CNS Lab Experiment No. 7

7.1 Aim:

Download, install Nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, TCP port scan, UDP port scan, etc.

7.2 Course Outcome:

Explain the fundamental concepts of computer security and network security.

7.3 Learning Objective:

To analyze the basic concepts of computer and network security.

7.4 Requirement:

Windows or Linux Operating System
Internet connection
Nmap tool installed

7.5 Related Theory:

Nmap (Network Mapper) is a powerful open-source tool for network discovery and security auditing. It is widely used to identify active hosts, open ports, running services, and operating system details in a network. Nmap supports different types of scans to gather this information, including:

Ping Scan: Determines which hosts are up in a network.

Command: nmap -sn <target>

TCP Port Scan: Scans for open TCP ports.

Command: nmap -sT <target>

UDP Port Scan: Scans for open UDP ports.

Command: nmap -sU <target>

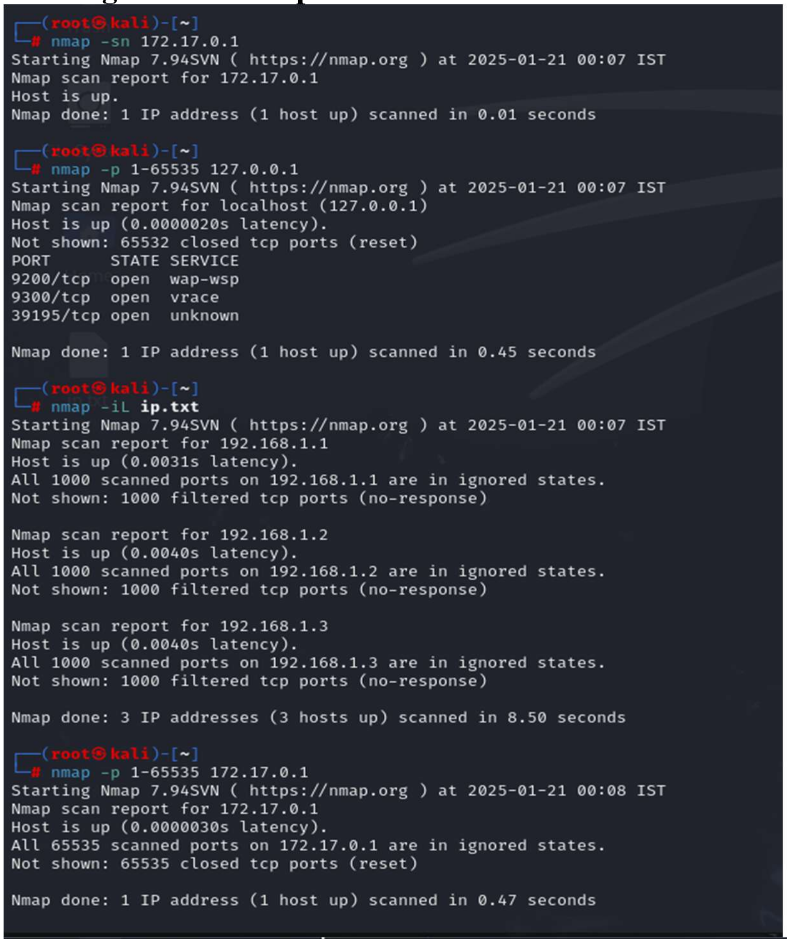
OS Fingerprinting: Detects the operating system of the target host.

Command: nmap -O <target>

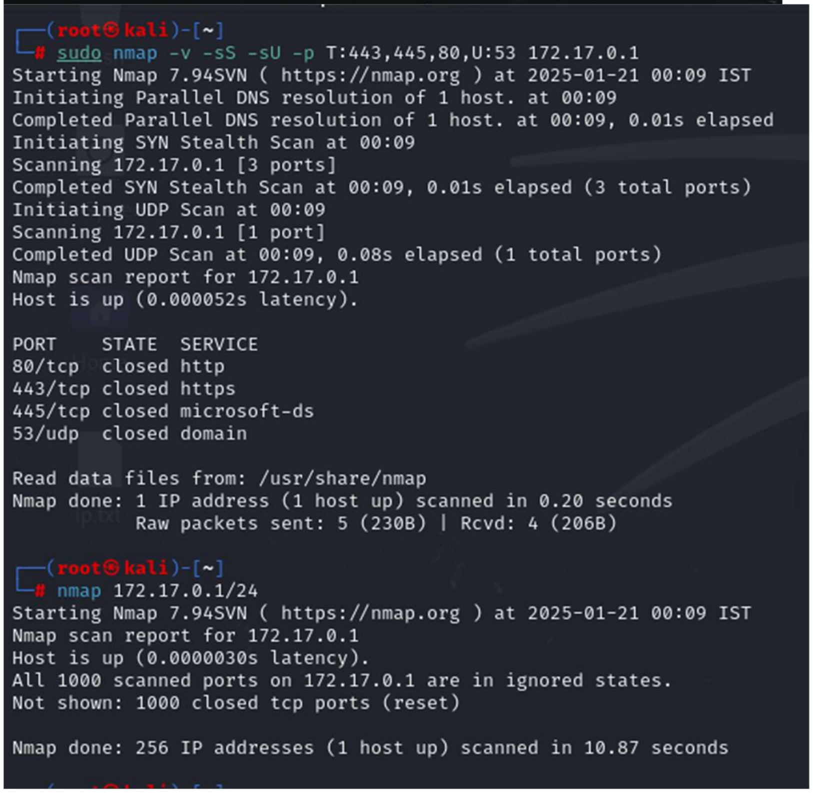
Service Version Detection: Identifies software and version information for open ports.

Command: nmap -sV <target>

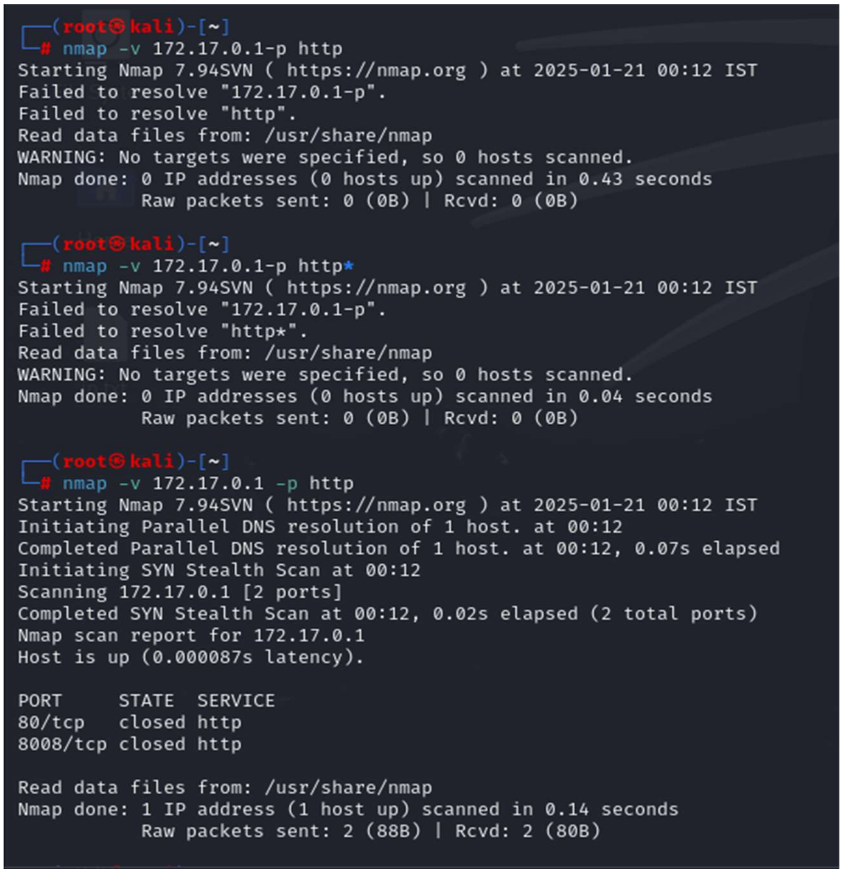
7.6 Program and Output:



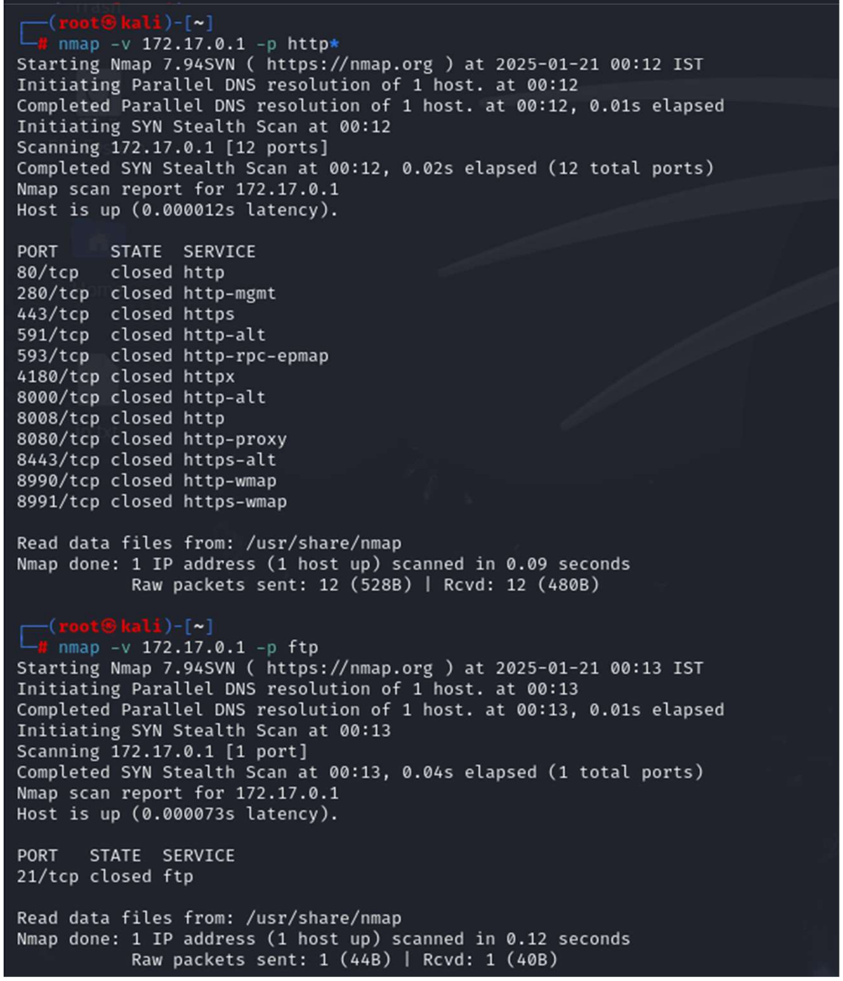
```
┌──(root㉿kali)-[~]
└─# nmap -sn 172.17.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:07 IST
Nmap scan report for 172.17.0.1
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 1-65535 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:07 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
9200/tcp  open  wap-wsp
9300/tcp  open  vrace
39195/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds

┌──(root㉿kali)-[~]
└─# nmap -iL ip.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:07 IST
Nmap scan report for 192.168.1.1
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.0040s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.3
Host is up (0.0040s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 3 IP addresses (3 hosts up) scanned in 8.50 seconds

┌──(root㉿kali)-[~]
└─# nmap -p 1-65535 172.17.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:08 IST
Nmap scan report for 172.17.0.1
Host is up (0.0000030s latency).
All 65535 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 65535 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```



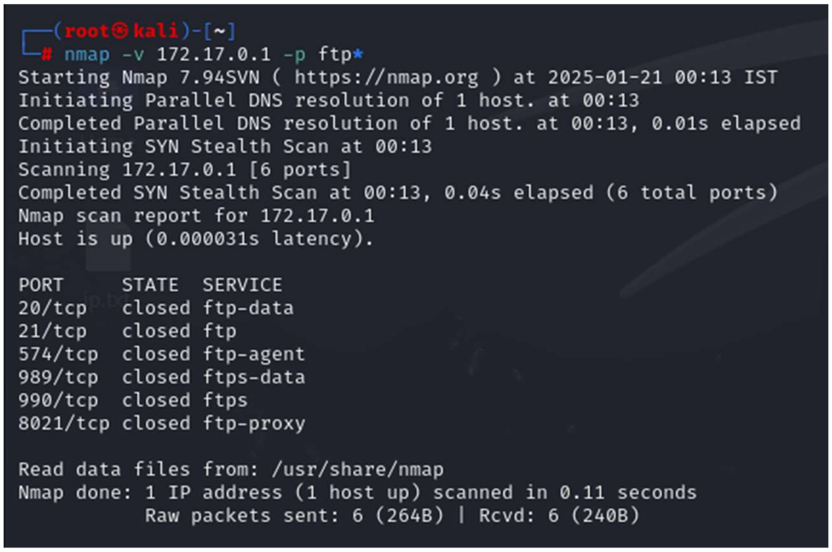
```
┌──(root㉿kali)-[~]
└─# sudo nmap -v -sS -sU -p T:443,445,80,U:53 172.17.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:09 IST
Initiating Parallel DNS resolution of 1 host. at 00:09
Completed Parallel DNS resolution of 1 host. at 00:09, 0.01s elapsed
Initiating SYN Stealth Scan at 00:09
Scanning 172.17.0.1 [3 ports]
Completed SYN Stealth Scan at 00:09, 0.01s elapsed (3 total ports)
Initiating UDP Scan at 00:09
Scanning 172.17.0.1 [1 port]
Completed UDP Scan at 00:09, 0.08s elapsed (1 total ports)
Nmap scan report for 172.17.0.1
Host is up (0.000052s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
445/tcp closed microsoft-ds
53/udp  closed domain

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
           Raw packets sent: 5 (230B) | Rcvd: 4 (206B)

┌──(root㉿kali)-[~]
└─# nmap 172.17.0.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:09 IST
Nmap scan report for 172.17.0.1
Host is up (0.0000030s latency).
All 1000 scanned ports on 172.17.0.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (1 host up) scanned in 10.87 seconds
```



```
┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1-p http
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:12 IST
Failed to resolve "172.17.0.1-p".
Failed to resolve "http".
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.43 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1-p http*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:12 IST
Failed to resolve "172.17.0.1-p".
Failed to resolve "http*".
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1 -p http
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:12 IST
Initiating Parallel DNS resolution of 1 host. at 00:12
Completed Parallel DNS resolution of 1 host. at 00:12, 0.07s elapsed
Initiating SYN Stealth Scan at 00:12
Scanning 172.17.0.1 [2 ports]
Completed SYN Stealth Scan at 00:12, 0.02s elapsed (2 total ports)
Nmap scan report for 172.17.0.1
Host is up (0.000087s latency).

PORT     STATE  SERVICE
80/tcp   closed http
8008/tcp closed http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
           Raw packets sent: 2 (88B) | Rcvd: 2 (80B)
```



```
┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1 -p http*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:12 IST
Initiating Parallel DNS resolution of 1 host. at 00:12
Completed Parallel DNS resolution of 1 host. at 00:12, 0.01s elapsed
Initiating SYN Stealth Scan at 00:12
Scanning 172.17.0.1 [12 ports]
Completed SYN Stealth Scan at 00:12, 0.02s elapsed (12 total ports)
Nmap scan report for 172.17.0.1
Host is up (0.000012s latency).

PORT     STATE  SERVICE
80/tcp   closed http
280/tcp  closed http-mgmt
443/tcp  closed https
591/tcp  closed http-alt
593/tcp  closed http-rpc-epmap
4180/tcp closed httpx
8000/tcp closed http-alt
8008/tcp closed http
8080/tcp closed http-proxy
8443/tcp closed https-alt
8990/tcp closed http-wmap
8991/tcp closed https-wmap

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
           Raw packets sent: 12 (528B) | Rcvd: 12 (480B)

┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1 -p ftp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:13 IST
Initiating Parallel DNS resolution of 1 host. at 00:13
Completed Parallel DNS resolution of 1 host. at 00:13, 0.01s elapsed
Initiating SYN Stealth Scan at 00:13
Scanning 172.17.0.1 [1 port]
Completed SYN Stealth Scan at 00:13, 0.04s elapsed (1 total ports)
Nmap scan report for 172.17.0.1
Host is up (0.000073s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
           Raw packets sent: 1 (44B) | Rcvd: 1 (40B)
```



```
┌──(root㉿kali)-[~]
└─# nmap -v 172.17.0.1 -p ftp*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:13 IST
Initiating Parallel DNS resolution of 1 host. at 00:13
Completed Parallel DNS resolution of 1 host. at 00:13, 0.01s elapsed
Initiating SYN Stealth Scan at 00:13
Scanning 172.17.0.1 [6 ports]
Completed SYN Stealth Scan at 00:13, 0.04s elapsed (6 total ports)
Nmap scan report for 172.17.0.1
Host is up (0.000031s latency).

PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
574/tcp  closed ftp-agent
989/tcp  closed ftps-data
990/tcp  closed ftps
8021/tcp closed ftp-proxy

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
           Raw packets sent: 6 (264B) | Rcvd: 6 (240B)
```

7.7 Conclusion:

In this practical, we successfully installed and used Nmap to perform various types of network scans, including open port detection, OS fingerprinting, and service version identification. This demonstrated how Nmap can be utilized for network security analysis and troubleshooting.