Name: Harsh Mishra
Roll no: 64
Batch: T21

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

Theory :

Nmap:

Nmap (Network Mapper) is a widely used open-source network scanning tool designed to discover hosts and services on a computer network. Its primary functions include mapping network infrastructure, identifying active devices, and detecting vulnerabilities. It operates by sending specially crafted packets to target hosts and analyzing their responses.

Key Features

1. Port Scanning:
    - nmap identifies open ports on a target machine. By probing various ports, it determines which are accessible and responsive, which can help in assessing the exposure of services.
2. Service Detection:
    - Beyond detecting open ports, nmap can probe those ports to identify the services running on them. This includes determining the version of the service, which helps in identifying potential vulnerabilities specific to that version.
3. Operating System Detection:
    - Using techniques like TCP/IP stack fingerprinting, nmap estimates the operating system of the target device. It analyzes responses to certain packets to deduce characteristics of the OS.
4. Network Mapping:
    - nmap can map out a network by discovering which hosts are active and how they are interconnected. This can be useful for understanding network architecture and detecting unauthorized devices.
5. Vulnerability Scanning:
    - Through the use of the Nmap Scripting Engine (NSE), nmap can run scripts to

Name: Harsh Mishra
Roll no: 64
Batch: T21

check for specific vulnerabilities or security issues on the target systems.

Common Scanning Techniques

1. TCP SYN Scan (Stealth Scan):
    - Sends SYN packets to target ports. If a SYN-ACK is received, the port is open. This method is less likely to be logged by the target's firewall or intrusion detection system.
2. TCP Connect Scan:
    - Completes the TCP handshake to determine open ports. This scan is more intrusive and detectable compared to the SYN scan but can be more accurate.
3. UDP Scan:
    - Sends UDP packets to ports and waits for responses. Since UDP is connectionless, it can be less reliable and slower to scan compared to TCP.
4. Aggressive Scan:
    - Combines several scans and techniques (OS detection, version detection, script scanning) into a single scan, providing a comprehensive overview but potentially more detectable.

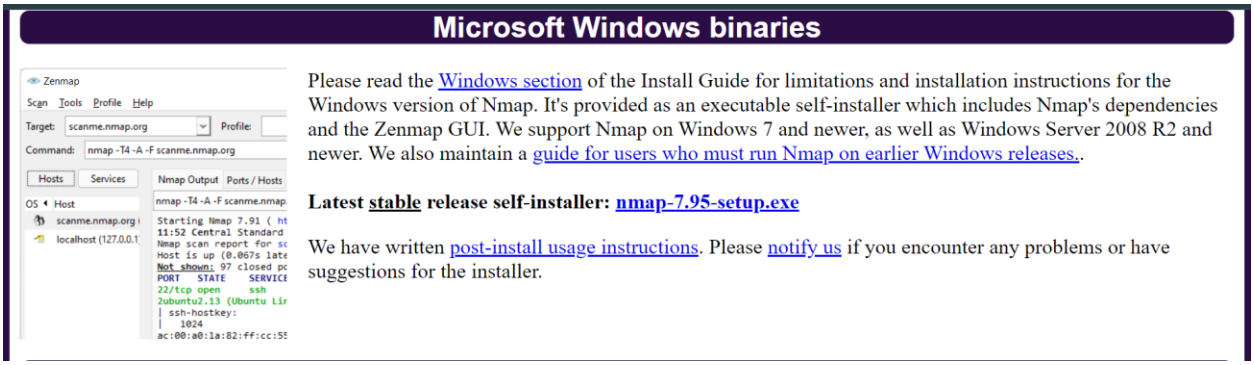
Practical Applications

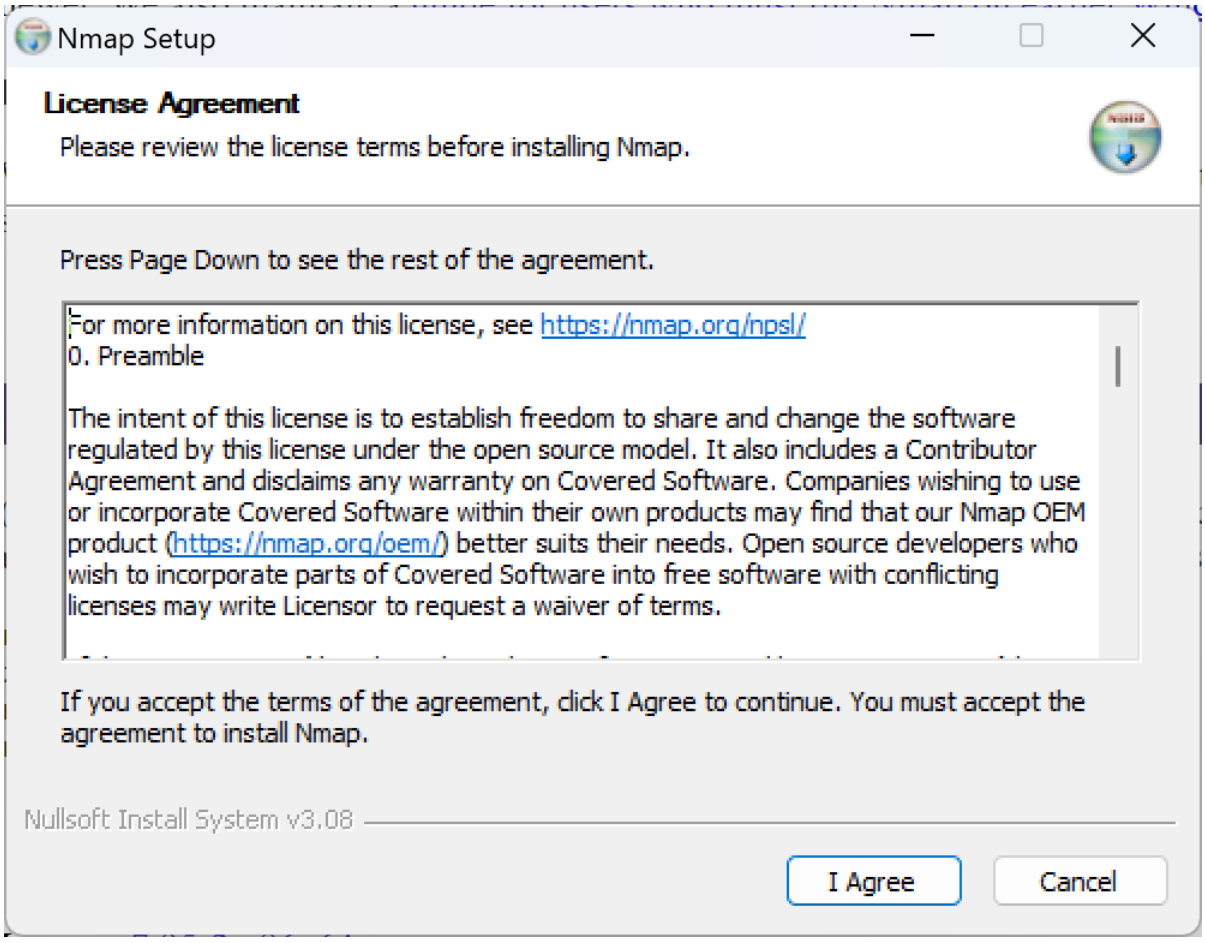
- Security Assessment:
    - Used by security professionals to find vulnerabilities, misconfigurations, and security holes in a network.
- Network Inventory:
    - Helps network administrators maintain an inventory of devices and their services, ensuring network hygiene.
- Troubleshooting:
    - Assists in diagnosing network issues by revealing misconfigured or malfunctioning services.

Name: Harsh Mishra
Roll no: 64
Batch: T21

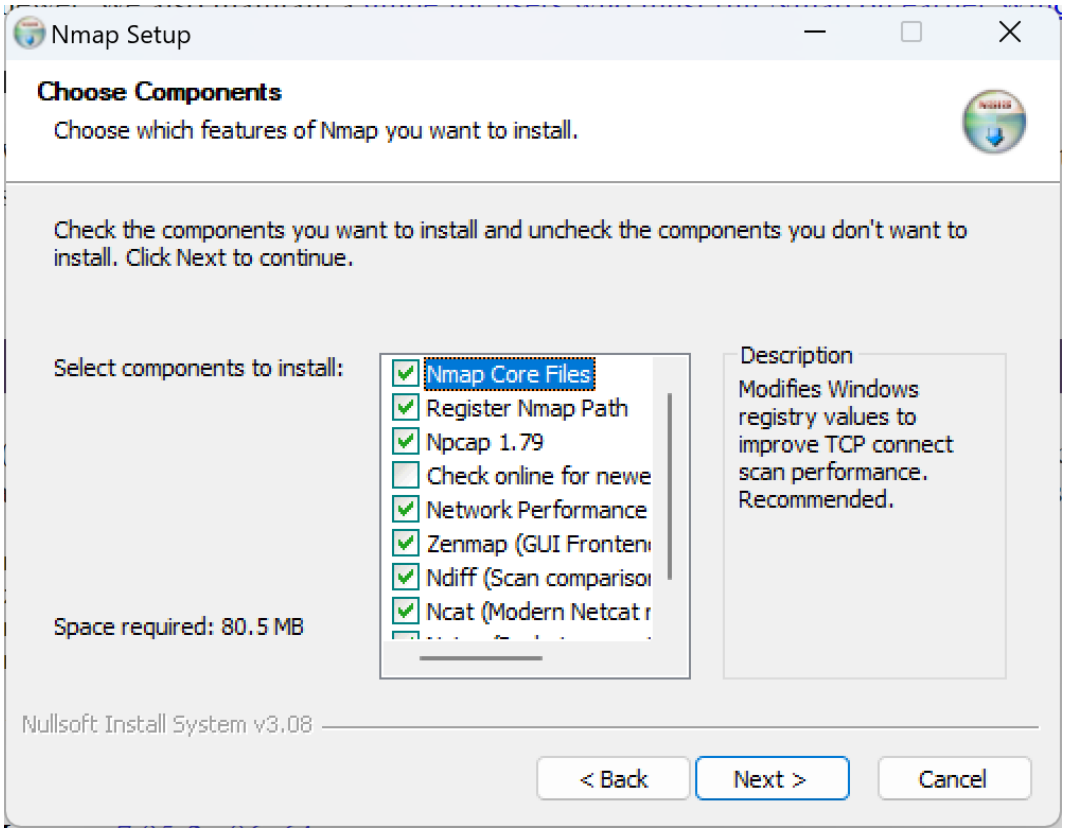
Output:

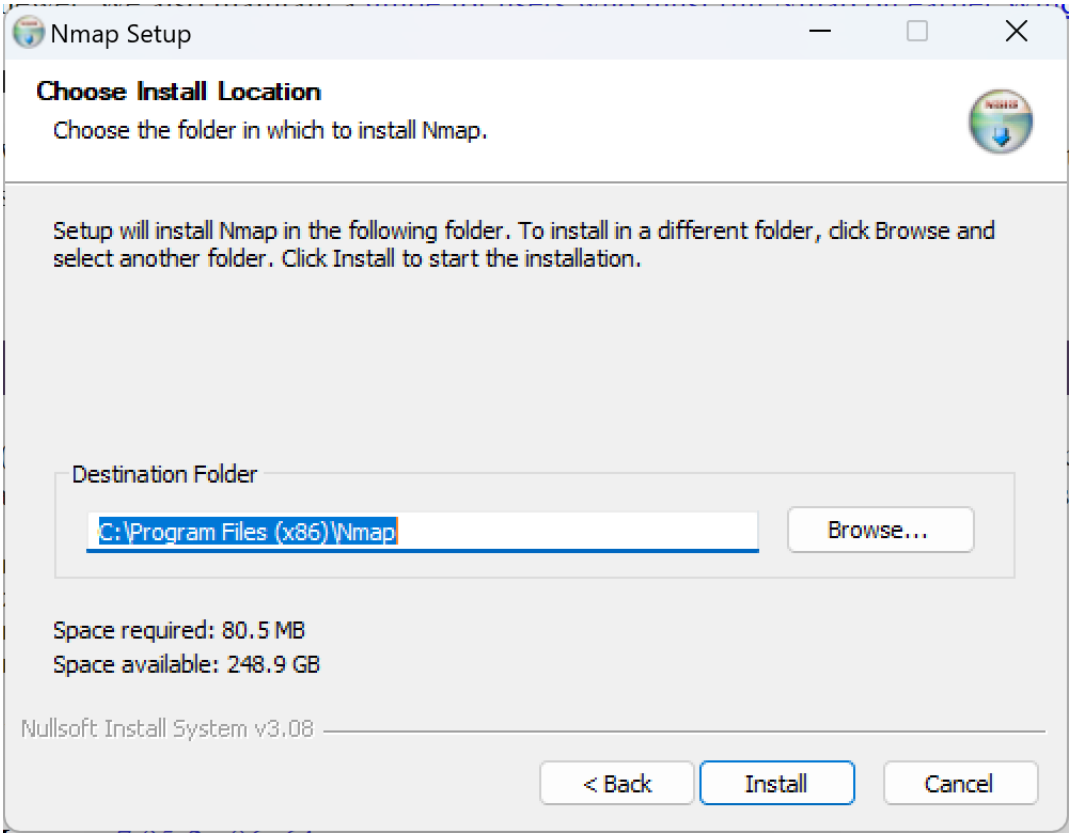
Nmap Installation:



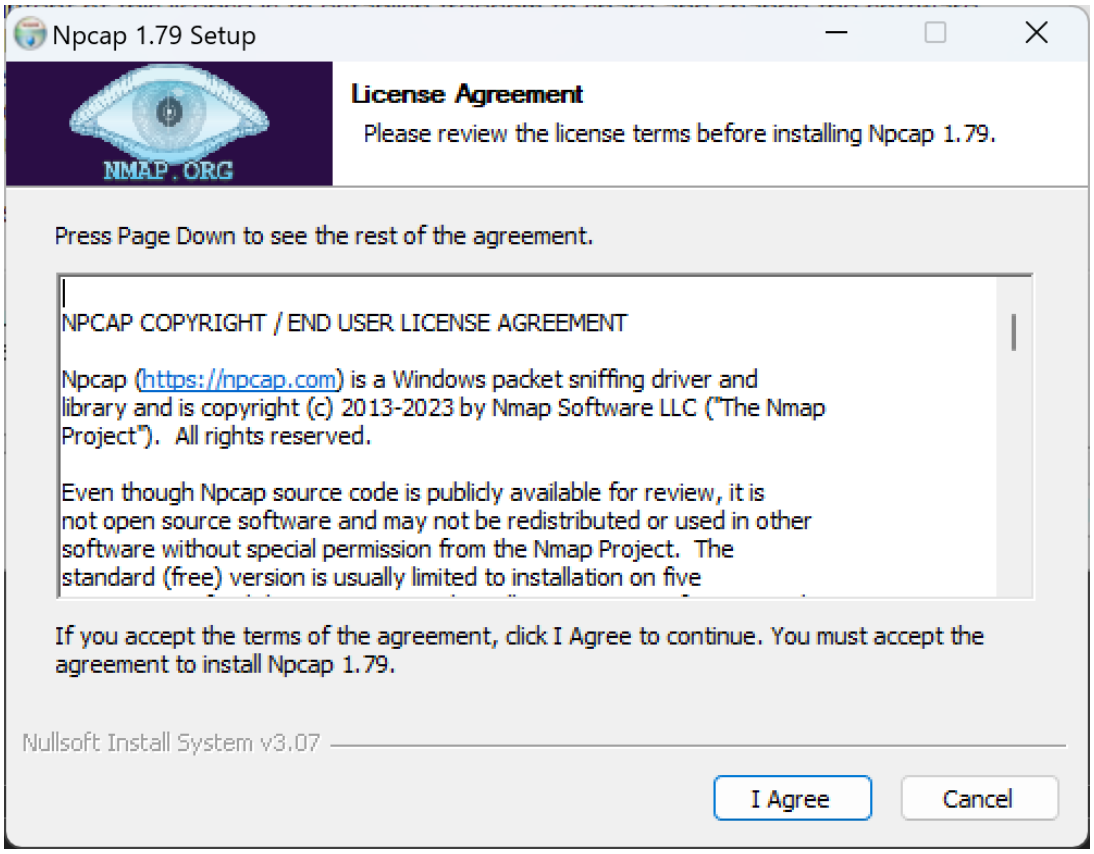


Name: Harsh Mishra
Roll no: 64
Batch: T21

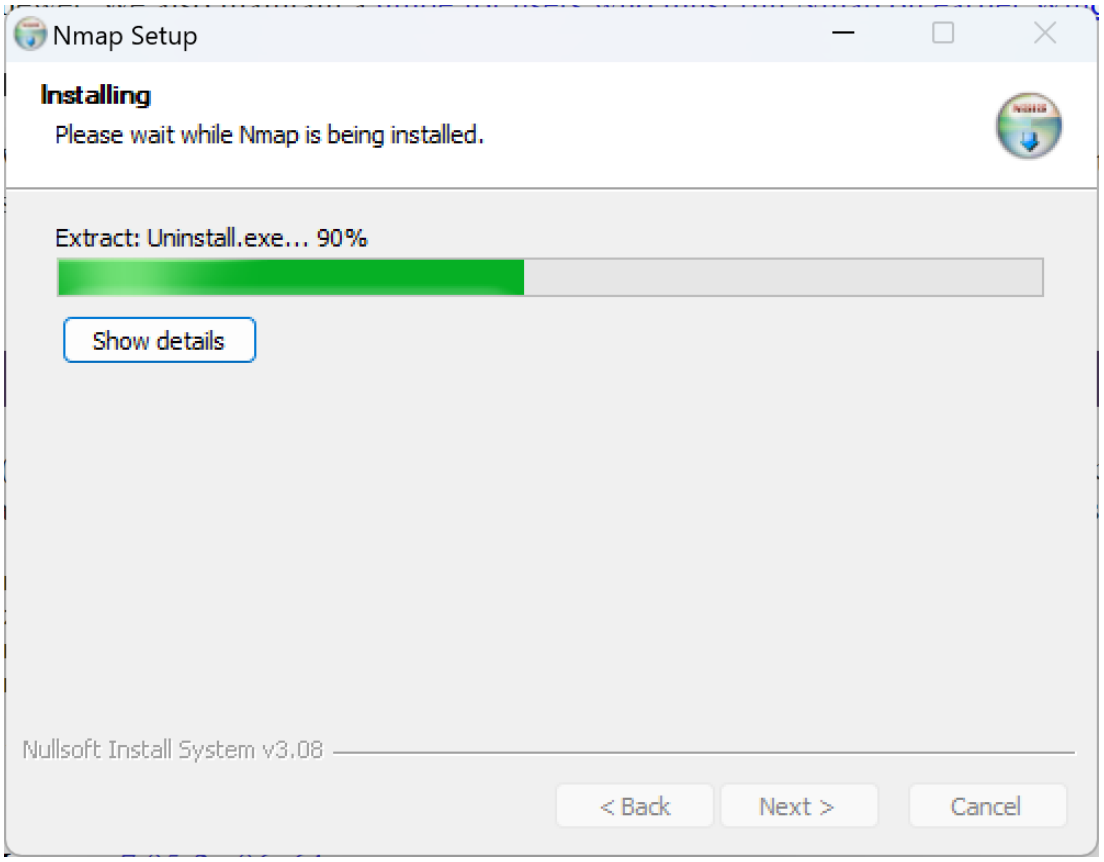




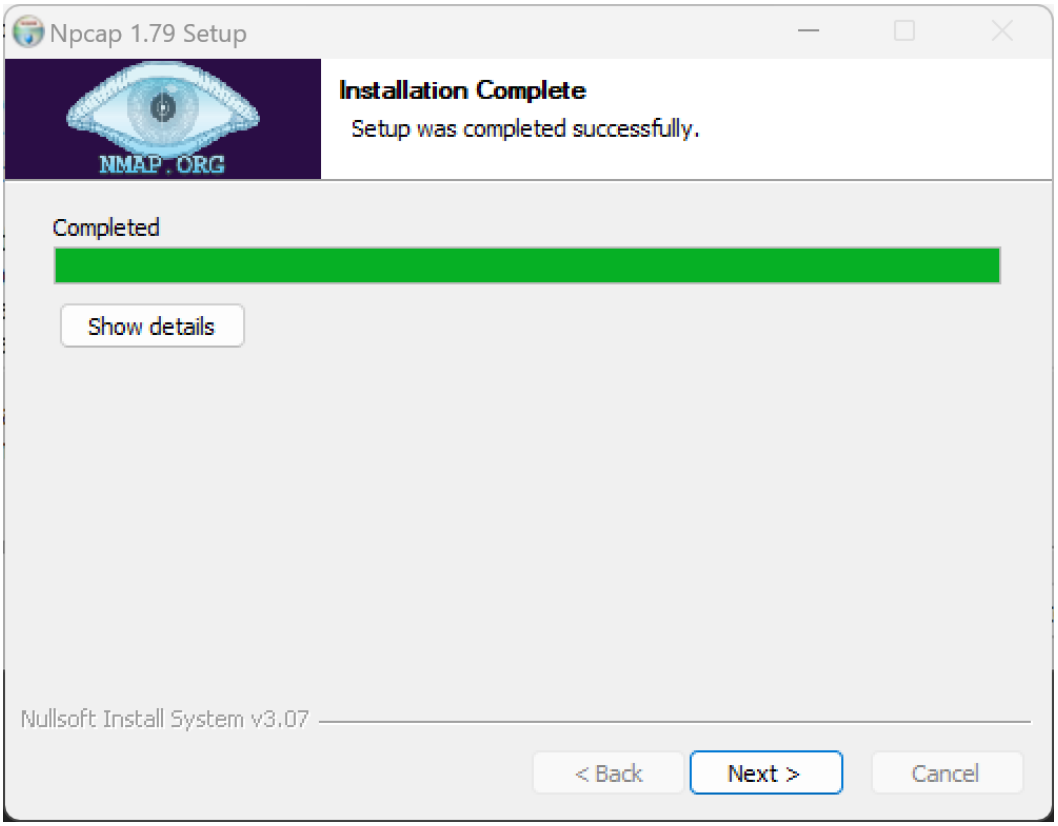
Name: Harsh Mishra
Roll no: 64
Batch: T21

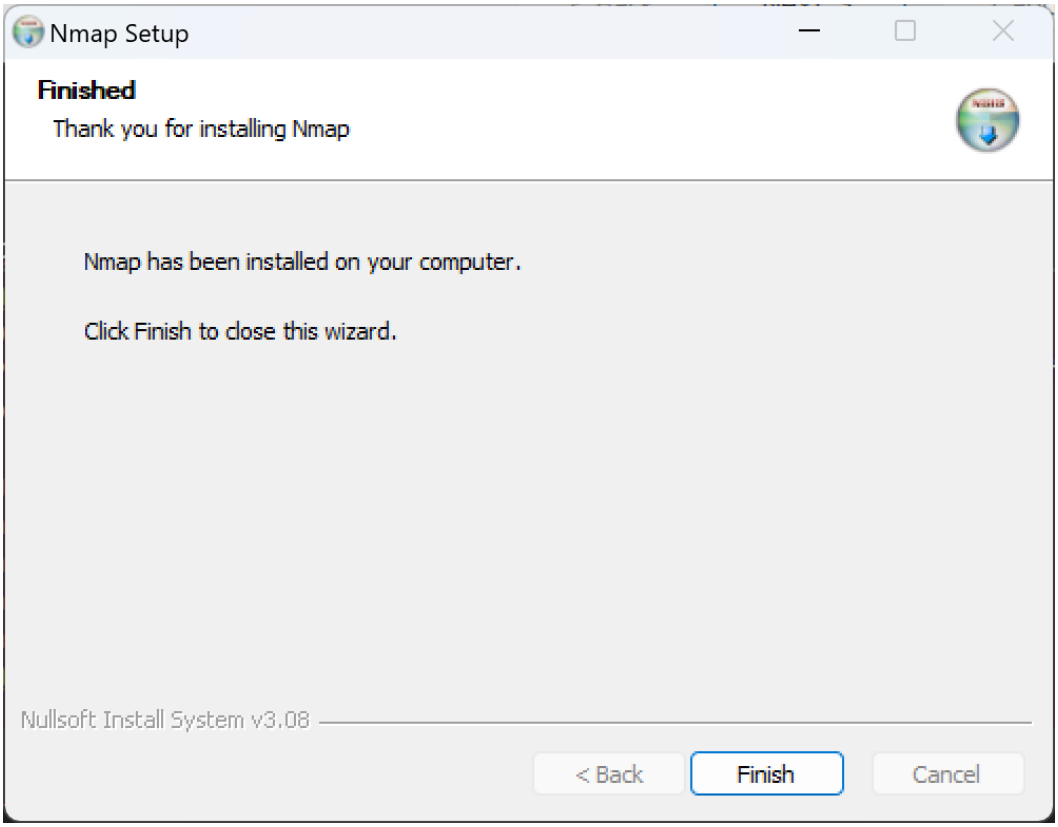


Name: Harsh Mishra
Roll no: 64
Batch: T21



Name: Harsh Mishra
Roll no: 64
Batch: T21





Name: Harsh Mishra
Roll no: 64
Batch: T21

Commands:

1. Scan Open Ports

```
C:\Program Files (x86)\Nmap>nmap 162.241.70.62
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-19 09:56 India Standard Time
Nmap scan report for 162-241-70-62.webhostbox.net (162.241.70.62)
Host is up (0.26s latency).
Not shown: 915 filtered tcp ports (no-response), 15 filtered tcp ports (host-prohibited), 59 closed tcp ports (res
et)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
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
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 10.32 seconds
```

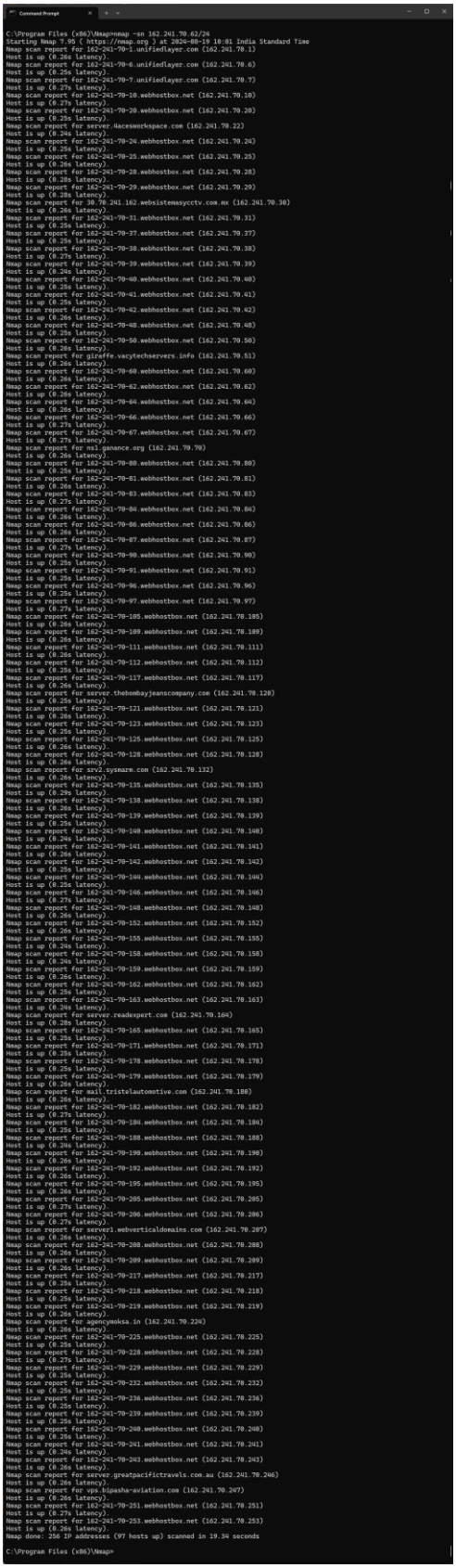
2. OS Fingerprinting

```
C:\Program Files (x86)\Nmap>nmap -O 162.241.70.62
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-19 09:56 India Standard Time
Nmap scan report for 162-241-70-62.webhostbox.net (162.241.70.62)
Host is up (0.26s latency).
Not shown: 915 filtered tcp ports (no-response), 15 filtered tcp ports (host-prohibited), 59 closed tcp ports (res
et)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
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
3306/tcp open  mysql
Aggressive OS guesses: Linux 4.19 - 5.15 (92%), Linux 3.4 (91%), Linux 4.15 (90%), Linux 3.11 - 4.9 (88%), Linux 3
.2 - 3.8 (88%), Android TV OS 11 (Linux 4.19) (86%), Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39
(86%), Linux 3.10 - 3.12 (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds
```

3. Ping Scan

Name: Harsh Mishra
Roll no: 64
Batch: T21



Name: Harsh Mishra
Roll no: 64
Batch: T21

4. TCP Port Scan

```
C:\Program Files (x86)\Nmap>nmap -sT 162.241.70.62
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-19 10:05 India Standard Time
Nmap scan report for 162-241-70-62.webhostbox.net (162.241.70.62)
Host is up (0.26s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
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
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

5. UDP Port Scan

```
C:\Program Files (x86)\Nmap>nmap -sU 142.250.217.68
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-19 10:24 India Standard Time
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.40% done; ETC: 10:29 (0:01:10 remaining)
Stats: 0:03:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.55% done; ETC: 10:29 (0:01:09 remaining)
Nmap scan report for sea09s29-in-f4.1e100.net (142.250.217.68)
Host is up (0.26s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
33459/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 222.04 seconds
```

Conclusion: Used tools like sniffers, port scanners and other related tools for analyzing packets in a network (LO4 is achieved).