Title: Vulnerability Assessment using Nmap

Internship: RD INFRO TECHNOLOGY

Name: **A.Nivetha**

Email**: nivetha.240217@aidsritchennai.edu**

Date:10/07/2025

Objective:

To use Nmap to identify open ports and services on a target system to understand its vulnerabilities.

Tool Used:

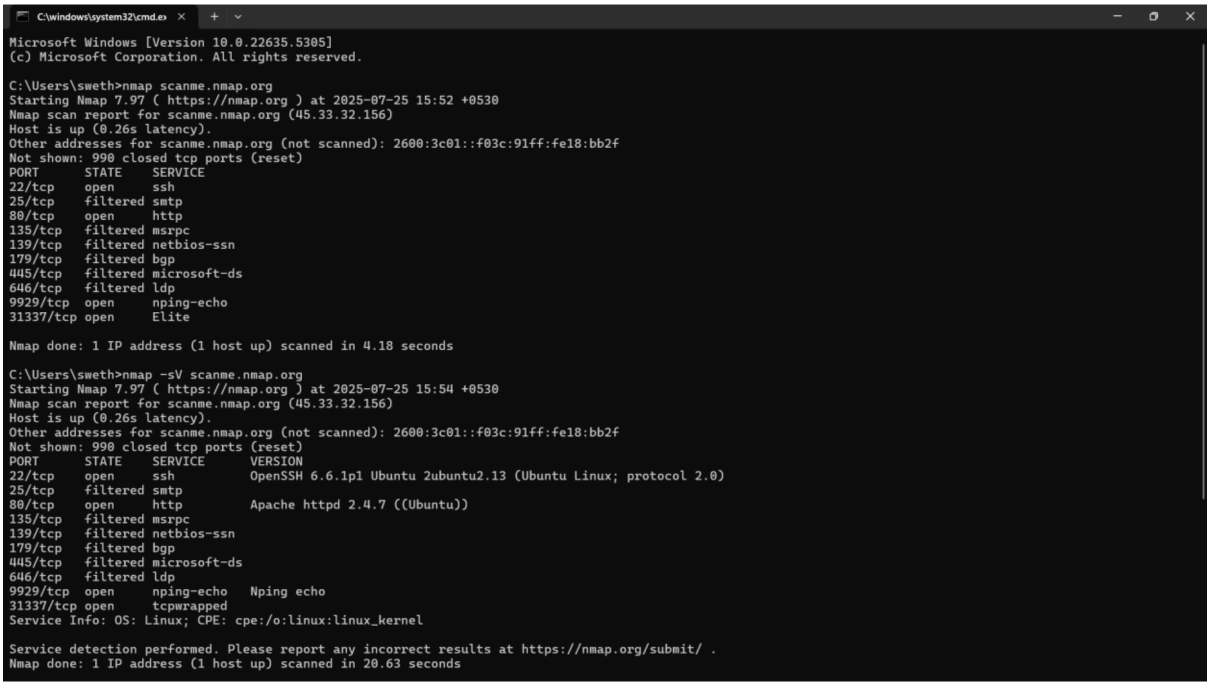
- **Nmap** (Network Mapper)

Command Used:

```
nmap scanme.nmap.org

nmap -sV scanme.nmap.org
```

Output Screenshot



```
Microsoft Windows [Version 10.0.22635.5305]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sweth>nmap scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25 15:52 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 990 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
179/tcp   filtered bgp
445/tcp   filtered microsoft-ds
646/tcp   filtered ldp
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 4.18 seconds

C:\Users\sweth>nmap -sV scanme.nmap.org
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25 15:54 +0530
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 990 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
179/tcp   filtered bgp
445/tcp   filtered microsoft-ds
646/tcp   filtered ldp
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: 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 20.63 seconds
```

Summary:

- Port 22/tcp (SSH) is open
- Port 80/tcp (HTTP) is open
- Port 31337/tcp is open
- Apache HTTP server and OpenSSH service detected
- Some ports were filtered or closed
- These open ports may allow access and should be tested further in real-world cases

Conclusion:

Nmap successfully identified open ports and services. This basic scan demonstrates how vulnerability assessment is done in the real world.