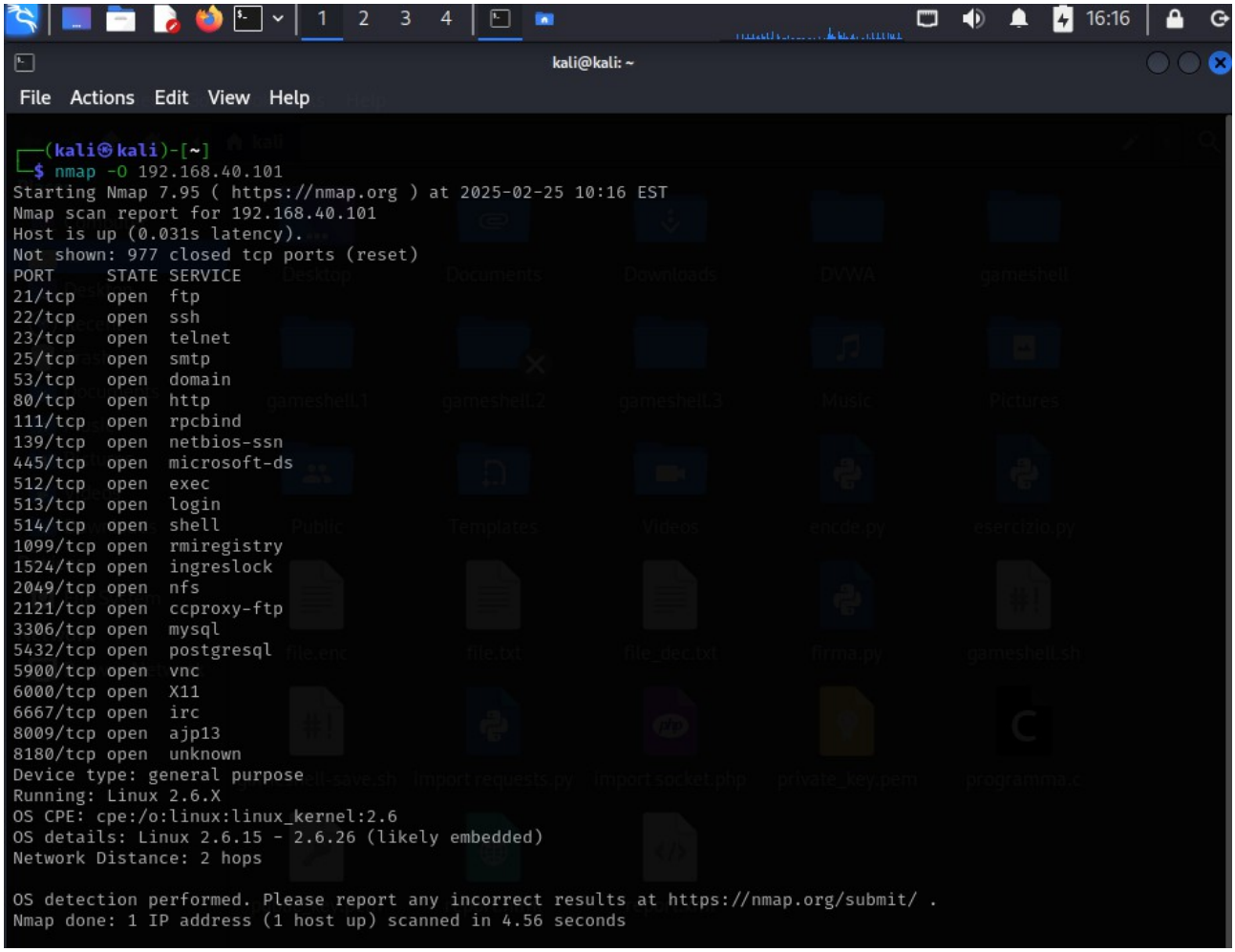
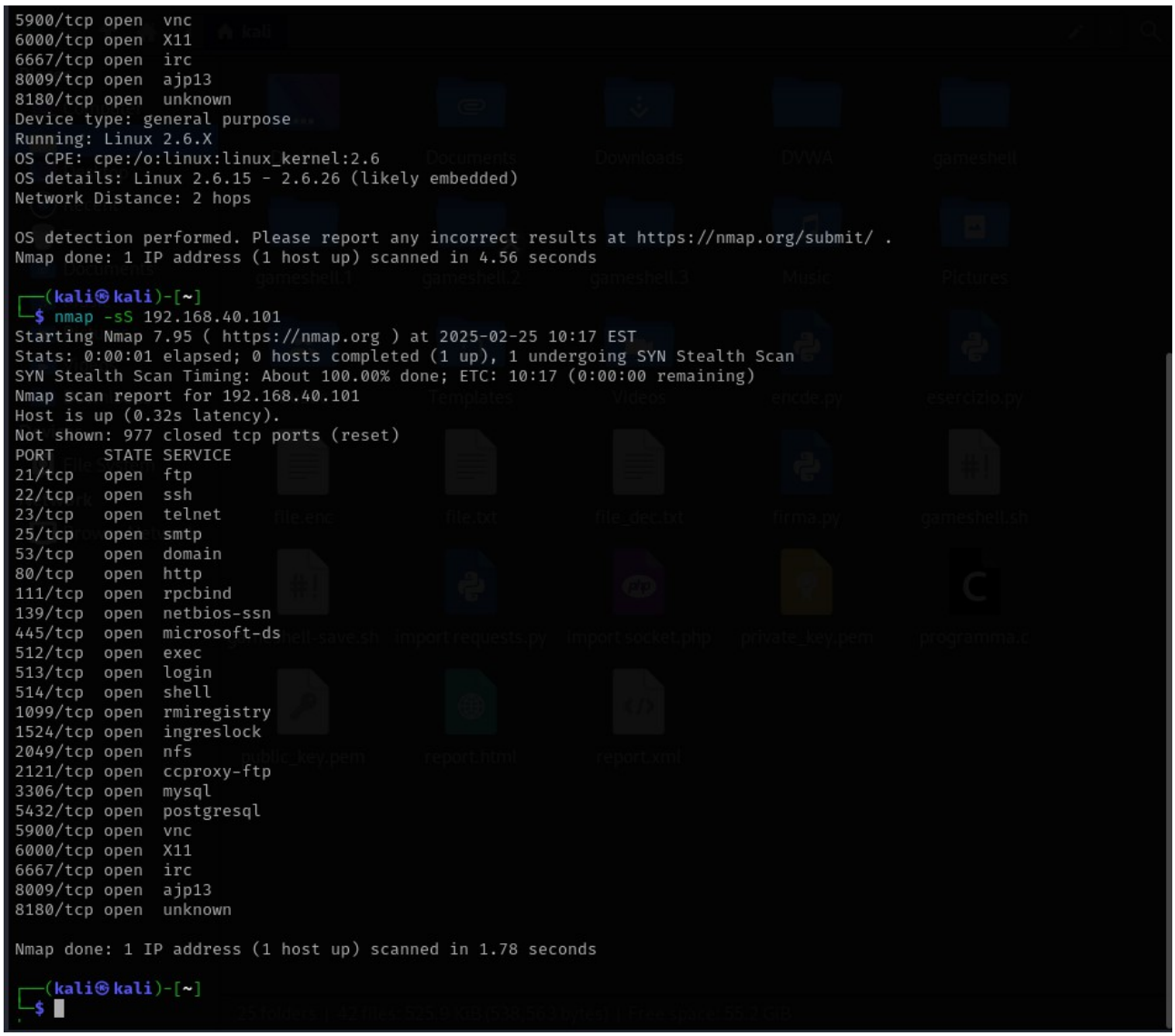

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -O 192.168.40.101
Starting Nmap 7.95 (https://nmap.org) at 2025-02-25 10:16 EST
Nmap scan report for 192.168.40.101
Host is up (0.031s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds


5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded)
Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds
(kali㉿kali)-[~]
$ nmap -sS 192.168.40.101
Starting Nmap 7.95 (https://nmap.org) at 2025-02-25 10:17 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 100.00% done; ETC: 10:17 (0:00:00 remaining)
Nmap scan report for 192.168.40.101
Host is up (0.32s 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
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
(kali㉿kali)-[~]
$

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.40.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 10:18 EST
Nmap scan report for 192.168.40.101
Host is up (0.068s latency).
Not shown: 977 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.40.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 10:25 EST
Nmap scan report for 192.168.40.101
Host is up (0.11s 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?
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  ccproxy-ftp?
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)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 175.95 seconds
```

Scan Summary

Nmap 7.95 was initiated at Tue Feb 25 08:16:32 2025 with these arguments:
/usr/lib/nmap/nmap --privileged -sS -O -oX report.xml 192.168.50.102

Verbosity: 0; Debug level 0

Nmap done at Tue Feb 25 08:16:51 2025; 1 IP address (1 host up) scanned in 19.71 seconds

192.168.50.102

Address

- 192.168.50.102 (ipv4)
- 08:00:27:06:2D:D3 - PCS Systemtechnik/Oracle VirtualBox virtual NIC (mac)

Ports

The 982 ports scanned but not shown below are in state: **closed**

- 982 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
7	tcp	open	echo	syn-ack			
9	tcp	open	discard	syn-ack			
13	tcp	open	daytime	syn-ack			
17	tcp	open	qotd	syn-ack			
19	tcp	open	chargen	syn-ack			
80	tcp	open	http	syn-ack			
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
1801	tcp	open	msmq	syn-ack			
2103	tcp	open	zephyr-clt	syn-ack			
2105	tcp	open	eklogin	syn-ack			
2107	tcp	open	msmq-mgmt	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
5432	tcp	open	postgresql	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8080	tcp	open	http-proxy	syn-ack			
8443	tcp	open	https-alt	syn-ack			

Remote Operating System Detection

- Used port: **7/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **32358/udp** (**closed**)
- OS match: **Microsoft Windows 10 1507 - 1607** (**100%**)

Misc Metrics (click to expand)