

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
```

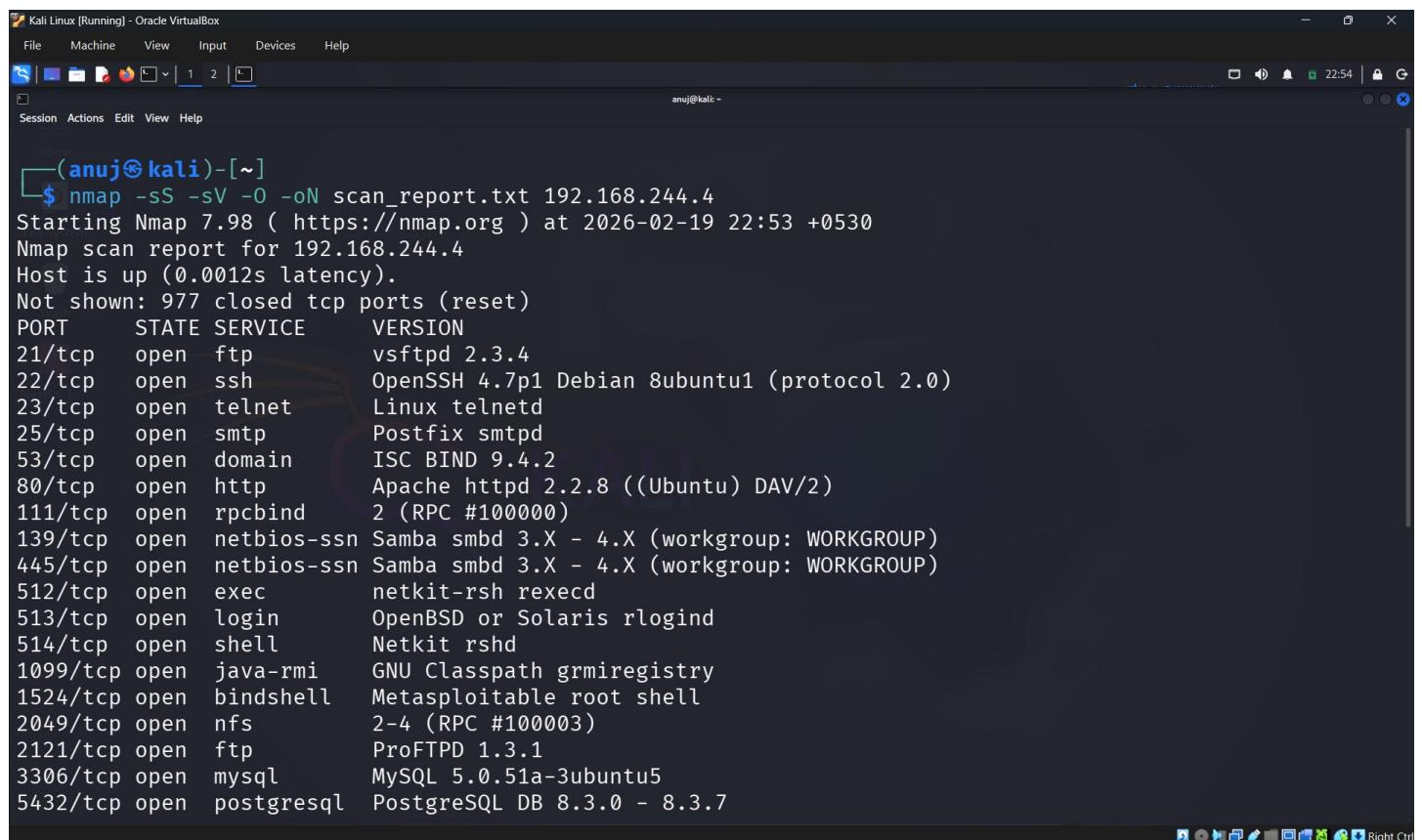
Where:

- -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.



The screenshot shows a terminal window titled "Kali Linux [Running] - Oracle VirtualBox". The command \$ nmap -sS -sV -O -oN scan_report.txt 192.168.244.4 was run. The output shows the following:

```
(anuj㉿kali)-[~]
$ nmap -sS -sV -O -oN scan_report.txt 192.168.244.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-19 22:53 +0530
Nmap scan report for 192.168.244.4
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
```

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

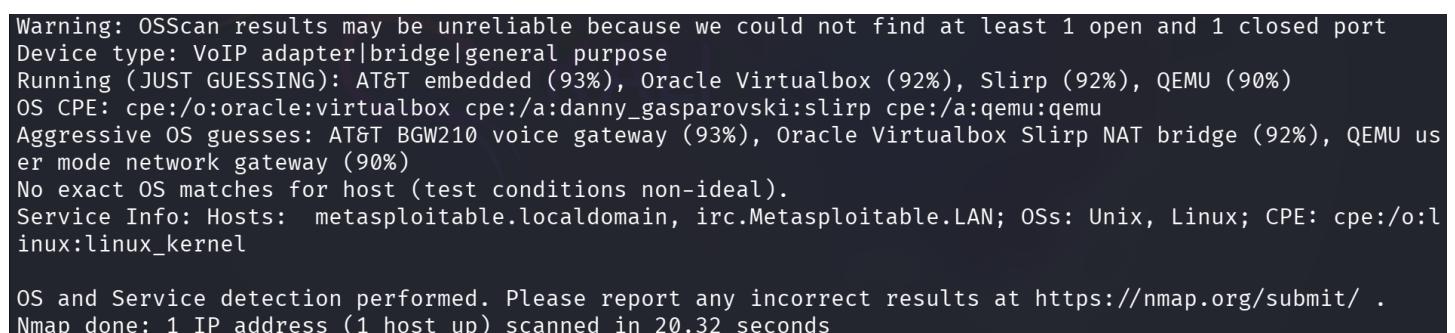
6. Open Ports and Services Identified:

| 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.



The screenshot shows a terminal window with the following OS detection output:

```
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 user 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:linux: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-----