Cybersecurity Internship – Phase 1 (Hands-on Task 2)

TASK 2: Perform a Basic Network Scan Using Nmap

1. Commands Used and Descriptions

- **Basic Scan:**

nmap scanme.nmap.org

Description: Performs a basic scan on the target. Detects open TCP ports using the default settings.

- **Service Version Detection:**

nmap -sV scanme.nmap.org

Description: Attempts to determine service/version info on open ports. Useful for identifying what software is running.

- **OS Detection:**

nmap -O scanme.nmap.org

Description: Uses TCP/IP stack fingerprinting to guess the remote operating system.

- **Full Port Range Scan:**

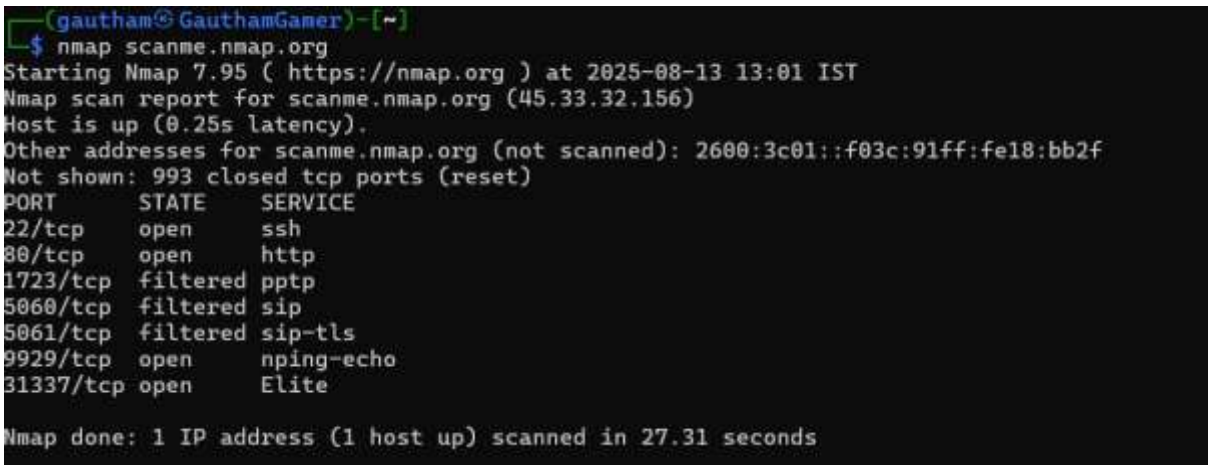
nmap -p- scanme.nmap.org

Description: Scans all 65,535 TCP ports (instead of the default top 1,000).

---

2. Scan Output (Paste or Screenshot Results)

- **Basic Scan Output:**



🔹 **Service Detection (-sV) Output:**

```
┌──(gautham㉿GauthamGamer)-[~]
└─$ nmap -sV scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 13:03 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.27s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
1723/tcp  filtered pptp
5060/tcp  filtered sip
5061/tcp  filtered sip-tls
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 42.48 seconds
```

🔹 **OS Detection (-O) Output:**

```
┌──(gautham㉿GauthamGamer)-[~]
└─$ nmap -O scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 13:05 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
1723/tcp  filtered pptp
5060/tcp  filtered sip
5061/tcp  filtered sip-tls
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 4.19 - 5.15 (98%), Linux 4.15 (93%), IPFire 2.27 (Linux 5.15 - 6.1) (93%), Linux 5.4 (93%),
 Linux 5.0 - 5.14 (91%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (91%), Linux 3.11 - 4.9 (90%), Linux 3.2 - 3.8 (90%),
 Linux 4.15 - 5.19 (89%), Android TV OS 11 (Linux 4.19) (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.21 seconds
```

🔹 **All Ports (-p-) Output:**

(Took so long and returned timeout status)

🧠 **3. Summary of Findings**

- **Total open ports found**: 7
(22/tcp, 80/tcp, 9929/tcp, 31337/tcp, and others filtered)

- **Common services discovered**:

  - **22/tcp:** OpenSSH 6.6.1p1 running on Ubuntu Linux
  - **80/tcp:** Apache httpd 2.4.7 (Ubuntu)
  - **9929/tcp:** nping-echo service
  - **31337/tcp:** tcpwrapped (showing as "Elite" in OS detection)

- **Filtered ports detected**:

  - 1723/tcp (PPTP)

- 5060/tcp (SIP)
- 5061/tcp (SIP-TLS)

- **Operating System Guess**:
Linux kernel versions between 4.19 and 5.15 most likely (98% confidence). No exact match found, but it's definitely a Linux-based OS.

- **Network Distance**: 19 hops between your host and the target server.

📘 4. Key Concepts Observed

Concept	Notes
Open Port	[E.g. Port 22 – SSH is accepting connections]
Closed Port	[E.g. Port 21 – explicitly rejected connection]
Filtered Port	[E.g. Port 25 – no response, possibly firewalled]
Service Detection	[Used -sV to identify service versions]
OS Fingerprinting	[Used -O, result: Linux or Unix-based OS]
Full Port Range	[Used -p-, discovered additional non-standard ports]
Ethical Scanning	[Scanned scanme.nmap.org – authorized for practice]

🎯 5. Learning Outcomes

By completing this task, I have:

- Learned to use basic and advanced nmap scanning commands
- Understood the difference between open, closed, and filtered ports
- Observed how attackers or penetration testers gather information
- Practiced analyzing and interpreting port scan results

💉 6. Interview Questions and Answers

1. **What is the purpose of Nmap in cybersecurity?**
   Nmap is a network scanning tool used to discover hosts, services, and vulnerabilities on a network. It's used for reconnaissance in penetration testing.
2. **What's the difference between TCP and UDP scanning?**
   TCP scans establish full connections (or attempt to), while UDP scans send datagrams and rely on ICMP or lack of response. UDP is harder to scan reliably.

3. **Explain what the -sV and -O flags do.**
   -sV detects service versions running on open ports. -O attempts to determine the operating system of the host via fingerprinting.

4. **Why should you never run Nmap scans without permission?**
   Unauthorized scanning can be considered illegal or malicious. It can disrupt services or trigger alarms; always get consent first.

5. **What are filtered ports?**
   Ports that don't respond, likely because of a firewall or filtering rules. Nmap can't determine if they are open or closed.

6. **How does OS fingerprinting work in Nmap?**
   It analyzes responses to various TCP/IP probes and compares them to a database of known OS signatures.

7. **What is banner grabbing?**
   Retrieving metadata or welcome messages from services (e.g., HTTP or FTP) that reveal software version or system details.

8. **Why is port scanning important in penetration testing?**
   It identifies potential entry points into a system or network. Knowing what's open helps prioritize vulnerabilities.

9. **List 3 common ports and their services.**
   - Port 22: SSH
   - Port 80: HTTP
   - Port 443: HTTPS

10. **What does a "closed" port indicate?**
    The port is accessible but no service is listening. The system responded with a "connection refused".