TASK–02: Nmap Scanning & Vulnerability Detection Report

1. Objective

The objective of this task is to perform network reconnaissance and basic vulnerability assessment using **Nmap**.
The task focuses on identifying open ports, running services, operating system details, and potential vulnerabilities on a **lab machine only** using different Nmap scan techniques.

2. Tool Used

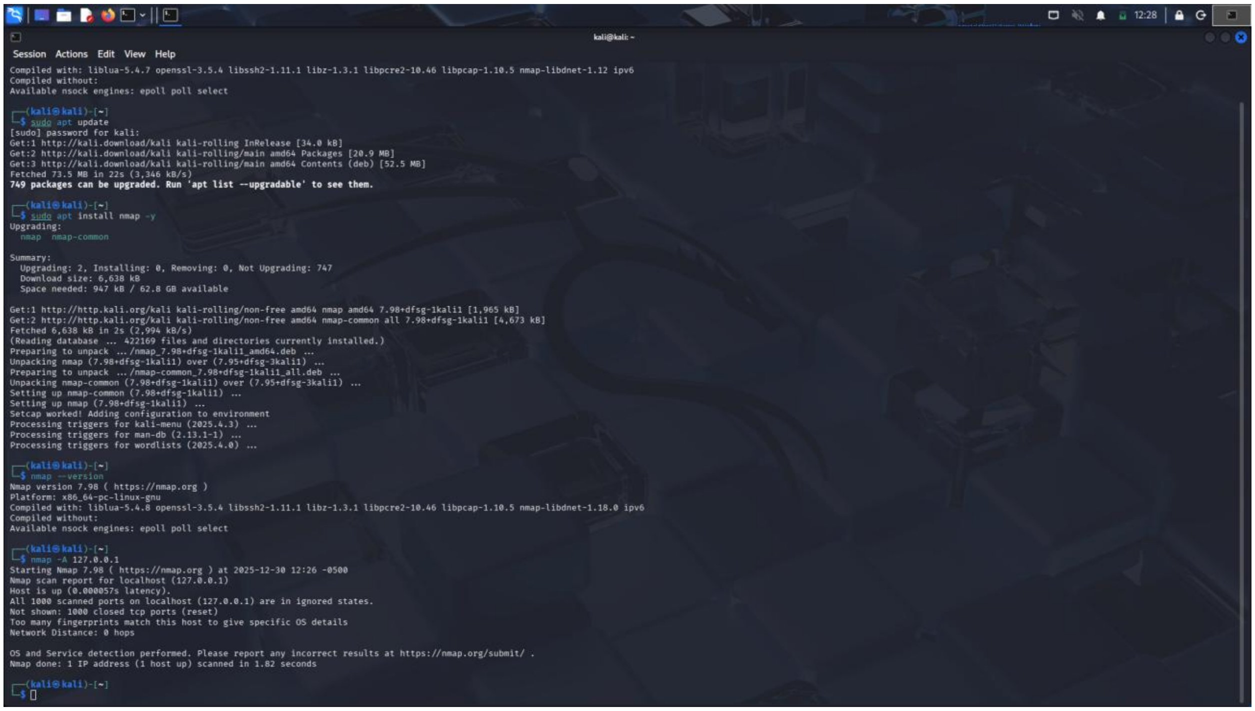
- **Tool Name:** Nmap (Network Mapper)
- **Operating System:** Kali Linux
- **Version:** Nmap 7.98
- **Target Machine:** Localhost (127.0.0.1) – Lab Environment

3. Methodology

Multiple Nmap scans were executed on the target system to gather network and service information.
Each scan served a different purpose, as explained below.

4. Scans Performed & Analysis

4.1 Full Scan (-A)



```
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)-[~]
└─$ 
```

Command Used:

nmap -A 127.0.0.1

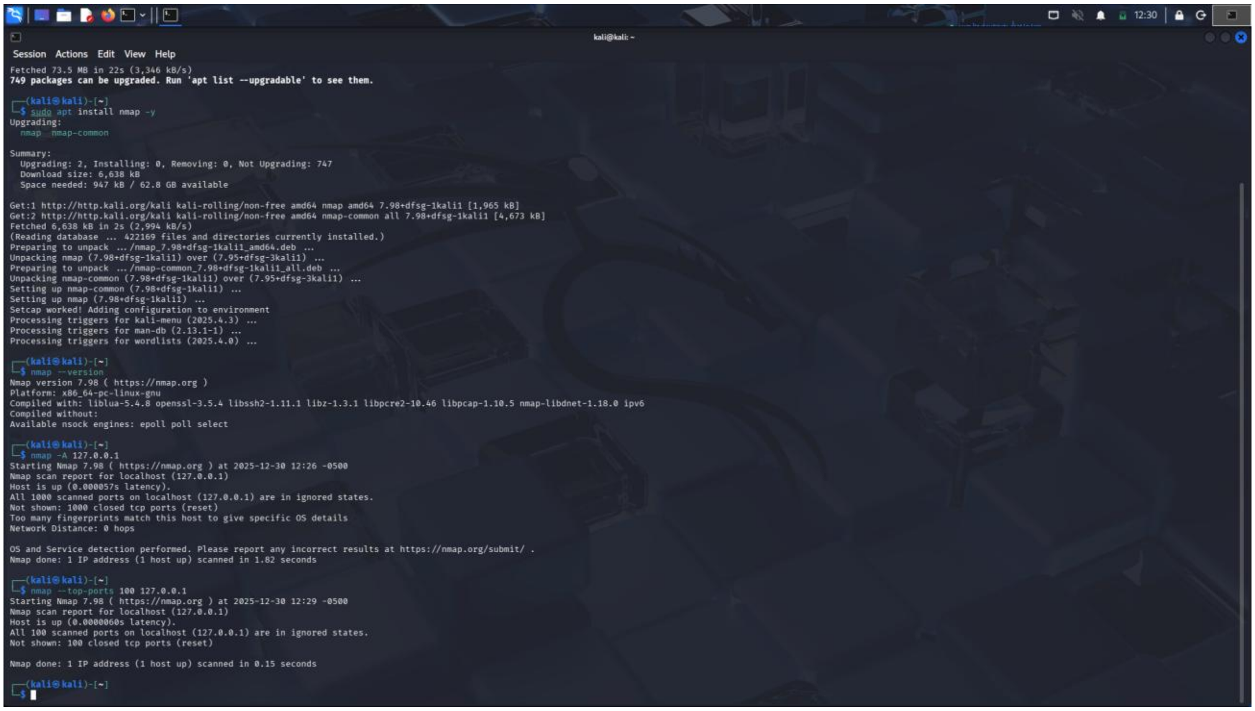
Purpose:

- Detect open ports
- Identify running services
- Perform OS detection
- Enable script scanning and traceroute

Observation:

- The host was found to be **up**
- All scanned ports were in a **closed or filtered state**
- OS detection was attempted but could not determine specific OS details
- No active services were detected on the target

4.2 Top Ports Scan



```
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)-[~]
└─$ 
```

Command Used:

nmap --top-ports 100 127.0.0.1

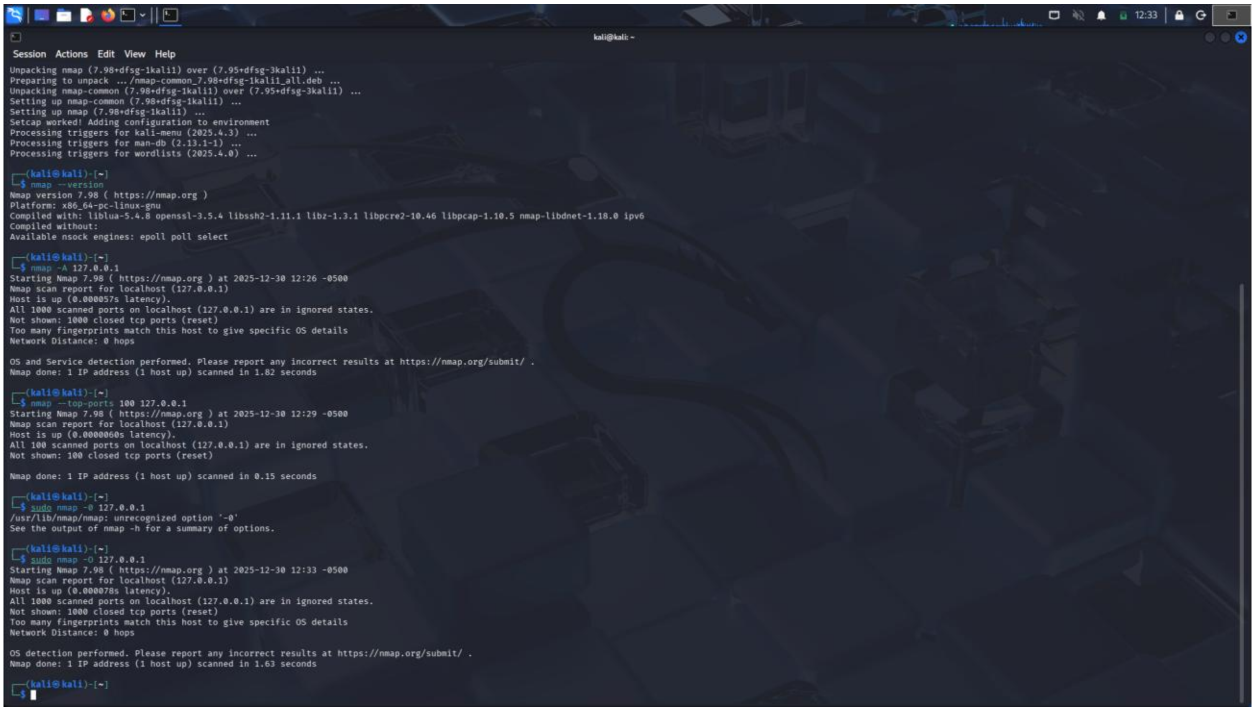
Purpose:

- Quickly scan the most commonly used 100 ports

Observation:

- The system responded successfully
- No open ports were detected among the top 100 ports
- All scanned ports were reported as closed

4.3 OS Detection Scan



```
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)-[~]
└─$ 
```

Command Used:

sudo nmap -O 127.0.0.1

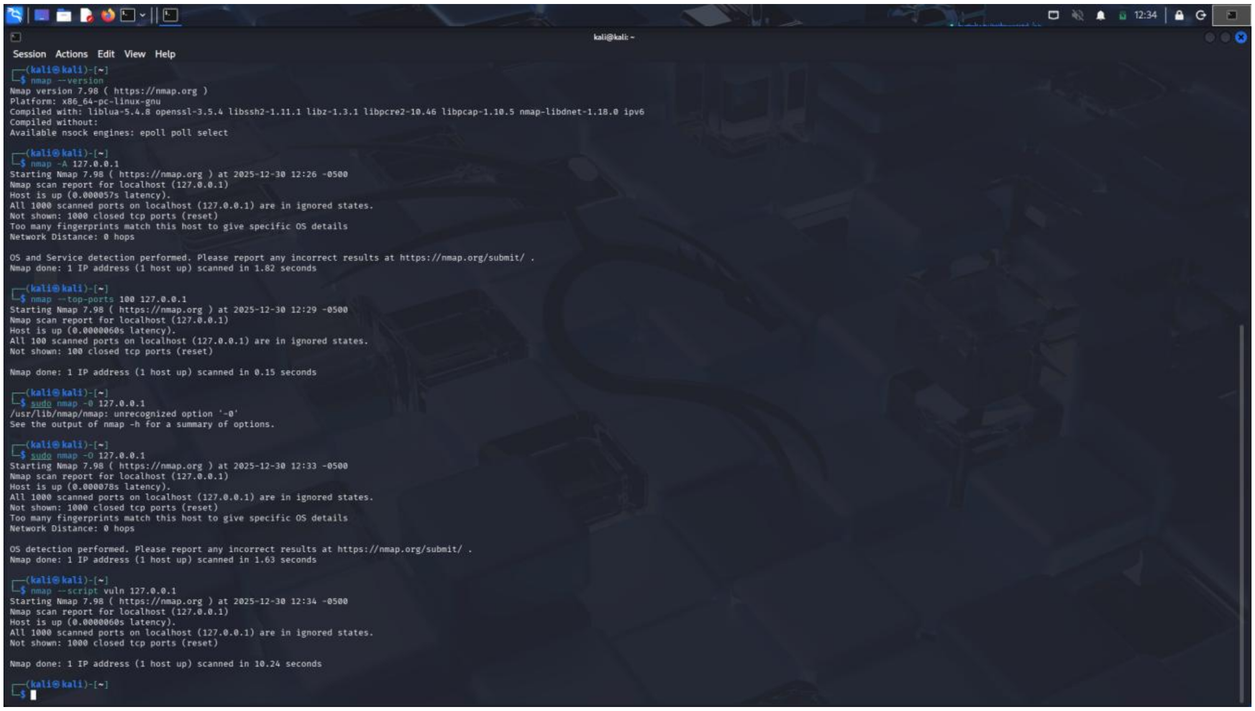
Purpose:

- Identify the operating system running on the target machine

Observation:

- Nmap attempted OS fingerprinting
- Due to lack of sufficient open ports, OS detection was inconclusive
- Network distance was reported as 0 hops (local system)

4.4 Vulnerability Script Scan



```
┌──(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)-[~]
└─$ 
```

Command Used:

nmap --script vuln 127.0.0.1

Purpose:

- Run vulnerability detection scripts
- Identify known security vulnerabilities

Observation:

- Vulnerability scripts executed successfully
- No vulnerabilities were detected
- The system appeared secure under basic vulnerability scanning

(Insert Screenshot: Vulnerability Scan Output)

---

5. Results Summary

- The target system was reachable and responsive
- No open ports were detected
- No running network services were exposed

- OS detection could not be confirmed due to limited response
- No known vulnerabilities were identified during script scanning

---

6. Conclusion

This task demonstrated the use of **Nmap** for network scanning and vulnerability detection.
The scans confirmed that the lab system had no exposed services or open ports, indicating a secure baseline configuration.
Nmap proved to be an effective tool for reconnaissance, service discovery, and preliminary security assessment.

---

7. Ethical Consideration

All scans were performed strictly on a **lab machine (localhost)** for educational purposes only.
No unauthorized systems were scanned.