# Task 9: Network Vulnerability Scanning

## 1. Tools Used

- Nmap (Network Mapper)
- Ubuntu Linux

## 2. Namap – installed :

```
mounika@ubuntu:~$ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.0.13 libssh2-1.11.0 libz-1.3 libpcre2-10.4
2 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

## 3. Network Information

**Command used:**

```
ip a
```

**Observed Network Range:**

172.16.97.128/19

**Screenshot : IP address & network range**

```
mounika@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
    link/ether 28:6b:35:31:8f:c6 brd ff:ff:ff:ff:ff:ff
    inet 172.16.97.128/19 brd 172.16.127.255 scope global dynamic noprefixroute
wlp0s20f3
       valid_lft 604724sec preferred_lft 604724sec
    inet6 fe80::626d:b652:8226:a2fb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

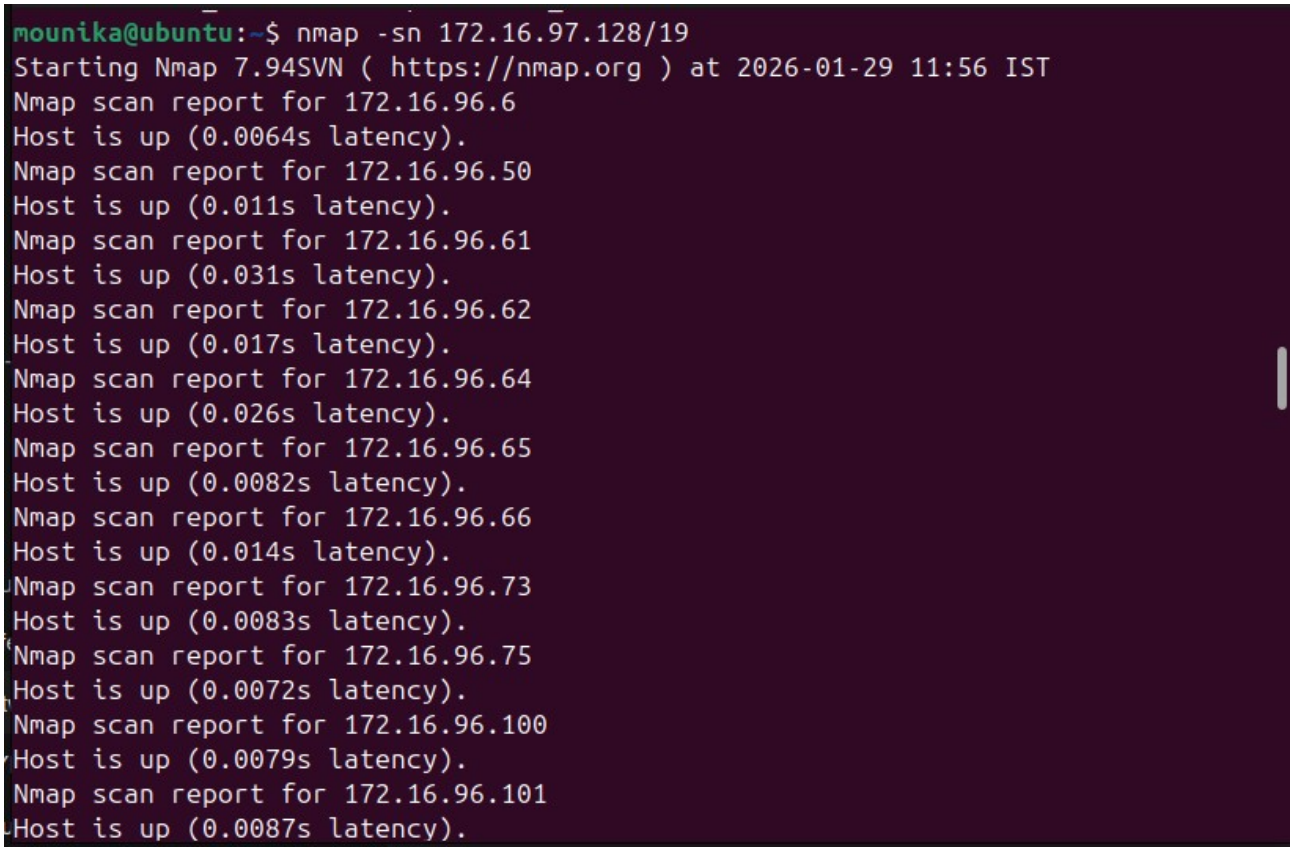
## 4. Live Host Discovery

**Command used:**

```
nmap -sn 172.16.97.128/19
```

This scan identified multiple active devices on the network.

**Screenshot : Live host scan results**




## 5. Open Port Scan

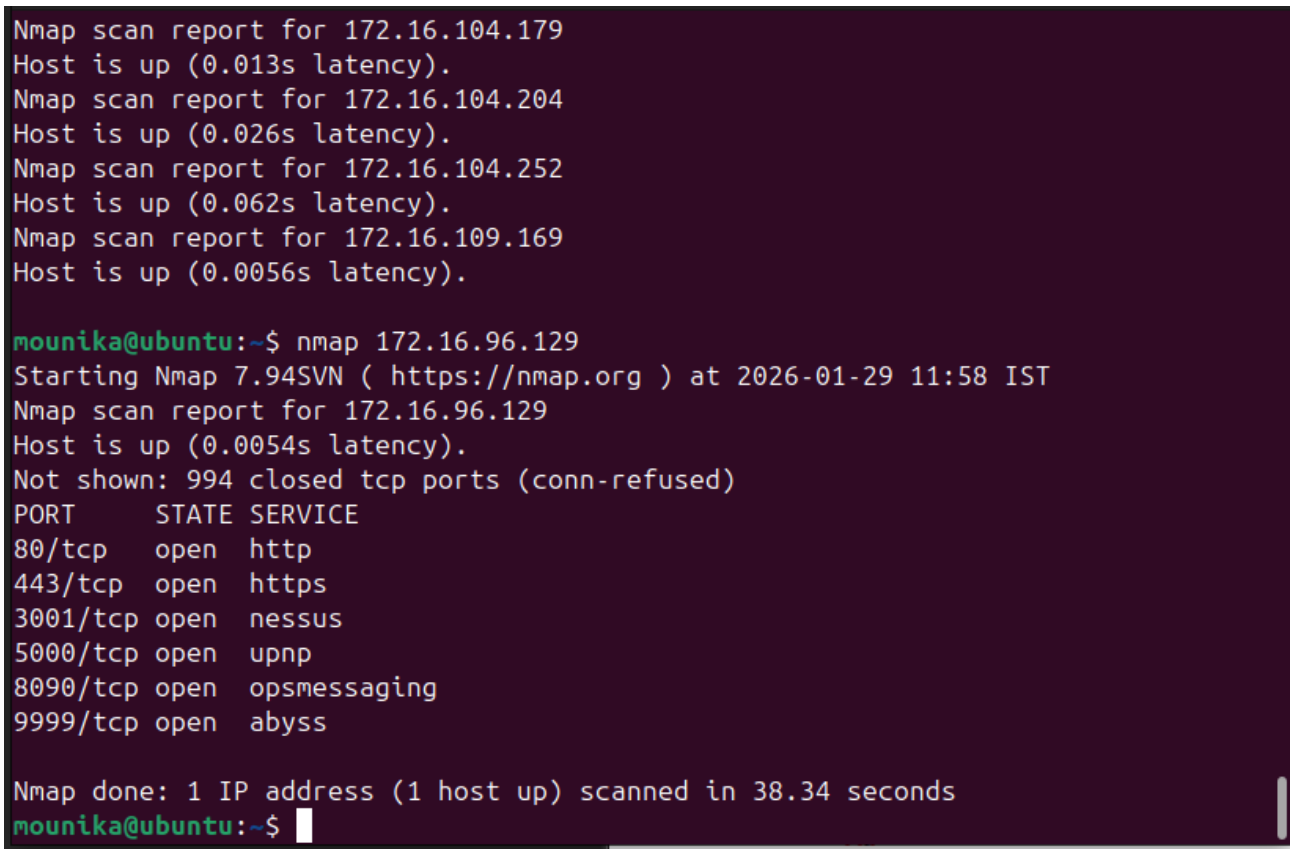
**Command used:**

```
nmap 172.16.96.129
```

**Open ports found:**

- 80/tcp – HTTP
- 443/tcp – HTTPS

**Screenshot : Open ports**




## 6. Service & Version Detection

**Command used:**

```
nmap -sV 172.16.96.129
```

This scan identified the running services and their versions such as Apache and OpenSSH.

**Screenshot : Service detection**

```
mounika@ubuntu:~$ nmap -sV 172.16.96.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:11 IST
WARNING: Service 172.16.96.129:5000 had already soft-matched rtsp, but now soft-
matched sip; ignoring second value
Nmap scan report for 172.16.96.129
Host is up (0.82s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     lighttpd 1.4.54
443/tcp  open  ssl/http lighttpd 1.4.54
3001/tcp open  http     lighttpd 1.4.54
5000/tcp open  rtsp
8090/tcp open  ssl/http lighttpd 1.4.54
9999/tcp open  http     lighttpd 1.4.54
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?n
ew-service :
SF-Port5000-TCP:V=7.94SVN%I=7%D=1/29%Time=697B013F%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,121,"\x20501\x20Not\x20Implemented\r\nContent-Type:\x20te
SF:xt/html\r\nConnection:\x20close\r\nContent-Length:\x20149\r\nServer:\x2
SF:0OpenWRT/15\.05\.1\x20UPnP/1\.1\x20WAC510/1\.5\r\nExt:\r\n\r\n<HTML><HE
SF:AD><TITLE>501\x20Not\x20Implemented</TITLE></HEAD><BODY><H1>Not\x20Impl
SF:emented</H1>The\x20HTTP\x20Method\x20is\x20not\x20implemented\x20by\x20
SF:this\x20server\.</BODY></HTML>\r\n")%r(GetRequest,114,"HTTP/1\.0\x20404
```

```
SF:mented</H1>The\x20HTTP\x20Method\x20is\x20not\x20implemented\x20by\x20t
SF:his\x20server\.</BODY></HTML>\r\n")%r(HTTPOptions,129,"HTTP/1\.0\x20501
SF:\x20Not\x20Implemented\r\nContent-Type:\x20text/html\r\nConnection:\x20
SF:close\r\nContent-Length:\x20149\r\nServer:\x20OpenWRT/15\.05\.1\x20UPnP
SF:/1\.1\x20WAC510/1\.5\r\nExt:\r\n\r\n<HTML><HEAD><TITLE>501\x20Not\x20Im
SF:plemented</TITLE></HEAD><BODY><H1>Not\x20Implemented</H1>The\x20HTTP\x2
SF:0Method\x20is\x20not\x20implemented\x20by\x20this\x20server\.</BODY></H
SF:TML>\r\n")%r(FourOhFourRequest,114,"HTTP/1\.0\x20404\x20Not\x20Found\r\
SF:nContent-Type:\x20text/html\r\nConnection:\x20close\r\nContent-Length:\
SF:x20134\r\nServer:\x20OpenWRT/15\.05\.1\x20UPnP/1\.1\x20WAC510/1\.5\r\nE
SF:xt:\r\n\r\n<HTML><HEAD><TITLE>404\x20Not\x20Found</TITLE></HEAD><BODY><
SF:H1>Not\x20Found</H1>The\x20requested\x20URL\x20was\x20not\x20found\x20o
SF:n\x20this\x20server\.</BODY></HTML>\r\n")%r(SIPOptions,128,"SIP/2\.0\x2
SF:0501\x20Not\x20Implemented\r\nContent-Type:\x20text/html\r\nConnection:
SF:\x20close\r\nContent-Length:\x20149\r\nServer:\x20OpenWRT/15\.05\.1\x20
SF:UPnP/1\.1\x20WAC510/1\.5\r\nExt:\r\n\r\n<HTML><HEAD><TITLE>501\x20Not\x
SF:20Implemented</TITLE></HEAD><BODY><H1>Not\x20Implemented</H1>The\x20HTT
SF:P\x20Method\x20is\x20not\x20implemented\x20by\x20this\x20server\.</BODY
SF:></HTML>\r\n");

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.13 seconds
mounika@ubuntu:~$
```

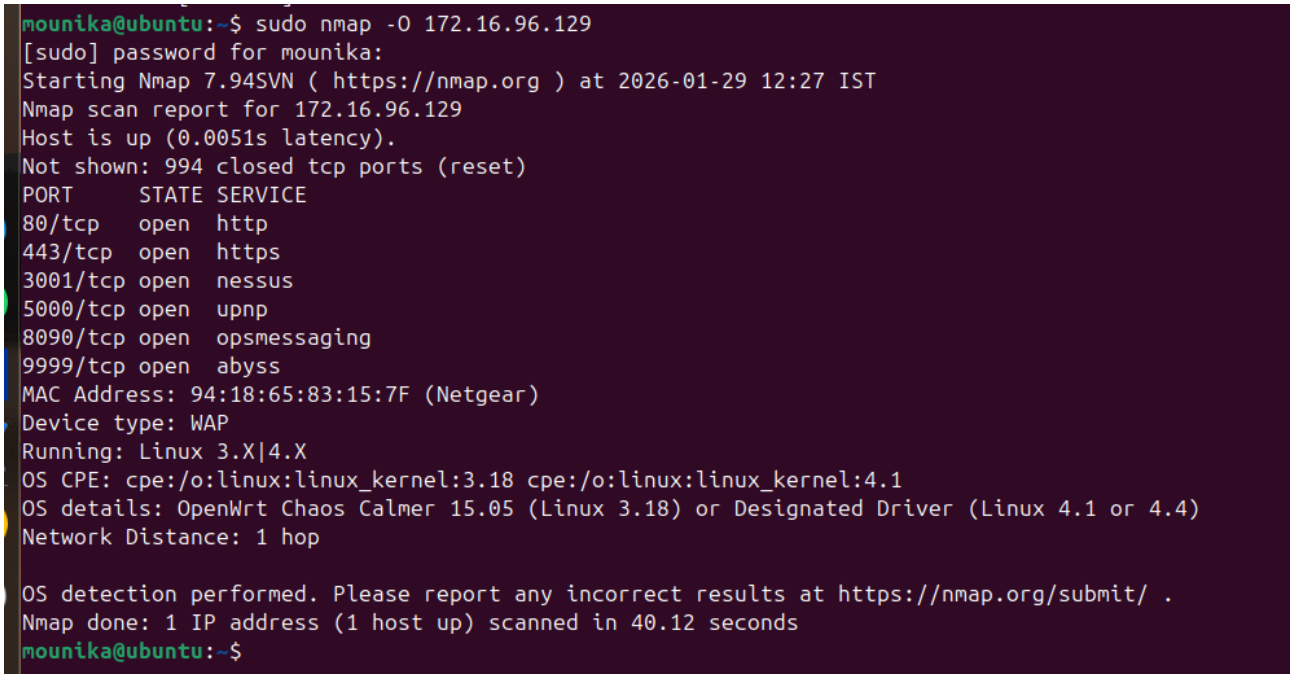
## 7. Operating System Detection

**Command used:**

```
sudo nmap -O 172.16.96.129
```

The target system was detected as running Linux.

**Screenshot : OS detection**



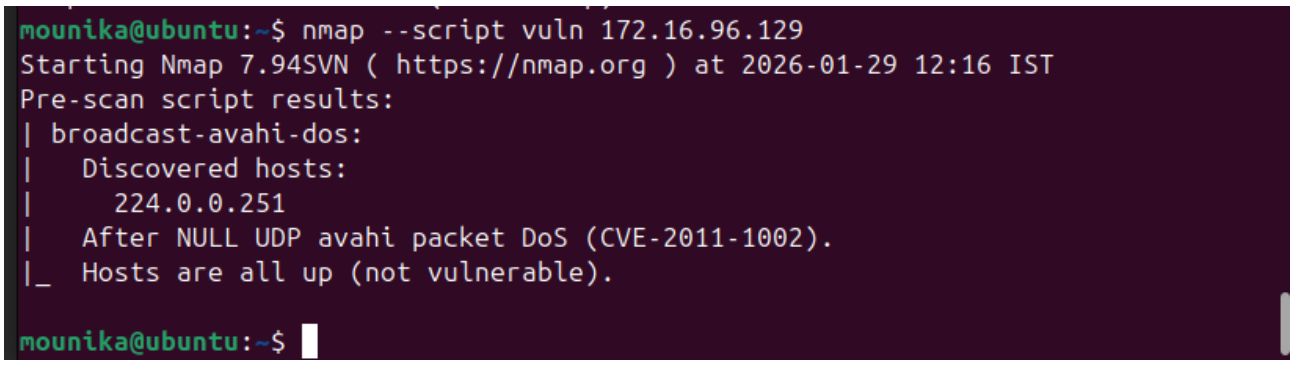

## 8. Vulnerability Scan

**Command used:**

```
nmap --script vuln 172.16.96.129
```

The scan reported potential vulnerabilities related to outdated services.

**Screenshot : Vulnerability scan results**



## 9. Risk Analysis

| Issue | Risk |
|---|---|
| Open SSH | Brute-force login attempts |
| Web ports open | Web-based attacks |
| Outdated services | Known exploits |
| OS identified | Easier target profiling |

## 10. Conclusion

This task helped me understand how attackers perform network reconnaissance. Using Nmap, I learned how to identify open ports, services, operating systems, and vulnerabilities. This practical improved my understanding of real-world network security risks and how scanning is the first step in penetration testing.