Nmap Scan Report

1. Environment

- Attacker VM: Kali Linux (VirtualBox)
- Target VM: Metasploitable2 (VirtualBox)
- Network: Host-only (192.168.56.0/24)

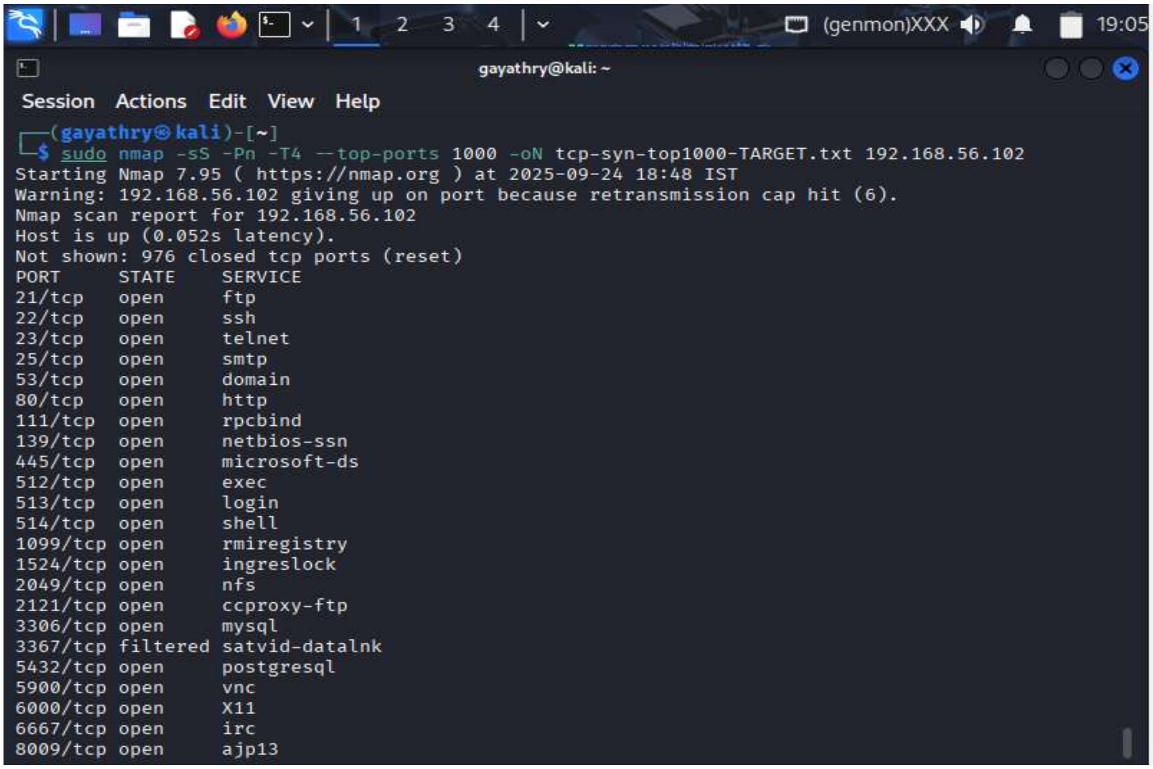
2. overview of the flags

- -sS — **TCP SYN (half-open) scan**. Fast, common, stealthier than a full TCP connect. Requires root.
- -sU — **UDP scan**. Discovers UDP services. Much slower and noisier; often requires root.
- -sV — **Service/version detection**. Probes open ports to learn software name & version.
- -O — **OS detection**. Tries to fingerprint the target OS via TCP/IP stack characteristics. Requires root and responsive targets.

3. Commands run

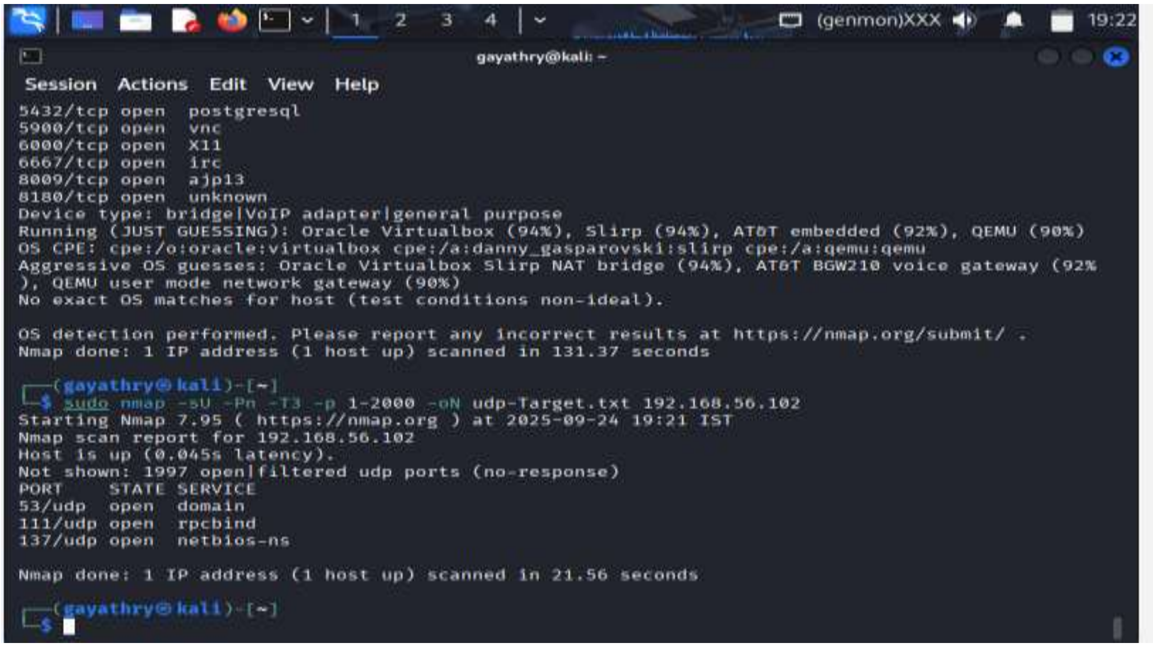
- ping -c 4 192.168.56.102
- sudo nmap -sS -Pn -T4 --top-ports 1000 -oN tcp_syn_top1000_TARGET.txt 192.168.56.102
- sudo nmap -sU -Pn -T3 -p 1-2000 -oN udp_TARGET.txt 192.168.56.102
- sudo nmap -O -Pn -T4 -ON os-detect-TARGET.txt 192.168.56.102
- sudo nmap -sS -sV -Pn -T4 --top-ports 1000 -oN svc_version_TARGET.txt 192.168.56.102

4. Findings



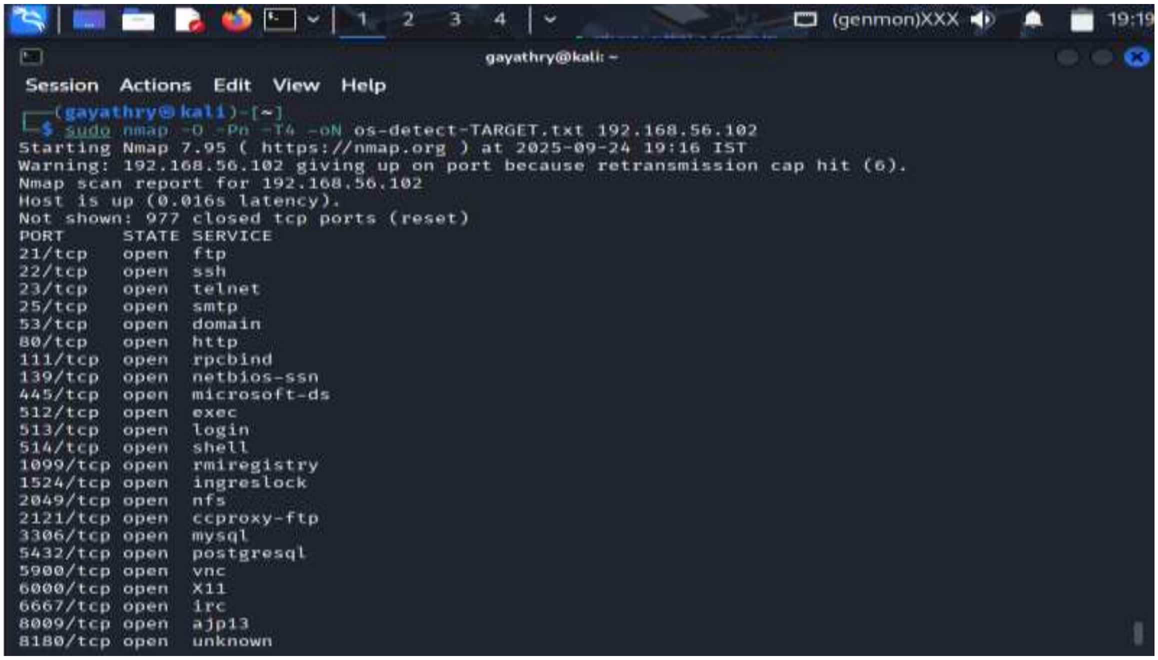
```
┌──(gayathry㉿kali)-[~]
└─$ sudo nmap -sS -Pn -T4 --top-ports 1000 -oN tcp-syn-top1000-TARGET.txt 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 18:48 IST
Warning: 192.168.56.102 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.56.102
Host is up (0.052s latency).
Not shown: 976 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
512/tcp  open     exec
513/tcp  open     login
514/tcp  open     shell
1099/tcp open     rmiregistry
1524/tcp open     ingreslock
2049/tcp open     nfs
2121/tcp open     ccproxy-ftp
3306/tcp open     mysql
3367/tcp filtered satvid-datalnk
5432/tcp open     postgresql
5900/tcp open     vnc
6000/tcp open     X11
6667/tcp open     irc
8009/tcp open     ajp13
```

TCP SCAN



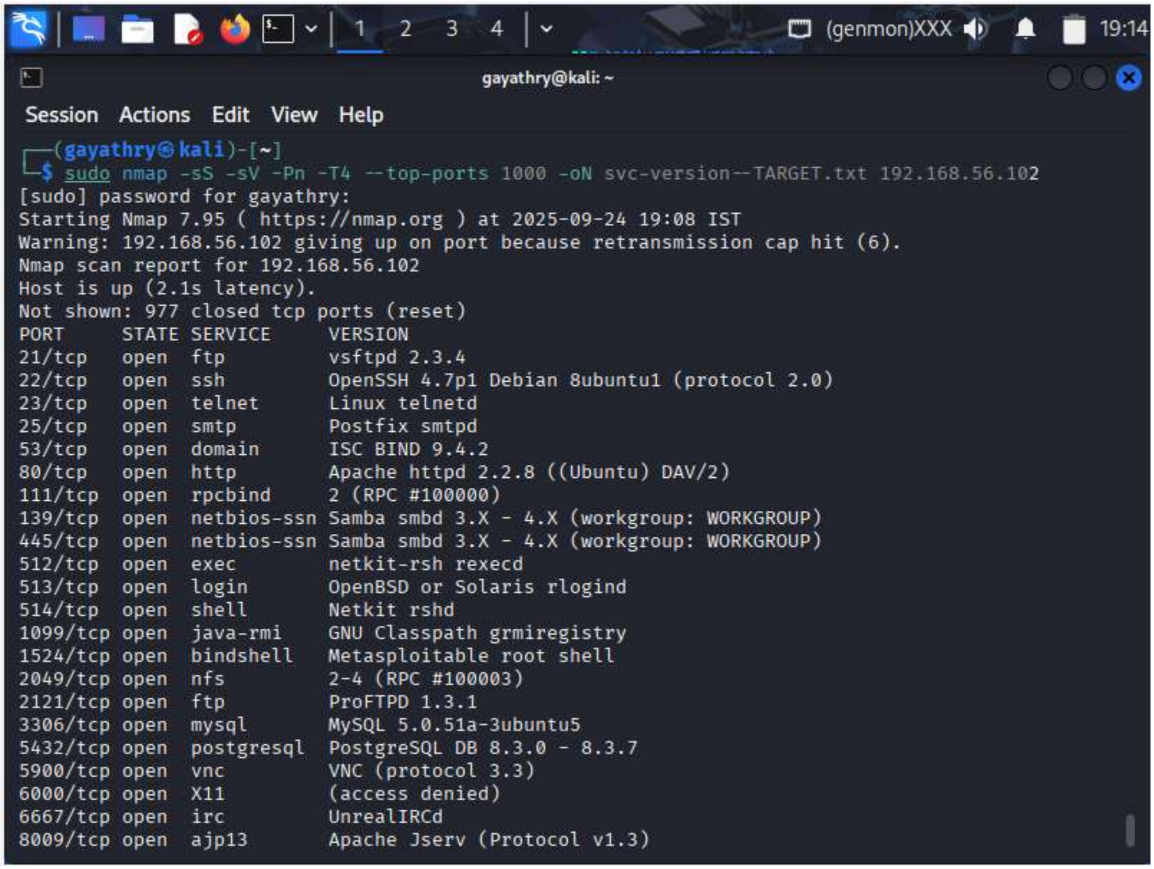
```
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (94%), Slirp (94%), AT&T embedded (92%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (94%), AT&T BGW210 voice gateway (92%
), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.37 seconds

┌──(gayathry㉿kali)-[~]
└─$ sudo nmap -sU -Pn -T3 -p 1-2000 -oN udp-Target.txt 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 19:21 IST
Nmap scan report for 192.168.56.102
Host is up (0.045s latency).
Not shown: 1997 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
111/udp open  rpcbind
137/udp open  netbios-ns

Nmap done: 1 IP address (1 host up) scanned in 21.56 seconds

┌──(gayathry㉿kali)-[~]
└─$ 
```

UDP SCAN



```
┌──(gayathry㉿kali)-[~]
└─$ sudo nmap -O -Pn -T4 -oN os-detect-TARGET.txt 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 19:16 IST
Warning: 192.168.56.102 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.56.102
Host is up (0.016s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

OS Detection Scan



```
┌──(gayathry㉿kali)-[~]
└─$ sudo nmap -sS -sV -Pn -T4 --top-ports 1000 -oN svc-version--TARGET.txt 192.168.56.102
[sudo] password for gayathry:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-24 19:08 IST
Warning: 192.168.56.102 giving up on port because retransmission cap hit (6).
Nmap scan report for 192.168.56.102
Host is up (2.1s 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
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
```

SVC Detection Scan