Task 9 – Network Scanning and Vulnerability Assessment using Nmap

Internship: Cyber Security Internship
Task Number: Task 9
Operating System: Kali Linux
Tool Used: Nmap
Date: 29/01/2026

1. Objective

The objective of this task was to perform network scanning to:

- Discover live hosts in the local network
- Identify open ports and running services
- Detect the target operating system
- Identify potential vulnerabilities using Nmap scripting engine (NSE)

2. Network Discovery (Live Host Identification)

A ping scan was performed to identify active hosts within the local network range.

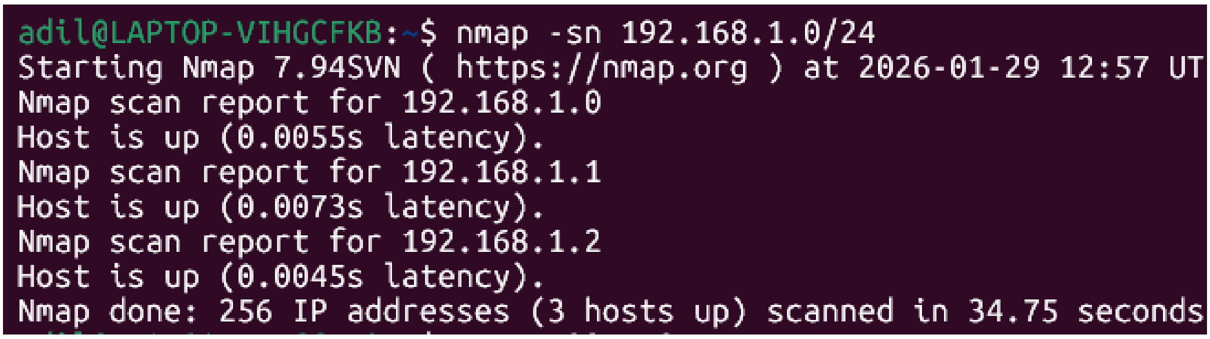
Command Used:

nmap -sn 192.168.1.0/24

Result:

- Multiple hosts were detected as active.
- The primary target host selected for further analysis was **192.168.1.1**.

Screenshot – 1:



```
adil@LAPTOP-VIHGCFKB:~$ nmap -sn 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:57 UT
Nmap scan report for 192.168.1.0
Host is up (0.0055s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0073s latency).
Nmap scan report for 192.168.1.2
Host is up (0.0045s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 34.75 seconds
```

3. Basic Port Scan of Target Host

An initial scan was performed on the target host to check its availability.

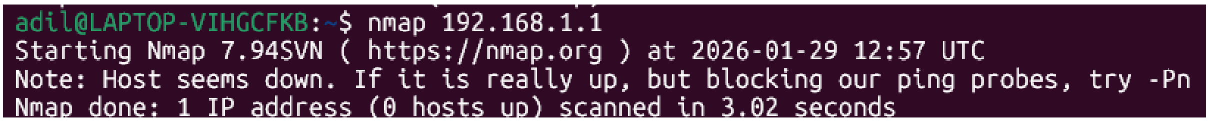
Command Used:

nmap 192.168.1.1

Observation:

- The host appeared to block ICMP ping requests.
- This behavior is common for routers or secured systems.

Screenshot – 2:



```
adil@LAPTOP-VIHGCFKB:~$ nmap 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:57 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.02 seconds
```

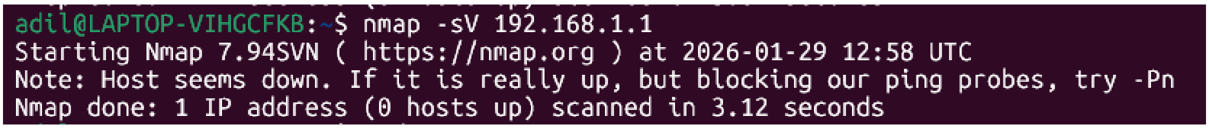
4. Service Version Detection

A service version scan was performed to identify running services and their versions.

Command Used:

nmap -sV 192.168.1.1

Screenshot – 3:



```
adil@LAPTOP-VIHGCFKB:~$ nmap -sV 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:58 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
```

5. Operating System Detection and Open Ports

An OS detection scan was executed using root privileges.

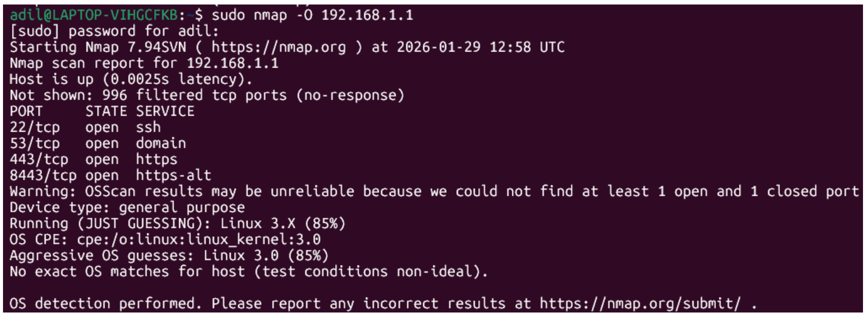
Command Used:

sudo nmap -O 192.168.1.1

Findings:

- Operating System: Linux (Debian-based)
- Open Ports Identified:
    - **22/tcp** – SSH
    - **53/tcp** – DNS
    - **443/tcp** – HTTPS
    - **8443/tcp** – HTTPS-ALT

Screenshot – 4 (IMPORTANT):



```
adil@LAPTOP-VIHGCFKB:~$ sudo nmap -O 192.168.1.1
[sudo] password for adil:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:58 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
443/tcp  open  https
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 3.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.0
Aggressive OS guesses: Linux 3.0 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

6. Vulnerability Scanning using Nmap Scripts

Nmap vulnerability scripts were executed to identify security weaknesses on the target host.

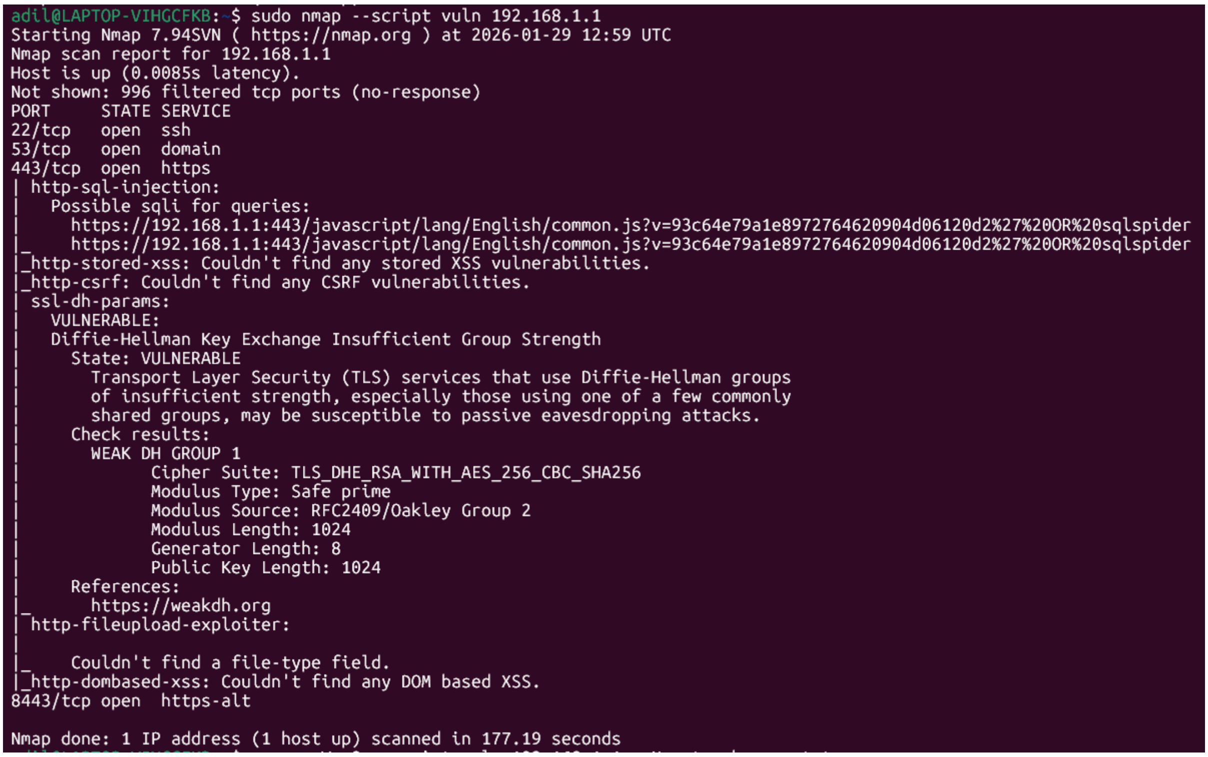
Command Used:

sudo nmap --script vuln 192.168.1.1

Vulnerabilities Identified:

- Possible **SQL Injection** vulnerability
- **Weak Diffie-Hellman Key Exchange**
- TLS services using insufficient key strength (1024-bit DH groups)

Screenshot – 5 (MOST IMPORTANT):



```
adil@LAPTOP-VIHGCFKB:~$ sudo nmap --script vuln 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-29 12:59 UTC
Nmap scan report for 192.168.1.1
Host is up (0.0085s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
443/tcp  open  https
| http-sql-injection:
|   Possible sqli for queries:
|     https://192.168.1.1:443/javascript/lang/English/common.js?v=93c64e79a1e8972764620904d06120d2%27%20OR%20sqlspider
|_    https://192.168.1.1:443/javascript/lang/English/common.js?v=93c64e79a1e8972764620904d06120d2%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
|_http-dombased-xss: Couldn't find any DOM based XSS.
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 177.19 seconds
```

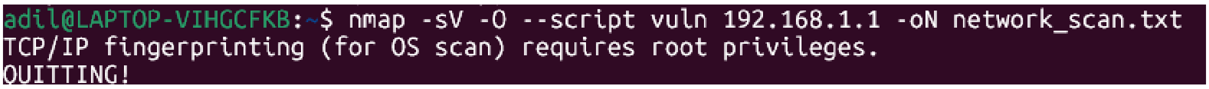
7. Saving Scan Output

The scan results were saved to a text file for documentation and analysis.

Command Used:

sudo nmap -sV -O --script vuln 192.168.1.1 -oN network_scan.txt

Screenshot – 6 (Optional):



```
adil@LAPTOP-VIHGCFKB:~$ nmap -sV -O --script vuln 192.168.1.1 -oN network_scan.txt
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
```

8. Conclusion

This task demonstrated the use of Nmap for network reconnaissance and vulnerability assessment. The scan successfully identified live hosts, open ports, running services, operating system details, and multiple security vulnerabilities. These findings highlight the importance of regular network scanning and secure configuration of exposed services.

9. Screenshots Summary (MANDATORY ORDER)

Screenshot No.	Description
SS-1	Network discovery (nmap -sn)
SS-2	Basic host scan
SS-3	Service version scan
SS-4	OS detection & open ports
SS-5	Vulnerability scan (script vuln)
SS-6	Saved output (optional)