ELEVATE LABS
TASK 9
Network Vulnerability Scanning

Student Name: Chalumuri Sri Venkata Srinivas

University: Aditya University

Domain: Cybersecurity

Duration: 1st January 2026 to 30th April 2026

1. Scan local network.

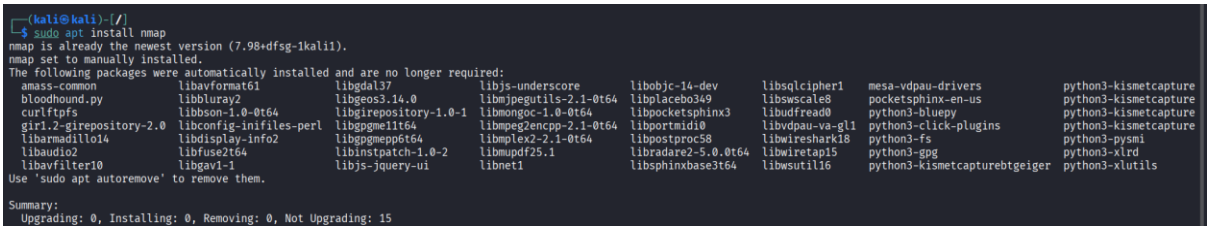
Local network scanning means discovering devices (hosts) connected to the same network (LAN) as your system.

Why we scan a local network

- Identify **connected devices** (PCs, mobiles, routers, servers)
- Find **live IP addresses**
- Detect **open ports & services**
- Used in:
    - Network administration
    - Ethical hacking & penetration testing
    - Troubleshooting network issues

Step 1: Install Nmap

sudo apt install nmap



Step 2: Scan for Live Hosts (Ping Scan)

nmap -sn ip address

```
┌──(kali㉿kali)-[/]
└─$ nmap -sn 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:01 -0500
Nmap scan report for 192.168.10.3
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

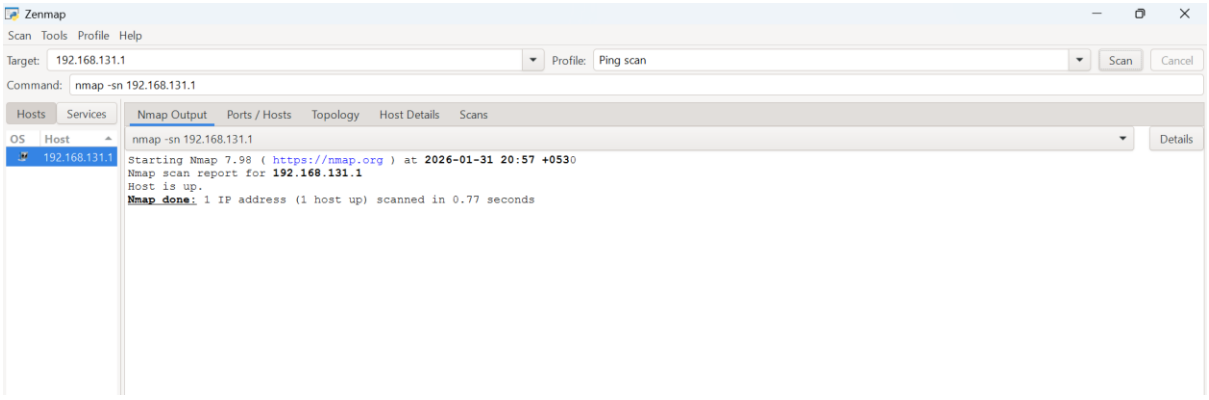
Practical 2: Scan Open Ports on a Specific Host

```
┌──(kali㉿kali)-[/]
└─$ nmap 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:04 -0500
Nmap scan report for 192.168.10.3
Host is up (0.00015s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
```

Practical 3: Scan All Ports (Advanced

```
┌──(kali㉿kali)-[/]
└─$ nmap -p-  192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:05 -0500
Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.15% done; ETC: 10:08 (0:00:33 remaining)
Nmap scan report for 192.168.10.3
Host is up (0.00015s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
```

IN windows ZENMAP



2. Identify open ports

A port is a logical communication endpoint.

Each service listens on a port number.

Why Identify Open Ports?

- Discover running services
- Find attack surface
- First step in penetration testing
- Used in network administration

Step 1: Basic Open Port Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:35 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000039s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
```

Step 2: Scan Specific Ports

nmap -p 22,80,443 ip address

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22,80,443 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:37 -0500
Nmap scan report for 192.168.10.3
Host is up (0.00018s latency).

PORT    STATE    SERVICE
22/tcp  filtered ssh
80/tcp  open     http
443/tcp filtered https
```

Step 3: Scan All Ports

```
┌──(kali㉿kali)-[~]
└─$ nmap -p-  192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:38 -0500
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.47% done; ETC: 10:40 (0:00:52 remaining)
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 86.33% done; ETC: 10:40 (0:00:15 remaining)
Nmap scan report for 192.168.10.3
Host is up (0.000061s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
```

Step 4: Service Version Detection

nmap -Sv

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:41 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
```

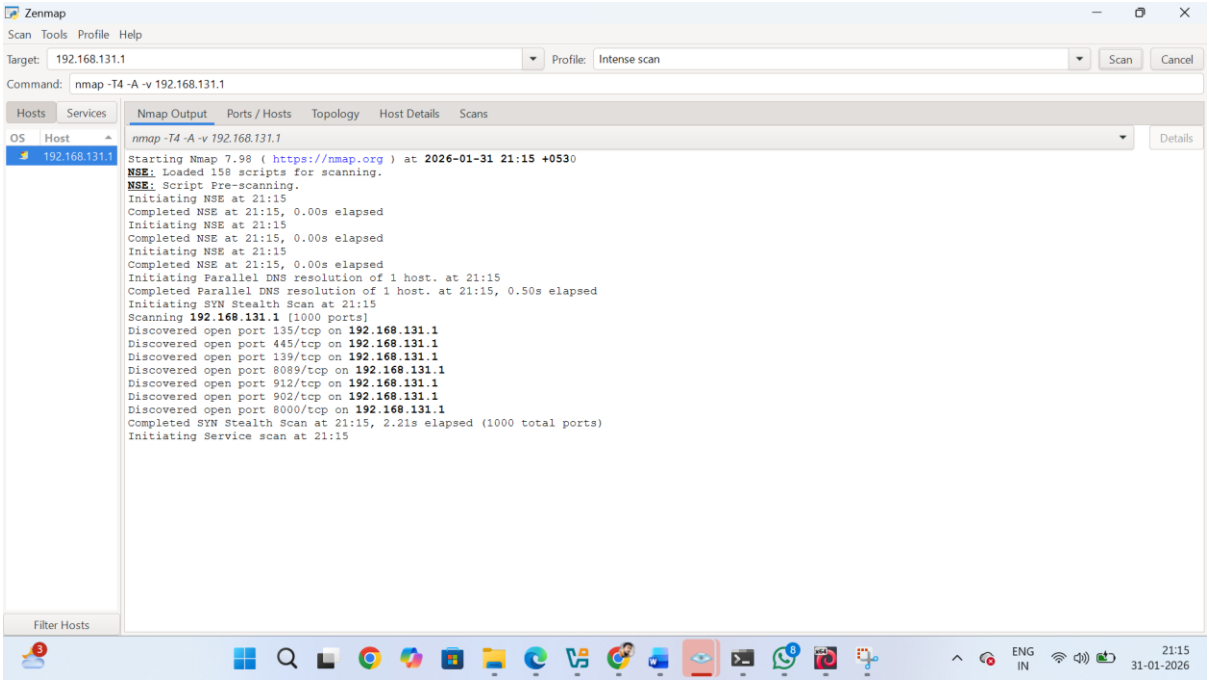
Step 5: Aggressive Scan

nmap -A

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:43 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000083s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))
|_http-server-header: Apache/2.4.66 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
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 16.67 seconds
```

Windows



3. Detect services

Service detection is the process of identifying the exact services and their versions running on open ports of a system. When a port is found open, it only indicates that some application is listening; service detection goes a step further by determining *what* application it is, such as Apache web server, OpenSSH, FTP, or MySQL, and often its version number. Tools like Nmap perform service detection by sending specially crafted probes to open ports and analyzing the responses or banners returned by the target system. This information is very important in network security and ethical hacking because outdated or misconfigured services may contain known vulnerabilities. Service detection helps security professionals and system administrators understand the services exposed on a network, assess potential risks, and plan appropriate security measures or further testing.

Step 1: Identify Target IP
192.168.10.3

Step 2: Basic Service Detection

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:51 -0500
Nmap scan report for 192.168.10.3
Host is up (0.00012s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

Step 3: Service Detection on Specific Ports

nmap -sV -p 22,80,3306

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 22,80,3306 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:52 -0500
Nmap scan report for 192.168.10.3
Host is up (0.00019s latency).

PORT     STATE    SERVICE VERSION
22/tcp   filtered ssh
80/tcp   open     http    Apache httpd 2.4.66 ((Debian))
3306/tcp filtered mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.91 seconds
```

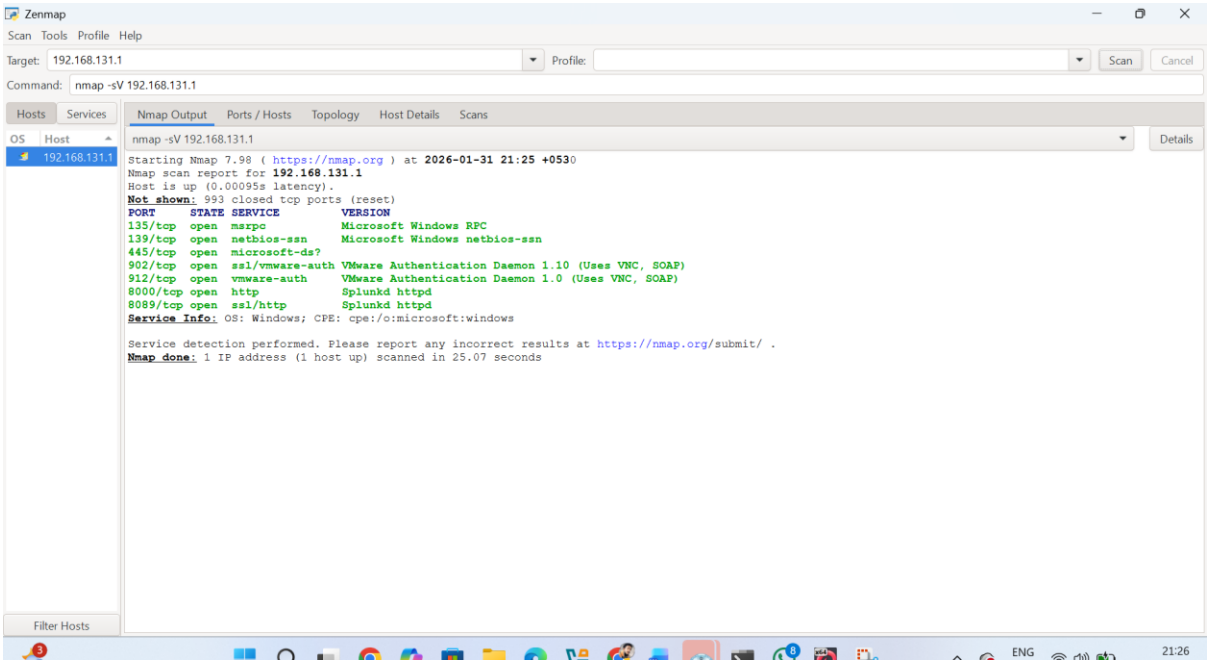
Step 5: Increase Accuracy

nmap -sV --version-intensity 9

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-intensity 9 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 10:54 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000042s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.93 seconds
```

Windows:-



4. Identify OS :-

1. OS identification is also known as OS fingerprinting
2. It detects the type of operating system (Windows, Linux, Unix, etc.)
3. Uses TCP/IP stack behavior analysis
4. Helps in vulnerability assessment
5. Performed using tools like Nmap and ZenmaRequires at least one open and one closed port for accuracy

Step 1: Basic OS Detection

sudo nmap -O

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O  192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:02 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000092s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
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 6.26 seconds
```

Step 2: OS Detection with Service Scan (Recommended)

sudo nmap -A

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:03 -0500
Nmap scan report for 192.168.10.3
Host is up (0.00011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))
|_http-server-header: Apache/2.4.66 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
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 14.92 seconds
```

Step 3: Guess OS if Detection is Incomplete

sudo nmap -O --osscan-guess

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O --osscan-guess 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:05 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000080s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
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 6.26 seconds
```

5. ## Analyze vulnerability

Vulnerability analysis is the process of identifying security weaknesses in a system that could be exploited by attackers. These weaknesses may exist due to outdated software, misconfigured services, weak authentication, or unpatched operating systems. After identifying open ports, services, and the operating system, vulnerability analysis correlates this information with known vulnerabilities from databases such as CVE. Tools like Nmap use built-in scripts to automatically check for common vulnerabilities in running services. Vulnerability analysis is a critical phase in ethical hacking and network security, as it helps organizations understand their security risks and apply appropriate countermeasures before attackers exploit them.

Step 1: Basic Vulnerability Scan

sudo nmap --script vuln

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:09 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000053s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|   /info.php: Possible information file
|_  /server-status/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 37.84 seconds
```

Step 2: Vulnerability Scan on Specific Ports

sudo nmap --script vuln -p 80,443

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script vuln -p 80,443 192.168.10.3
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:11 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000070s latency).

PORT    STATE    SERVICE
80/tcp  open     http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /test.php: Test page
|   /info.php: Possible information file
|_  /server-status/: Potentially interesting folder
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 32.63 seconds
```

6. Save Scan Results

Saving scan results is the process of storing the output of network scans for future reference, analysis, and reporting. During penetration testing or network assessment, scans may generate large amounts of data such as open ports, detected services, operating systems, and vulnerabilities. Saving these results allows security professionals to review findings later, compare changes over time, and prepare security reports. Tools like Nmap support multiple output formats including normal text, XML, and HTML, making it easier to document results or integrate them with other security tools. Properly saved scan results are essential for evidence collection, auditing, and professional documentation.

7. Step 1: Save Scan Output in Normal Text Format

nmap ip address -oN scan.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.3 -oN scan.txt

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:18 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000043s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
```

Step 2: Save Scan Output in XML Format

nmap 192.168.1.5 -oX scan.xml

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.3 -oX scan.xml

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:19 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000040s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds

┌──(kali㉿kali)-[~]
```

Step 3: Save Scan Output in All Formats (Most Used)

nmap 192.168.1.5 -oA scan_result

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.10.3 -oA scan_result
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:20 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000036s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
```

Step 4: Save Advanced Scan Results

sudo nmap -A 192.168.1.5 -oA full_scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.10.3 -oA full_scan~
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-31 11:22 -0500
Nmap scan report for 192.168.10.3
Host is up (0.000058s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.66 ((Debian))
|_http-server-header: Apache/2.4.66 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 5.X|6.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:6
OS details: Linux 5.0 - 6.2
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 16.43 seconds
```

Step 5: View Saved Results

cat scan.txt

```
┌──(kali㉿kali)-[~]
└─$ cat scan.txt
# Nmap 7.98 scan initiated Sat Jan 31 11:18:12 2026 as: /usr/lib/nmap/nmap --privileged -oN scan.txt 192.168.10.3
Nmap scan report for 192.168.10.3
Host is up (0.000043s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

# Nmap done at Sat Jan 31 11:18:17 2026 -- 1 IP address (1 host up) scanned in 4.81 seconds
```

7.INTERPRET RESULTS

Interpreting scan results is the process of analyzing the information collected during network scanning to understand security risks. After identifying open ports, services, operating systems, and vulnerabilities, the tester evaluates which findings are critical, moderate, or low risk. This step focuses on understanding how discovered vulnerabilities could impact confidentiality, integrity, and availability of systems. Not

all vulnerabilities pose the same level of threat; therefore, interpretation helps prioritize remediation efforts. Proper risk interpretation is essential for making informed security decisions and preventing potential attacks.

8. DOCUMENT FINDINGS

This includes details such as identified hosts, open ports, detected services, operating systems, vulnerabilities, and associated risk levels. Documentation ensures that technical findings can be clearly communicated to stakeholders, system administrators, or management. Proper documentation is essential for compliance, auditing, remediation planning, and future reference. A well-written report serves as proof of assessment and guides corrective actions.