Title: Task -04
Tasks Covered:
• Wireshark Analysis
• Nmap Scanning & Vulnerability Detection
• Python Port Scanner Tool

Name: Faizan Nazir
Internship: Dg interns Hub
Date: 31-12-2025

---

1. INTRODUCTION

This report presents the final documentation of hands-on cybersecurity tasks performed during the internship.
The objective of these tasks was to gain **practical exposure** to network traffic analysis, reconnaissance techniques, and custom tool development using industry-standard tools.

The report includes:

- Network traffic analysis using Wireshark
- Network scanning using Nmap
- Development of a Python-based Port Scanner tool

---

2. WIRESHARK NETWORK TRAFFIC ANALYSIS

2.1 Objective

To capture and analyze live network traffic in order to understand protocol behavior and identify suspicious activity.

2.2 Methodology

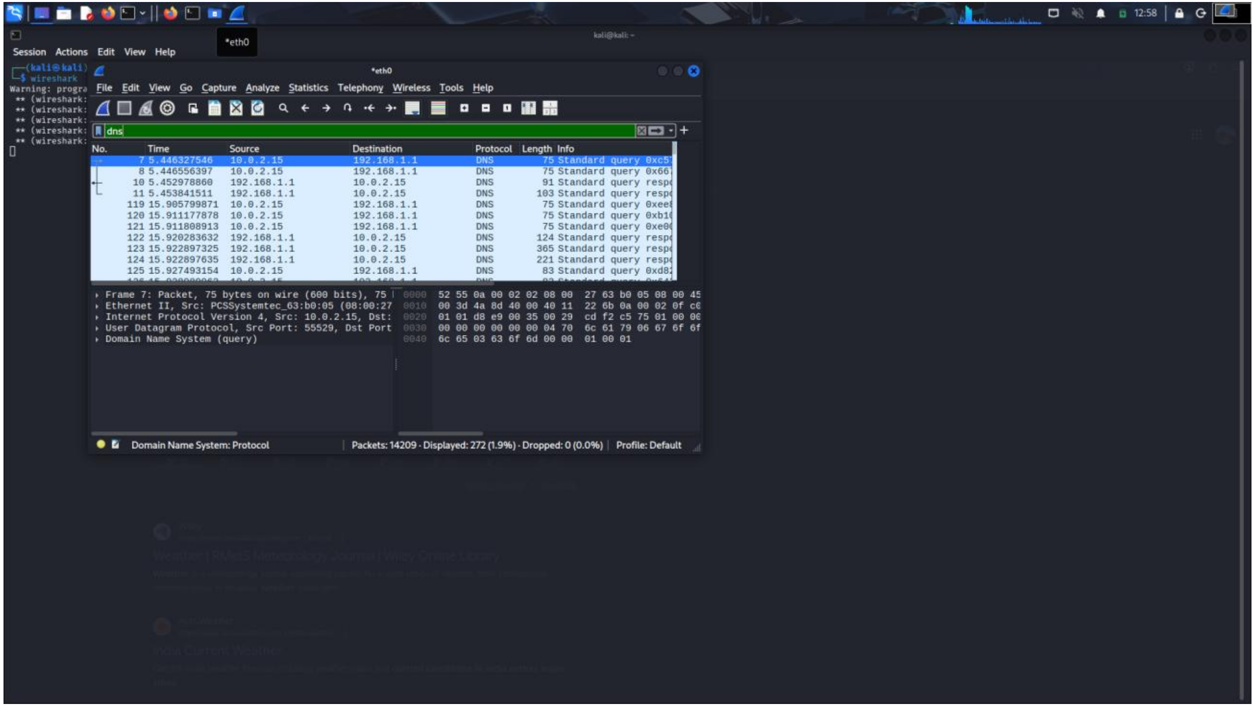
- Wireshark was launched on Kali Linux.
- Live packet capture was started on the active network interface.
- Protocol-based filters were applied for focused analysis.

2.3 Analysis Performed

2.3.1 DNS Analysis

DNS query and response packets were analyzed to understand domain name resolution.

📸 **INSERT SCREENSHOT HERE**
☞ *Wireshark DNS filter output*



```
┌──(kali㉿kali)
└─$ wireshark
Warning: progra
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
```

dns

```
No.   Time          Source        Destination   Protocol  Length Info
    7 5.446327546   10.0.2.15     192.168.1.1   DNS           75 Standard query 0xc5
    8 5.446556397   10.0.2.15     192.168.1.1   DNS           75 Standard query 0x66
   10 5.452978860   192.168.1.1   10.0.2.15     DNS           91 Standard query resp
   11 5.453841511   192.168.1.1   10.0.2.15     DNS          103 Standard query resp
  119 15.905799871  10.0.2.15     192.168.1.1   DNS           75 Standard query 0xee
  120 15.911177878  10.0.2.15     192.168.1.1   DNS           75 Standard query 0xb1
  121 15.911808913  10.0.2.15     192.168.1.1   DNS           75 Standard query 0xe0
  122 15.920283632  192.168.1.1   10.0.2.15     DNS          124 Standard query resp
  123 15.922897325  192.168.1.1   10.0.2.15     DNS          365 Standard query resp
  124 15.922897635  192.168.1.1   10.0.2.15     DNS          221 Standard query resp
  125 15.927493154  10.0.2.15     192.168.1.1   DNS           83 Standard query 0xd8
```

```
› Frame 7: Packet, 75 bytes on wire (600 bits), 75    0000  52 55 0a 00 02 02 08 00  27 63 b0 05 08 00 45
› Ethernet II, Src: PCSSystemtec_63:b0:05 (08:00:27   0010  00 3d 4a 8d 40 00 40 11  22 6b 0a 00 02 0f c0
› Internet Protocol Version 4, Src: 10.0.2.15, Dst:   0020  01 01 d8 e9 00 35 00 29  cd f2 c5 75 01 00 00
› User Datagram Protocol, Src Port: 55529, Dst Port   0030  00 00 00 00 00 00 04 70  6c 61 79 06 67 6f 6f
› Domain Name System (query)                          0040  6c 65 03 63 6f 6d 00 00  01 00 01
```

Domain Name System: Protocol | Packets: 14209 · Displayed: 272 (1.9%) · Dropped: 0 (0.0%) | Profile: Default

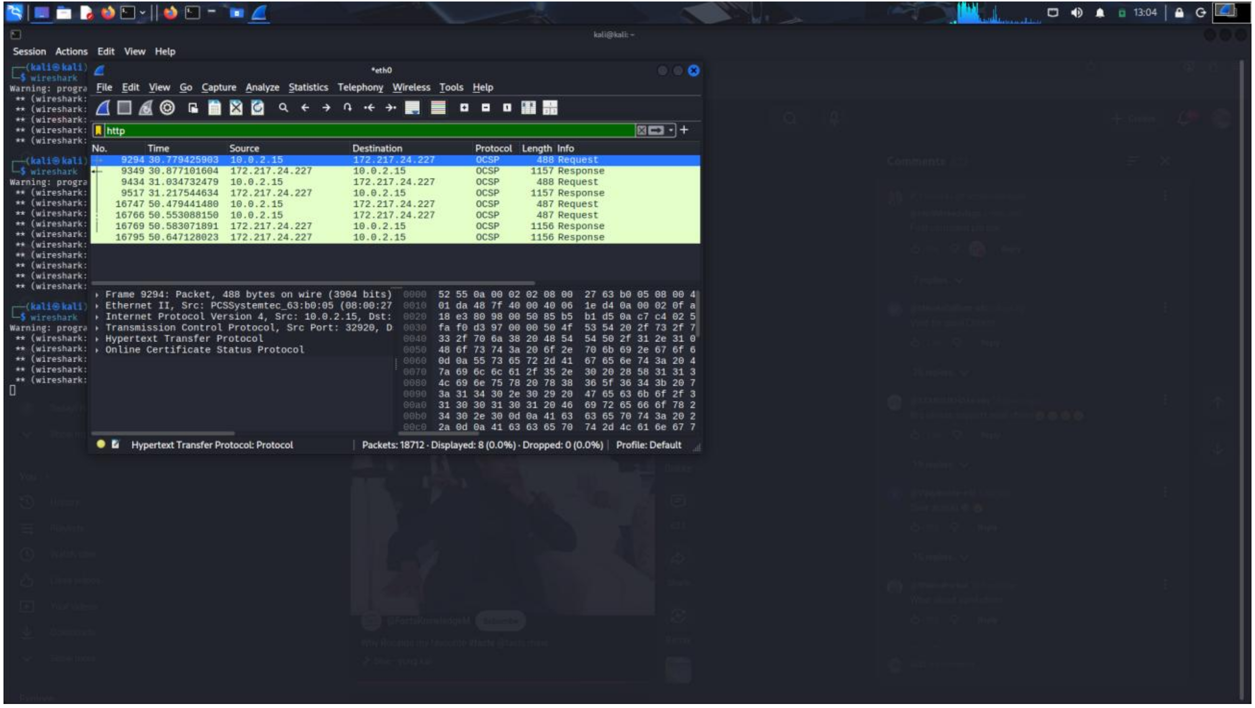
---

2.3.2 HTTP Traffic Analysis

HTTP GET/POST requests were inspected to observe web communication between client and server.

📷 **INSERT SCREENSHOT HERE**

☞ *Wireshark HTTP filter output*



```
┌──(kali㉿kali)
└─$ wireshark
Warning: progra
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
```

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.     Time          Source          Destination     Protocol Length Info
   9294 30.779425903  10.0.2.15       172.217.24.227  OCSP      488 Request
   9349 30.877101604  172.217.24.227  10.0.2.15       OCSP     1157 Response
   9434 31.034732479  10.0.2.15       172.217.24.227  OCSP      488 Request
   9517 31.217544634  172.217.24.227  10.0.2.15       OCSP     1157 Response
  16747 50.479441480  10.0.2.15       172.217.24.227  OCSP      487 Request
  16766 50.553088150  10.0.2.15       172.217.24.227  OCSP      487 Request
  16769 50.583071891  172.217.24.227  10.0.2.15       OCSP     1156 Response
  16795 50.647128023  172.217.24.227  10.0.2.15       OCSP     1156 Response
```

```
› Frame 9294: Packet, 488 bytes on wire (3904 bits)
› Ethernet II, Src: PCSSystemtec_63:b0:05 (08:00:27
› Internet Protocol Version 4, Src: 10.0.2.15, Dst:
› Transmission Control Protocol, Src Port: 32920, D
› Hypertext Transfer Protocol
› Online Certificate Status Protocol
```

```
0000  52 55 0a 00 02 02 08 00  27 63 b0 05 08 00 4
0010  01 da 48 7f 40 00 40 06  1e d4 0a 00 02 0f a
0020  18 e3 80 98 00 50 85 b5  b1 d5 0a c7 c4 02 5
0030  fa f0 d3 97 00 00 50 4f  53 54 20 2f 73 2f 7
0040  33 2f 70 6a 38 20 48 54  54 50 2f 31 2e 31 0
0050  48 6f 73 74 3a 20 6f 2e  70 6b 69 2e 67 6f 6
0060  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4
0070  7a 69 6c 6c 61 2f 35 2e  30 20 28 58 31 31 3
0080  4c 69 6e 75 78 20 78 38  36 5f 36 34 3b 20 7
0090  3a 31 34 30 2e 30 29 20  47 65 63 6b 6f 2f 3
00a0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2
00b0  34 30 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2
00c0  2a 0d 0a 41 63 63 65 70  74 2d 4c 61 6e 67 7
```

Hypertext Transfer Protocol: Protocol | Packets: 18712 · Displayed: 8 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

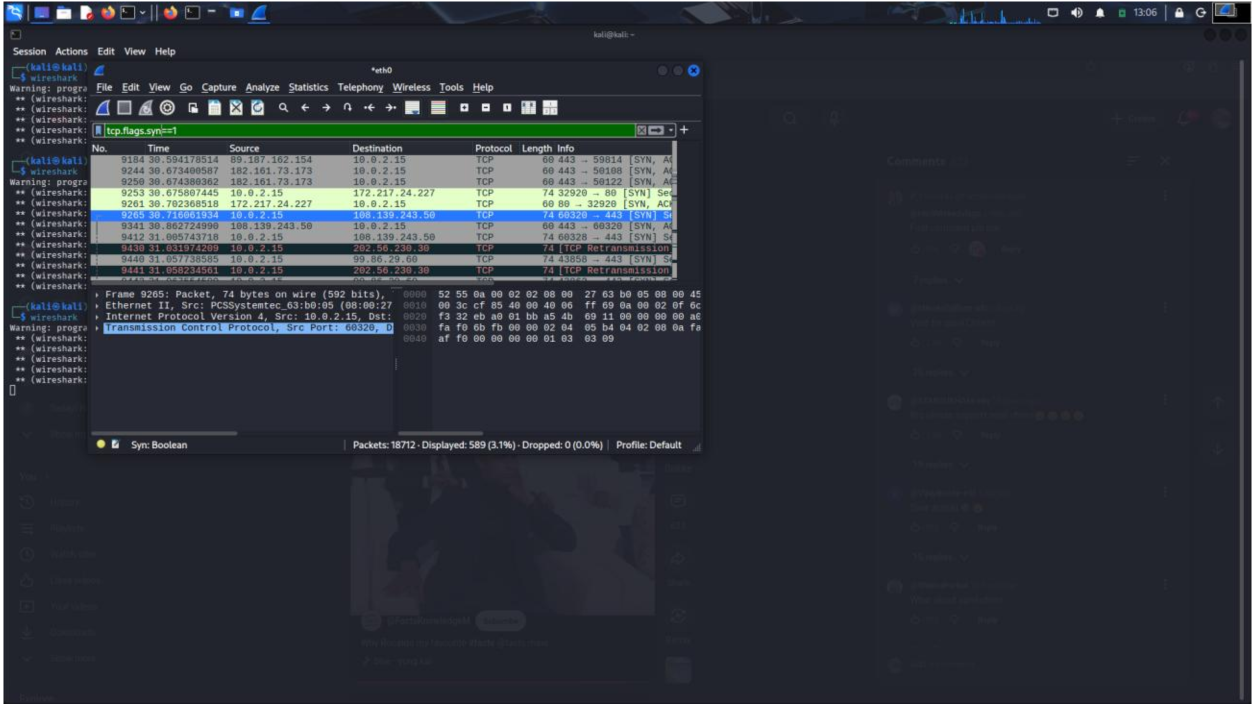
---

2.3.3 TCP Three-Way Handshake

TCP SYN packets were analyzed to understand the connection establishment process.

📷 **INSERT SCREENSHOT HERE**

☞ *Wireshark TCP SYN filter output*


Session Actions Edit View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
kali@kali: ~

```
tcp.flags.syn==1
```

```
No.   Time          Source            Destination       Protocol  Length Info
 9184 30.594178514  89.187.162.154    10.0.2.15         TCP       60 443 → 59814 [SYN, AC
 9244 30.673400587  182.161.73.173    10.0.2.15         TCP       60 443 → 50108 [SYN, AC
 9250 30.674380362  182.161.73.173    10.0.2.15         TCP       60 443 → 50122 [SYN, AC
 9253 30.675807445  10.0.2.15         172.217.24.227    TCP       74 32920 → 80 [SYN] Seq
 9261 30.702368518  172.217.24.227    10.0.2.15         TCP       60 80 → 32920 [SYN, ACK
 9265 30.716061934  10.0.2.15         108.139.243.50    TCP       74 60320 → 443 [SYN] Se
 9341 30.862724990  108.139.243.50    10.0.2.15         TCP       60 443 → 60320 [SYN, AC
 9412 31.005743718  10.0.2.15         108.139.243.50    TCP       74 60328 → 443 [SYN] Se
 9430 31.031974209  10.0.2.15         202.56.230.30     TCP       74 [TCP Retransmission
 9440 31.057738585  10.0.2.15         99.86.29.60       TCP       74 43858 → 443 [SYN] Se
 9441 31.058234561  10.0.2.15         202.56.230.30     TCP       74 [TCP Retransmission
```

```
› Frame 9265: Packet, 74 bytes on wire (592 bits),
› Ethernet II, Src: PCSSystemtec_63:b0:05 (08:00:27
› Internet Protocol Version 4, Src: 10.0.2.15, Dst:
› Transmission Control Protocol, Src Port: 60320, D
```

```
0000  52 55 0a 00 02 02 08 00  27 63 b0 05 08 00 45
0010  00 3c cf 85 40 00 40 06  ff 69 0a 00 02 0f 6c
0020  f3 32 eb a0 01 bb a5 4b  69 11 00 00 00 00 a0
0030  fa f0 6b fb 00 00 02 04  05 b4 04 02 08 0a fa
0040  af f0 00 00 00 00 01 03  03 09
```

```
┌──(kali㉿kali)
└─$ wireshark
Warning: progra
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
 ** (wireshark:
```

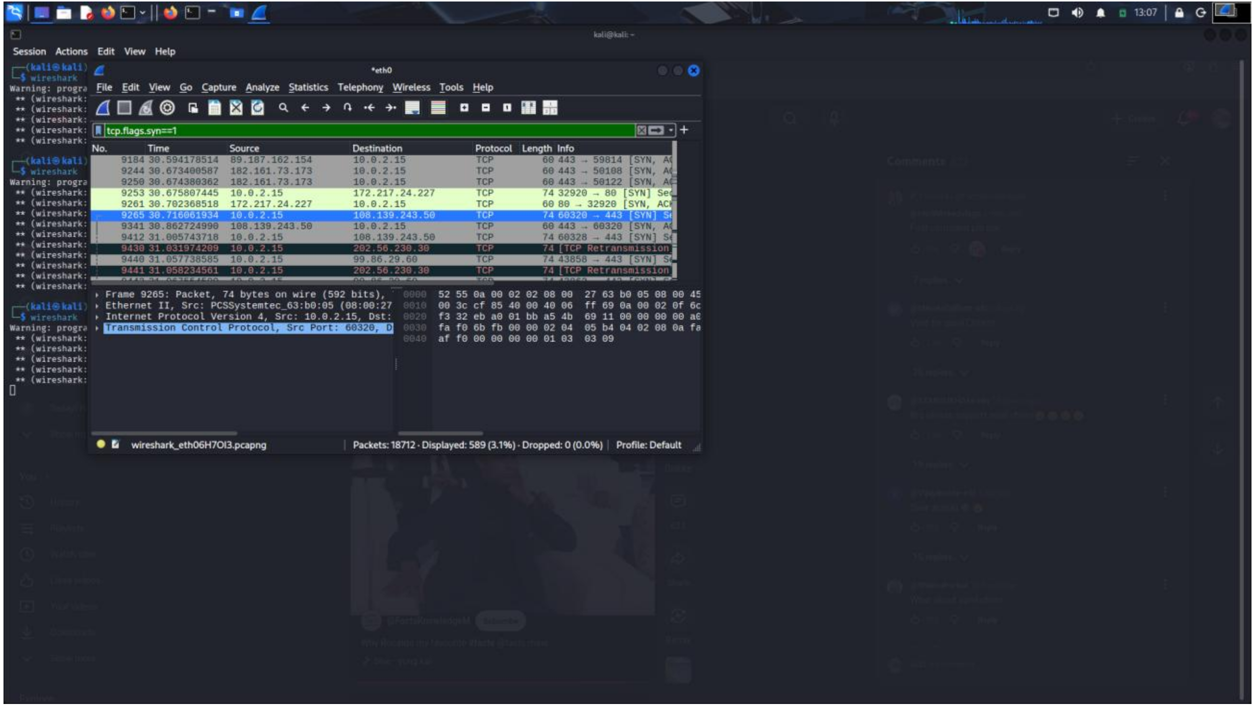
Syn: Boolean | Packets: 18712 · Displayed: 589 (3.1%) · Dropped: 0 (0.0%) | Profile: Default

---

2.3.4 Suspicious Packet Identification

Repeated SYN packets were identified, indicating potential scanning behavior.

📷 **INSERT SCREENSHOT HERE**
☞ *Suspicious TCP SYN packets*



```
tcp.flags.syn==1
No.    Time          Source           Destination      Protocol Length Info
  9184 30.594178514  89.187.162.154   10.0.2.15        TCP      60 443 → 59814 [SYN, AC
  9244 30.673400587  182.161.73.173   10.0.2.15        TCP      60 443 → 50108 [SYN, AC
  9250 30.674380362  182.161.73.173   10.0.2.15        TCP      60 443 → 50122 [SYN, AC
  9253 30.675807445  10.0.2.15        172.217.24.227   TCP      74 32920 → 80 [SYN] Seq
  9261 30.702368518  172.217.24.227   10.0.2.15        TCP      60 80 → 32920 [SYN, ACK
  9265 30.716061934  10.0.2.15        108.139.243.50   TCP      74 60320 → 443 [SYN] Se
  9341 30.862724990  108.139.243.50   10.0.2.15        TCP      60 443 → 60320 [SYN, AC
  9412 31.005743718  10.0.2.15        108.139.243.50   TCP      74 60328 → 443 [SYN] Se
  9430 31.031974209  10.0.2.15        202.56.230.30    TCP      74 [TCP Retransmission
  9440 31.057738585  10.0.2.15        99.86.29.60      TCP      74 43858 → 443 [SYN] Se
  9441 31.058234561  10.0.2.15        202.56.230.30    TCP      74 [TCP Retransmission

▸ Frame 9265: Packet, 74 bytes on wire (592 bits),    0000  52 55 0a 00 02 02 08 00  27 63 b0 05 08 00 45
▸ Ethernet II, Src: PCSSystemtec_63:b0:05 (08:00:27   0010  00 3c cf 85 40 00 40 06  ff 69 0a 00 02 0f 6c
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst:   0020  f3 32 eb a0 01 bb a5 4b  69 11 00 00 00 00 a0
▸ Transmission Control Protocol, Src Port: 60320, D   0030  fa f0 6b fb 00 00 02 04  05 b4 04 02 08 0a fa
                                                      0040  af f0 00 00 00 00 01 03  03 09

wireshark_eth06H7OI3.pcapng | Packets: 18712 · Displayed: 589 (3.1%) · Dropped: 0 (0.0%) | Profile: Default
```

kali@kali: ~
Session Actions Edit View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
13:07

---

3. NMAP SCANNING & RESULTS

3.1 Objective

To perform reconnaissance and identify open ports, services, and vulnerabilities on a target system in a lab environment.

3.2 Scans Performed

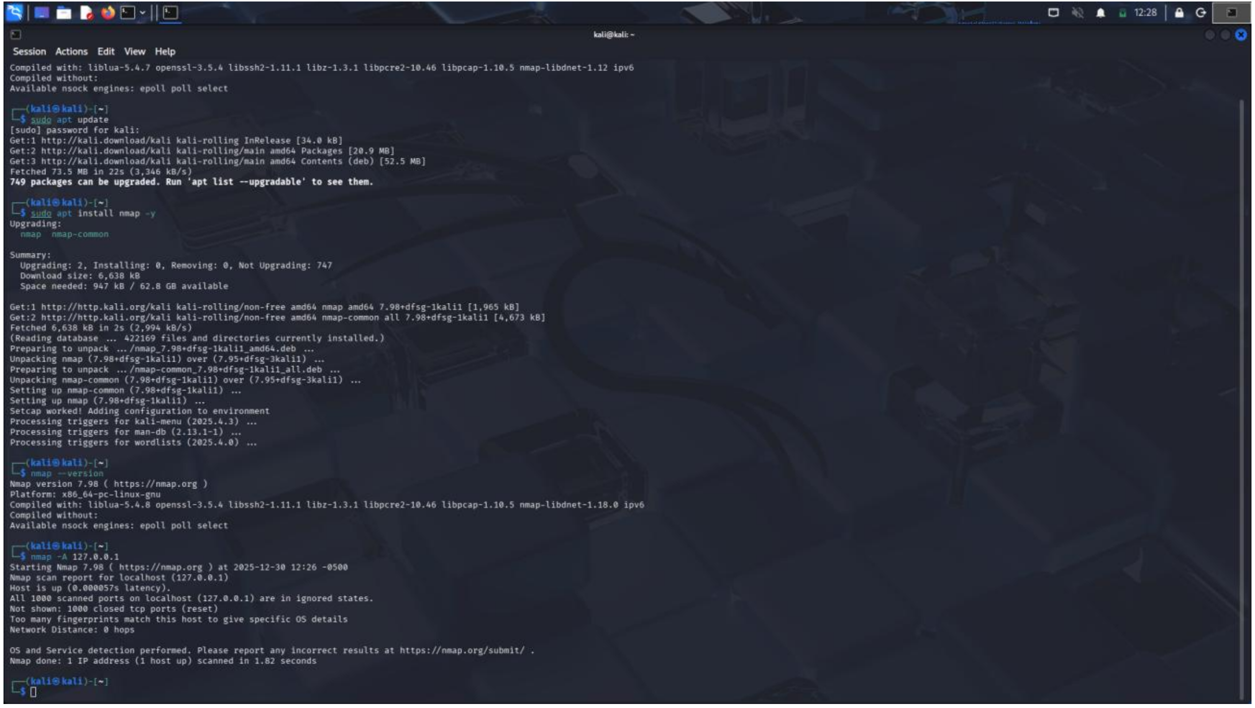
3.2.1 Full Scan

Command used:

```
nmap -A <target>
```

📷 INSERT SCREENSHOT HERE

☞ *Full scan output*



```
Compiled with: liblua-5.4.7 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5 MB]
Fetched 73.5 MB in 22s (3,346 kB/s)
749 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap -y
Upgrading:
  nmap  nmap-common

Summary:
  Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 747
  Download size: 6,638 kB
  Space needed: 947 kB / 62.8 GB available

Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.98+dfsg-1kali1 [1,965 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.98+dfsg-1kali1 [4,673 kB]
Fetched 6,638 kB in 2s (2,994 kB/s)
(Reading database ... 422169 files and directories currently installed.)
Preparing to unpack .../nmap_7.98+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Preparing to unpack .../nmap-common_7.98+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Setting up nmap-common (7.98+dfsg-1kali1) ...
Setting up nmap (7.98+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for wordlists (2025.4.0) ...

┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap -A 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:26 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 1.82 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

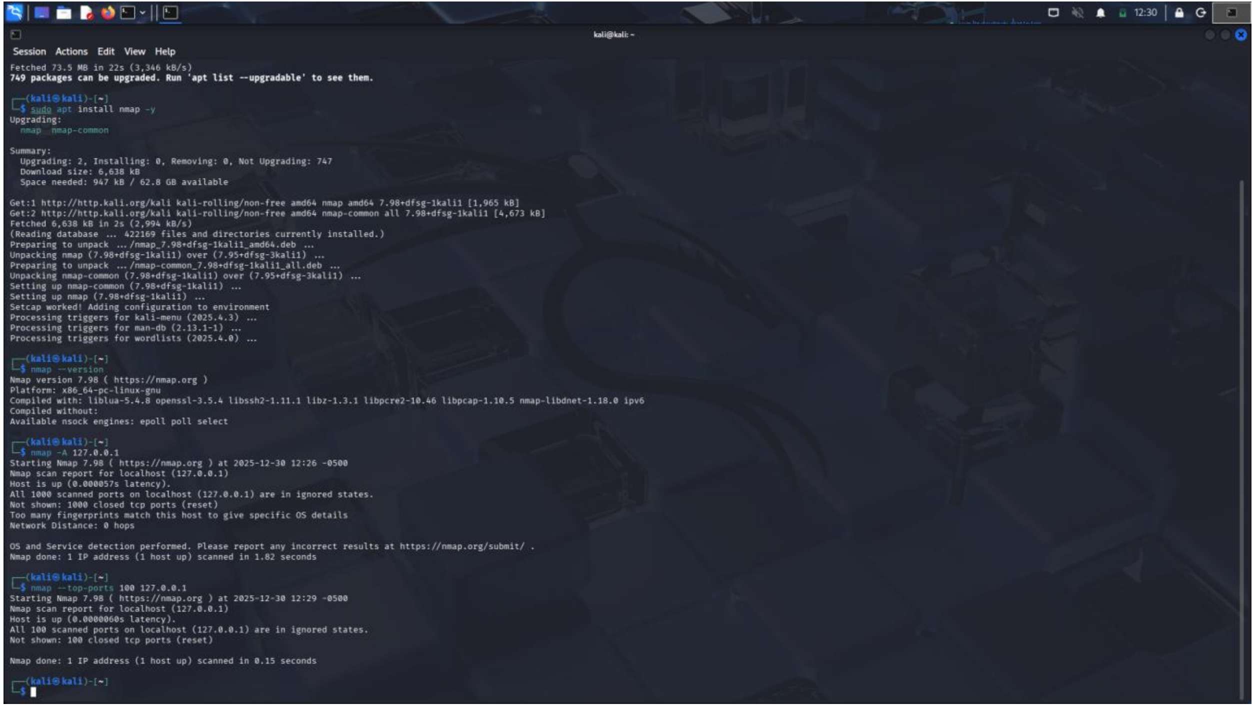
3.2.2 Top Ports Scan

Command used:

```
nmap --top-ports 100 <target>
```

📷 INSERT SCREENSHOT HERE

☞ *Top ports scan output*



```
Fetched 73.5 MB in 22s (3,346 kB/s)
749 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap -y
Upgrading:
  nmap  nmap-common

Summary:
  Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 747
  Download size: 6,638 kB
  Space needed: 947 kB / 62.8 GB available

Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.98+dfsg-1kali1 [1,965 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.98+dfsg-1kali1 [4,673 kB]
Fetched 6,638 kB in 2s (2,994 kB/s)
(Reading database ... 422169 files and directories currently installed.)
Preparing to unpack .../nmap_7.98+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Preparing to unpack .../nmap-common_7.98+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Setting up nmap-common (7.98+dfsg-1kali1) ...
Setting up nmap (7.98+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for wordlists (2025.4.0) ...

┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap -A 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:26 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 1.82 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --top-ports 100 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:29 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
All 100 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 100 closed tcp ports (reset)

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

┌──(kali㉿kali)-[~]
└─$ 
```

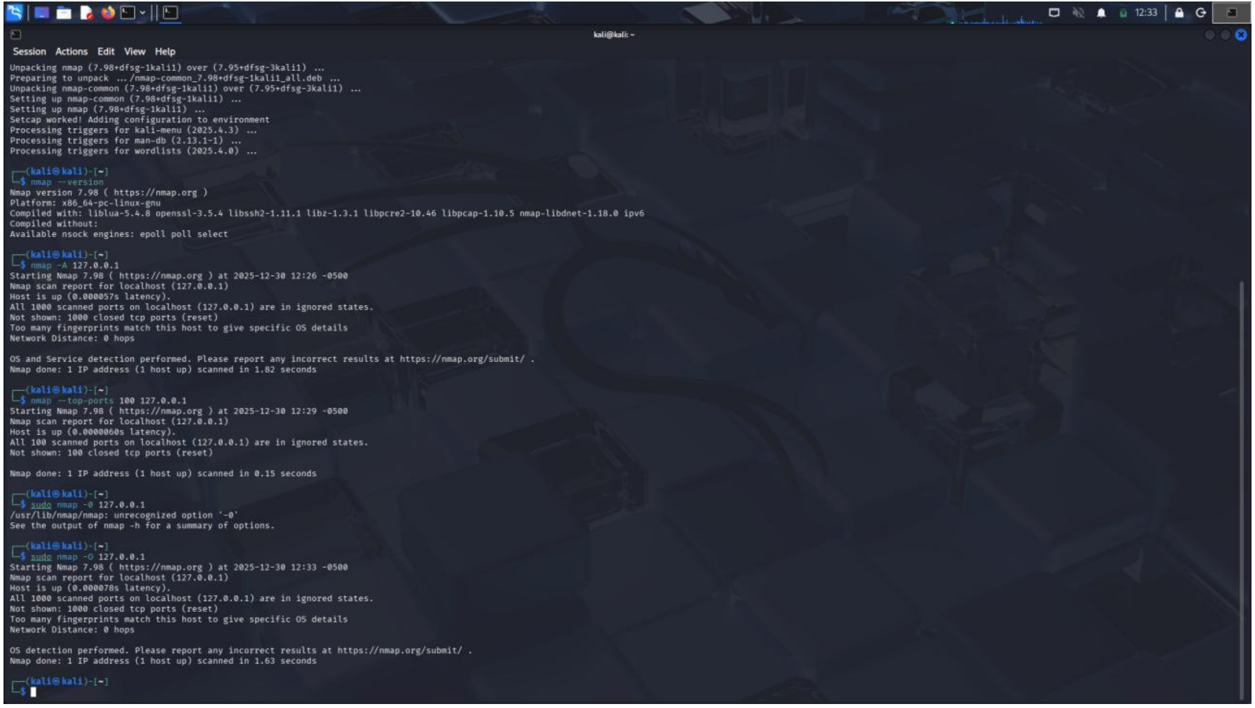
3.2.3 OS Detection

Command used:

```
nmap -O <target>
```

📷 INSERT SCREENSHOT HERE

☞ *OS detection output*



```
Unpacking nmap (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Preparing to unpack .../nmap-common_7.98+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.98+dfsg-1kali1) over (7.95+dfsg-3kali1) ...
Setting up nmap-common (7.98+dfsg-1kali1) ...
Setting up nmap (7.98+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for wordlists (2025.4.0) ...

┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap -A 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:26 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 1.82 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --top-ports 100 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:29 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
All 100 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 100 closed tcp ports (reset)

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

┌──(kali㉿kali)-[~]
└─$ sudo nmap -0 127.0.0.1
/usr/lib/nmap/nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:33 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000078s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
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 1.63 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

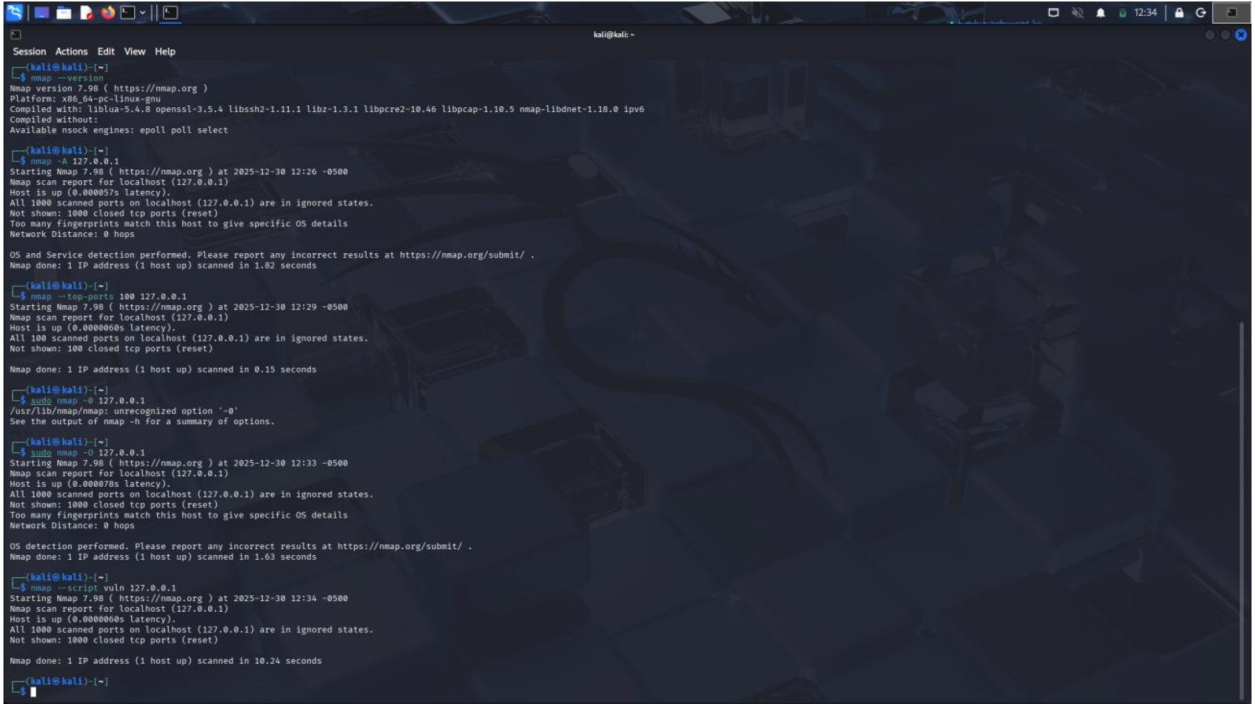
3.2.4 Vulnerability Script Scan

Command used:

```
nmap --script vuln <target>
```

📷 **INSERT SCREENSHOT HERE**

☞ *Vulnerability scan output*



```
┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.5.4 libssh2-1.11.1 libz-1.3.1 libpcre2-10.46 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ nmap -A 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:26 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000057s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

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 1.82 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --top-ports 100 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:29 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
All 100 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 100 closed tcp ports (reset)

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

┌──(kali㉿kali)-[~]
└─$ sudo nmap -0 127.0.0.1
/usr/lib/nmap/nmap: unrecognized option '-0'
See the output of nmap -h for a summary of options.

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:33 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000078s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
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 1.63 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 127.0.0.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-30 12:34 -0500
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 10.24 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

3.3 Result Summary

- Target system was reachable.
- No critical vulnerabilities were detected.
- Most ports were closed or filtered.

---

4. PYTHON PORT SCANNER TOOL

4.1 Objective

To design and implement a custom cybersecurity tool to understand basic reconnaissance techniques.

4.2 Tool Description

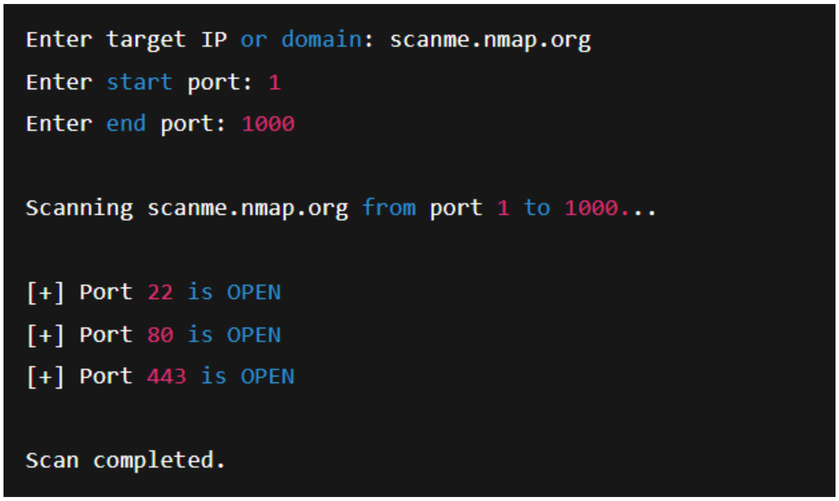
A Python-based Port Scanner was developed using socket programming to scan a target system and identify open TCP ports.

4.3 How the Tool Works

- Accepts target IP/domain and port range.
- Attempts TCP connections.
- Displays open ports in terminal output.

4.4 Tool Output

📷 INSERT SCREENSHOT HERE
☞ *Port scanner output screenshot*
Screenshot name:



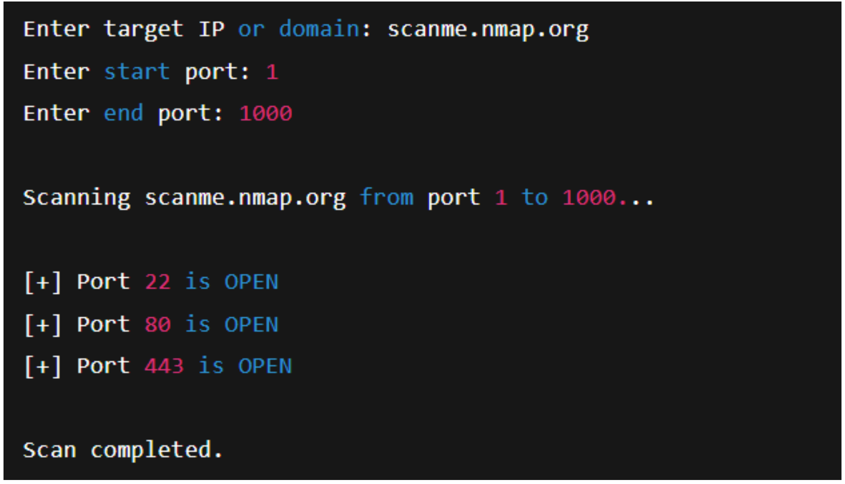
```
Enter target IP or domain: scanme.nmap.org
Enter start port: 1
Enter end port: 1000

Scanning scanme.nmap.org from port 1 to 1000...

[+] Port 22 is OPEN
[+] Port 80 is OPEN
[+] Port 443 is OPEN

Scan completed.
```

📷 INSERT SCREENSHOT HERE (optional)
☞ *Second output screenshot*



```
Enter target IP or domain: scanme.nmap.org
Enter start port: 1
Enter end port: 1000

Scanning scanme.nmap.org from port 1 to 1000...

[+] Port 22 is OPEN
[+] Port 80 is OPEN
[+] Port 443 is OPEN

Scan completed.
```

5. LEARNING OUTCOMES

- Understood packet-level network communication.
- Learned reconnaissance and scanning techniques.
- Gained experience with Wireshark and Nmap.
- Built a custom cybersecurity tool using Python.
- Developed SOC and network security fundamentals.

6. CONCLUSION

This final report demonstrates practical experience in cybersecurity tools and techniques.
By analyzing network traffic, performing reconnaissance, and developing a Python-based Port Scanner, I gained hands-on exposure to real-world cybersecurity workflows.