Port Scanning and Network Reconnaissance

Objective:

Perform port scanning using Nmap to identify open ports, active services, and system details on a target host.

What port scanning is

Port scanning is a technique used to identify open ports and the services running on a target host. It is commonly employed by security professionals to assess network defenses and by attackers to discover potential vulnerabilities. Unsecured or unnecessary open ports represent significant security risks if left exposed.

Tool used

The primary tool used in this lab was Nmap, a powerful and widely used open-source utility for network scanning and reconnaissance. It supports multiple scanning techniques, host discovery, and OS fingerprinting.

Important services & default ports (examples)

Below are common network services and their default ports. These are essential to recognize during both defensive audits and offensive testing.

- FTP → 21
- SSH → 22
- Telnet (insecure) → 23
- SMTP → 25
- DNS → 53
- HTTP → 80 (insecure/plaintext)
- HTTPS → 443 (secure)
- MySQL → 3306 *(note: occasionally mistyped as 3006)*

Types of scans

- TCP and UDP scans are the most common, used to detect active services.
- Stealth scans aim to minimize detection by intrusion detection/prevention systems (IDS/IPS).
- Ping sweeps (host discovery) are used to identify active hosts within a subnet before deeper scanning.

Key nmap commands shown

- Scan 1,000 most common TCP ports on a host or subnet:

nmap <IP-or-range>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:51 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000040s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

- Scan **all ports** (0–65535):

nmap -p- <IP-or-range>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p- localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:51 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
3306/tcp  open  mysql
37817/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

- Scan a **specific port**:

nmap -p 80 <target-IP>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 80 localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:52 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000084s latency).
Other addresses for localhost (not scanned): ::1

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

- Scan a **range** of ports:

nmap -p 80-100 <target-IP>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 80-100 localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:53 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Other addresses for localhost (not scanned): ::1

PORT    STATE  SERVICE
80/tcp  closed http
81/tcp  closed hosts2-ns
82/tcp  closed xfer
83/tcp  closed mit-ml-dev
84/tcp  closed ctf
85/tcp  closed mit-ml-dev
86/tcp  closed mfcobol
87/tcp  closed priv-term-l
88/tcp  closed kerberos-sec
89/tcp  closed su-mit-tg
90/tcp  closed dnsix
91/tcp  closed mit-dov
92/tcp  closed npp
93/tcp  closed dcp
94/tcp  closed objcall
95/tcp  closed supdup
96/tcp  closed dixie
97/tcp  closed swift-rvf
98/tcp  closed linuxconf
99/tcp  closed metagram
100/tcp closed newacct

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

- **OS fingerprinting** (requires elevated privileges):

sudo nmap -O <target-IP>

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -O localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:54 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000087s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql
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 detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

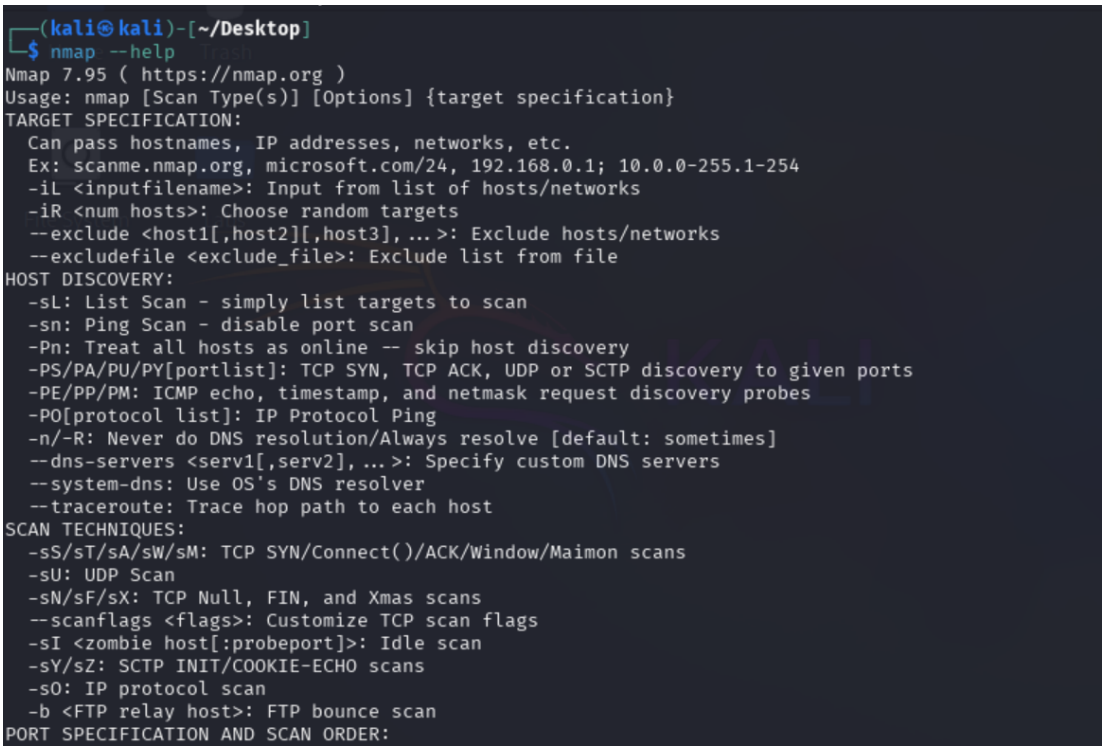
- **Ping sweep / host discovery**:

sudo nmap -sP 10.0.2.0/24

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sP 10.0.2.15/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 17:56 EDT
Nmap scan report for 10.0.2.2
Host is up (0.00039s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00055s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.03 seconds
```

- Get help:

nmap –help



Typical demo results (examples from the lab)

During the lab, scanning localhost revealed three open ports: **SSH (22)**, **HTTP (80)**, and **MySQL (3306)**.
A full-port scan confirmed that the remaining ports were closed.
OS fingerprinting identified the target as running **Linux kernel 2.6.x**.
A ping sweep across the **10.0.2.0/24** subnet identified active hosts (e.g., 10.0.2.2, 10.0.2.3, and 10.0.2.15).

Security implications / why it matters

Understanding open ports and the services running on them enables defenders to close unnecessary ones, apply patches, and reduce the attack surface.
Conversely, attackers use the same information to identify vulnerabilities and craft targeted exploits.

Techniques such as stealth scanning and targeted port probing are often used to minimize detection and bypass security monitoring.