Nmap Scan Report

Cybersecurity & Ethical Hacking Internship
Company: ApexPlanet Software Pvt. Ltd.

Tool Used: Nmap
Scanner Machine: Kali Linux
Target Machine: Metasploitable2

---

1. Objective

The objective of this scan is to identify open ports, running services, and operating system details of the target system using the Nmap network scanning tool. This helps in identifying exposed services that could potentially be exploited by attackers.

2. Tool Overview:

Nmap (Network Mapper) is an open-source network scanning tool used for:

• Host discovery
• Port scanning
• Service version detection
• Operating system detection

It is widely used in cybersecurity for vulnerability assessment and penetration testing.

3. Target Information:

Parameter	Value
Attacker Machine	Kali Linux
Target Machine	Metasploitable2
Target IP Address	192.168.244.4
Tool Used	Nmap

4. Scan Methodology:

The Nmap scan was performed using the following command:

```
nmap -sS -sV -O 192.168.244.4
```

Where:

• -sS → SYN Scan (Stealth Scan).
• -sV → Service Version Detection.
• -O → Operating System Detection.

This command performs an advanced scan to identify open ports, services, and OS details.

5. Scan Results:

The scan revealed multiple open ports and running services on the target system.

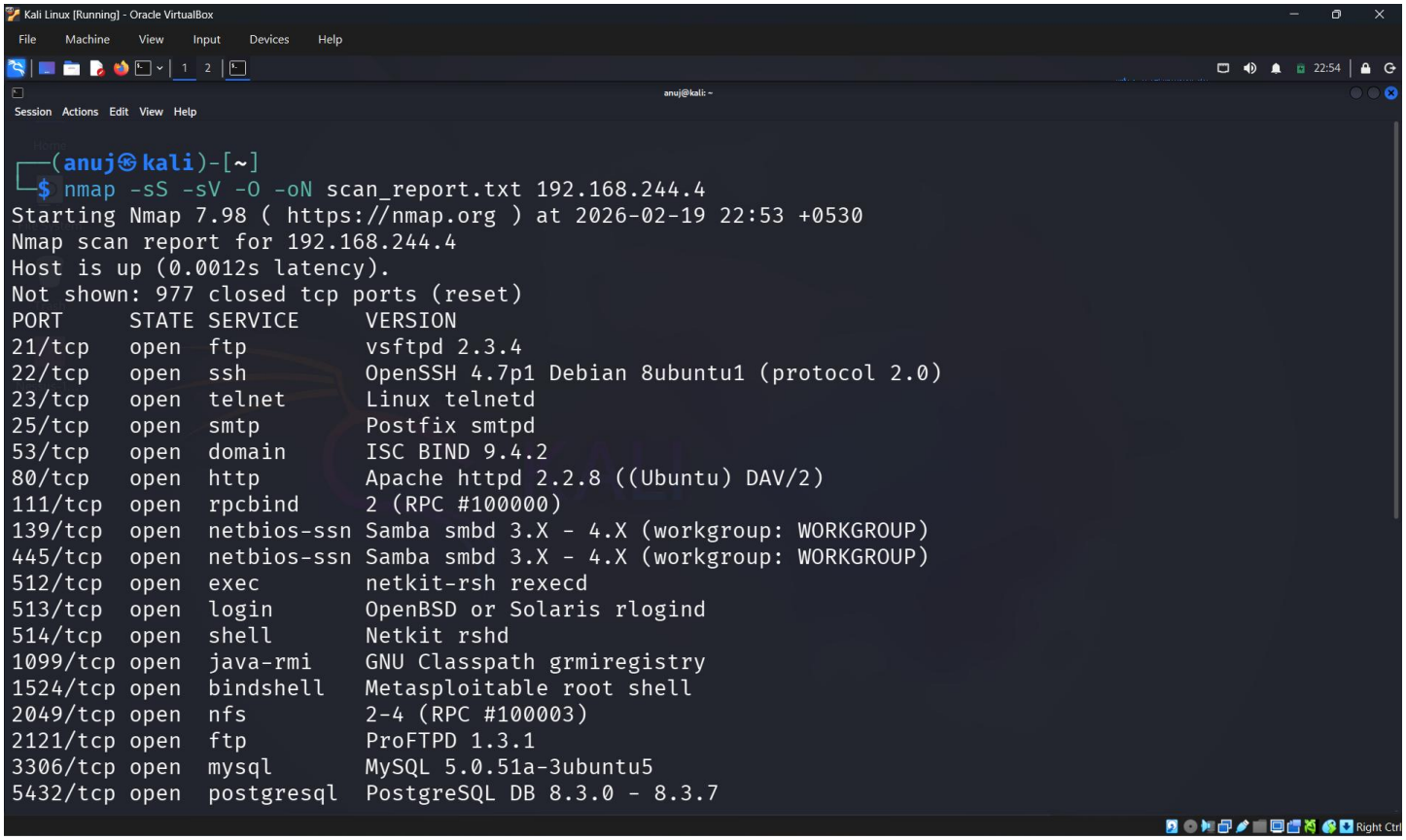

Figure 1: Nmap scan results identifying open ports and services.

6. Open Ports and Services Identified:

Port	State	Service	Version
21	Open	FTP	vsftpd 2.3.4
22	Open	SSH	OpenSSH
23	Open	Telnet	Telnet Service
80	Open	HTTP	Apache Web Server
3306	Open	MySQL	MySQL Database

These open ports indicate active services running on the target system.

7. Operating System Detection:

Nmap detected the target operating system as Linux based on TCP/IP fingerprinting.

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|bridge|general purpose
Running (JUST GUESSING): AT&T embedded (93%), Oracle Virtualbox (92%), Slirp (92%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: AT&T BGW210 voice gateway (93%), Oracle Virtualbox Slirp NAT bridge (92%), QEMU us
er mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:l
inux:linux_kernel

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 20.32 seconds
```

Figure 2: Operating System detection using Nmap.

8. Analysis:

The Nmap scan successfully identified multiple open ports and exposed services on the target system. These services could potentially serve as entry points for attackers if vulnerabilities exist.

Service version detection revealed outdated services, which may contain known vulnerabilities.

Operating system detection confirmed the target system is running a Linux-based operating system.

9. Security Implications:

Open ports and exposed services increase the attack surface of a system.

Potential risks include:

- Unauthorized access
- Service exploitation
- Data breach
- Remote code execution

Proper security measures such as firewall configuration and service hardening should be implemented.

10. Conclusion:

The Nmap scan successfully identified open ports, running services, and operating system details of the target system.

This scan provided valuable information about exposed services and potential attack vectors. Nmap proved to be an effective tool for network reconnaissance and security assessment.

This activity enhanced practical understanding of network scanning and service enumeration techniques used in cybersecurity.

------X------X------X------