Lab #11: Nmap

Each lab exercise will introduce students to fundamental **Nmap** commands, teaching them how to scan networks, detect open ports, identify services, and gather basic host information. Students must **take a screenshot** of their results and **submit it on Blackboard**.

🎯 Objective

Each lab exercise is designed to introduce students to the fundamentals of Nmap, helping them develop essential network scanning skills.

Step-by-Step Instructions / Summary

By completing this lab, students will:

1. **Understand Network Scanning Basics –** Learn how **Nmap** is used for discovering live hosts, scanning ports, and identifying services.
2. **Perform Host Discovery –** Identify active devices on a network using **ping scans.**
3. **Scan for Open Ports –** Understand how to detect open ports and determine potential entry points.
4. **Perform Targeted Port Scanning –** Learn how to scan specific ports instead of scanning an entire system.
5. **Detect Running Services and Versions –** Use Nmap to determine what services are running on open ports.
6. **Identify Operating Systems –** Use **OS detection techniques** to analyze remote systems.
7. **Execute Stealthy Scans – Perform SYN (stealth)** scans to bypass firewalls and detection systems.
8. **Conduct Aggressive Scans – Utilize Nmap's aggressive scanning mode** to gather detailed host information.
9. **Scan Multiple Targets Simultaneously –** Learn how to scan **multiple IP addresses** efficiently.
10. **Save and Analyze Scan Results –** Store scan data for documentation, reporting, and future analysis.

Steps and screenshots for this lab:

Lab 1: Basic Host Discovery (Ping Scan)

Checking the ip address ip a

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6e:2f:58 brd ff:ff:ff:ff:ff:ff
    inet 172.16.123.129/24 brd 172.16.123.255 scope global dynamic noprefixroute eth0
       valid_lft 947sec preferred_lft 947sec
    inet6 fe80::20c:29ff:fe6e:2f58/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Objective: Learn how to identify live hosts on a network.
nmap -sn 172.16.123.129/24

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 172.16.123.129/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:05 EDT
Nmap scan report for AlexPC447 (172.16.123.1)
Host is up (0.00034s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.123.2
Host is up (0.00031s latency).
MAC Address: 00:50:56:E1:46:7A (VMware)
Nmap scan report for 172.16.123.254
Host is up (0.00020s latency).
MAC Address: 00:50:56:FF:84:F4 (VMware)
Nmap scan report for 172.16.123.129
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.07 seconds
```

Lab 2: Simple Port Scanning -

Objective: Scan a target to find open ports.
nmap 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:04 EDT
Nmap scan report for 172.16.123.129
Host is up (0.0000090s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Lab 3: Scanning Specific Ports

Objective: Scan for specific ports instead of scanning all.
Task: Scan for **ports 22 (SSH), 80 (HTTP), and 443 (HTTPS)** and submit a screenshot.

nmap -p 22,80,443 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22,80,443 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:03 EDT
Nmap scan report for 172.16.123.129
Host is up (0.000047s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Lab 4: Full Port Scan (All 65,535 Ports)

Objective: Perform an exhaustive port scan.
nmap -p- 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:02 EDT
Nmap scan report for 172.16.123.129
Host is up (0.0000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.12 seconds
```

Lab 5: Service and Version Detection

Objective: Identify what services are running on open ports.
nmap -sV 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:01 EDT
Nmap scan report for 172.16.123.129
Host is up (0.000019s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.20 seconds
```

Lab 6: OS Detection

Objective: Determine the operating system of a target.
nmap -O 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:05 EDT
Nmap scan report for 172.16.123.129
Host is up (0.0038s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
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 1.79 seconds
```

Lab 7: Stealth Scan (SYN Scan)

Objective: Use a stealthy scan to bypass firewalls.
nmap -sS 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:07 EDT
Nmap scan report for 172.16.123.129
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Lab 8: Aggressive Scan

Objective: Perform an all-in-one aggressive scan.
nmap -A 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:08 EDT
Nmap scan report for 172.16.123.129
Host is up (0.00010s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.63 (Debian)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 9.95 seconds
```

Lab 9: Scanning Multiple Targets

Objective: Scan multiple IP addresses at once.
nmap -A 172.16.123.129 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 172.16.123.129 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:10 EDT
Nmap scan report for 172.16.123.129
Host is up (0.000072s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.63 (Debian)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for 172.16.123.129
Host is up (0.000086s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 5 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.63 ((Debian))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.63 (Debian)
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 16.03 seconds
```

Lab 10: Saving Scan Results

Objective: Save scan results for later analysis.
nmap -oN myscan.txt 172.16.123.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -oN myscan.txt 172.16.123.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 19:12 EDT
Nmap scan report for 172.16.123.129
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

After the text file is made:

```
┌──(kali㉿kali)-[~]
└─$ cat myscan.txt
# Nmap 7.95 scan initiated Tue Jul 29 19:12:53 2025 as: /usr/lib/nmap/nmap --privileged -oN myscan.txt 172.16.123.129
Nmap scan report for 172.16.123.129
Host is up (0.0000070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

# Nmap done at Tue Jul 29 19:13:06 2025 -- 1 IP address (1 host up) scanned in 13.11 seconds
```

🧰 Tools & Skills Used

Primary Tool: Nmap (Network Mapper)
Operating System: Linux Environment (using the terminal/command line)
Core Skills:

- **Host Discovery:** Identifying live hosts on a network segment using ping scans (`-sn`).
- **Port Scanning:** Detecting open TCP/UDP ports using various techniques, including default scans, specific port scans (`-p`), and full port scans (`-p-`).
- **Service & Version Detection:** Enumerating the specific applications and their versions running on open ports (`-sV`).
- **OS Detection:** Fingerprinting the remote operating system using TCP/IP stack analysis (`-O`).
- **Stealth Scanning:** Performing SYN scans (`-sS`) to identify open ports without completing the full TCP three-way handshake, making the scan less detectable.
- **Aggressive Scanning:** Combining multiple advanced techniques (including OS detection, version detection, script scanning, and traceroute) into a single, comprehensive scan (`-A`).
- **Target Selection:** Scanning single hosts, multiple specified hosts, and entire network subnets (CIDR notation).
- **Output Management:** Saving scan results to a text file for documentation and analysis (`-oN`).
- **Basic Networking:** Using the `ip a` command to identify the local machine's IP address and network configuration.

🧠 Reflection & Takeaways

In this lab, I gained hands-on experience with Nmap, a powerful and essential tool for network reconnaissance. I initially ran into a small issue by targeting the wrong IP address. This was a valuable mistake because it forced me to use the ip a command to verify my own machine's network details and correctly identify the target's subnet. This experience underscored the importance of proper reconnaissance and target validation before launching any scan.