

Introduction to Nmap

Nmap (Network Mapper) is a free and open-source tool used for network scanning, host discovery, and security auditing. It was developed by Gordon Lyon (Fyodor) and is one of the most popular tools in cybersecurity and networking.

Nmap works by sending packets to a target system and analyzing the responses. This helps in finding active hosts, open ports, running services, and sometimes the operating system of the target machine. Because of its power and flexibility, Nmap is often called the “Swiss Army Knife of network security.”

The tool supports many types of scans, such as TCP scans, UDP scans, and stealth (SYN) scans. It also has an **Nmap Scripting Engine (NSE)** which allows users to run scripts for tasks like vulnerability detection and advanced service discovery.

Nmap is useful for:

- **System administrators** – to monitor and troubleshoot networks.
- **Cybersecurity professionals** – to perform penetration testing and identify weaknesses.
- **Students and researchers** – to learn about networking and security.

Nmap can scan a single system, multiple systems, or entire subnets, making it suitable for both small and large networks. It also supports different output formats for saving scan results.

In conclusion, Nmap is a powerful and essential tool in the field of networking and cybersecurity. Learning Nmap helps students and professionals understand how networks work and how to secure them effectively.

 Aim

The aim of this practical is to study and perform different types of network scanning using Nmap in Kali Linux. The objective is to understand how Nmap is used for host discovery, port scanning, service and version detection, operating system identification, and network security auditing.

 Requirements

- 1. Hardware Requirements:**
- 2. A computer or laptop with at least 2 GB RAM and 20 GB storage**
- 3. Internet connection (optional, for updates)**
- 4. Software Requirements:**
- 5. Kali Linux (installed or running in VirtualBox/VMware)**
- 6. Nmap tool (pre-installed in Kali Linux)**
- 7. Knowledge Requirements:**
- 8. Basic understanding of networking (IP addresses, ports, services)**
- 9. Basic Linux command-line usage**

INDEX

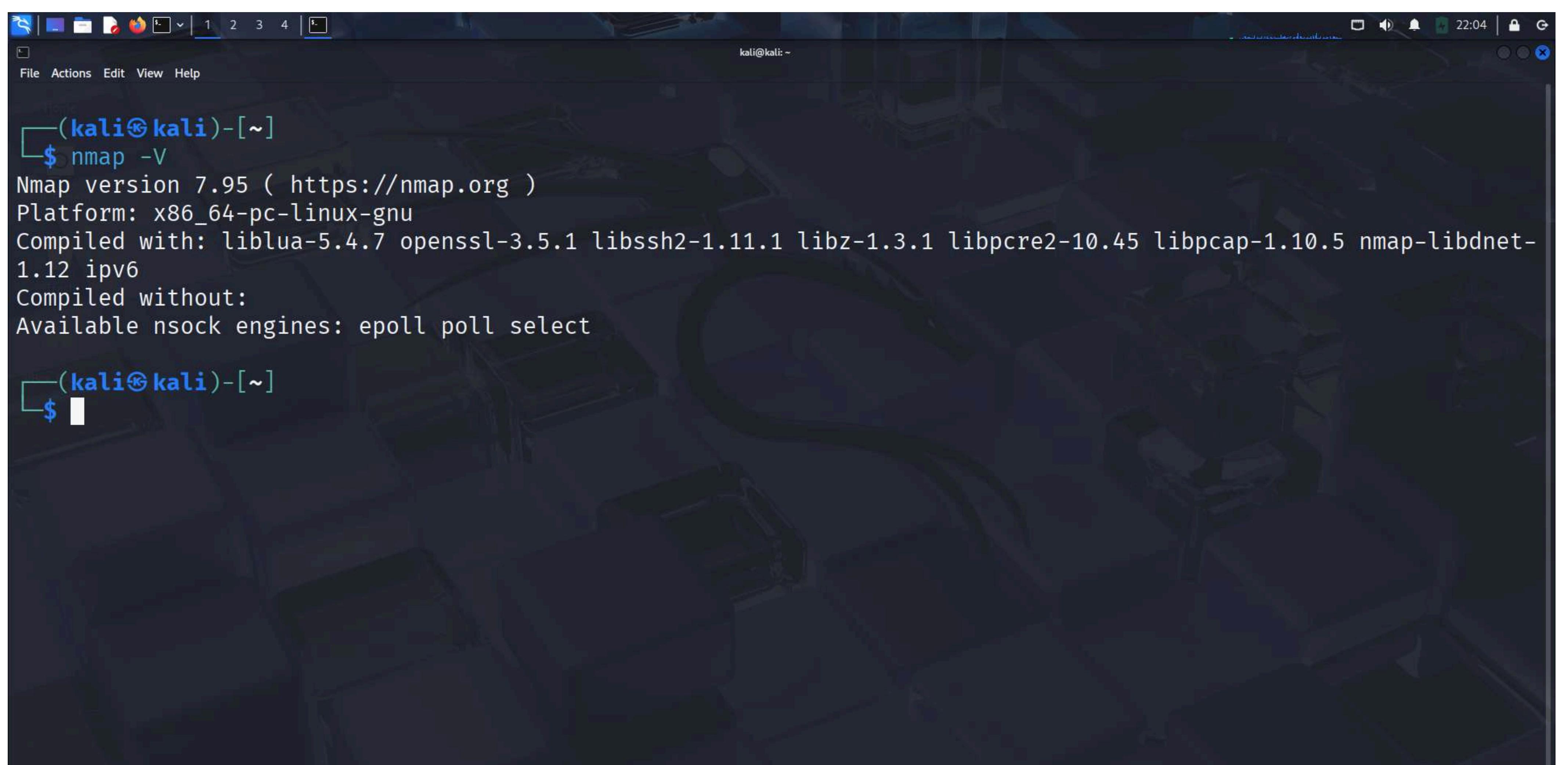
Sr. No.	Particular	Page No.	Remarks
1	Practical-1 Check NMAP Version	1	
2	Practical-2 Ping Scan	2-3	
3	Practical-3 Default Port Scan	4	
4	Practical-4 Scan Specific Port	5	
5	Practical-5 Scan Multiple Ports	6	
6	Practical-6 Scan Port Range	7	
7	Practical-7 Service Version detection	8	
8	Practical-8 Operating System Detection	9	
9	Practical-9 Aggressive Scan	10-12	
10	Practical-10 Scan Multiple IPs	13	
11	Practical-11 Scan Entire Subnet	14	
12	Practical-12 Stealth Scan(SYN Scan)	15	
13	Practical-13 UDP Scan	16	
14	Practical-14 Save Output to File	17	
15	Practical-15 Script Scan (NSE)	18-20	
16	Practical-16 Fast Scan	21	
17	Practical-17 Scan without DNS resolution	22	
18	Practical-18 Detect Firewall/Packet Filters	23-24	
19	Practical-19 Idle Scan (Anonymous Scan)	25-26	
20	Practical-20 Timing Templates	27	
21	Practical-21 Scan and Save Output in All formats	28	
22	Practical-22 Detect Vulnerabilities (NSE Scripts)	29-36	
23	Practical-23 Detect Malware/Backdoors	37	
24	Practical-24 Detect HTTP Info (Web Servers)	38	
25	Practical-25 Scan IPv6 Targets	39	
	Conclusion	40	

Practical 1: Check Nmap Version

Command:

nmap -V

Explanation: Shows the version of Nmap installed.



```
(kali㉿kali)-[~]
$ nmap -V
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.1 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
(kali㉿kali)-[~]
$
```

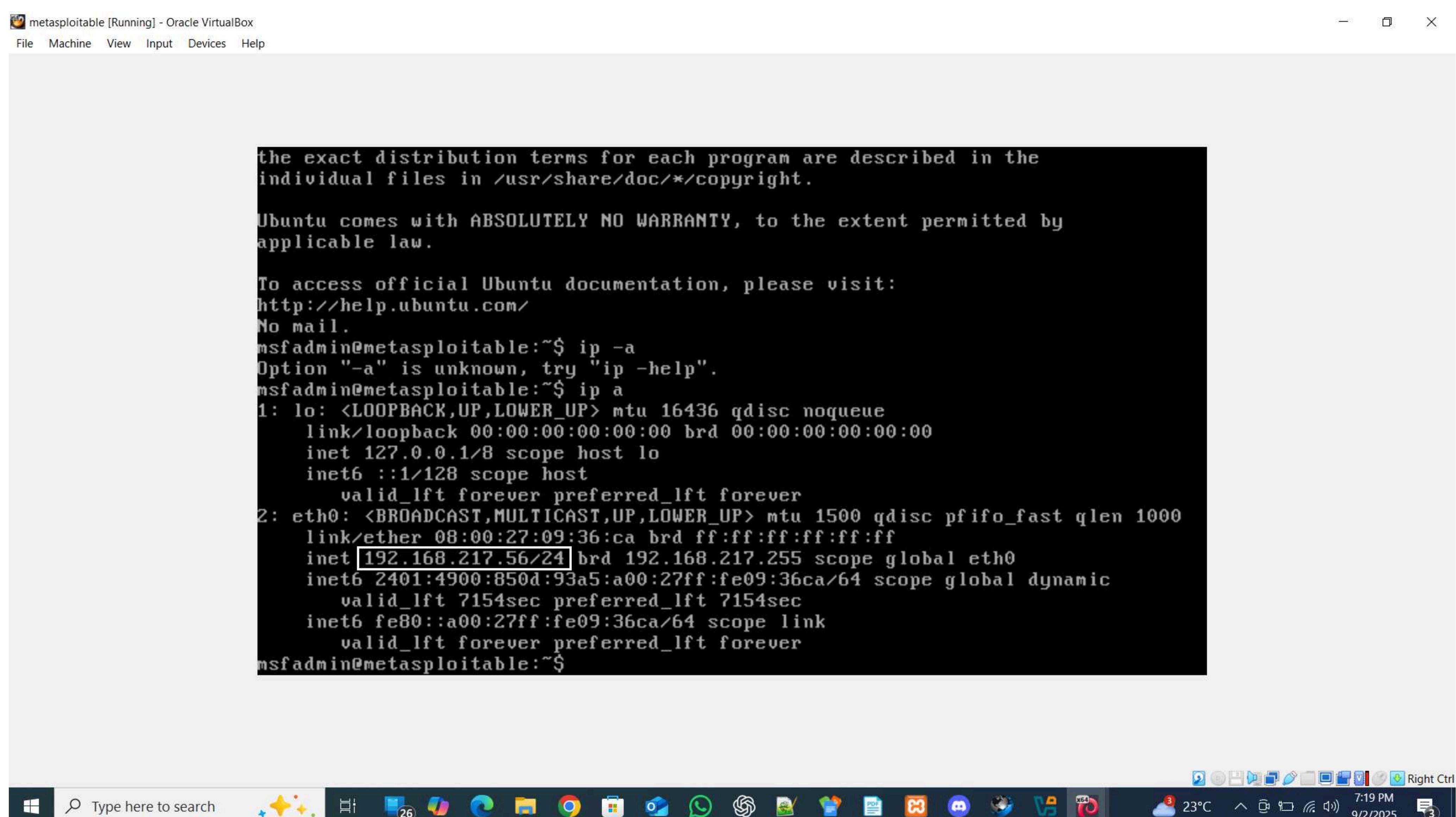
Practical 2: Ping Scan (Host Discovery)

Command:

nmap -sn <target-ip>

Explanation: Checks if a host is alive without scanning ports.

Firstly we need a metasploitable machine to perform ping scan:



```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ip -a
Option "-a" is unknown, try "ip -help".
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:09:36:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.217.56/24 brd 192.168.217.255 scope global eth0
        inet6 2401:4900:850d:93a5:a00:27ff:fe09:36ca/64 scope global dynamic
            valid_lft 7154sec preferred_lft 7154sec
        inet6 fe80::a00:27ff:fe09:36ca/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

IP Address of metasploitable machine is :

192.168.217.56/24

To find IP we use command: ip

```
(kali㉿kali)-[~]
$ nmap -sn 192.168.217.56/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:15 EDT
Nmap scan report for 192.168.217.0
Host is up (0.0021s latency).
Nmap scan report for 192.168.217.1
Host is up (1.00s latency).
Nmap scan report for 192.168.217.2
Host is up (1.00s latency).
Nmap scan report for 192.168.217.3
Host is up (1.00s latency).
Nmap scan report for 192.168.217.4
Host is up (1.00s latency).
Nmap scan report for 192.168.217.5
Host is up (1.00s latency).
Nmap scan report for 192.168.217.6
Host is up (1.00s latency).
Nmap scan report for 192.168.217.7
Host is up (0.0027s latency).
Nmap scan report for 192.168.217.8
```

```
Host is up (0.39s latency).
Nmap scan report for 192.168.217.248
Host is up (0.39s latency).
Nmap scan report for 192.168.217.249
Host is up (0.39s latency).
Nmap scan report for 192.168.217.250
Host is up (0.39s latency).
Nmap scan report for 192.168.217.251
Host is up (0.39s latency).
Nmap scan report for 192.168.217.252
Host is up (0.39s latency).
Nmap scan report for 192.168.217.253
Host is up (0.39s latency).
Nmap scan report for 192.168.217.254
Host is up (0.39s latency).
Nmap scan report for 192.168.217.255
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 7.15 seconds

(kali㉿kali)-[~]
$
```

“Host is up” shows that machine is live

Practical 3: Default Port Scan

Command:

nmap <target-ip>

Explanation: Scans the most common 1000 TCP ports.

```
(kali㉿kali)-[~]
$ nmap 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:41 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0096s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

```
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

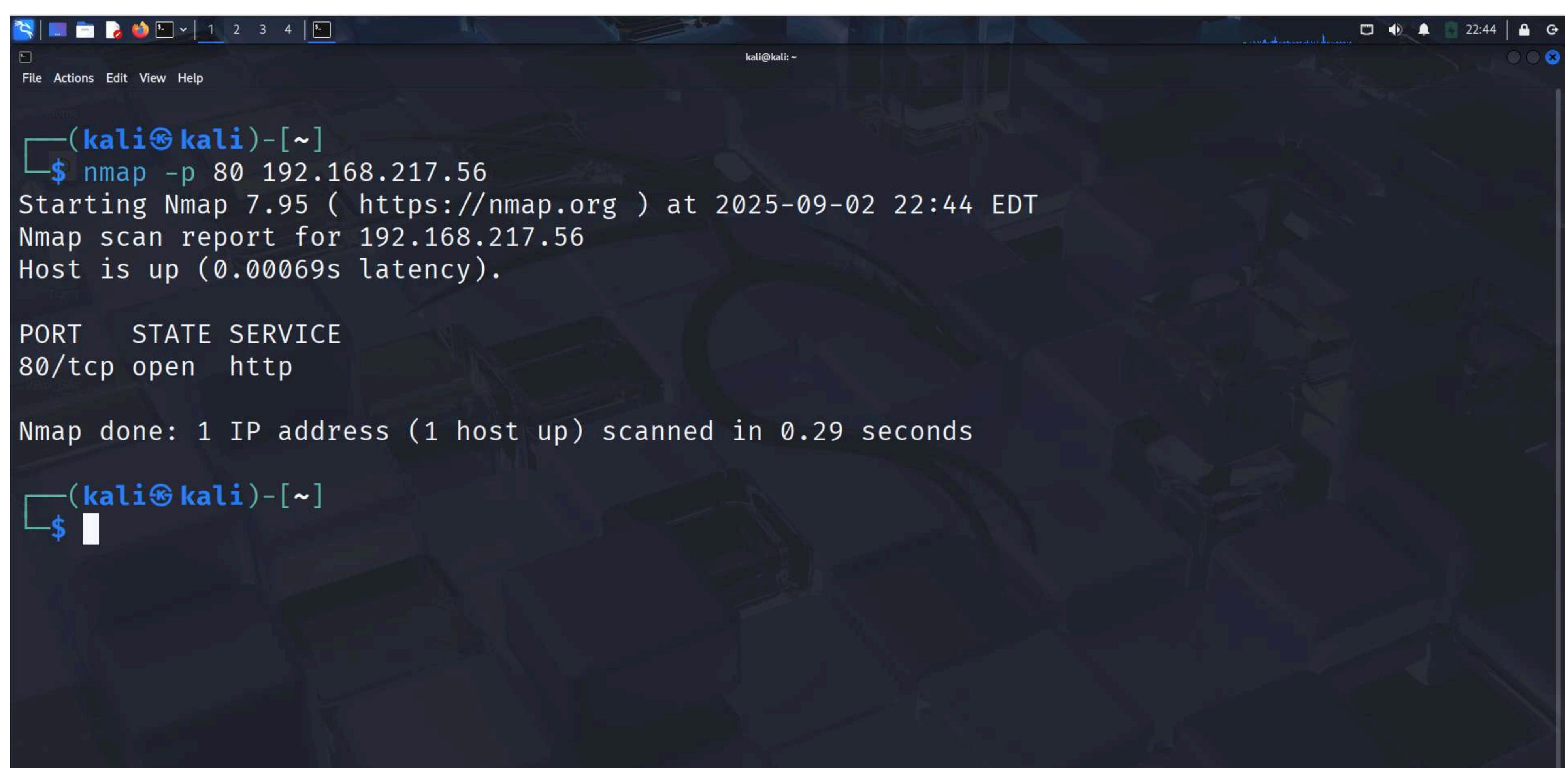
Nmap done: 1 IP address (1 host up) scanned in 5.26 seconds
```

Practical 4: Scan Specific Port

Command:

nmap -p 80 <target-ip>

Explanation: Scans only port 80 on the target



```
(kali㉿kali)-[~]
$ nmap -p 80 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:44 EDT
Nmap scan report for 192.168.217.56
Host is up (0.00069s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

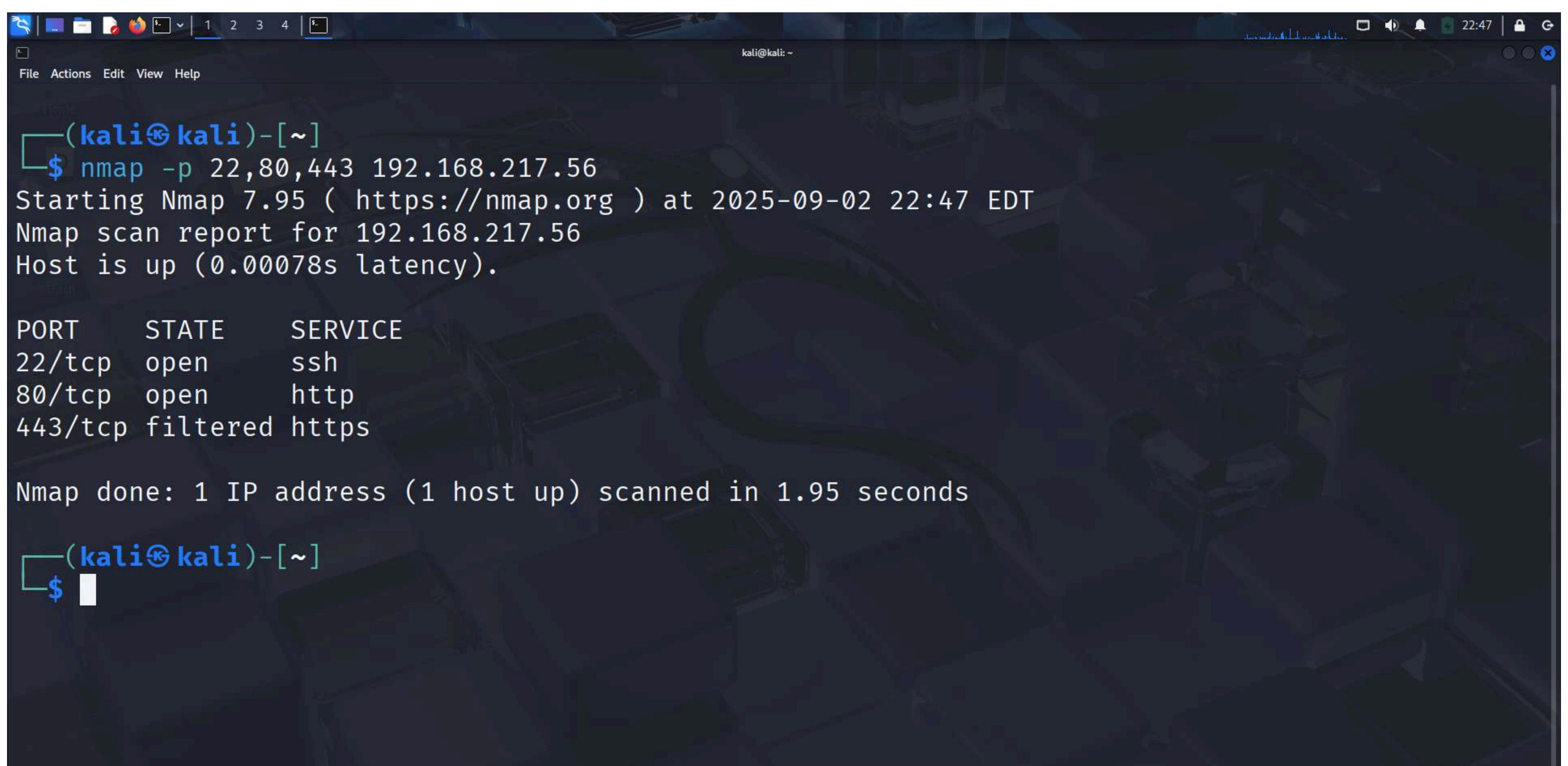
$
```

Practical 5: Scan Multiple Ports

Command:

nmap -p 22,80,443 <target-ip>

Explanation: Scans selected ports (22, 80, and 443)



```
(kali㉿kali)-[~]
$ nmap -p 22,80,443 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:47 EDT
Nmap scan report for 192.168.217.56
Host is up (0.00078s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds

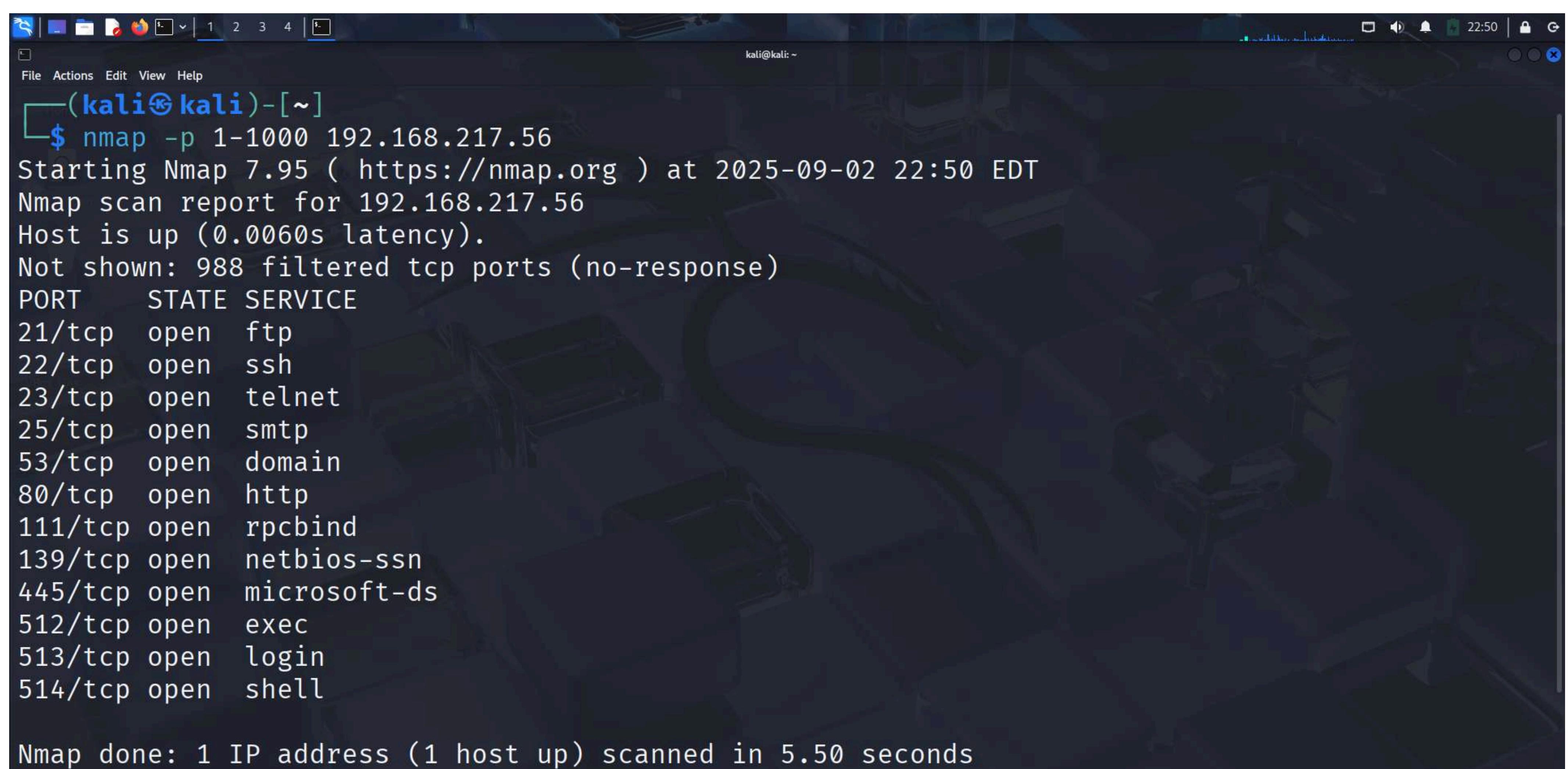
(kali㉿kali)-[~]
```

Practical 6: Scan Port Range

Command:

nmap -p 1-1000 <target-ip>

Explanation: Scans a range of ports (1 to 1000).



A screenshot of a terminal window on a Kali Linux desktop. The terminal shows the command \$ nmap -p 1-1000 192.168.217.56 being run. The output indicates that the host is up with 0.0060s latency. It lists 13 open TCP ports: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 80/tcp (http), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 512/tcp (exec), 513/tcp (login), and 514/tcp (shell). A note states 'Not shown: 988 filtered tcp ports (no-response)'. The scan took 5.50 seconds.

```
(kali㉿kali)-[~]
$ nmap -p 1-1000 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:50 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0060s latency).

Not shown: 988 filtered tcp ports (no-response)
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

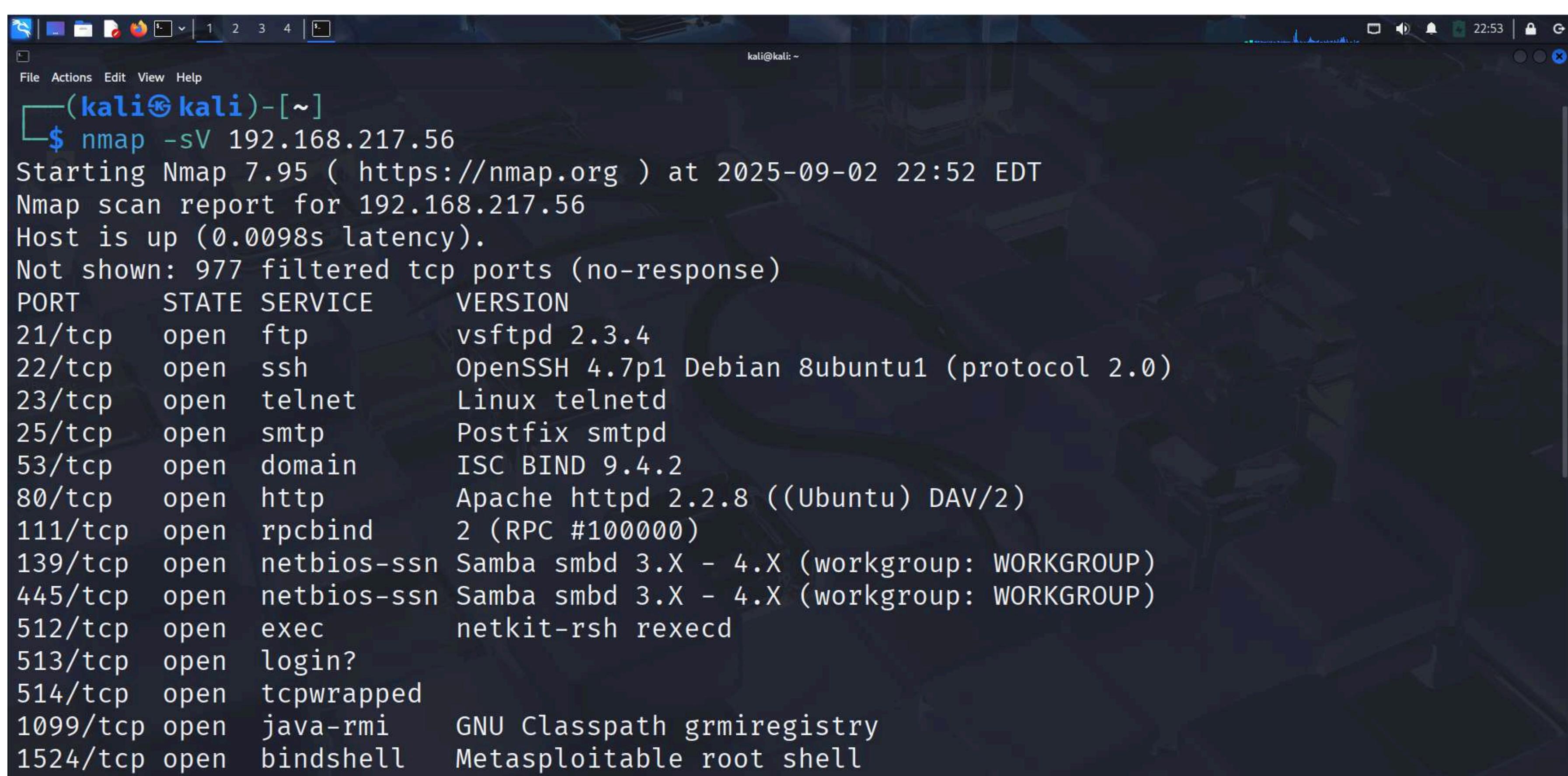
Nmap done: 1 IP address (1 host up) scanned in 5.50 seconds
```

Practical 7: Service Version Detection

Command:

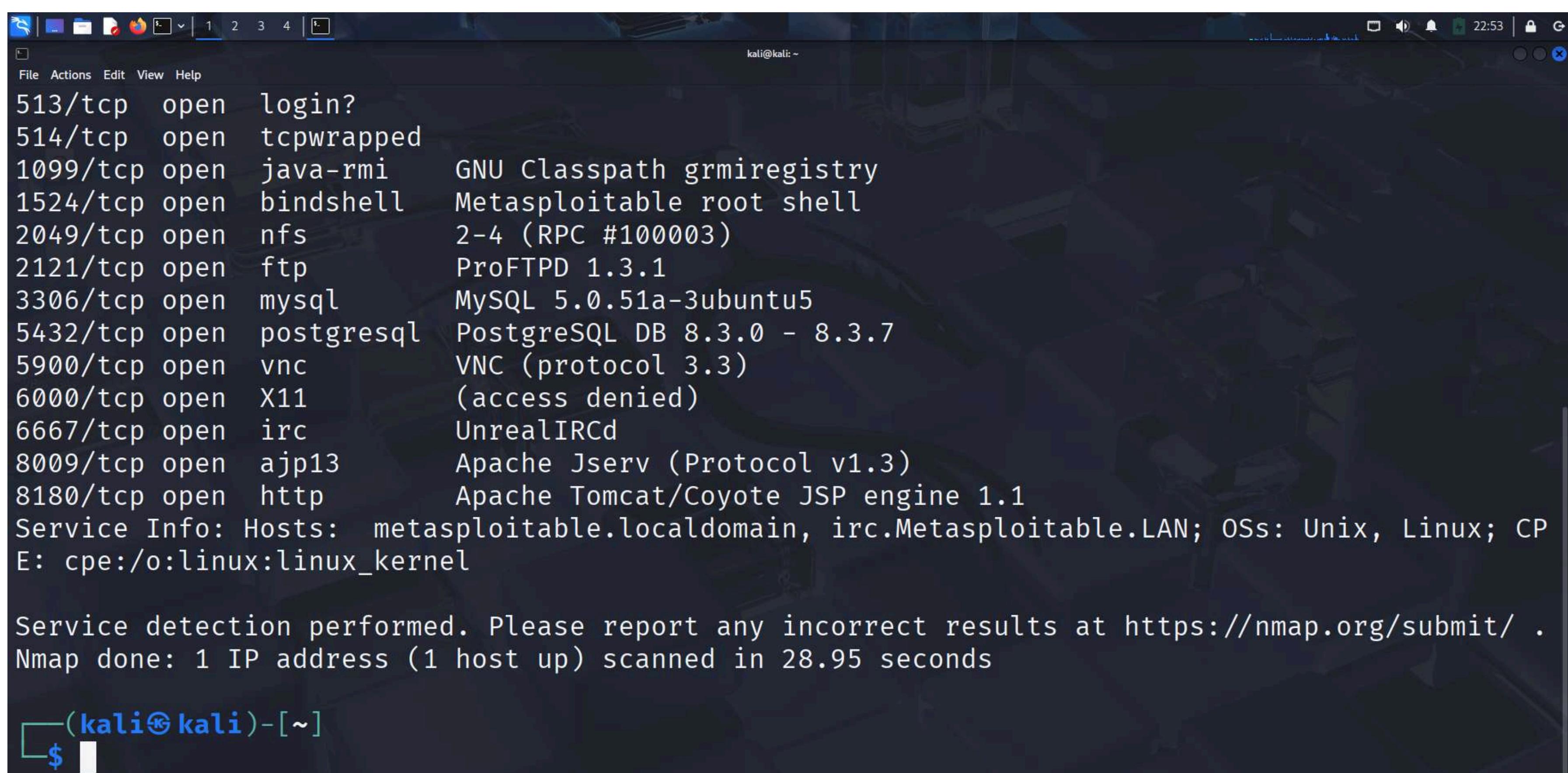
nmap -sV <target-ip>

Explanation: Detects the service and version running on open ports



```
(kali㉿kali)-[~]
$ nmap -sV 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:52 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0098s latency).

Not shown: 977 filtered tcp ports (no-response)
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 smptd
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?      login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
```



```
(kali㉿kali)-[~]
$ nmap -sV 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:53 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0098s latency).

Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
513/tcp   open  login?      login?
514/tcp   open  tcpwrapped
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)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP
E: cpe:/o:linux:linux_kernel

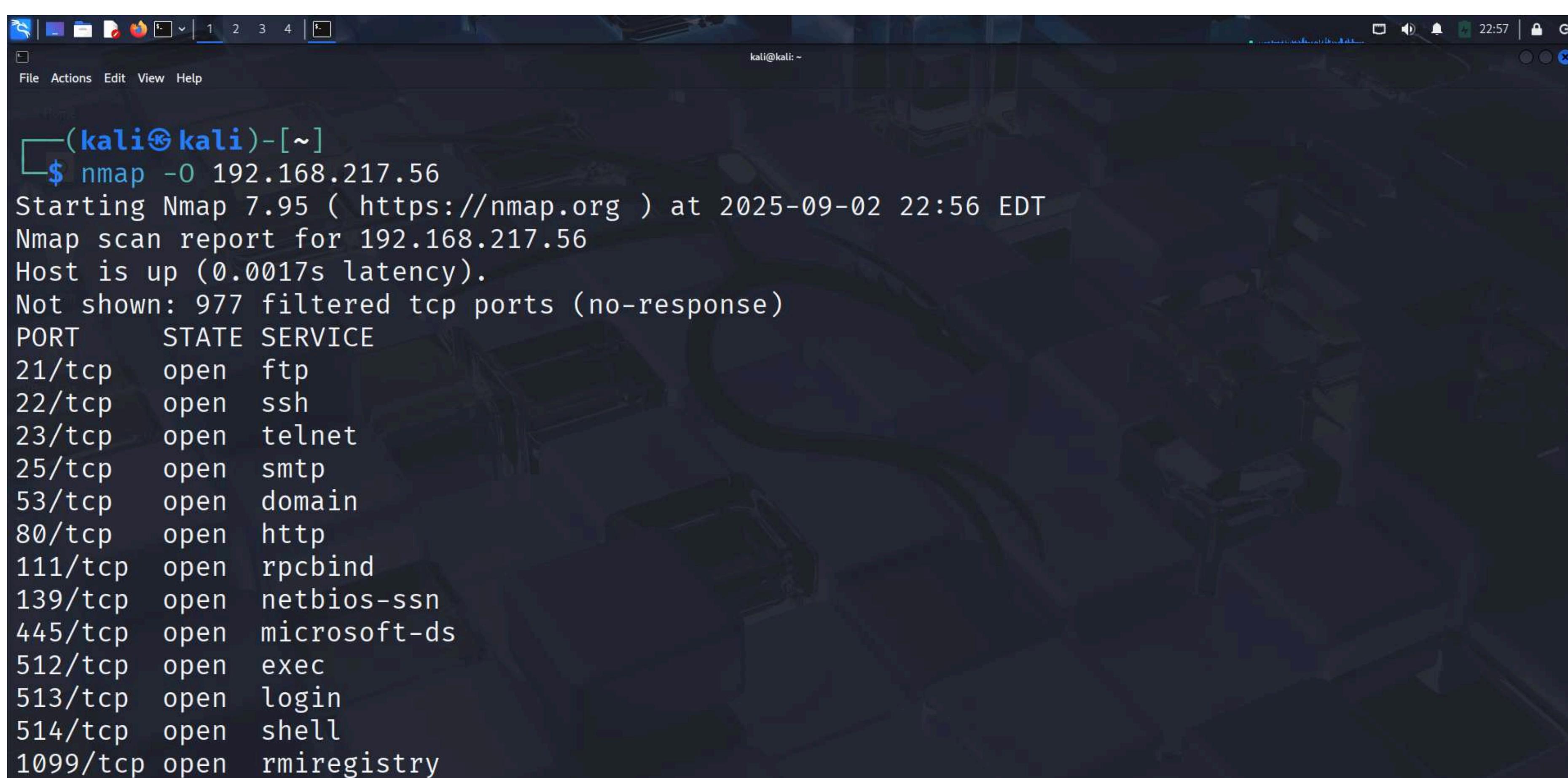
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.95 seconds
```

Practical 8: Operating System Detection

Command:

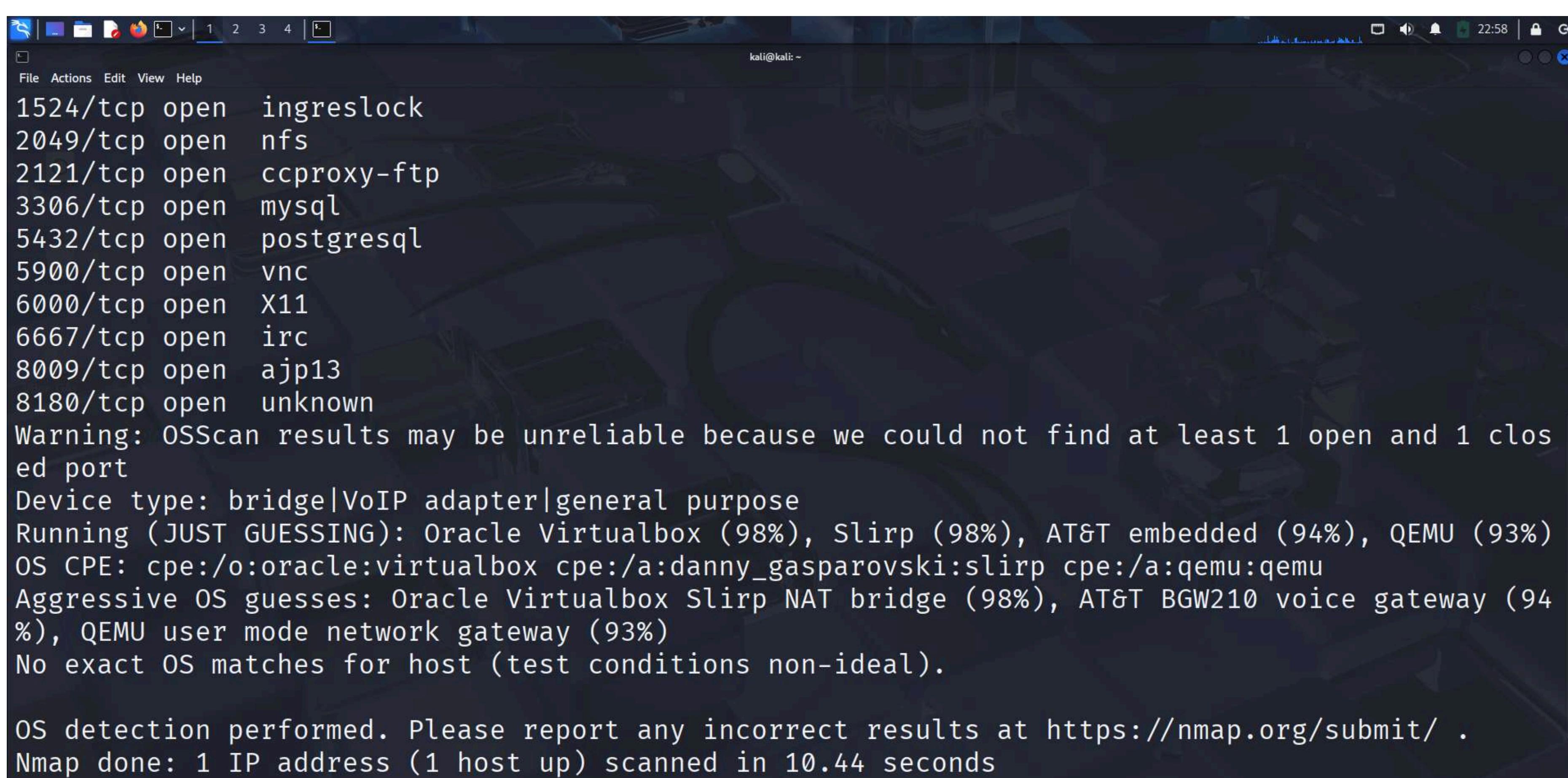
nmap -O <target-ip>

Explanation: Attempts to detect the target's operating system.



```
(kali㉿kali)-[~]
$ nmap -O 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 22:56 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0017s latency).

Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (94%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (94%),
QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

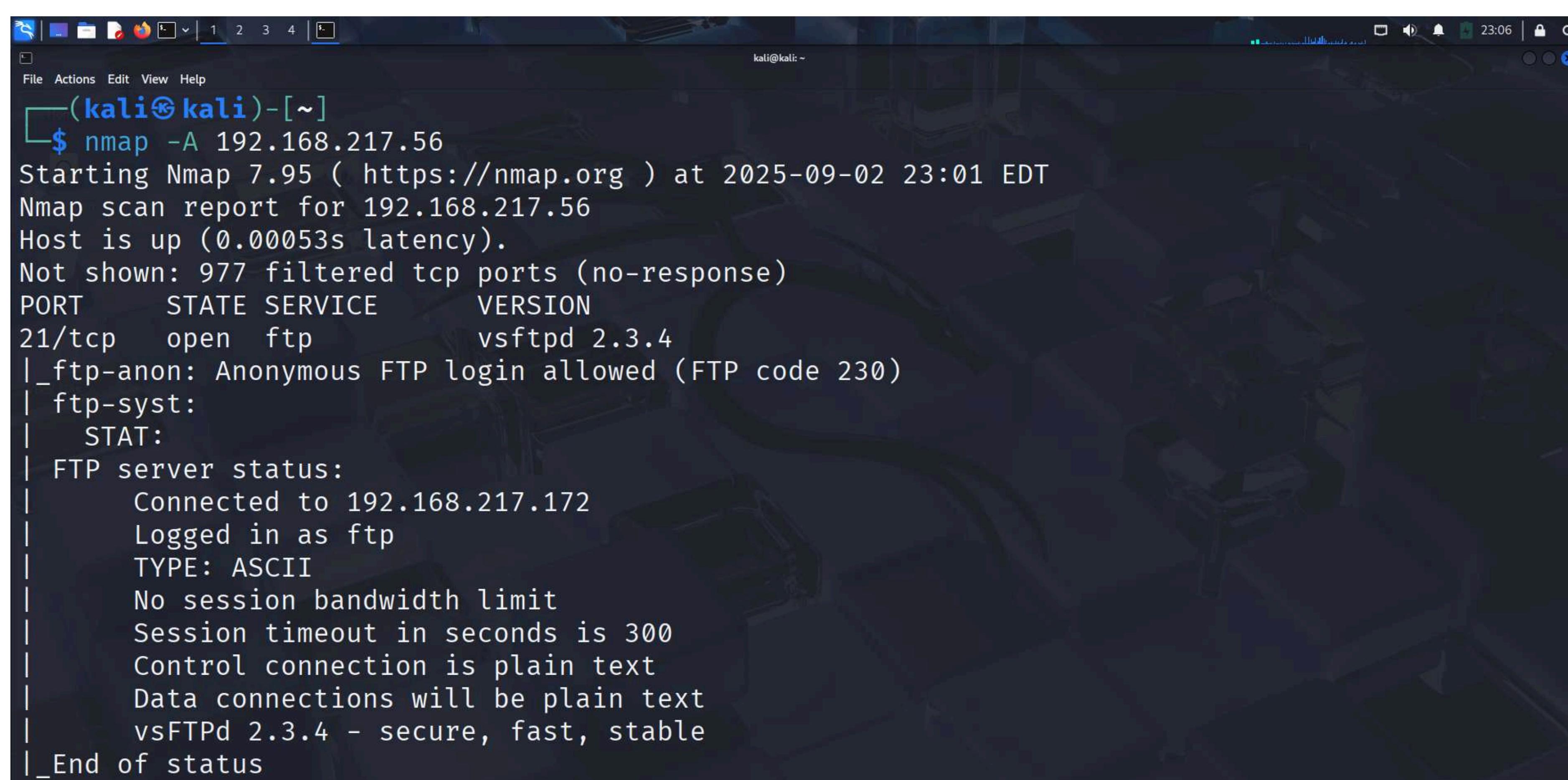
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.44 seconds
```

Practical 9: Aggressive Scan (All-in-One)

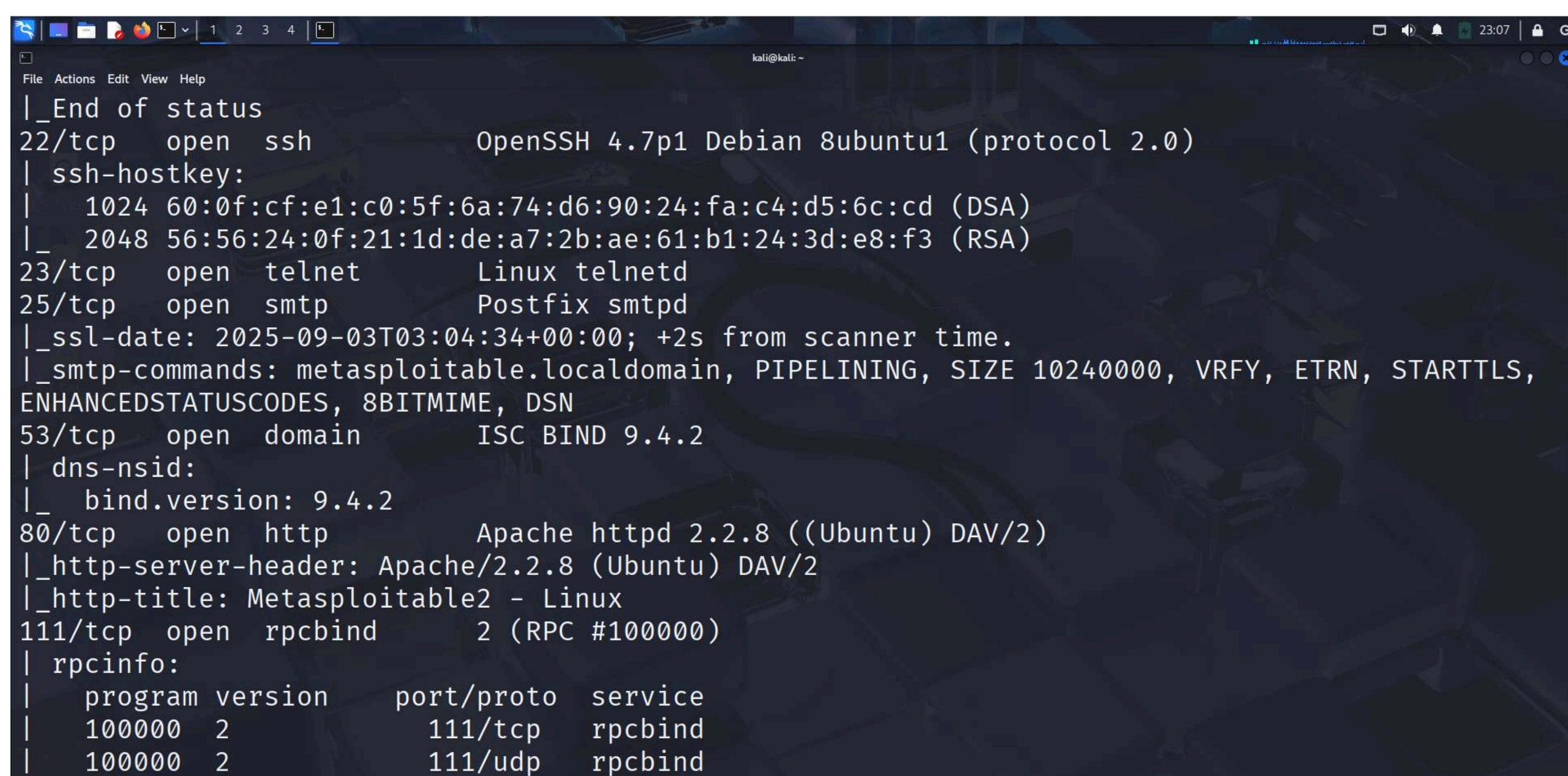
Command:

nmap -A <target-ip>

Explanation: Performs OS detection, version detection, script scanning, and traceroute.



```
(kali㉿kali)-[~]
$ nmap -A 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:01 EDT
Nmap scan report for 192.168.217.56
Host is up (0.00053s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.217.172
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
```



```
|_End of status
22/tcp  open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet        Linux telnetd
25/tcp  open  smtp         Postfix smtpd
|_ssl-date: 2025-09-03T03:04:34+00:00; +2s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain       ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp  open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp   rpcbind
```

```
kali@kali: ~
111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     42615/udp mountd
|   100005  1,2,3     44098/tcp mountd
|   100021  1,3,4     38957/udp nlockmgr
|   100021  1,3,4     44060/tcp nlockmgr
|   100024  1          44641/udp status
|   100024  1          59964/tcp status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
```

```
kali@kali: ~
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 14
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, LongColumnFlag, ConnectWithDatabase
|   Status: Autocommit
|   Salt: FBUDwLS>xdknf7|,d4si
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-09-03T03:04:34+00:00; +2s from scanner time.
5900/tcp open  vnc        VNC (protocol 3.3)
| vnc-info:
```

```
kali@kali: ~
5900/tcp open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|   VNC Authentication (2)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:53:59
|   source ident: nmap
|   source host: 5920C25A.E44F82CA.FFFA6D49.IP
|_ error: Closing Link: oumivfjkn[192.168.217.172] (Quit: oumivfjkn)
8009/tcp open  ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
```

```
|_ajp-methods: Failed to get a valid response for the OPTION request  
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
|_http-favicon: Apache Tomcat  
|_http-title: Apache Tomcat/5.5  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: bridge|VoIP adapter|general purpose  
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)  
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu  
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CP  
E: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_smb2-time: Protocol negotiation failed (SMB2)  
| smb-security-mode:  
|   account_used: <blank>  
|   authentication_level: user
```

```
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
| smb-os-discovery:  
|   OS: Unix (Samba 3.0.20-Debian)  
|   Computer name: metasploitable  
|   NetBIOS computer name:  
|   Domain name: localdomain  
|   FQDN: metasploitable.localdomain  
|_ System time: 2025-09-02T23:04:07-04:00  
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 1s  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 0.39 ms 192.168.217.56  
  
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 197.59 seconds
```

Practical 10: Scan Multiple IPs

Command:

nmap <ip1> <ip2>

Explanation: Scans more than one system at the same time.

```
(kali㉿kali)-[~]
$ nmap 192.168.217.172 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:20 EDT
Nmap scan report for 192.168.217.172
Host is up (0.0030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap scan report for 192.168.217.56
Host is up (0.014s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

```
File Actions Edit View Help
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

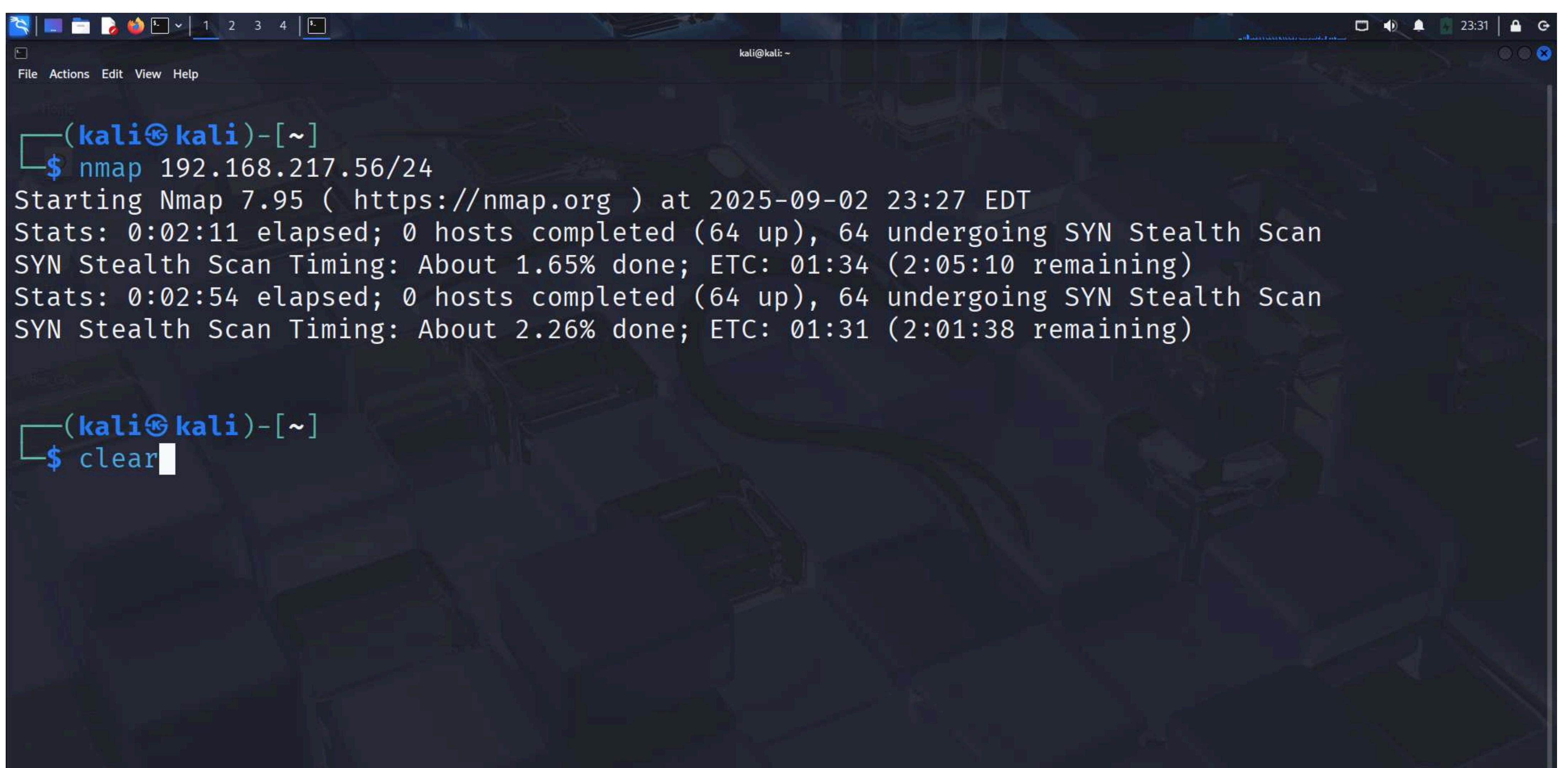
Nmap done: 2 IP addresses (2 hosts up) scanned in 7.67 seconds
```

Practical 11: Scan Entire Subnet

Command:

nmap 192.168.1.0/24

Explanation: Scans all devices in the given subnet.



The screenshot shows a terminal window on a Kali Linux desktop. The terminal prompt is '(kali㉿kali)-[~]'. The user has run the command '\$ nmap 192.168.217.56/24'. The output shows the progress of the SYN Stealth Scan. It starts by stating the scan is at 2025-09-02 23:27 EDT, with 64 hosts undergoing the scan. The SYN Stealth Scan Timing indicates about 1.65% done with an estimated time of 01:34 remaining. After a short pause, it shows another update where 64 hosts are completed and 64 are still being scanned. The SYN Stealth Scan Timing is now about 2.26% done with an estimated time of 01:31 remaining. Finally, the user types '\$ clear' to clear the terminal screen.

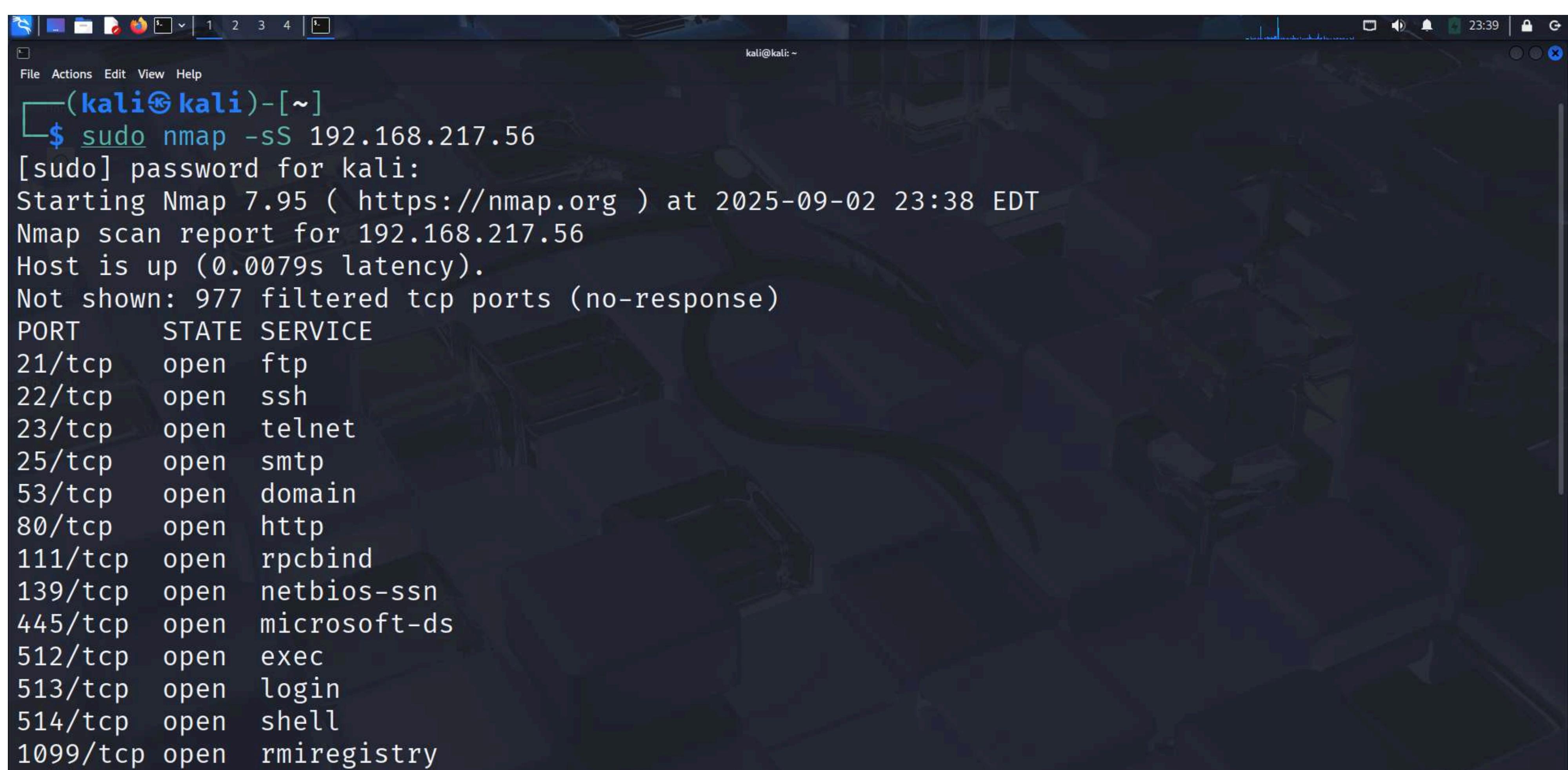
**It will take approximately 1 – 2 hours to complete scan the entire subnet,
We can check the progress by pressing “space” key**

Practical 12: Stealth Scan (SYN Scan)

Command:

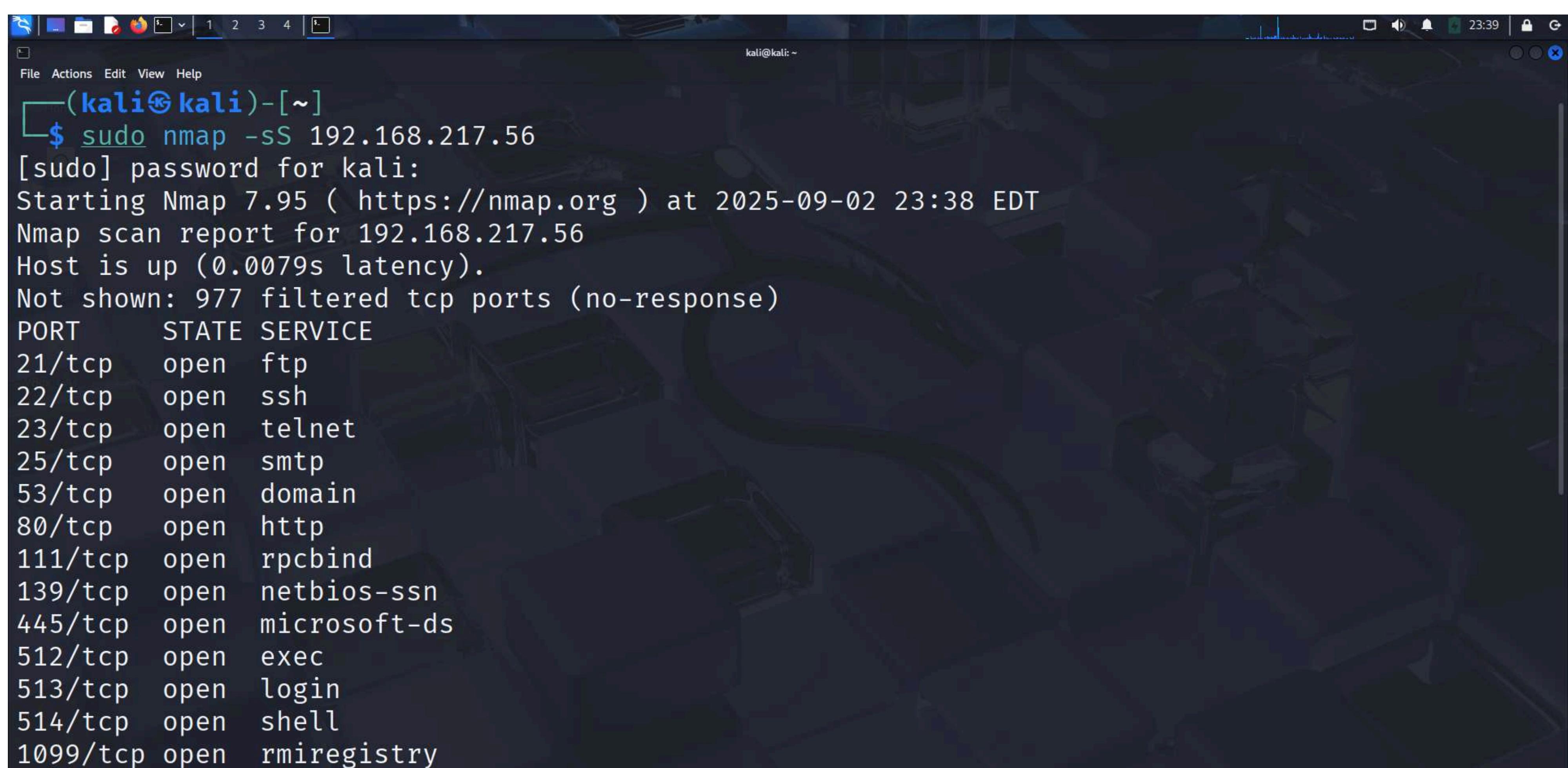
sudo nmap -sS <target-ip>

Explanation: Performs a stealthy SYN scan (half-open scan).



```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.217.56
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:38 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0079s latency).

Not shown: 977 filtered tcp ports (no-response)
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
```



```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.217.56
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:38 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0079s latency).

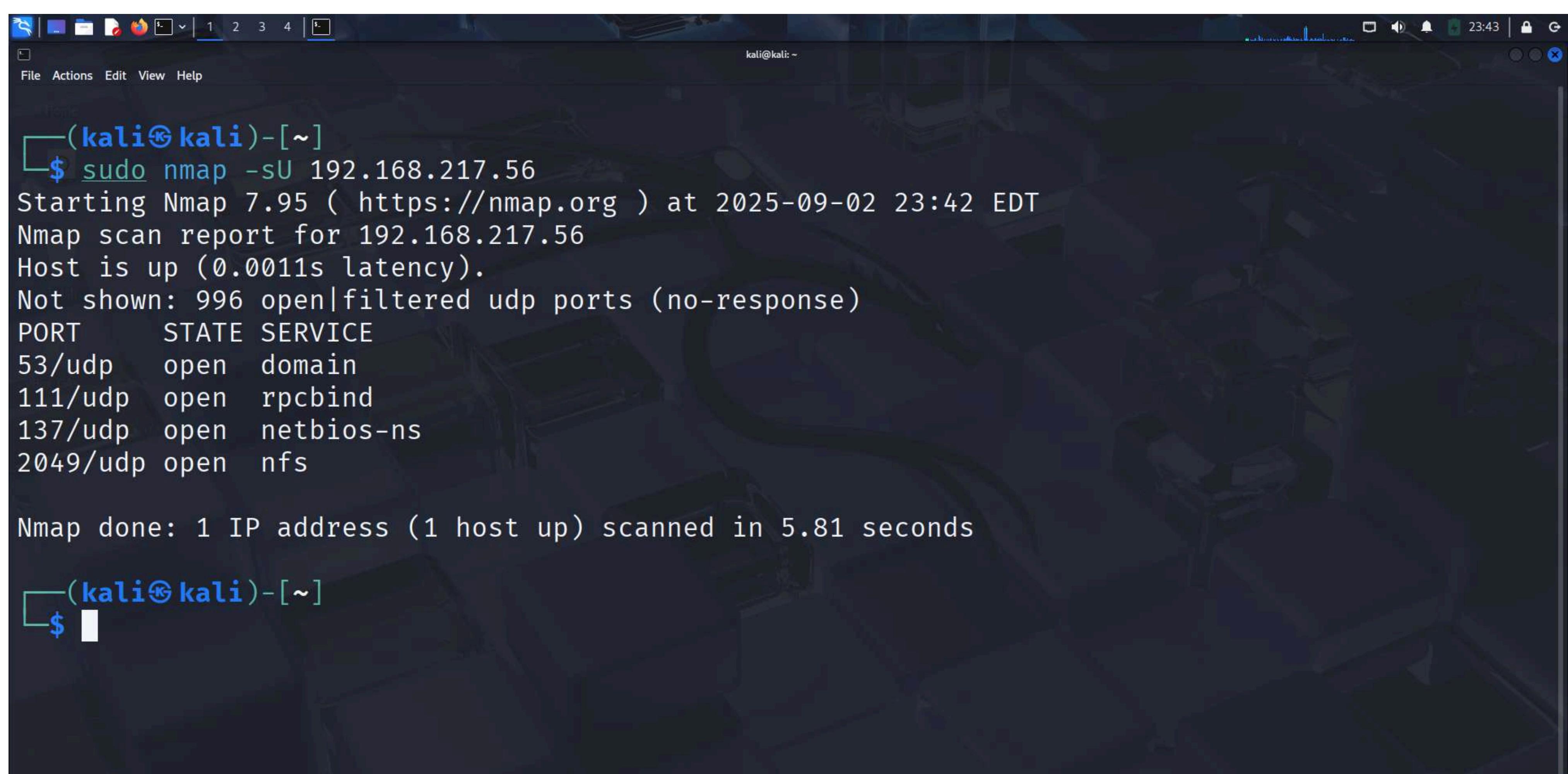
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
```

Practical 13: UDP Scan

Command:

sudo nmap -sU <target-ip>

Explanation: Scans for open UDP ports.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal prompt is `(kali㉿kali)-[~]`. The user runs the command `sudo nmap -sU 192.168.217.56`. The output shows the following results:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 23:42 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0011s latency).
Not shown: 996 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs

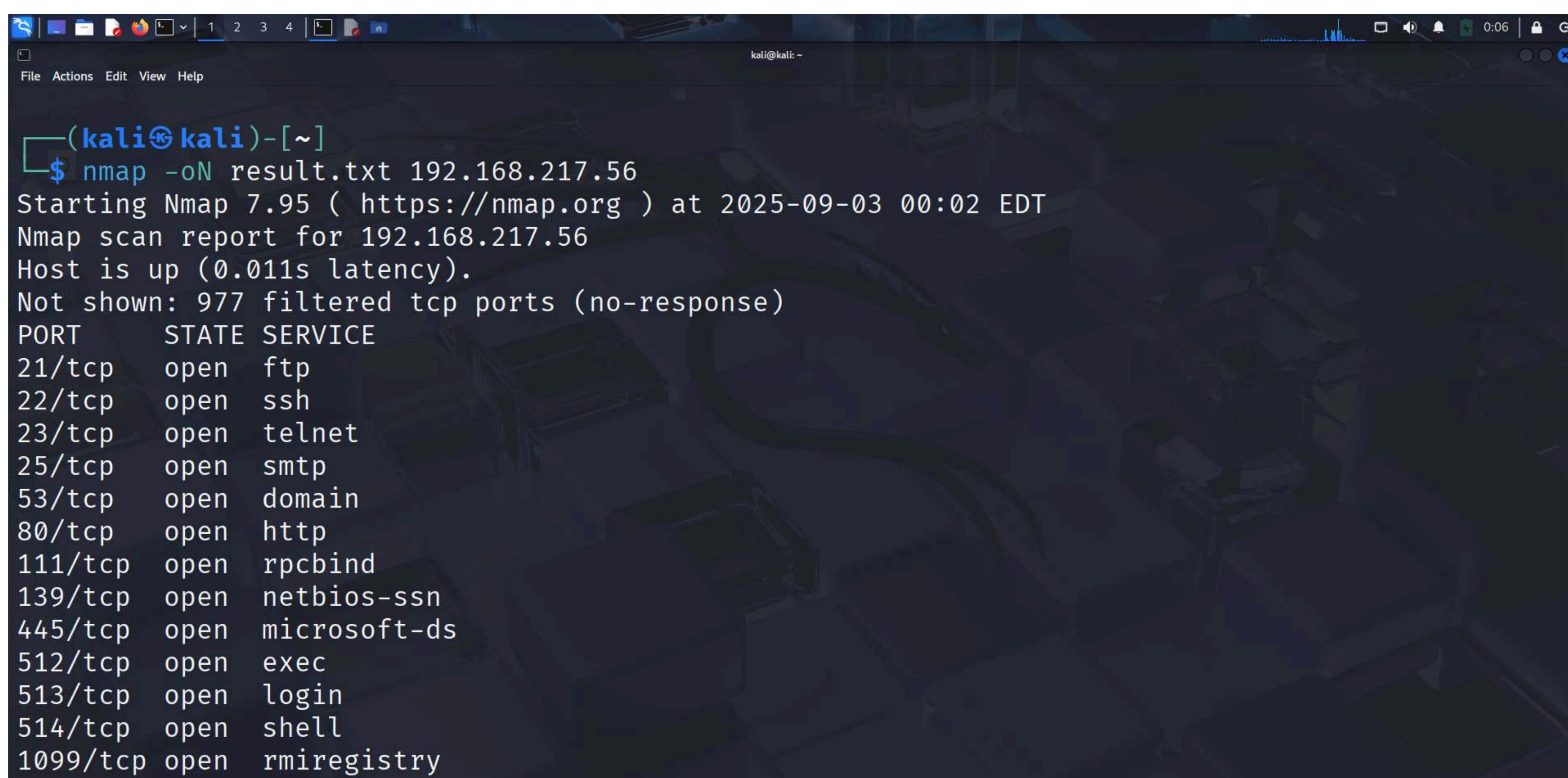
Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

The terminal window has a dark background with light-colored text. It includes standard Linux desktop icons in the top bar and a terminal history at the bottom.

Practical 14: Save Output to File Command:

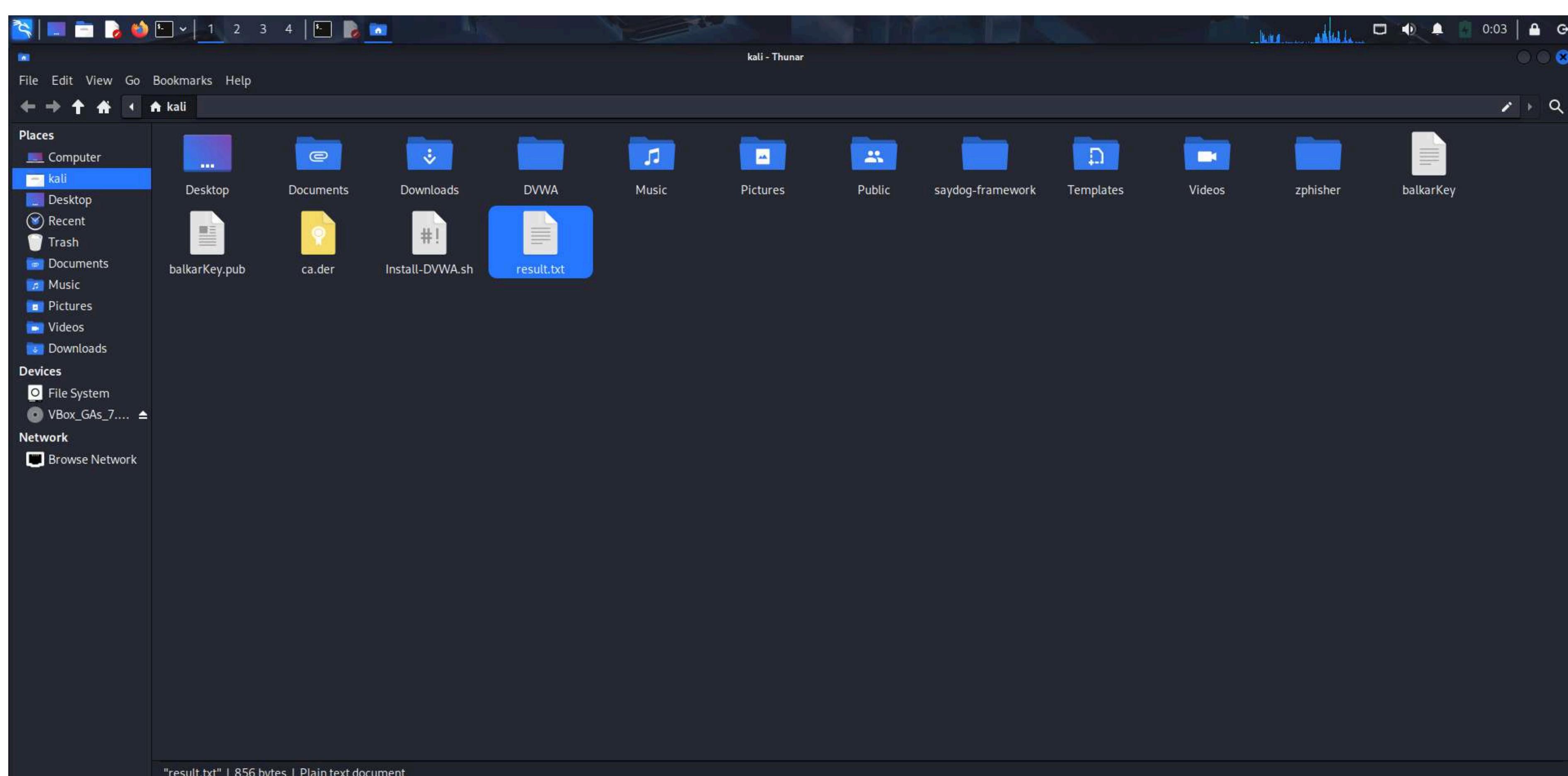
nmap -oN result.txt <target-ip>

Explanation: Saves the scan results into a text file.



```
(kali㉿kali)-[~]
$ nmap -oN result.txt 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:02 EDT
Nmap scan report for 192.168.217.56
Host is up (0.011s latency).

Not shown: 977 filtered tcp ports (no-response)
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
```

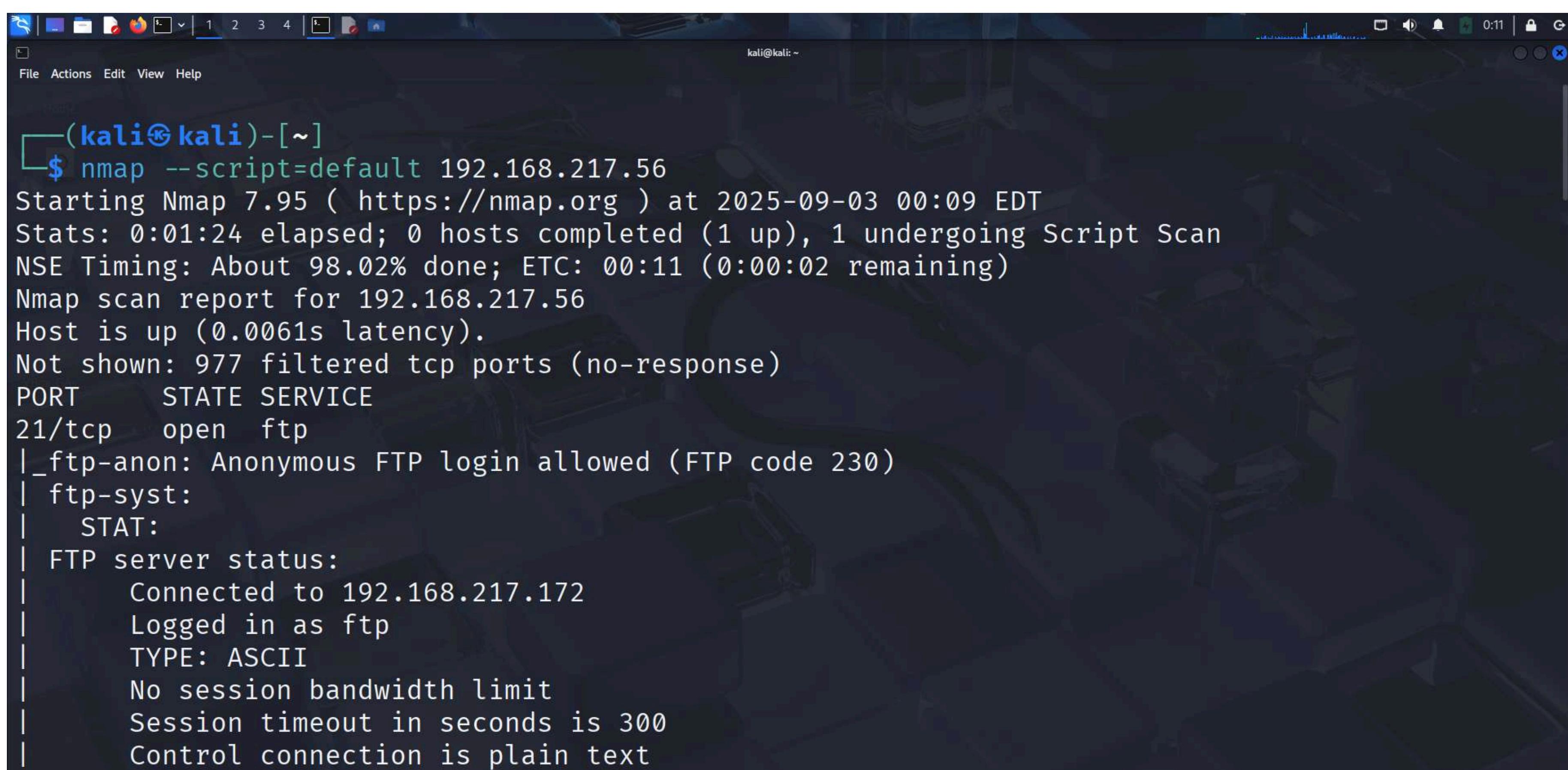


Practical 15: Script Scan (NSE)

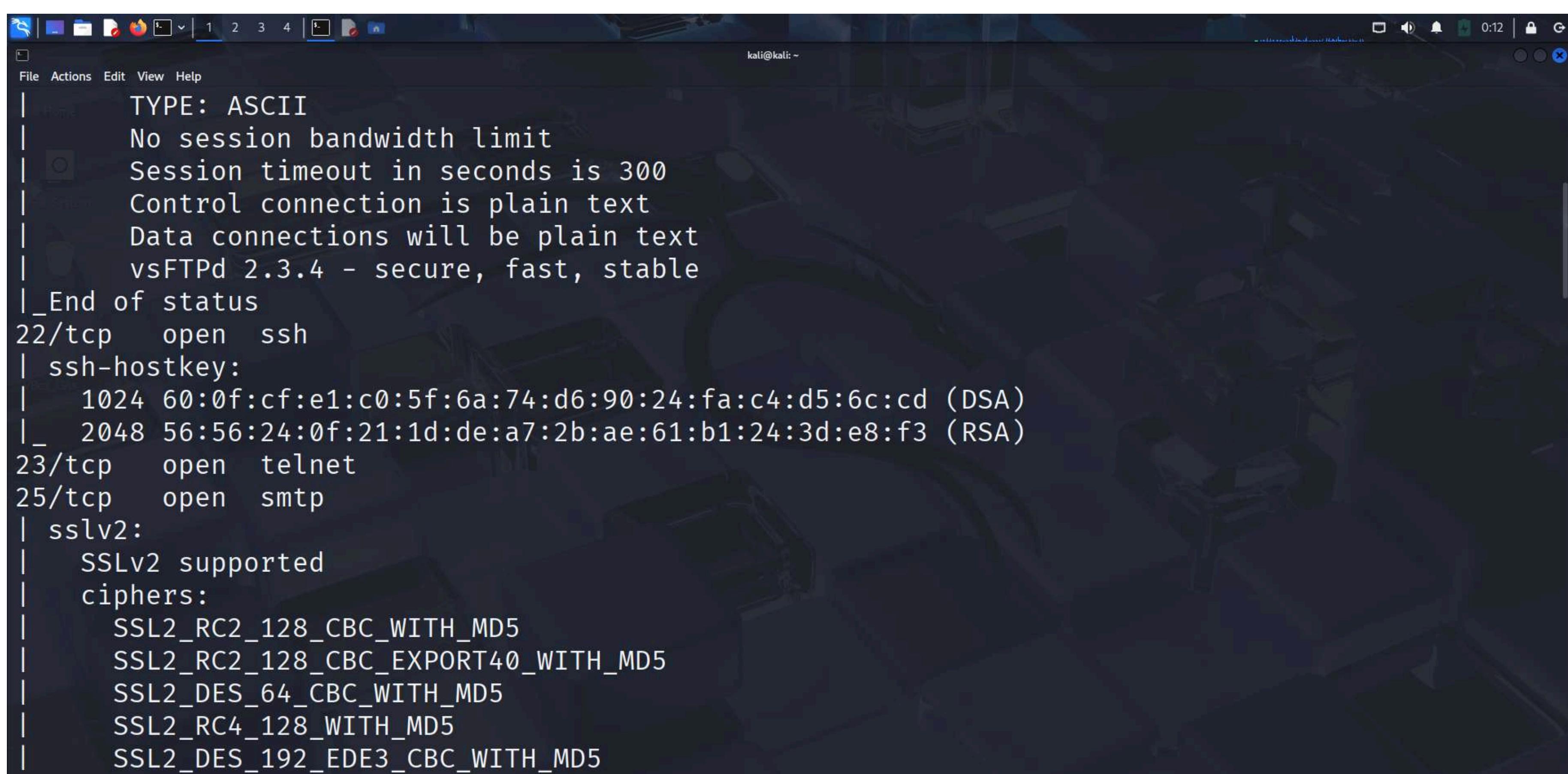
Command:

nmap --script=default <target-ip>

Explanation: Runs default Nmap scripts for detailed scanning.



```
(kali㉿kali)-[~]
$ nmap --script=default 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:09 EDT
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.02% done; ETC: 00:11 (0:00:02 remaining)
Nmap scan report for 192.168.217.56
Host is up (0.0061s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.217.172
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
```



```
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet
25/tcp    open  smtp
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2 DES_192_EDE3_CBC_WITH_MD5
```

```
kali@kali: ~
File Actions Edit View Help
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_   SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2025-09-03T04:10:44+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp  open  domain
| dns-nsid:
| bind.version: 9.4.2
80/tcp  open  http
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind
| rpcinfo:
|   program version      port/proto  service
|   100000  2              111/tcp    rpcbind
|   100000  2              111/udp   rpcbind
|   100003  2,3,4          2049/tcp   nfs
|   100003  2,3,4          2049/udp  nfs

```

```
kali@kali: ~
File Actions Edit View Help
| 100000  2              111/udp   rpcbind
| 100003  2,3,4          2049/tcp   nfs
| 100003  2,3,4          2049/udp  nfs
| 100005  1,2,3          42615/udp mountd
| 100005  1,2,3          44098/tcp mountd
| 100021  1,3,4          38957/udp nlockmgr
| 100021  1,3,4          44060/tcp nlockmgr
| 100024  1              44641/udp status
|_ 100024  1              59964/tcp status
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
| mysql-info:
|   Protocol: 10

```

```
kali@kali: ~
File Actions Edit View Help
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 31
| Capabilities flags: 43564
| Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsCompression, SupportsTransactions, SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew
| Status: Autocommit
|_ Salt: v~9=ddI!cQ0t}9@uNc*C
5432/tcp open  postgresql
|_ssl-date: 2025-09-03T04:11:27+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_  VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc

```

```
kali@kali: ~
File Actions Edit View Help
|_ VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkno
wn)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
```

```
kali@kali: ~
File Actions Edit View Help
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkno
wn)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2025-09-03T00:10:08-04:00
|_clock-skew: mean: 1h00m03s, deviation: 2h00m00s, median: 2s

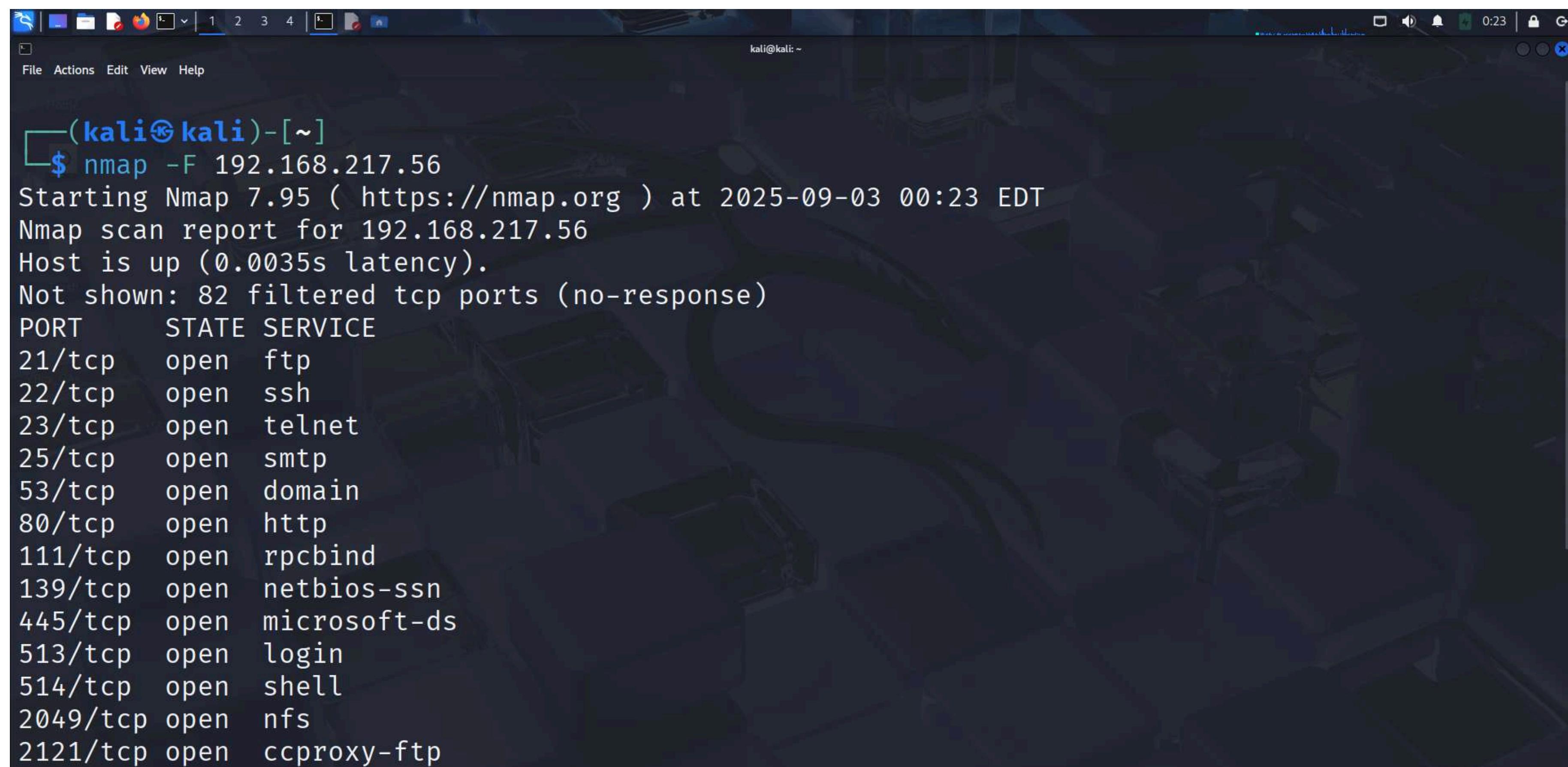
Nmap done: 1 IP address (1 host up) scanned in 100.84 seconds

└─(kali㉿kali)-[~]
└─$
```

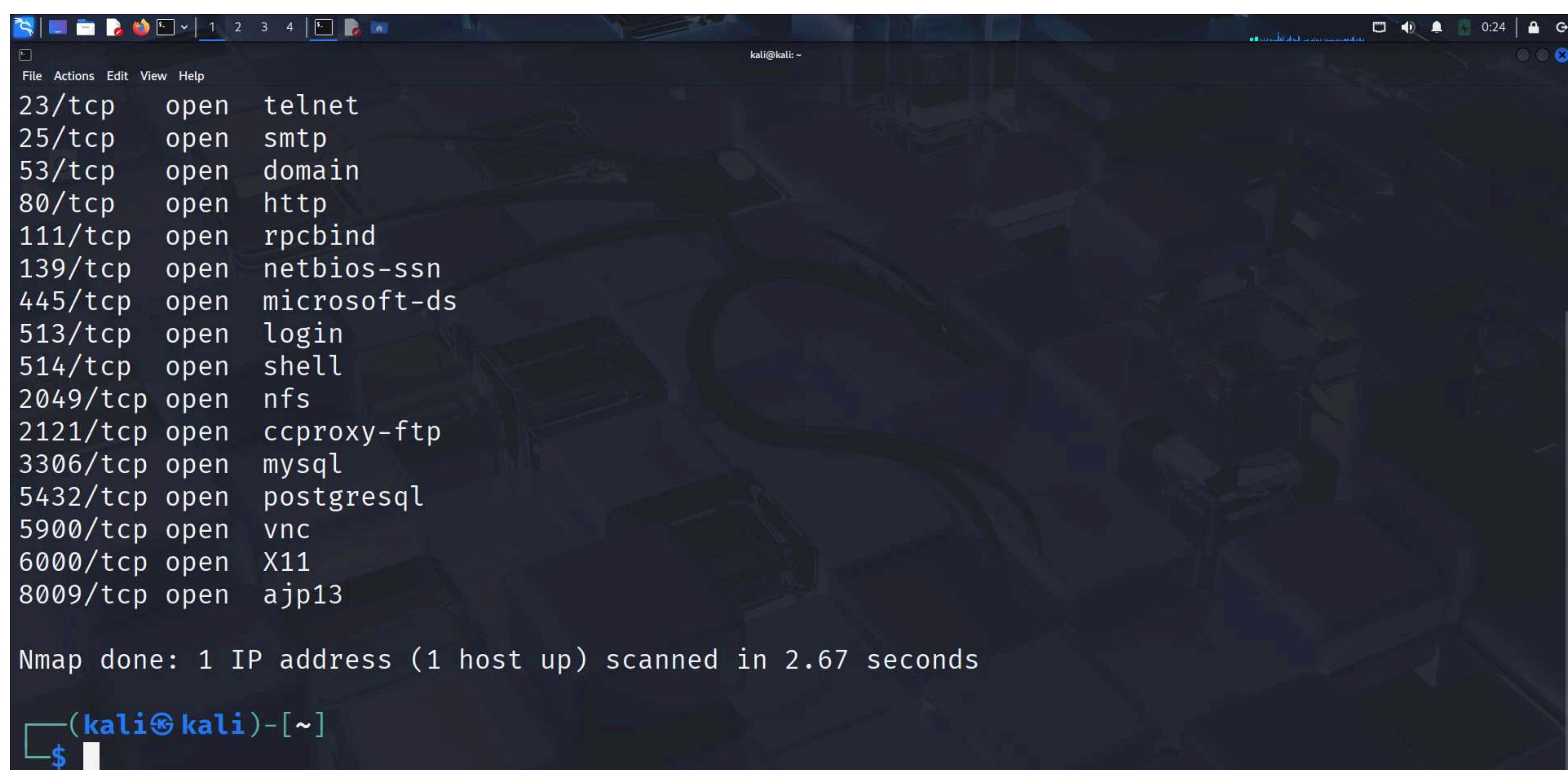
Practical-16: Fast Scan

nmap -F <target-ip>

👉 Scans the top 100 most common ports (faster than normal scan).



```
(kali㉿kali)-[~]
$ nmap -F 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:23 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0035s latency).
Not shown: 82 filtered tcp ports (no-response)
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
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
```



```
File Actions Edit View Help
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
513/tcp   open  login
514/tcp   open  shell
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
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 2.67 seconds
(kali㉿kali)-[~]
```

Practical-17: Scan Without DNS Resolution

nmap -n <target-ip>

👉 Skips DNS resolution (faster scan if DNS is slow).

```
(kali㉿kali)-[~]
$ nmap -n 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:26 EDT
Nmap scan report for 192.168.217.56
Host is up (0.011s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

```
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

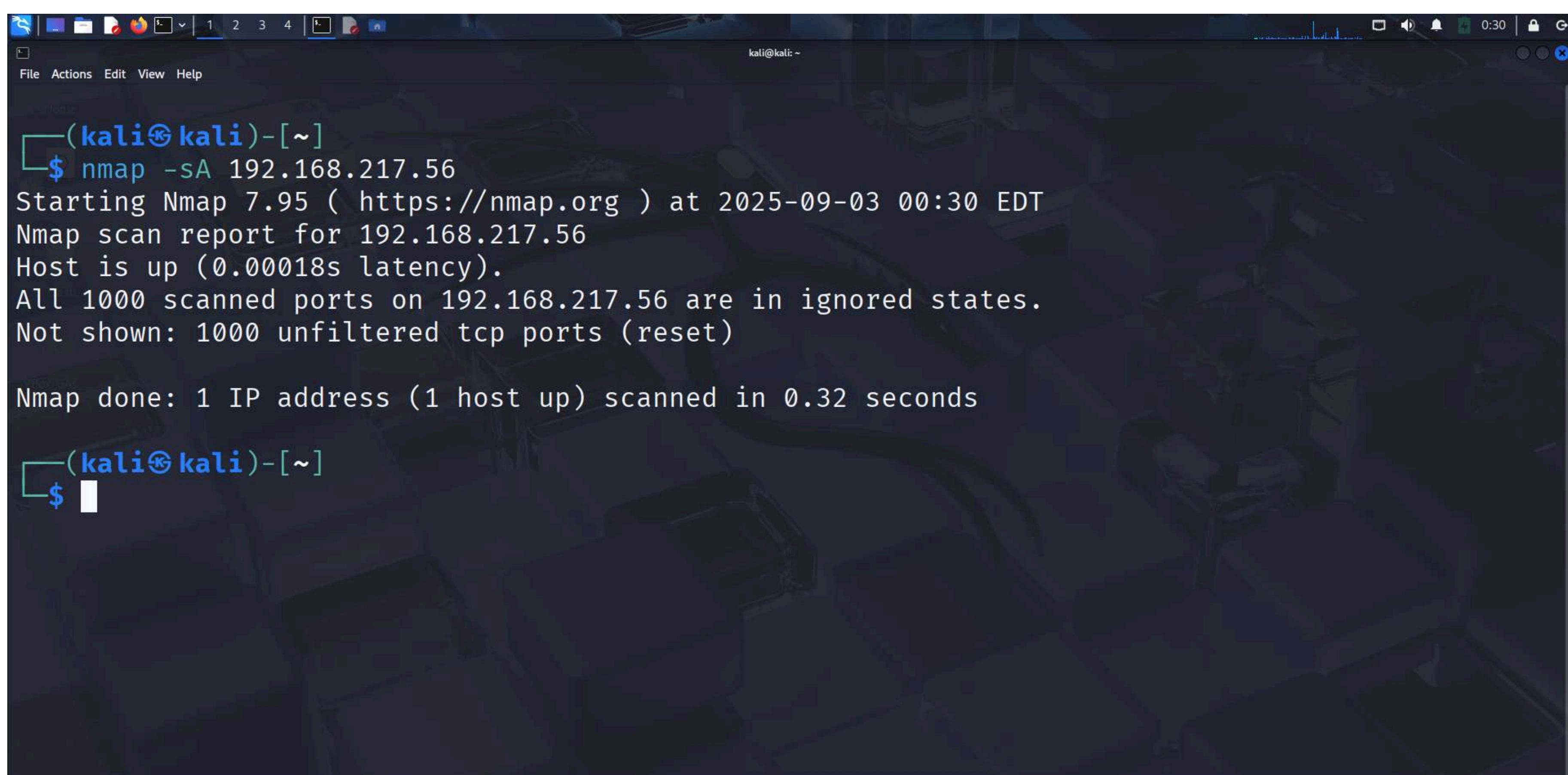
Nmap done: 1 IP address (1 host up) scanned in 5.21 seconds

(kali㉿kali)-[~]
```

Practical-18: Detect Firewall/Packet Filters

nmap -sA <target-ip>

👉 Performs an ACK scan to check if a firewall is filtering packets.



```
(kali㉿kali)-[~]
$ nmap -sA 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 00:30 EDT
Nmap scan report for 192.168.217.56
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.217.56 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(kali㉿kali)-[~]
```

- If firewall is NOT present
 - Ports will usually show as open or closed.
 - Example: 80/tcp open
- If firewall IS present (packet filtering)
 - Ports will often show as filtered or unfiltered.
 - Example output:

Not shown: 1000 unfiltered tcp ports

🔍 Meaning:

- unfiltered → Nmap was able to send ACK packets and receive responses, but it cannot confirm if the port is open or closed. This usually means a firewall is blocking deeper inspection.
- filtered → Nmap could not get a proper reply; packets are being blocked by firewall rules.
- open / closed → No firewall is blocking; Nmap can see the real status.

- Practical-19: Idle Scan (Anonymous Scan)
- nmap -sl <zombie-ip> <target-ip>
- ➡ Uses a “zombie” machine to scan another target without revealing your IP.
- What is an Idle Scan?
- • Idle Scan is a stealth technique in Nmap.
- • Instead of scanning the target directly from your IP, you use a third machine (called a “zombie”) to perform the scan.
- • This way, the target system thinks the scan is coming from the zombie machine, hiding your real identity.
-
- ◆ Command Format
- nmap -sl <zombie-ip> <target-ip>
- • <zombie-ip> = IP address of the machine you use as a middleman (must be “idle” = very quiet, not much network traffic).
- • <target-ip> = The system you actually want to scan.
-
- ◆ Steps to Perform Idle Scan
- Find a Zombie Host
- You need a system that is online but has very little traffic (so Nmap can predict its IP ID sequence numbers).
- Usually done inside your own lab (e.g., another VM).
- Run Idle Scan Command
- Example:
- nmap -sl 192.168.1.5 192.168.1.10
- Here:
- 192.168.1.5 = zombie system (quiet host)
- 192.168.1.10 = target system
- Check Results

If the scan works, it will show open/closed ports on the target, but the scan will appear to come from the zombie host.

Practical-20: Timing Templates

nmap -T4 <target-ip>

👉 Adjusts speed of scanning (T0 = slowest, T5 = fastest).

```
(kali㉿kali)-[~]
$ nmap -T4 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 01:43 EDT
Nmap scan report for 192.168.217.56
Host is up (0.010s latency).

Not shown: 977 filtered tcp ports (no-response)
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
```

```
(kali㉿kali)-[~]
$ nmap -T5 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 01:45 EDT
Nmap scan report for 192.168.217.56
Host is up (0.010s latency).

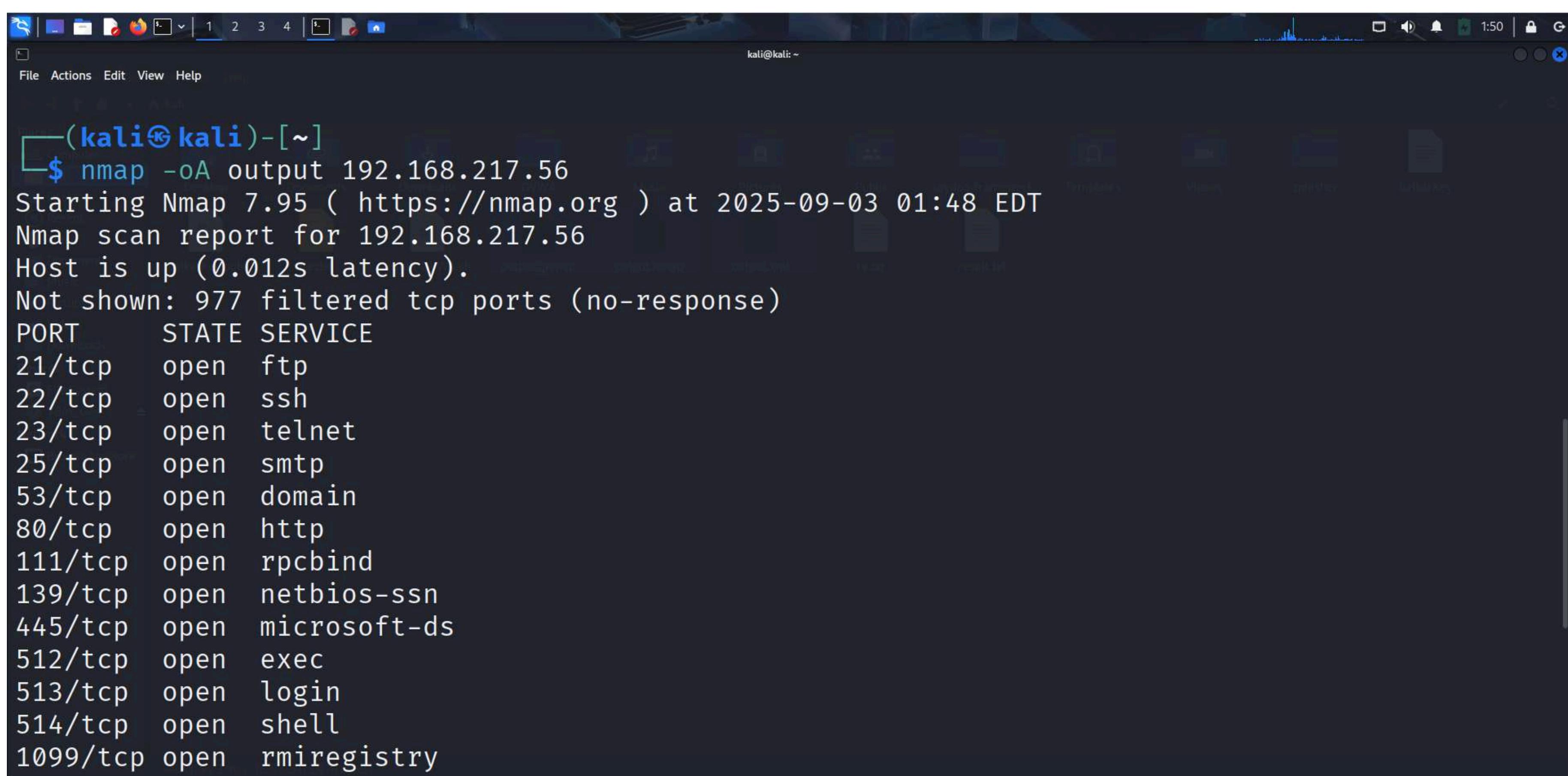
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  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 4.98 seconds
```

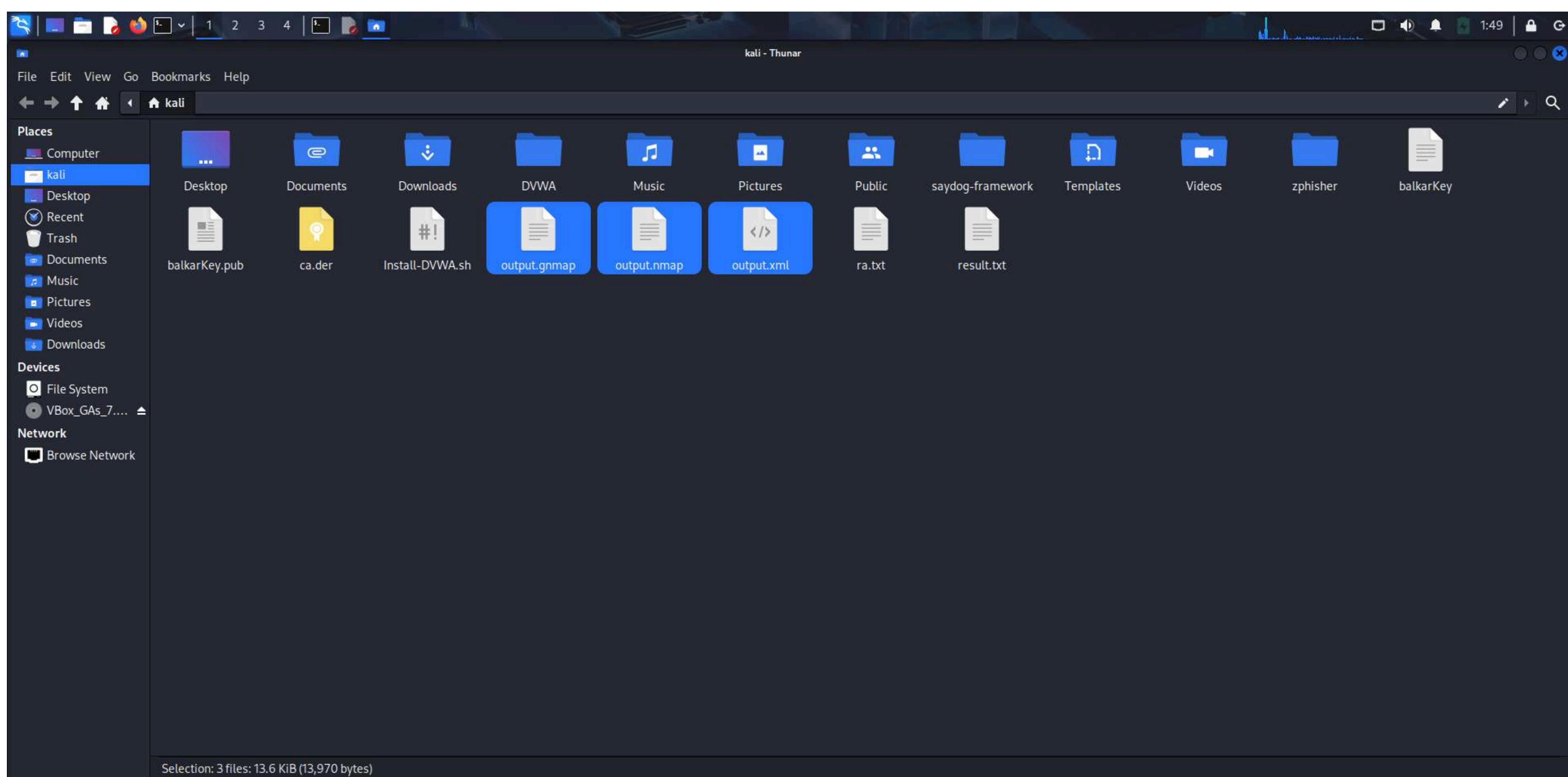
Practical-21: Scan and Save Output in All Formats

nmap -oA output <target-ip>

👉 Saves results in 3 formats: normal, XML, and grepable.



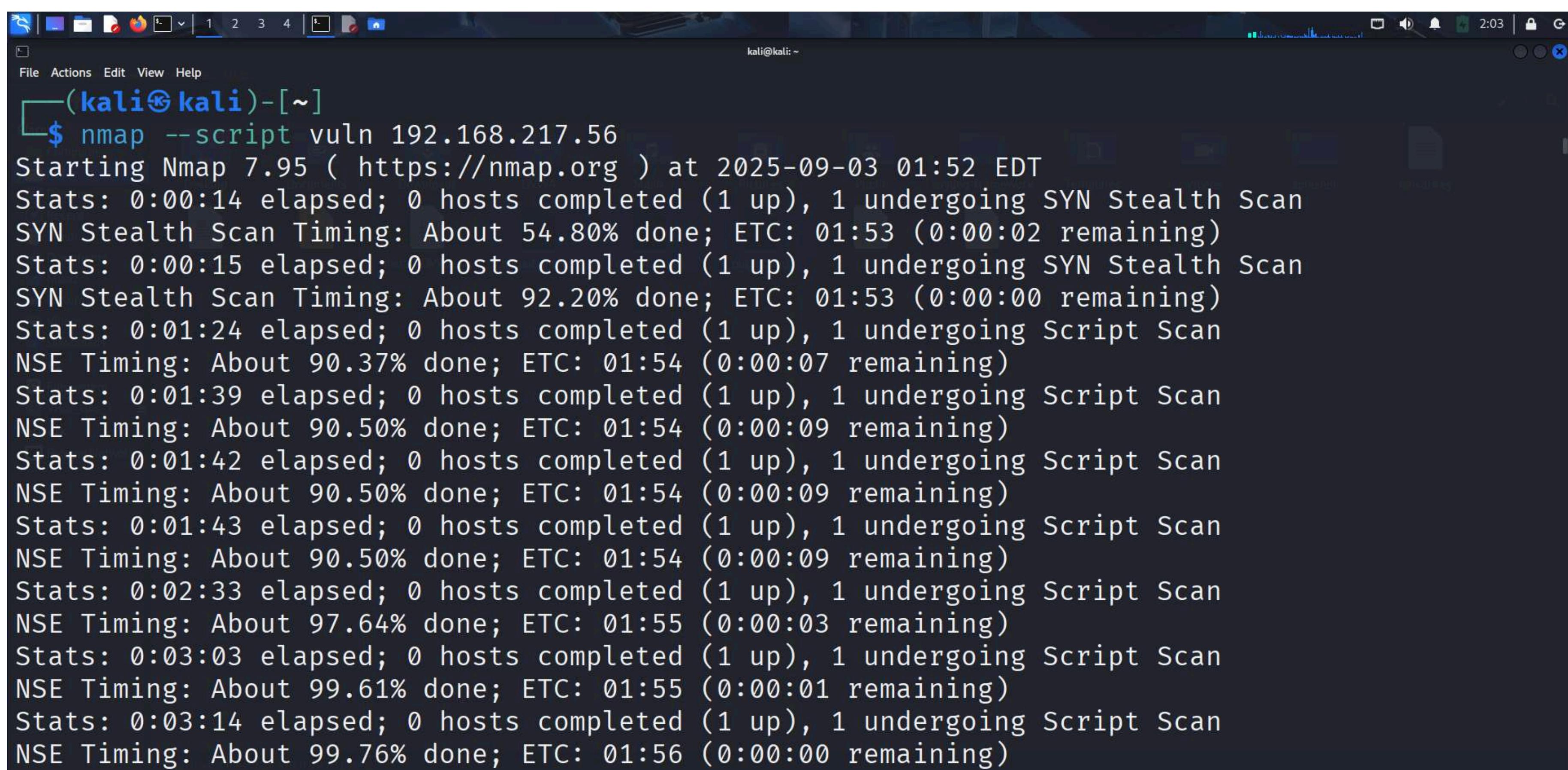
```
(kali㉿kali)-[~]
$ nmap -oA output 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 01:48 EDT
Nmap scan report for 192.168.217.56
Host is up (0.012s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    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
```



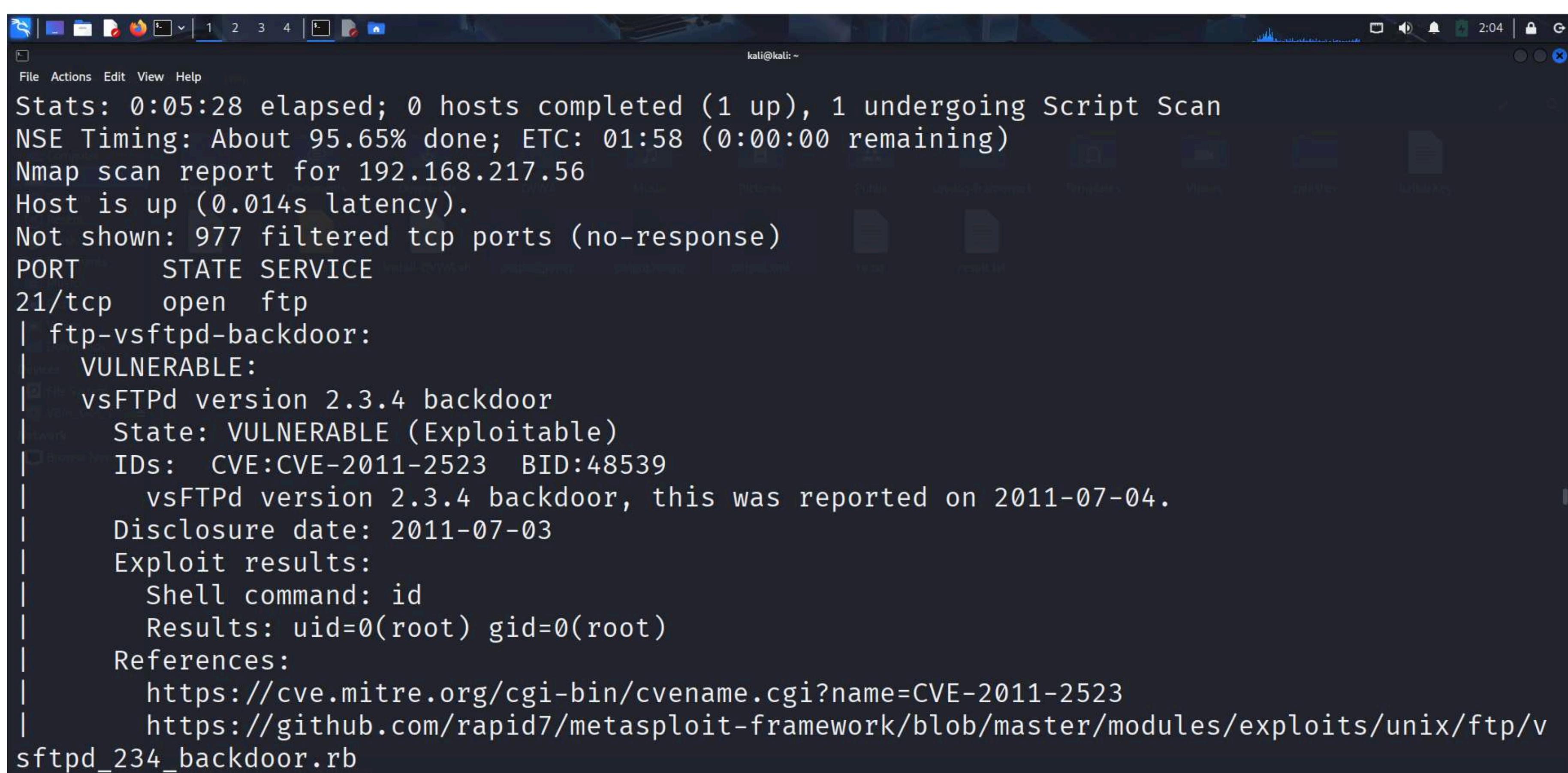
Practical-22: Detect Vulnerabilities (NSE Scripts)

nmap --script vuln <target-ip>

👉 Runs vulnerability detection scripts.



```
kali㉿kali:[~]
$ nmap --script vuln 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 01:52 EDT
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 54.80% done; ETC: 01:53 (0:00:02 remaining)
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.20% done; ETC: 01:53 (0:00:00 remaining)
Stats: 0:01:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.37% done; ETC: 01:54 (0:00:07 remaining)
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.50% done; ETC: 01:54 (0:00:09 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.50% done; ETC: 01:54 (0:00:09 remaining)
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.50% done; ETC: 01:54 (0:00:09 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.64% done; ETC: 01:55 (0:00:03 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.61% done; ETC: 01:55 (0:00:01 remaining)
Stats: 0:03:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 01:56 (0:00:00 remaining)
```



```
kali㉿kali:[~]
Stats: 0:05:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.65% done; ETC: 01:58 (0:00:00 remaining)
Nmap scan report for 192.168.217.56
Host is up (0.014s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|         Exploit results:
|           Shell command: id
|           Results: uid=0(root) gid=0(root)
|         References:
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|           https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
```

```
kali@kali: ~
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/v
sftpd_234_backdoor.rb
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://www.securityfocus.com/bid/48539
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
ssl-dh-params:
VULNERABLE:
Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
State: VULNERABLE
Transport Layer Security (TLS) services that use anonymous Diffie-Hellman key exchange only provide protection against passive eavesdropping, and are vulnerable to active man-in-the-middle attacks which could completely compromise the confidentiality and integrity of any data exchanged over the resulting session.
Check results:
ANONYMOUS DH GROUP 1
Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
Modulus Type: Safe prime
```

```
kali@kali: ~
ANONYMOUS DH GROUP 1
Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 512
Generator Length: 8
Public Key Length: 512
References:
https://www.ietf.org/rfc/rfc2246.txt

Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
State: VULNERABLE
IDs: CVE:CVE-2015-4000 BID:74733
The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.
Disclosure date: 2015-5-19
```

```
kali@kali: ~
to more easily break the encryption and monitor or tamper with
the encrypted stream.
Disclosure date: 2015-5-19
Check results:
EXPORT-GRADE DH GROUP 1
Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 512
Generator Length: 8
Public Key Length: 512
References:
https://www.securityfocus.com/bid/74733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
https://weakdh.org

Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups of insufficient strength, especially those using one of a few commonly shared groups, may be susceptible to passive eavesdropping attacks.
```

```
kali@kali: ~
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: postfix builtin
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024
References:
    https://weakdh.org
smtp-vuln-cve2010-4344:
    The SMTP server is not Exim: NOT VULNERABLE
ssl-poodle:
    VULNERABLE:
    SSL POODLE information leak
    State: VULNERABLE
    IDs: CVE:CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
```

```
kali@kali: ~
File Actions Edit View Help
http-CSRF:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.217.56
Found the following possible CSRF vulnerabilities:

Path: http://192.168.217.56:80/dvwa/
Form id:
Form action: login.php

Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/passwd/TWiki/WebHome

Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/passwd/Main/WebHome

Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/edit/TWiki/

Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
```

```
kali@kali: ~
File Actions Edit View Help
State: VULNERABLE
IDs: CVE:CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain cleartext data via a
padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
    TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
References:
    https://www.imperialviolet.org/2014/10/14/poodle.html
    https://www.securityfocus.com/bid/70574
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
    https://www.openssl.org/~bodo/ssl-poodle.pdf
sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp open domain
80/tcp open http
http-dombased-xss: Couldn't find any DOM based XSS.
http-CSRF:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.217.56
Found the following possible CSRF vulnerabilities:
```

```
kali@kali: ~
Form action: http://TWiki.org/cgi-bin/edit/TWiki/
Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins

Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
Form id:
Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
http-sql-injection:
Possible sql for queries:
http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=N%3B0%3DD%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
```

```
20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
```

```
http://192.168.217.56:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=login.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
http://192.168.217.56:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
```

```
dae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.217.56:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
| http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider
```

```
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
http://192.168.217.56:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider&param1=1.10
| http://192.168.217.56:80/oops/TWiki/TWikiHistory?template=oopsrev&param1=1.10%27%20OR%20sqlspider
| http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
| http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.9%27%20OR%20sqlspider
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.9%27%20OR%20sqlspider&rev1=1.10
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.9&rev1=1.10%27%20OR%20sqlspider
| http://192.168.217.56:80/oops/TWiki/TWikiHistory?template=oopsrev%27%20OR%20sqlspider&param1=1.10
| http://192.168.217.56:80/oops/TWiki/TWikiHistory?template=oopsrev&param1=1.10%27%20OR%20sqlspider
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.8%27%20OR%20sqlspider&rev1=1.9
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
| http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
| http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
```

```
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.8&rev1=1.9%27%20OR%20sqlspider
http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.7%27%20OR%20sqlspider
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7%27%20OR%20sqlspider&rev1=1.8
http://192.168.217.56:80/rdiff/TWiki/TWikiHistory?rev2=1.7&rev1=1.8%27%20OR%20sqlspider
http://192.168.217.56:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=N%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=S%3B0%3DD%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=N%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=M%3B0%3DD%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=N%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=D%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=N%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3B0%3DD%27%20OR%20sqlspider
```

```
kali@kali: ~
| http://192.168.217.56:80/dav/?C=S%3B0%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3B0%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3B0%3DD%27%20OR%20sqlspider
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

| Disclosure date: 2009-09-17
| References:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-vuln-cve2017-100100: ERROR: Script execution failed (use -d to debug)
| http-trace: TRACE is enabled
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
```

```
kali@kali: ~
| _http-trace: TRACE is enabled
| _http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
| /index/: Potentially interesting folder
| http-fileupload-exploiter:

| Couldnt't find a file-type field.
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
| rmi-vuln-classloader:
```

```
kali@kali: ~
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
| VULNERABLE:
| RMI registry default configuration remote code execution vulnerability
| State: VULNERABLE
| Default configuration of RMI registry allows loading classes from remote URLs which ca
n lead to remote code execution.

| References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc
/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| _ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-dh-params:
| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
```

```
kali@kali: ~
ssl-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
    Transport Layer Security (TLS) services that use Diffie-Hellman groups
    of insufficient strength, especially those using one of a few commonly
    shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
    Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    Modulus Type: Safe prime
    Modulus Source: Unknown/Custom-generated
    Modulus Length: 1024
    Generator Length: 8
    Public Key Length: 1024
    References:
        https://weakdh.org
ssl-ccs-injection:
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
```

```
kali@kali: ~
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
    OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
    does not properly restrict processing of ChangeCipherSpec messages,
    which allows man-in-the-middle attackers to trigger use of a zero
    length master key in certain OpenSSL-to-OpenSSL communications, and
    consequently hijack sessions or obtain sensitive information, via
    a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
    http://www.cvedetails.com/cve/2014-0224
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
    http://www.openssl.org/news/secadv_20140605.txt
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: CVE:CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
```

```
kali@kali: ~
State: VULNERABLE
IDs: CVE:CVE-2014-3566 BID:70574
    The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
    products, uses nondeterministic CBC padding, which makes it easier
    for man-in-the-middle attackers to obtain cleartext data via a
    padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
    TLS_RSA_WITH_AES_128_CBC_SHA
References:
    https://www.imperialviolet.org/2014/10/14/poodle.html
    https://www.securityfocus.com/bid/70574
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
    https://www.openssl.org/~bodo/ssl-poodle.pdf
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
 irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/
fulldisclosure/2010/Jun/277
8009/tcp open ajp13
8180/tcp open unknown
```

Practical-23: Detect Malware/Backdoors

nmap --script malware <target-ip>

👉 Checks for possible malware or backdoors on target.

```
(kali㉿kali)-[~]
$ nmap --script malware 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 02:43 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0096s latency).
Not shown: 977 filtered tcp ports (no-response)
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
```

```
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
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/
fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 27.46 seconds

(kali㉿kali)-[~]
```

Practical-24: Detect HTTP Info (Web Servers)

nmap --script http-title <target-ip>

👉 Shows the title of web pages hosted on target.

```
(kali㉿kali)-[~]
$ nmap --script http-title 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 02:49 EDT
Nmap scan report for 192.168.217.56
Host is up (0.012s latency).
Not shown: 977 filtered tcp ports (no-response)
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
|_http-title: Metasploitable2 - Linux
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
```

```
File Actions Edit View Help
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
|_http-title: Apache Tomcat/5.5

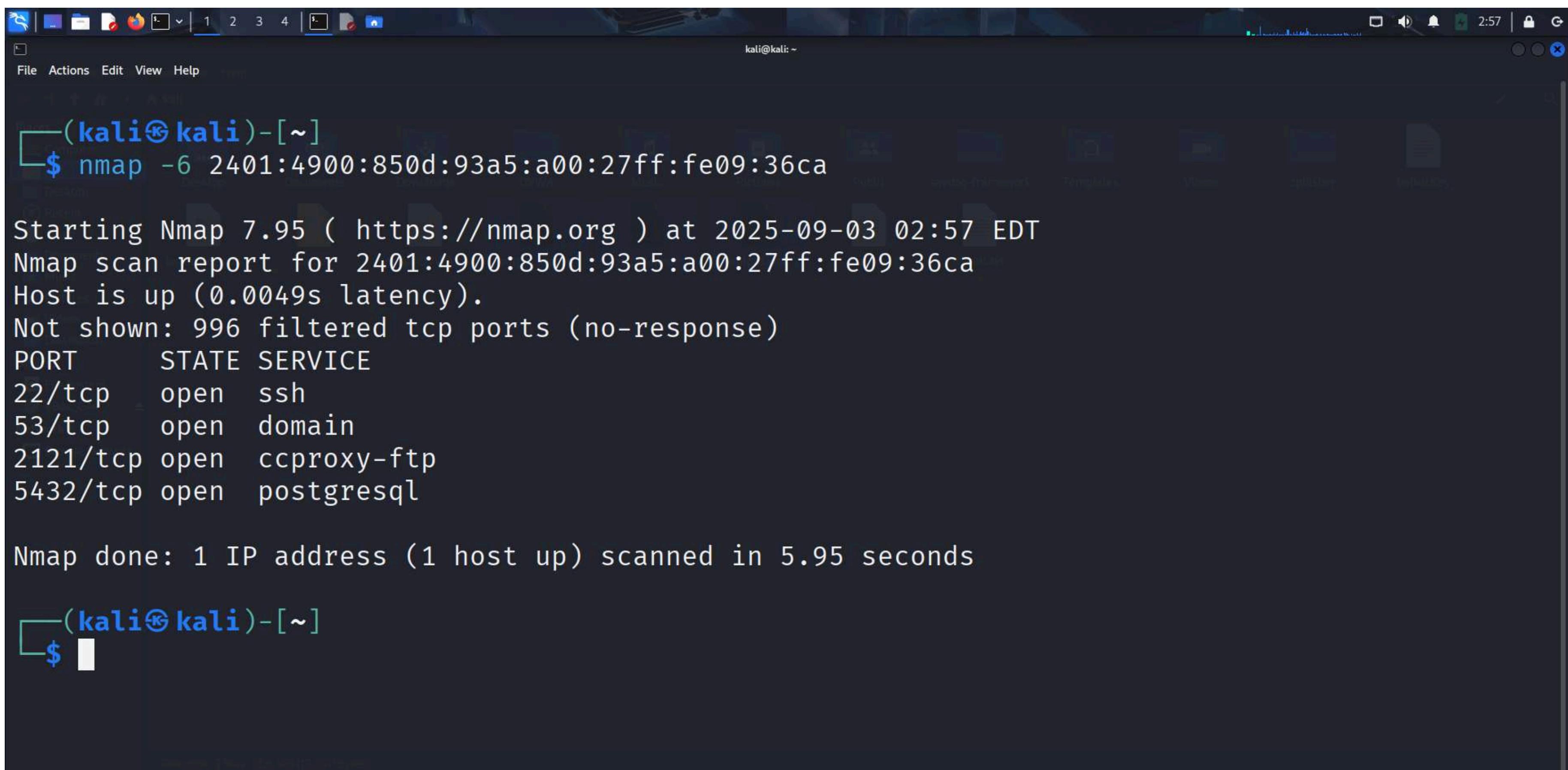
Nmap done: 1 IP address (1 host up) scanned in 6.16 seconds

(kali㉿kali)-[~]
```

Practical-25: Scan IPv6 Targets

nmap -6 <ipv6-address>

👉 Performs scanning on IPv6 addresses.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal prompt is '(kali㉿kali)-[~]'. The user has run the command 'nmap -6 2401:4900:850d:93a5:a00:27ff:fe09:36ca'. The output of the scan is displayed, showing the host is up with 0.0049s latency. It lists several open ports: 22/tcp (ssh), 53/tcp (domain), 2121/tcp (ccproxy-ftp), and 5432/tcp (postgresql). The scan took 5.95 seconds. The terminal window also shows icons for various applications like a file manager, terminal, and browser.

```
(kali㉿kali)-[~]
$ nmap -6 2401:4900:850d:93a5:a00:27ff:fe09:36ca
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 02:57 EDT
Nmap scan report for 2401:4900:850d:93a5:a00:27ff:fe09:36ca
Host is up (0.0049s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
2121/tcp  open  ccproxy-ftp
5432/tcp  open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds

(kali㉿kali)-[~]
```

Conclusion

From this practical, I learned how to use Nmap in Kali Linux for network scanning and security analysis. By performing different commands, I was able to:

- ● Discover live hosts in a network
- ● Identify open ports and running services
- ● Detect service versions and operating systems
- ● Save scan results for further analysis

This practical helped me understand the importance of Nmap as a powerful tool for ethical hacking, penetration testing, and network defense. It is widely used by system administrators and cybersecurity professionals to monitor, secure, and troubleshoot networks.