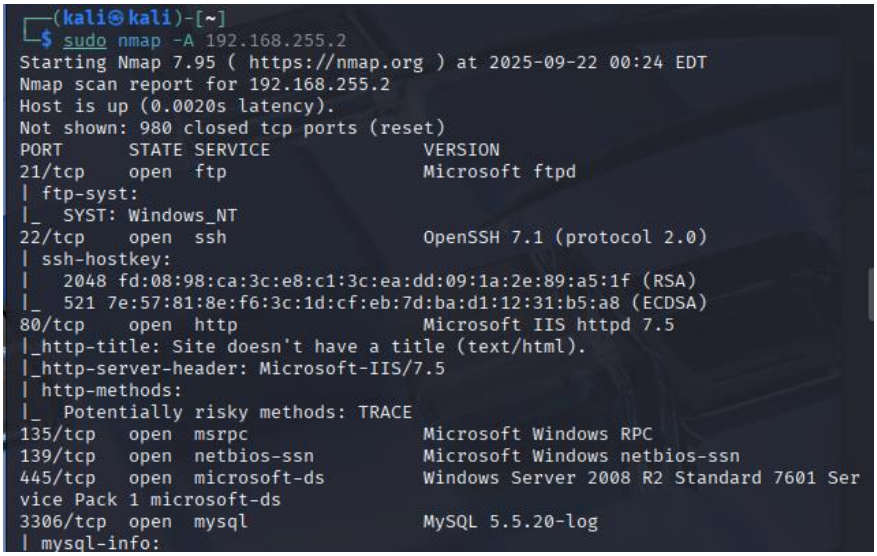
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.255.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 00:13 EDT
Nmap scan report for 192.168.255.3
Host is up (0.0025s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux
3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.1
6 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux
4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), A
ndroid 8 - 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
```

6. -sV switch- asks nmap to probe the open ports to see the service running

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.255.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 00:18 EDT
Nmap scan report for 192.168.255.2
Host is up (0.0019s latency).
Not shown: 980 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
21/tcp    open  ftp                Microsoft ftpd
22/tcp    open  ssh                OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http               Microsoft IIS httpd 7.5
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 201
microsoft-ds
3306/tcp  open  mysql              MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
4848/tcp  open  ssl/http           Oracle Glassfish Application Server
5985/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp  open  http               Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http               Apache httpd
9200/tcp  open  http               Elasticsearch REST API 1.1.1 (name: Mis
er Doll; Lucene 4.7)
49152/tcp open  msrpc              Microsoft Windows RPC
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.255.3
Starting Nmap 7.95 ( https://nm p.org ) at 2025-09-22 00:20 EDT
Nmap scan report for 192.168.25 .3
Host is up (0.0036s latency).
Not shown: 991 filtered tcp por s (no-response)
PORT     STATE  SERVICE     VER ION
21/tcp   open   ftp         Pro TPD 1.3.5
22/tcp   open   ssh         Ope SSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
 protocol 2.0)
80/tcp   open   http        Apa he httpd 2.4.7
445/tcp  open   netbios-ssn Sam a smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUP 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MyS L (unauthorized)
8080/tcp open   http        Jet y 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:42:51:79  PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: 127.0.0.1,  METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Pl ase report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host  up) scanned in 27.27 seconds
```

7. -A this is an aggressive scan which is the combination of all previous scans and is much for noisy and obvious and shouldn't be used if not authorized.



8. -p1-1024 (Skip ping discovery, then probe TCP ports 1 → 1024)