

CYBERSECURITY INTERNSHIP

Organization name: Elevate labs

Student Name: Radhika Lakshmi. Teeramdasu

University: Aditya University

Domain: Cybersecurity

Duration: 1st January 2026 to 30th April 2026

TASK-9: Network Vulnerability Scanning

Network vulnerability scanning is the process of identifying security weaknesses in networked systems by scanning hosts, open ports, running services, operating systems, and known vulnerabilities using automated tools. It helps organizations discover potential entry points before attackers can exploit them.

- **Scan Local Network:**

Local network scanning means identifying all active devices (hosts) connected to the same network. This helps understand what systems are reachable and could be potential attack targets.

1. To find IP address – **ipconfig** (windows), **ifcongif** (linux)
2. To scan the local network – **nmap -sn (ip address).0/24**

```
radhika@Radhika: ~ radhika@Radhika: ~
(radhika@Radhika) [~]
$ nmap 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 21:06 EST
Stats: 0:00:14 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 5 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.56.1
Host is up (0.0010s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 0A:00:27:00:00:10 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:D0:C0:95 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.105
```

```
radhika@Radhika: ~ radhika@Radhika: ~
Session Actions Edit View Help
radhika@Radhika: ~ radhika@Radhika: ~
Nmap scan report for 192.168.56.105
Host is up (0.010s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrqdp
MAC Address: 08:00:27:DD:C7:7E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.106
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:9B:B0:1F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.107
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
```

```
radhika@Radhika: ~ radhika@Radhika: ~
Session Actions Edit View Help
radhika@Radhika: ~ radhika@Radhika: ~
Nmap scan report for 192.168.56.106
Host is up (0.00057s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:9B:B0:1F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.107
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
23/tcp     open  telnet
25/tcp     open  smtp
53/tcp     open  domain
80/tcp     open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
512/tcp    open  exec
513/tcp    open  login
514/tcp    open  shell
```

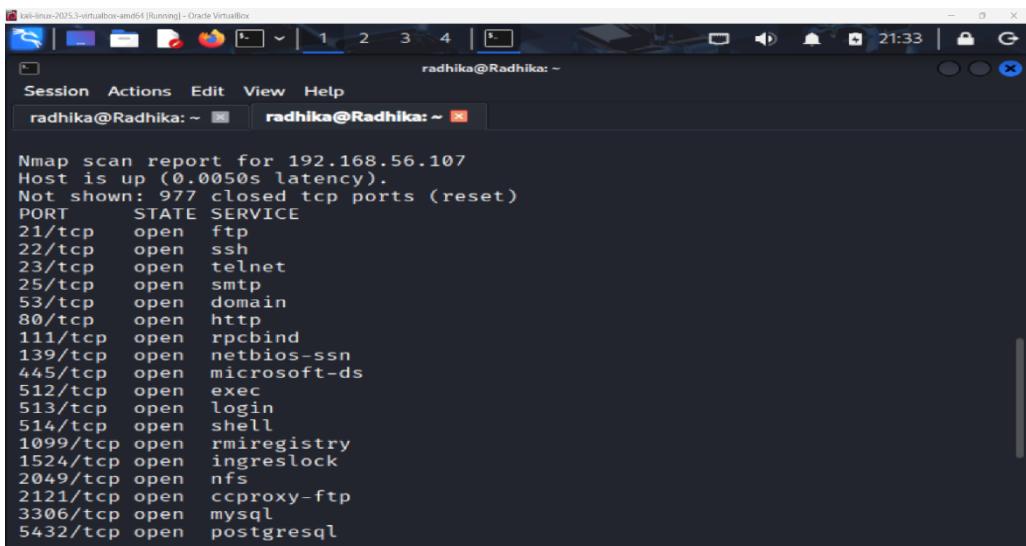
- **Identify open ports:**

Open ports are communication endpoints that accept incoming connections. Identifying them shows which services are accessible from the network.

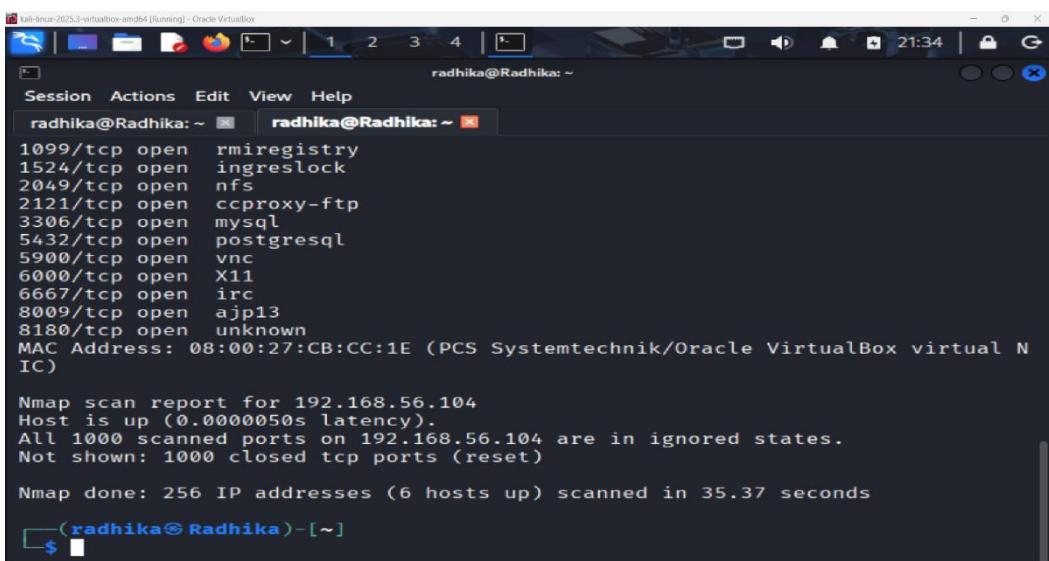
Common ports:

1. 80 – HTTP
2. 443 – HTTPS
3. 22 – SSH
4. 21 – FTP

Open ports can become attack points if poorly secured.



```
Nmap scan report for 192.168.56.107
Host is up (0.0050s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
```

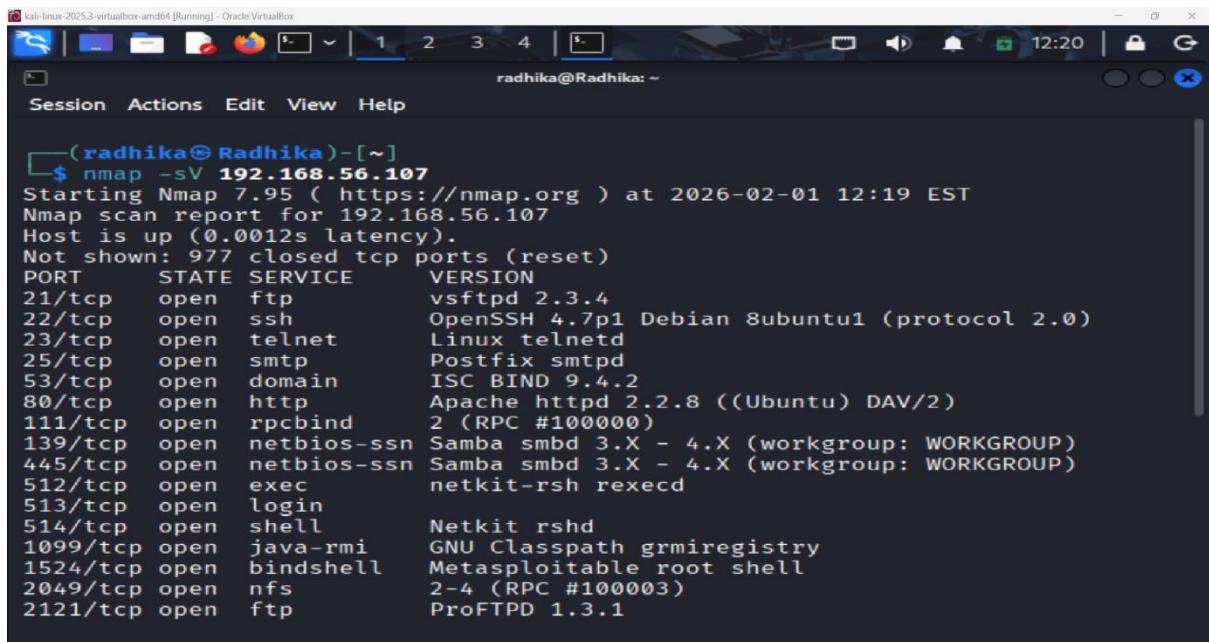


```
Nmap scan report for 192.168.56.104
Host is up (0.0000050s latency).
All 1000 scanned ports on 192.168.56.104 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

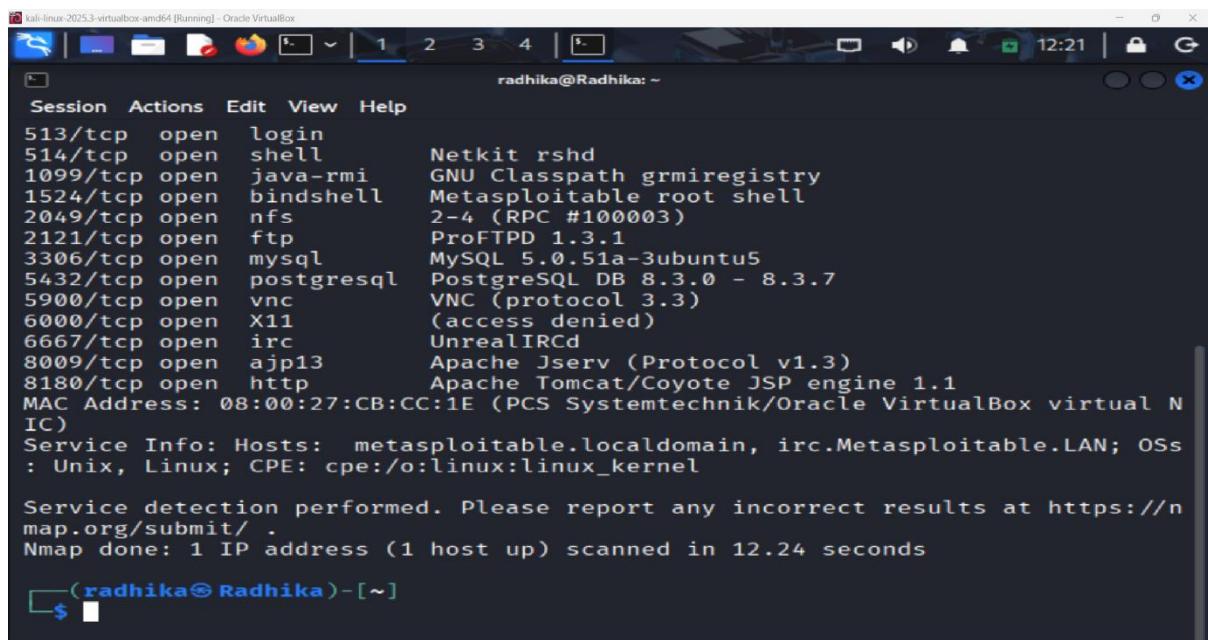
Nmap done: 256 IP addresses (6 hosts up) scanned in 35.37 seconds
```

- Detect Services:

Service detection identifies what application is running on each open port, such as: Apache or Nginx web server, SSH daemon, FTP service. This step helps attackers and defenders understand what software is exposed.



```
(radhika@Radhika)-[~]
$ nmap -sV 192.168.56.107
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 12:19 EST
Nmap scan report for 192.168.56.107
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
```



```
(radhika@Radhika)-[~]
$ nmap -sV 192.168.56.107
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 12:21 EST
Nmap scan report for 192.168.56.107
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
513/tcp   open  login        Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CB:CC:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.24 seconds

(radhika@Radhika)-[~]
```

- **Identify OS:**

OS detection attempts to determine whether the target system is running - Windows, Linux, macOS, Network devices (routers, firewalls). Knowing the OS helps in mapping OS-specific vulnerabilities.

nmap -o (ip address)

```
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs : Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.24 seconds
└─$ █
```

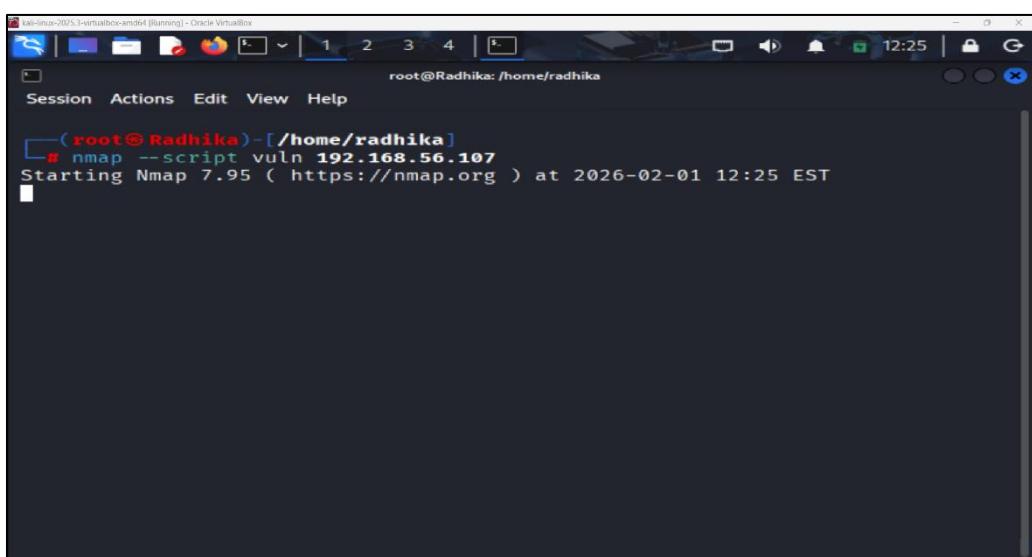
- **Analyze vulnerabilities:**

By combining open ports, services, and OS details, potential vulnerabilities can be inferred, such as:

- Outdated software versions
- Unencrypted services
- Misconfigured services

This step does not exploit, only identifies weaknesses.

nmap --script vuln (target ip address)



The screenshot shows a terminal window titled "Debian-2023-11-01-16:45:45 (Running) - Oracle VM VirtualBox". The window has a dark theme. The command "nmap --script vuln 192.168.56.107" is typed into the terminal, and the output begins with "Starting Nmap 7.95 (https://nmap.org) at 2026-02-01 12:25 EST".

```

root@Radhika: /home/radhika
# nmap --script vuln 192.168.56.107
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 12:25 EST
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.68% done; ETC: 12:26 (0:00:07 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.68% done; ETC: 12:26 (0:00:07 remaining)
Stats: 0:00:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 84.68% done; ETC: 12:26 (0:00:07 remaining)
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 12:27 (0:00:01 remaining)
Nmap scan report for 192.168.56.107
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539  CVE: CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03

```

```

root@Radhika: /home/radhika
Session Actions Edit View Help
/ /admin/cp.jsp: Possible admin folder
/ /admin/account.jsp: Possible admin folder
/ /admin/admin_login.jsp: Possible admin folder
/ /admin/adminLogin.jsp: Possible admin folder
/ /manager/html/upload: Apache Tomcat (401 Unauthorized)
/ /manager/html: Apache Tomcat (401 Unauthorized)
/ /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
/ /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
/ /admin/jscript/upload.html: Lizard Cart/Remote File upload
/ /webdav/: Potentially interesting folder
MAC Address: 08:00:27:CB:CC:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 323.96 seconds

```

• Document Findings:

All results are recorded in a structured report including:

- Target IP
- Open ports
- Services detected