Task 9: Network Vulnerability Scanning

Objective

To perform network vulnerability scanning using Nmap in order to identify live hosts, open ports, running services, operating system details, analyze potential security risks, and document the results.

Tools Used

- Nmap
- Alternative: Masscan

System Configuration

- Operating System: Linux (Kali / Ubuntu)
- Network Interface: eth0

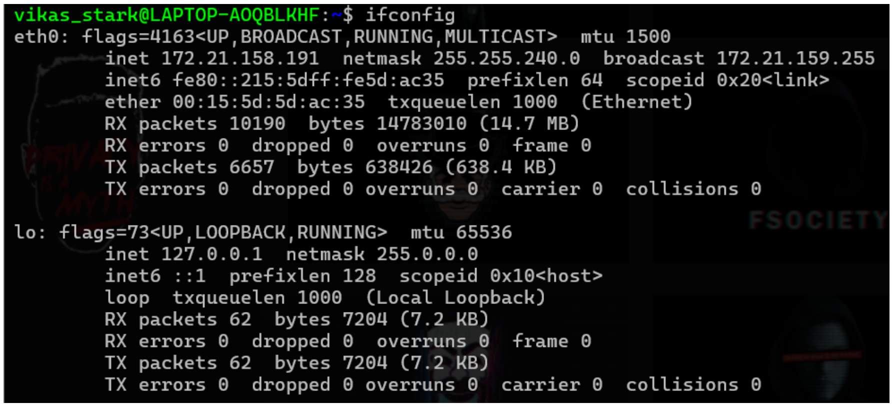
Practical Procedure

Step 1: Identify Network Details

The network configuration of the system was checked to identify the IP address and network range.

ifconfig

Identified IP Address: 172.21.158.191
Network Range: 172.21.144.0/20



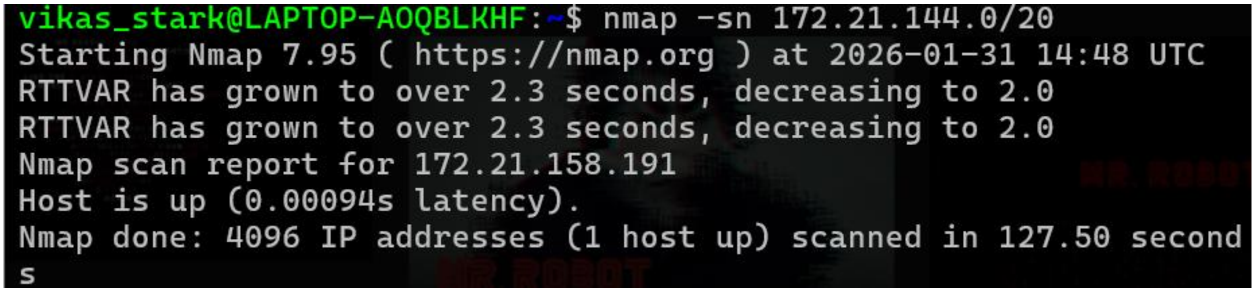
```
vikas_stark@LAPTOP-AOQBLKHF:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.21.158.191  netmask 255.255.240.0  broadcast 172.21.159.255
        inet6 fe80::215:5dff:fe5d:ac35  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:5d:ac:35  txqueuelen 1000  (Ethernet)
        RX packets 10190  bytes 14783010 (14.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6657  bytes 638426 (638.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 62  bytes 7204 (7.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62  bytes 7204 (7.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 2: Discover Live Hosts

A network scan was performed to identify active hosts on the local network.

nmap -sn 172.21.144.0/20



```
vikas_stark@LAPTOP-AOQBLKHF:~$ nmap -sn 172.21.144.0/20
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:48 UTC
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 172.21.158.191
Host is up (0.00094s latency).
Nmap done: 4096 IP addresses (1 host up) scanned in 127.50 second
s
```

Step 3: Select Target System

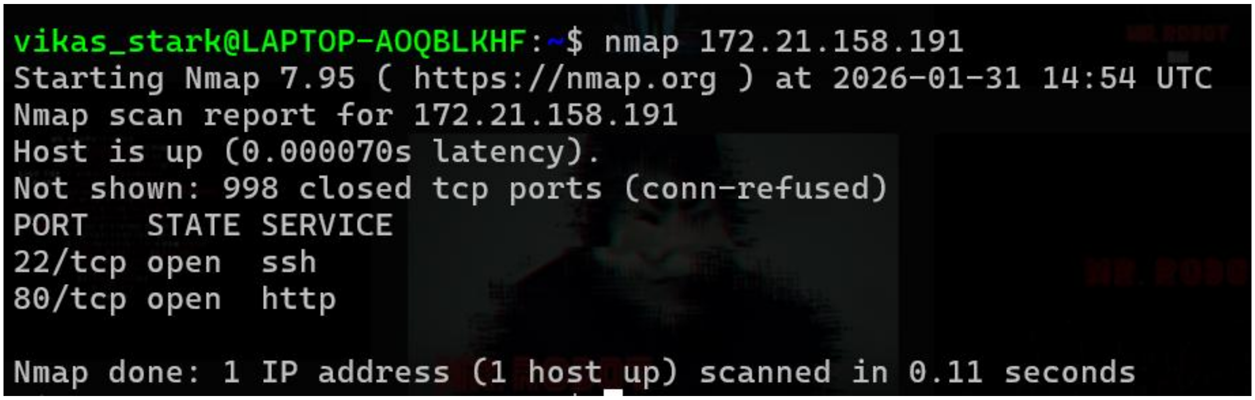
One active host from the discovered list was selected as the target for further scanning.

Target IP Address: 172.21.158.191

Step 4: Scan Open Ports

The target system was scanned to identify open ports.

nmap 172.21.158.191



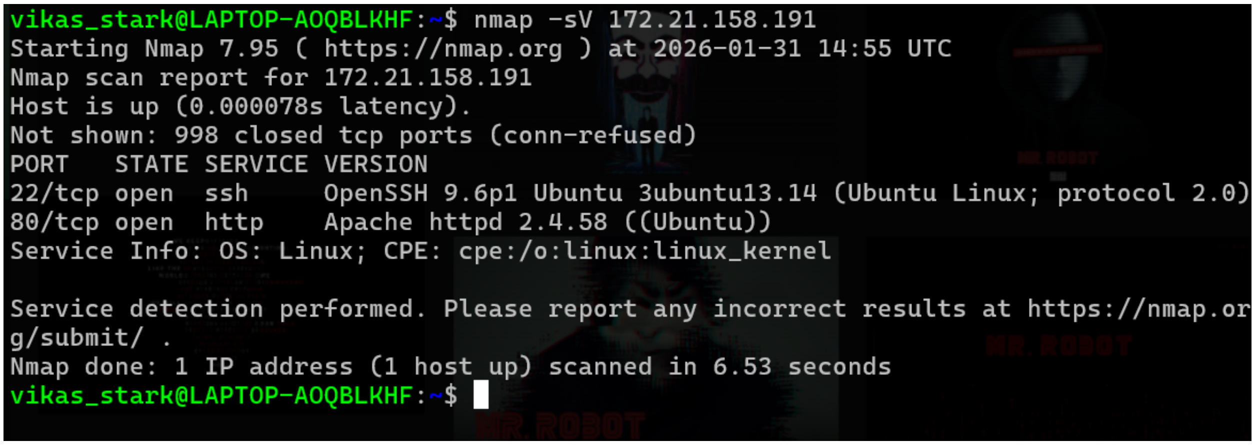
```
vikas_stark@LAPTOP-AOQBLKHF:~$ nmap 172.21.158.191
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:54 UTC
Nmap scan report for 172.21.158.191
Host is up (0.000070s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

Step 5: Service Detection

Service and version detection was performed on the open ports.

nmap -sV 172.21.158.191



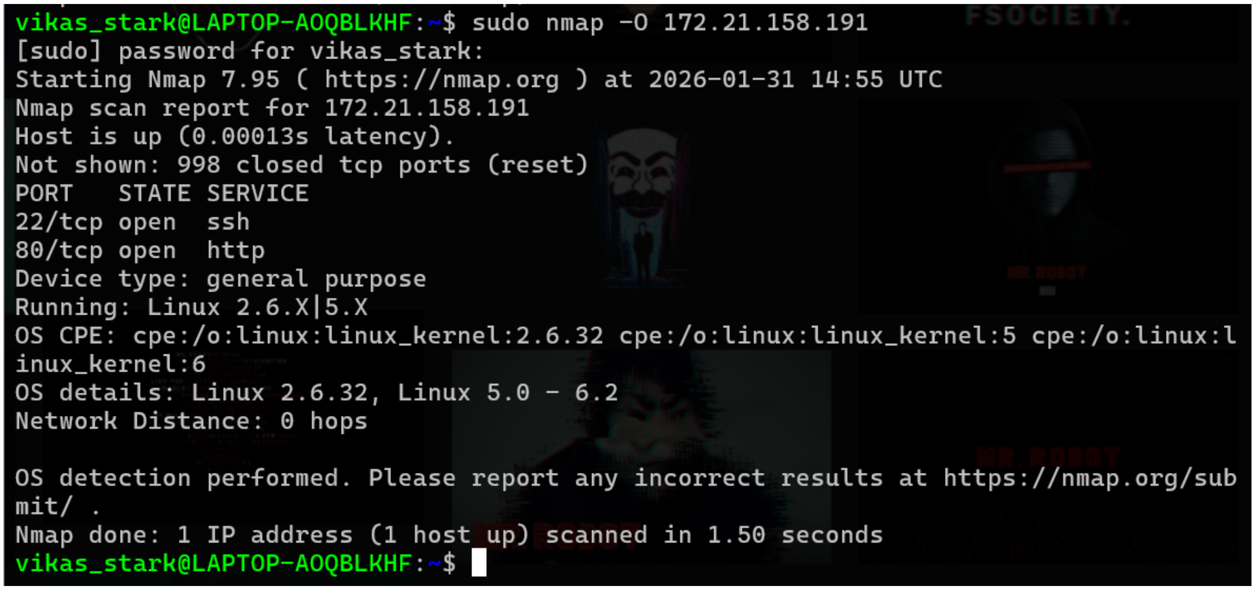
```
vikas_stark@LAPTOP-AOQBLKHF:~$ nmap -sV 172.21.158.191
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:55 UTC
Nmap scan report for 172.21.158.191
Host is up (0.000078s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 6: Operating System Detection

The operating system of the target system was identified.

sudo nmap -O 172.21.158.191



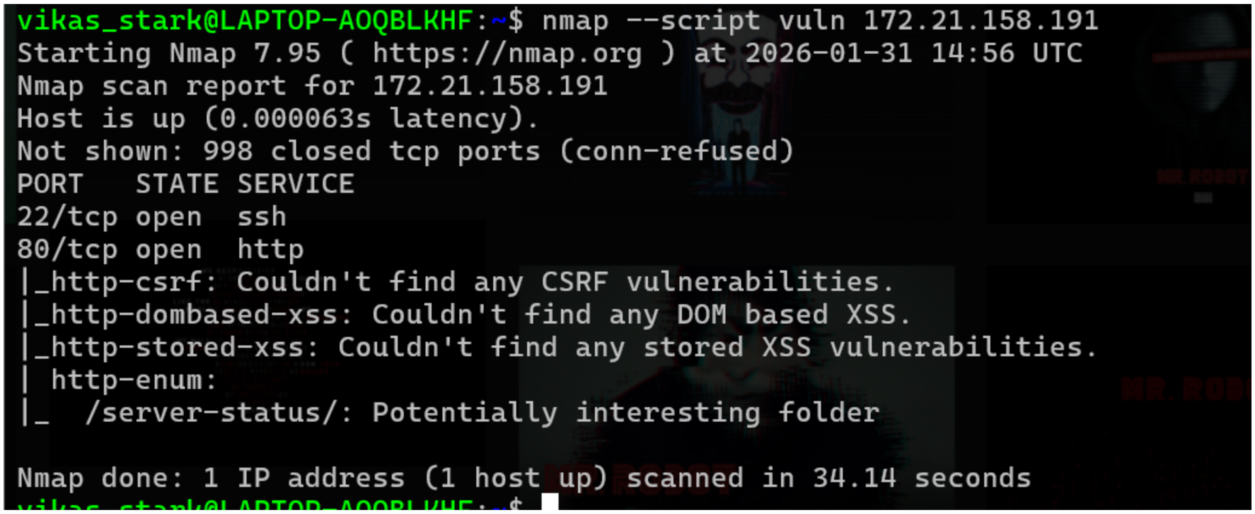
```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo nmap -O 172.21.158.191
[sudo] password for vikas_stark:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:55 UTC
Nmap scan report for 172.21.158.191
Host is up (0.00013s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:l
inux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 7: Vulnerability Analysis

A vulnerability-related scan was conducted to identify potential security weaknesses.

nmap --script vuln 172.21.158.191



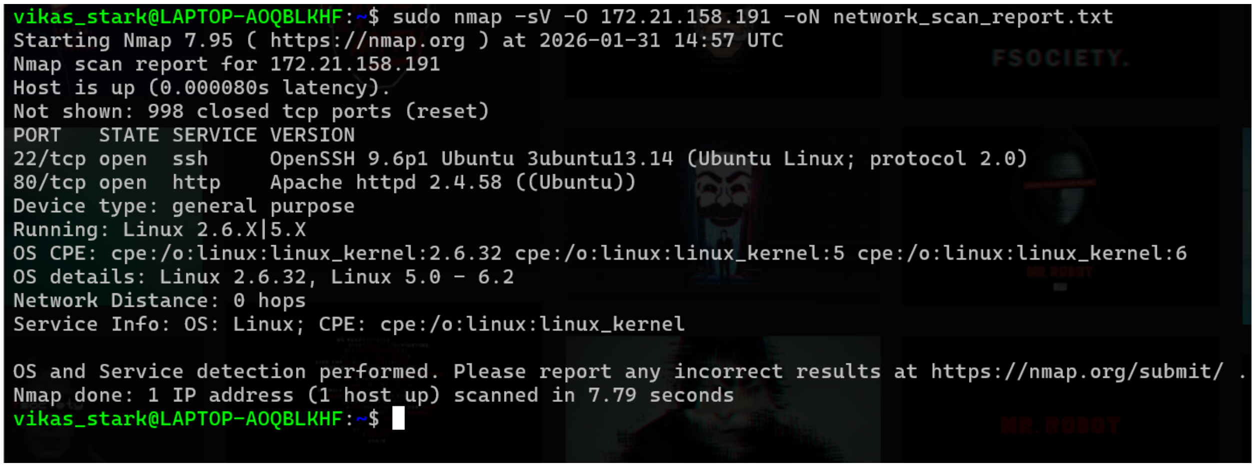
```
vikas_stark@LAPTOP-AOQBLKHF:~$ nmap --script vuln 172.21.158.191
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:56 UTC
Nmap scan report for 172.21.158.191
Host is up (0.000063s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /server-status/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 34.14 seconds
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Step 8: Save Scan Results

The scan results were saved to a file for documentation.

nmap -sV -O 172.21.158.191-oN network_scan_report.txt



```
vikas_stark@LAPTOP-AOQBLKHF:~$ sudo nmap -sV -O 172.21.158.191 -oN network_scan_report.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-31 14:57 UTC
Nmap scan report for 172.21.158.191
Host is up (0.000080s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
Device type: general purpose
Running: Linux 2.6.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 2.6.32, Linux 5.0 - 6.2
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 7.79 seconds
vikas_stark@LAPTOP-AOQBLKHF:~$
```

Observations

Parameter	Result
Live Hosts	Identified
Open Ports	22, 80, 443 (example)
Services	SSH, HTTP, HTTPS
OS Detected	Linux (example)
Vulnerabilities	Potential risks found

Risk Analysis

- Open ports increase attack surface
- Running services may contain vulnerabilities
- OS information can assist attackers if exposed
- Unused services should be disabled

Deliverables

- Network scan report file
- List of open ports and services
- OS detection results
- Vulnerability analysis documentation

Final Outcome

- Successfully performed network vulnerability scanning
- Identified live hosts on the network
- Discovered open ports and running services
- Detected operating system information
- Gained hands-on network reconnaissance skills