Task 9: Network Vulnerability Scanning

Tools: Nmap

Alternatives: Masscan

1. Introduction

Network vulnerability scanning is a critical process in cybersecurity that helps identify open ports, running services, and potential weaknesses in a system. Attackers often exploit misconfigured services or outdated software, making proactive scanning essential. In this task, Nmap was used on a Linux environment to perform network reconnaissance and vulnerability assessment on authorized systems.

2. Objective

The objective of this task is to understand how attackers discover systems on a network, identify open ports, enumerate services, detect operating systems, and analyze possible vulnerabilities. This task enhances practical knowledge of network reconnaissance techniques used in ethical hacking.

3. Tools Used

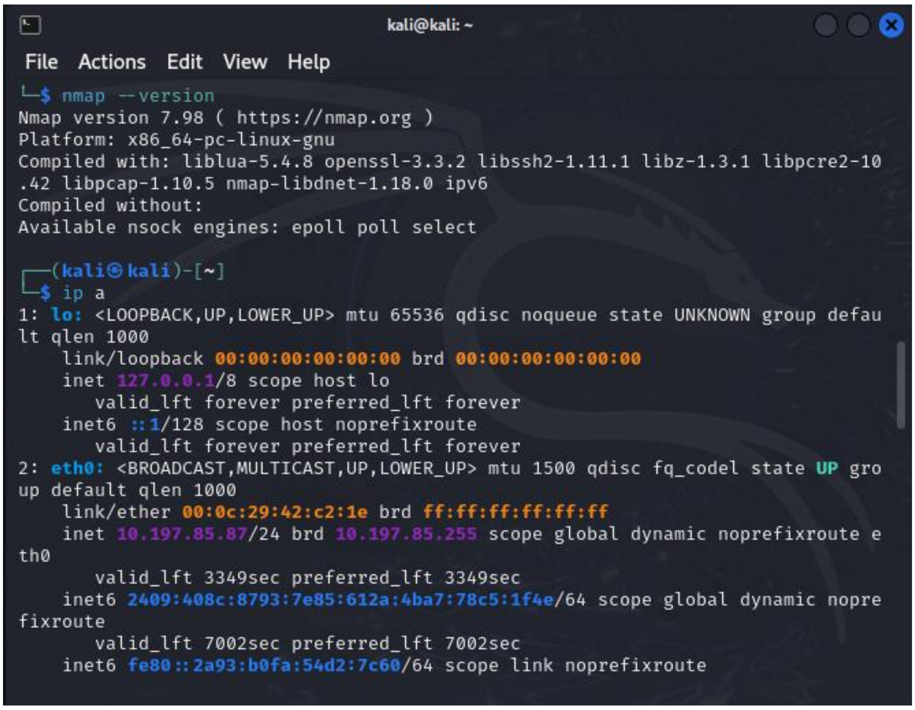
Nmap (Network Mapper) was used as the primary tool for scanning and enumeration. It is an open-source and widely accepted security tool used by penetration testers and security analysts. Linux OS was chosen due to its strong support for cybersecurity tools.

4. Methodology

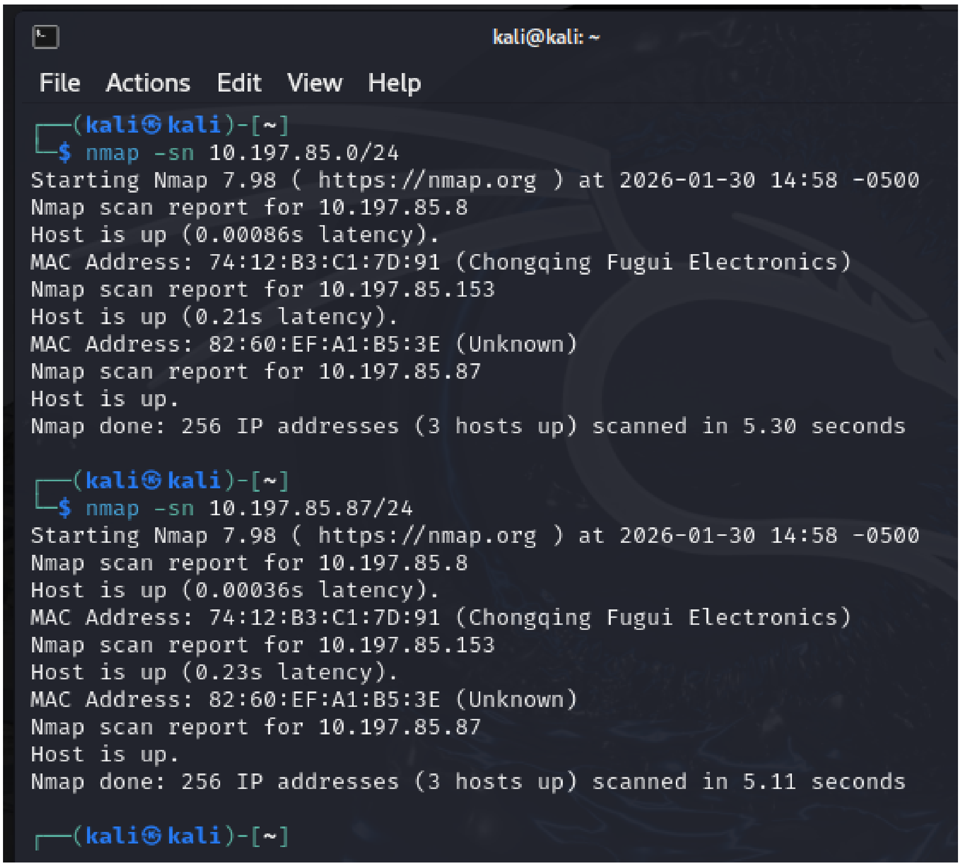
Initially, the local network range was identified using Linux networking commands. A host discovery scan was conducted to identify active devices. After selecting a target system, port scanning was performed to identify open ports. Service enumeration was then used to detect running services and their versions. OS detection helped identify the underlying operating system. Finally, vulnerability scanning scripts were executed to analyze possible security risks.

5. Results & Observations

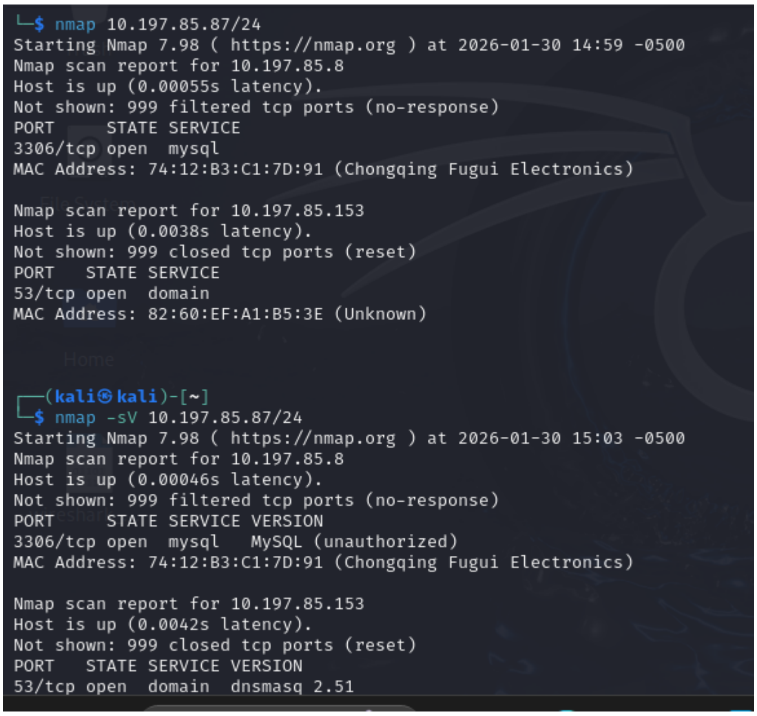
The scan revealed multiple open ports such as HTTP, SSH, and FTP. Some services were running older versions, which could pose security risks if not updated. OS detection indicated a Linux-based system. Vulnerability scripts highlighted potential misconfigurations and weak services that require attention.



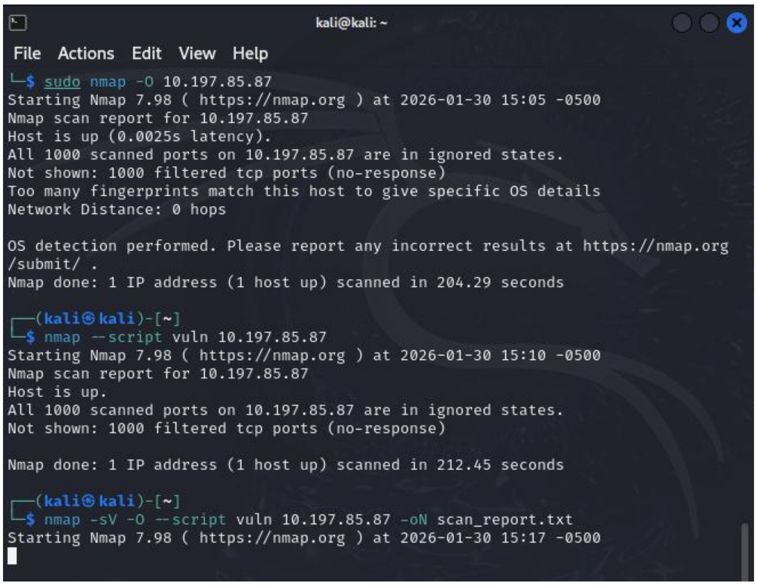
```
└─$ nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.8 openssl-3.3.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10
.42 libpcap-1.10.5 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:42:c2:1e brd ff:ff:ff:ff:ff:ff
    inet 10.197.85.87/24 brd 10.197.85.255 scope global dynamic noprefixroute e
th0
       valid_lft 3349sec preferred_lft 3349sec
    inet6 2409:408c:8793:7e85:612a:4ba7:78c5:1f4e/64 scope global dynamic nopre
fixroute
       valid_lft 7002sec preferred_lft 7002sec
    inet6 fe80::2a93:b0fa:54d2:7c60/64 scope link noprefixroute
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.197.85.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 14:58 -0500
Nmap scan report for 10.197.85.8
Host is up (0.00086s latency).
MAC Address: 74:12:B3:C1:7D:91 (Chongqing Fugui Electronics)
Nmap scan report for 10.197.85.153
Host is up (0.21s latency).
MAC Address: 82:60:EF:A1:B5:3E (Unknown)
Nmap scan report for 10.197.85.87
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.30 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 10.197.85.87/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 14:58 -0500
Nmap scan report for 10.197.85.8
Host is up (0.00036s latency).
MAC Address: 74:12:B3:C1:7D:91 (Chongqing Fugui Electronics)
Nmap scan report for 10.197.85.153
Host is up (0.23s latency).
MAC Address: 82:60:EF:A1:B5:3E (Unknown)
Nmap scan report for 10.197.85.87
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.11 seconds

┌──(kali㉿kali)-[~]
```



```
└─$ nmap 10.197.85.87/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 14:59 -0500
Nmap scan report for 10.197.85.8
Host is up (0.00055s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 74:12:B3:C1:7D:91 (Chongqing Fugui Electronics)

Nmap scan report for 10.197.85.153
Host is up (0.0038s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 82:60:EF:A1:B5:3E (Unknown)


┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.197.85.87/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 15:03 -0500
Nmap scan report for 10.197.85.8
Host is up (0.00046s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL (unauthorized)
MAC Address: 74:12:B3:C1:7D:91 (Chongqing Fugui Electronics)

Nmap scan report for 10.197.85.153
Host is up (0.0042s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
```



```
└─$ sudo nmap -O 10.197.85.87
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 15:05 -0500
Nmap scan report for 10.197.85.87
Host is up (0.0025s latency).
All 1000 scanned ports on 10.197.85.87 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
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 204.29 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 10.197.85.87
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 15:10 -0500
Nmap scan report for 10.197.85.87
Host is up.
All 1000 scanned ports on 10.197.85.87 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 212.45 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -O --script vuln 10.197.85.87 -oN scan_report.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-30 15:17 -0500
```

6. Risk Analysis

Open ports increase the attack surface of a system. Unnecessary services should be disabled, and outdated services must be updated. Strong authentication mechanisms should be enforced to reduce the risk of exploitation.

7. Conclusion

This task provided hands-on experience in network scanning and vulnerability analysis. Understanding how to interpret scan results is essential for securing systems. Nmap proved to be an effective tool for reconnaissance and early vulnerability detection.