

LAB 1

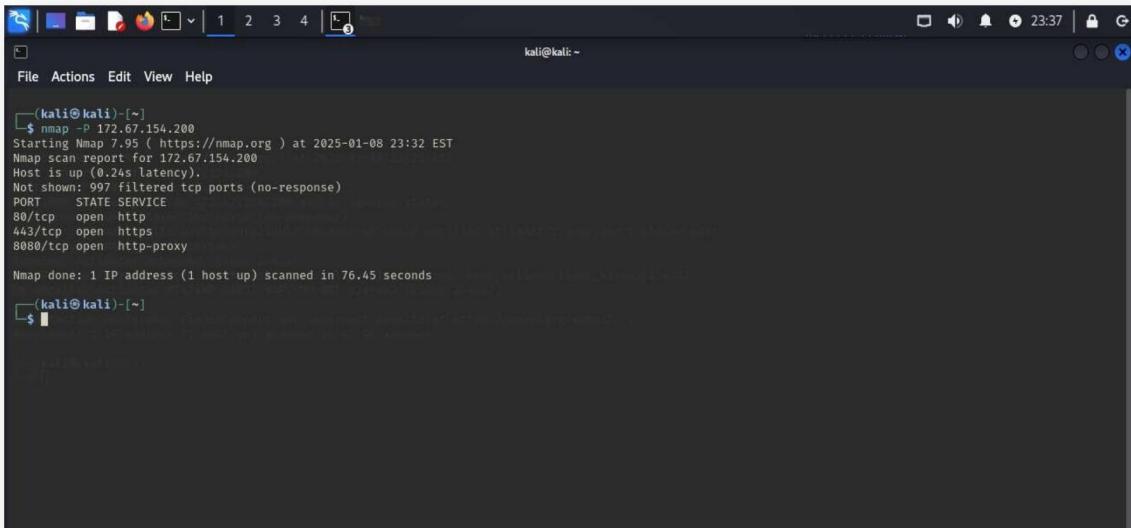
AIM: Network scanning and reconnaissance using nmap and identify open ports, operating system and potential vulnerabilities.

Objective:

- Identify open ports on target machine.
- Determine the operating system running on target machine.
- Detects potential vulnerabilities that may exist based on ports and service running.

Tools Require: Nmap

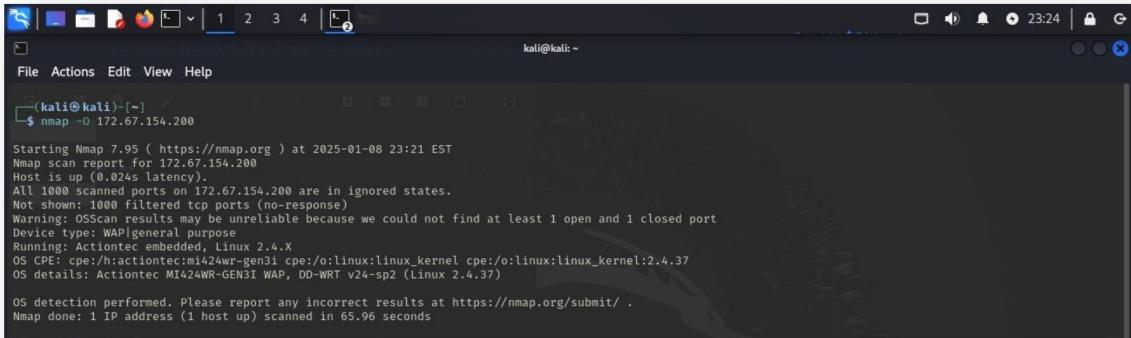
- Identify open ports on target machine



```
(kali㉿kali)-[~]
$ nmap -P 172.67.154.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 23:32 EST
Nmap scan report for 172.67.154.200
Host is up (0.24s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 76.45 seconds
(kali㉿kali)-[~]
```

- Determine the operating system running on target machine



```
(kali㉿kali)-[~]
$ nmap -O 172.67.154.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 23:21 EST
Nmap scan report for 172.67.154.200
Host is up (0.024s latency).
All 1000 scanned ports on 172.67.154.200 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose
Running: Actiontec embedded, Linux 2.4.x
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.96 seconds
(kali㉿kali)-[~]
```

- Detects potential vulnerabilities that may exist based on ports and service running

```

kali@kali: ~
$ nmap --script vuln 172.67.154.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-08 23:25 EST
Nmap scan report for 172.67.154.200
Host is up (0.076s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp    open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 167.05 seconds

```

Report:

Service	Port	Version	Vulnerability found
http	80	Not found	Not found
https	443	Not found	Not found
http-proxy	8080	Not found	Not found

Conclusion:

Nmap identifies open ports on the target machine, revealing active services. It detects the operating system in use. Nmap also checks for known vulnerabilities in the services running on those ports. This helps identify security risks and areas to improve.