Experiment–03

3.1 Aim:

Network Reconnaissance using Nmap: Learn basic network scanning techniques to identify live hosts, open ports, and running services on target virtual machines.

3.2 Course Outcome:

Apply network reconnaissance techniques using tools like Nmap to gather information about hosts, ports, and services in a target environment.

3.3 Lab Objective:

To understand and demonstrate the use of Nmap for discovering live hosts, scanning open ports, and identifying running services on a network.

3.4 Requirements:

- **Operating System:** Kali Linux / Ubuntu / Windows with Nmap installed
- **Tool:** Nmap
- **Target:** Local virtual network, Metasploitable VM, or any safe test environment

3.5 Theory:

Network reconnaissance is the initial phase in ethical hacking and penetration testing. It involves gathering information about systems on a network to identify potential vulnerabilities. **Nmap (Network Mapper)** is a powerful open-source tool used to discover hosts and services on a computer network.

Basic Nmap Techniques:

- **Host Discovery:**
  Identify live hosts using ICMP (`nmap -sn <target>`)
- **Port Scanning:**
  Discover open ports using TCP SYN scan (`nmap -sS <target>`)
- **Service Version Detection:**
  Identify services running on open ports (`nmap -sV <target>`)
- **OS Detection:**
  Determine the operating system of a target (`nmap -O <target>`)

Applications:

- Network inventory management
- Vulnerability assessment
- Penetration testing

- Security auditing

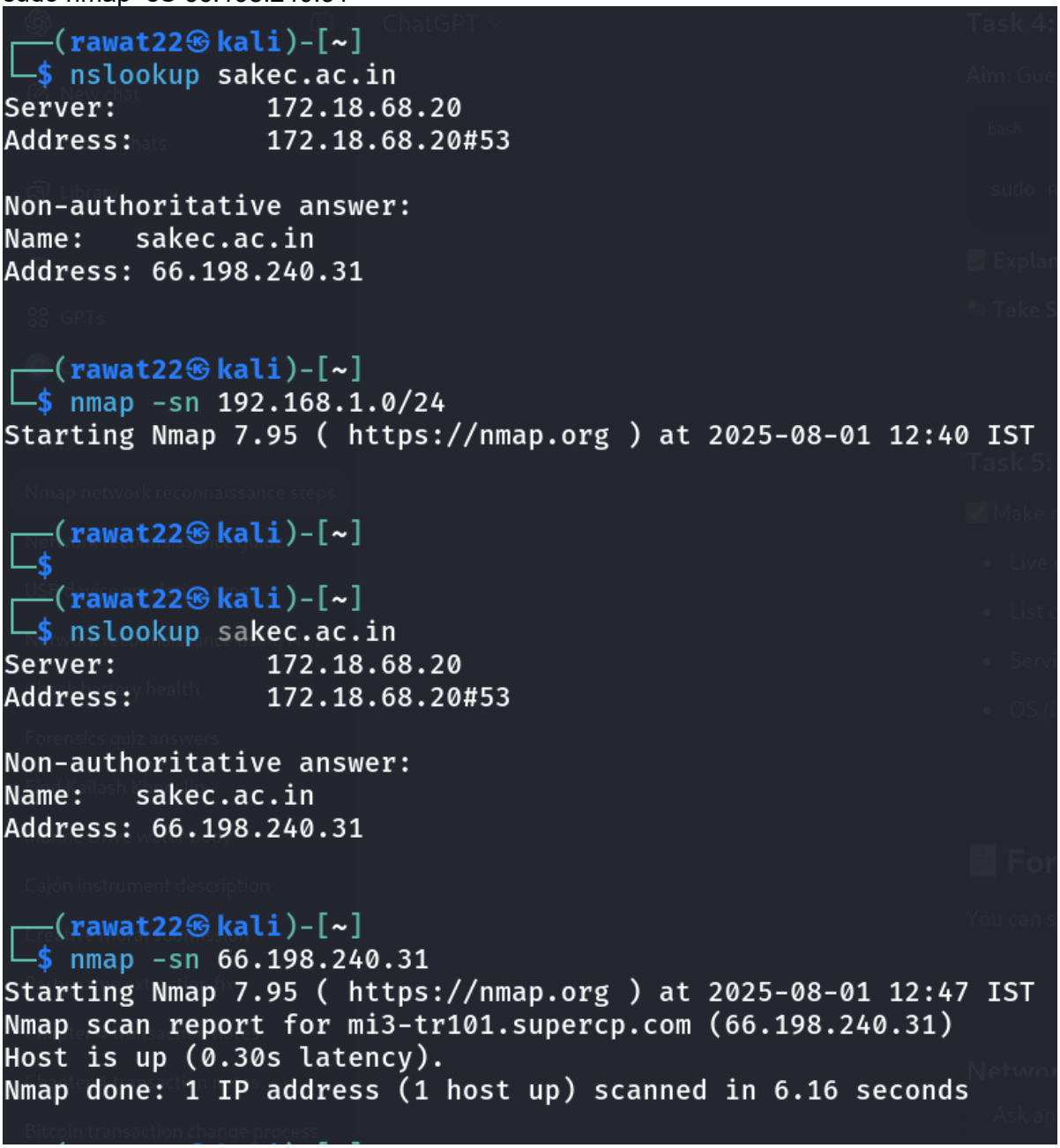
3.6 Tasks:

Task 1: Host Discovery
Command used:
nmap -sn 192.168.1.0/24

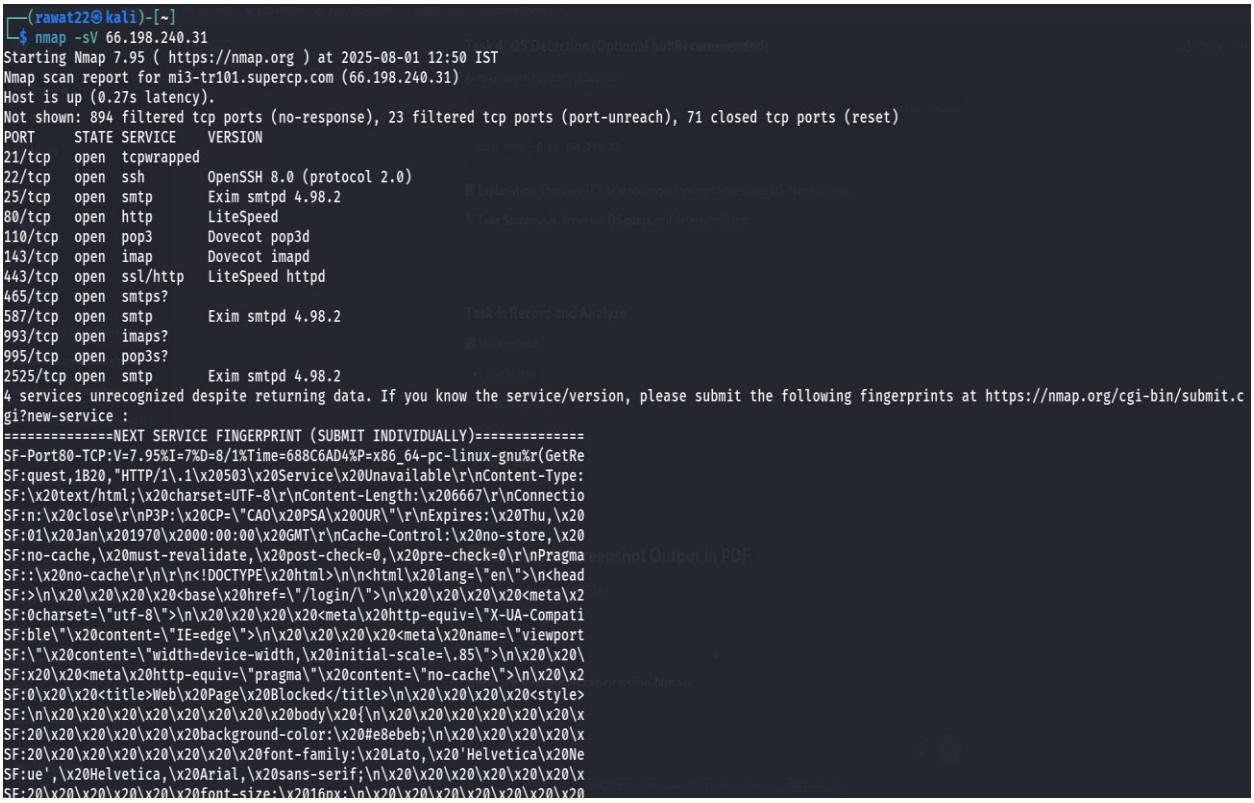
```
┌──(rawat22㉿kali)-[~]
└─$ sudo nmap -O 66.198.240.31
[sudo] password for rawat22:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 12:50 IST
Nmap scan report for mi3-tr101.supercp.com (66.198.240.31)
Host is up (0.28s latency).
Not shown: 901 filtered tcp ports (no-response), 16 filtered tcp ports (port-unreach), 71 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2525/tcp open  ms-v-worlds
Aggressive OS guesses: Android TV OS 11 (Linux 4.19) (89%), IPFire 2.25 firewall (Linux 4.14) (89%), IPFire 2.27 (Linux 5.15 - 6.1) (89%), Linux 2.6.32 (89%),
 Linux 2.6.32 or 3.10 (89%), Linux 2.6.39 (89%), Linux 3.10 - 3.12 (89%), Linux 3.4 (89%), Linux 3.5 (89%), Linux 4.0 - 4.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.26 seconds
```

This shows host discovery on a local subnet using -sn flag.

Task 2: TCP SYN Scan
Command used:
sudo nmap -sS 66.198.240.31



Task 3: Service Version Detection
Command used:
nmap -sV 66.198.240.31



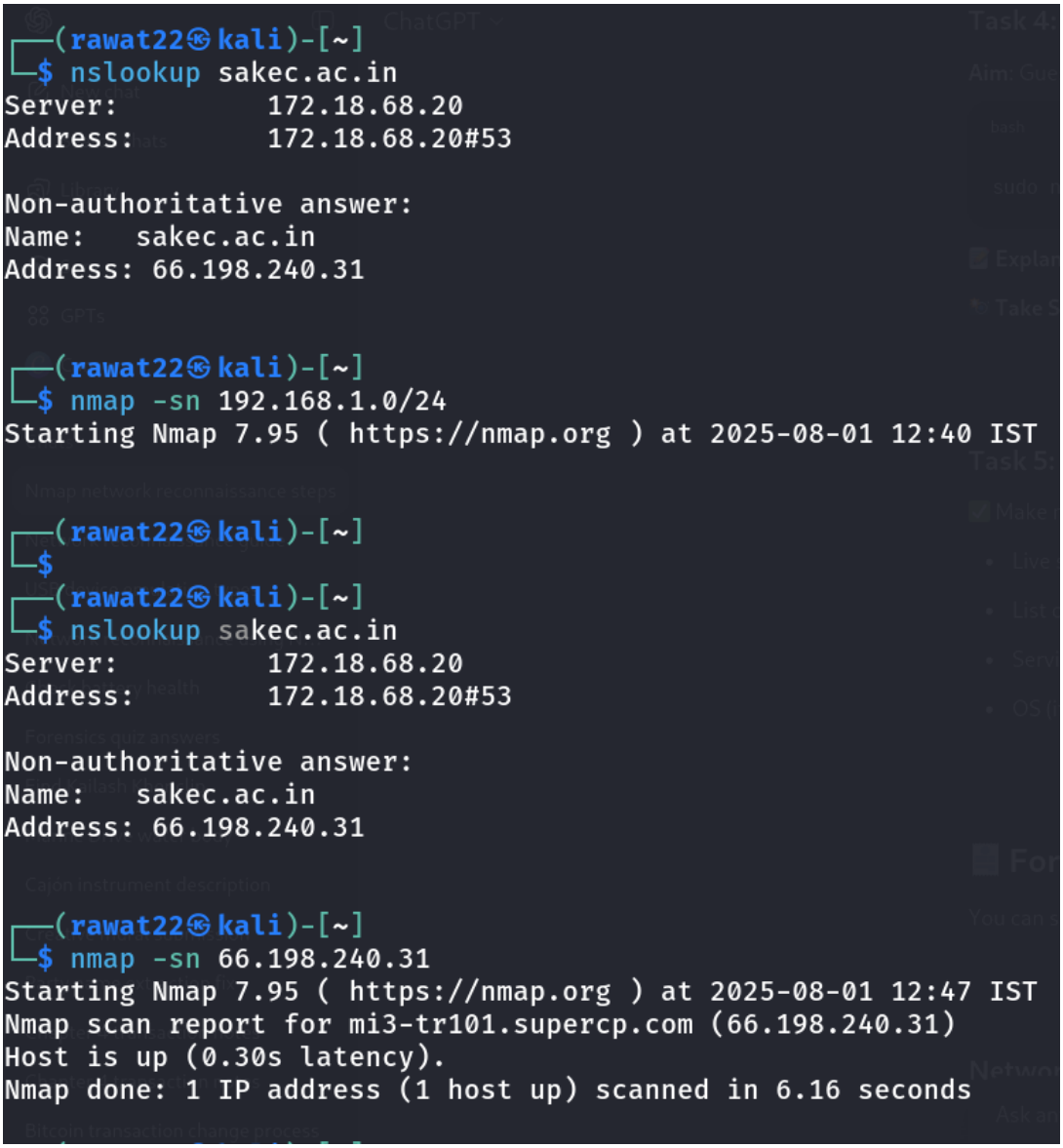
```
┌──(rawat22㉿kali)-[~]
└─$ nmap -sV 66.198.240.31
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 12:50 IST
Nmap scan report for mi3-tr101.supercp.com (66.198.240.31)
Host is up (0.27s latency).
Not shown: 894 filtered tcp ports (no-response), 23 filtered tcp ports (port-unreach), 71 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  ssh        OpenSSH 8.0 (protocol 2.0)
25/tcp   open  smtp       Exim smtpd 4.98.2
80/tcp   open  http       LiteSpeed
110/tcp  open  pop3       Dovecot pop3d
143/tcp  open  imap       Dovecot imapd
443/tcp  open  ssl/http   LiteSpeed httpd
465/tcp  open  smtps?
587/tcp  open  smtp       Exim smtpd 4.98.2
993/tcp  open  imaps?
995/tcp  open  pop3s?
2525/tcp open  smtp       Exim smtpd 4.98.2
4 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.c
gi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.95%I=7%D=8/1%Time=688C6AD4%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,1B20,"HTTP/1\.1\x20503\x20Service\x20Unavailable\r\nContent-Type:
SF:\x20text/html;\x20charset=UTF-8\r\nContent-Length:\x206667\r\nConnectio
SF:n:\x20close\r\nP3P:\x20CP=\"CAO\x20PSA\x20OUR\"\r\nExpires:\x20Thu,\x20
SF:01\x20Jan\x201970\x2000:00:00\x20GMT\r\nCache-Control:\x20no-store,\x20
SF:no-cache,\x20must-revalidate,\x20post-check=0,\x20pre-check=0\r\nPragma
SF::\x20no-cache\r\n\r\n<!DOCTYPE\x20html>\n\n<html\x20lang=\"en\">\n<head
SF:>\n\x20\x20\x20\x20<base\x20href=\"/login/\">\n\x20\x20\x20\x20<meta\x2
SF:0charset=\"utf-8\">\n\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compati
SF:ble\"\x20content=\"IE=edge\">\n\x20\x20\x20\x20<meta\x20name=\"viewport
SF:\"\x20content=\"width=device-width,\x20initial-scale=\.85\">\n\x20\x20\
SF:x20\x20<meta\x20http-equiv=\"pragma\"\x20content=\"no-cache\">\n\x20\x2
SF:0\x20\x20<title>Web\x20Page\x20Blocked</title>\n\x20\x20\x20\x20<style>
SF:\n\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20background-color:\x20#e8ebeb;\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20font-family:\x20Lato,\x20'Helvetica\x20Ne
SF:ue',\x20Helvetica,\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20font-size:\x2016px;\n\x20\x20\x20\x20\x20\x20\x20
```

This displays detailed information about services and versions running on open ports.

Task 4: OS Detection (Optional)

Command used:

sudo nmap -O 66.198.240.31



3.8 Conclusion

In this experiment, we successfully performed network reconnaissance using Nmap to identify live hosts, open ports, and services running on a target system. By executing various Nmap scans including host discovery, TCP SYN scan, service version detection, and OS fingerprinting, we gathered critical information about the target's network configuration. This hands-on exercise enhanced our understanding of network enumeration and its importance in vulnerability assessment and ethical hacking. The skills practiced here are fundamental for penetration testing, network security audits, and incident response.