📖 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

Practical 1: Check Nmap Version

Command:

nmap -V

Explanation: Shows the version of Nmap installed.

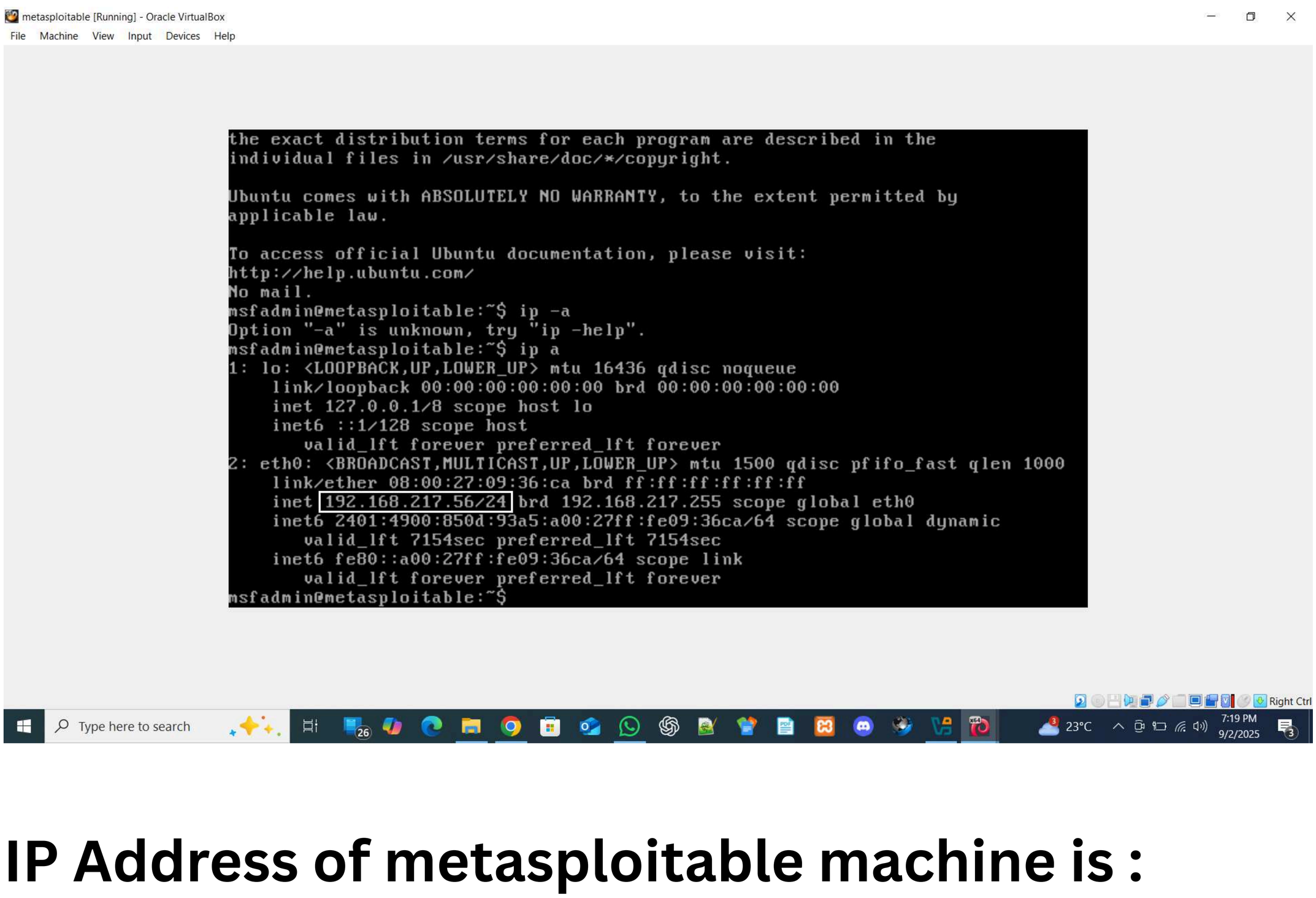
Practical 2: Ping Scan (Host Discovery)

Command:

nmap -sn <target-ip>

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

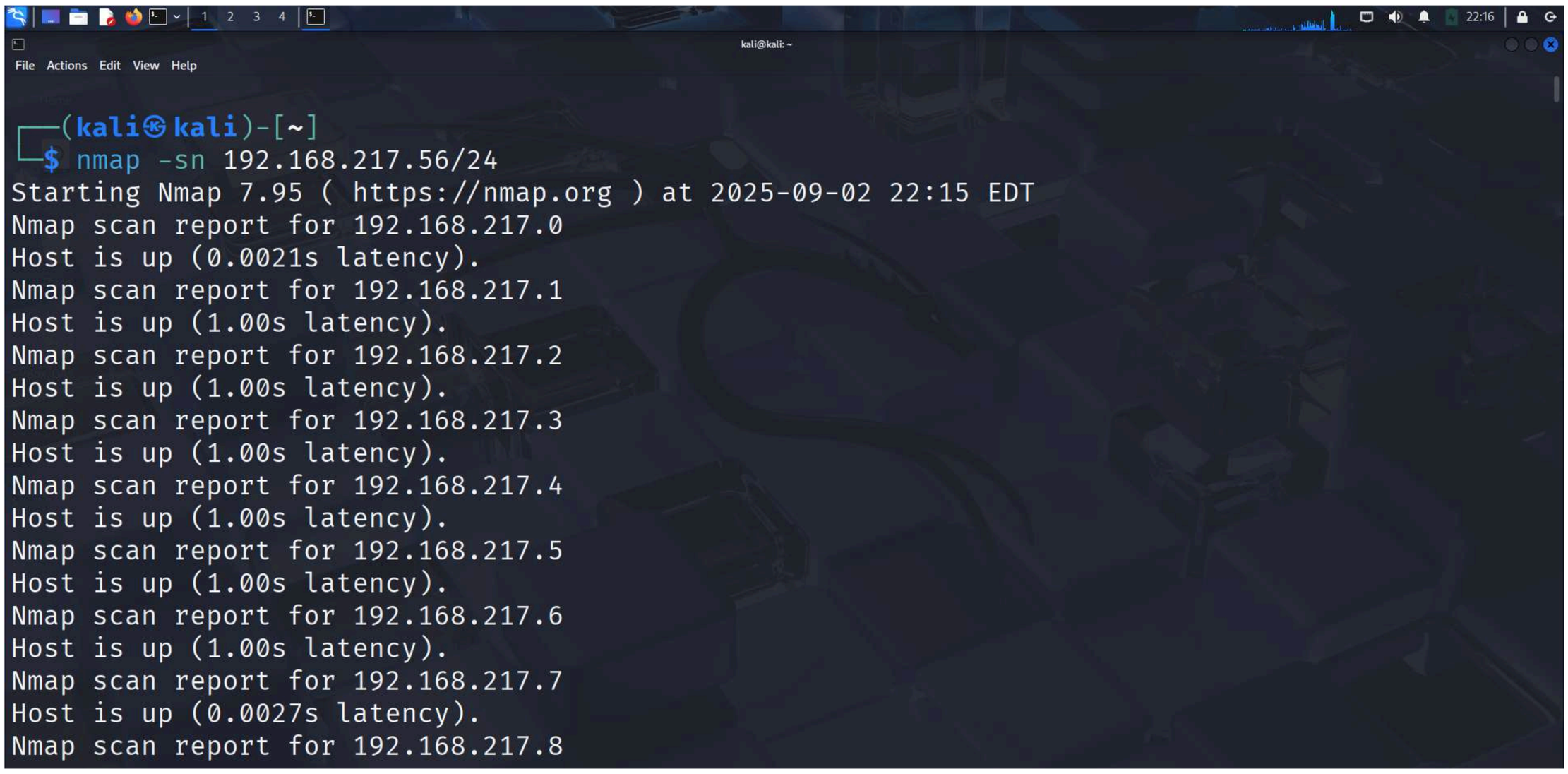
Firstly we need a metasploitable machine to perform ping scan:

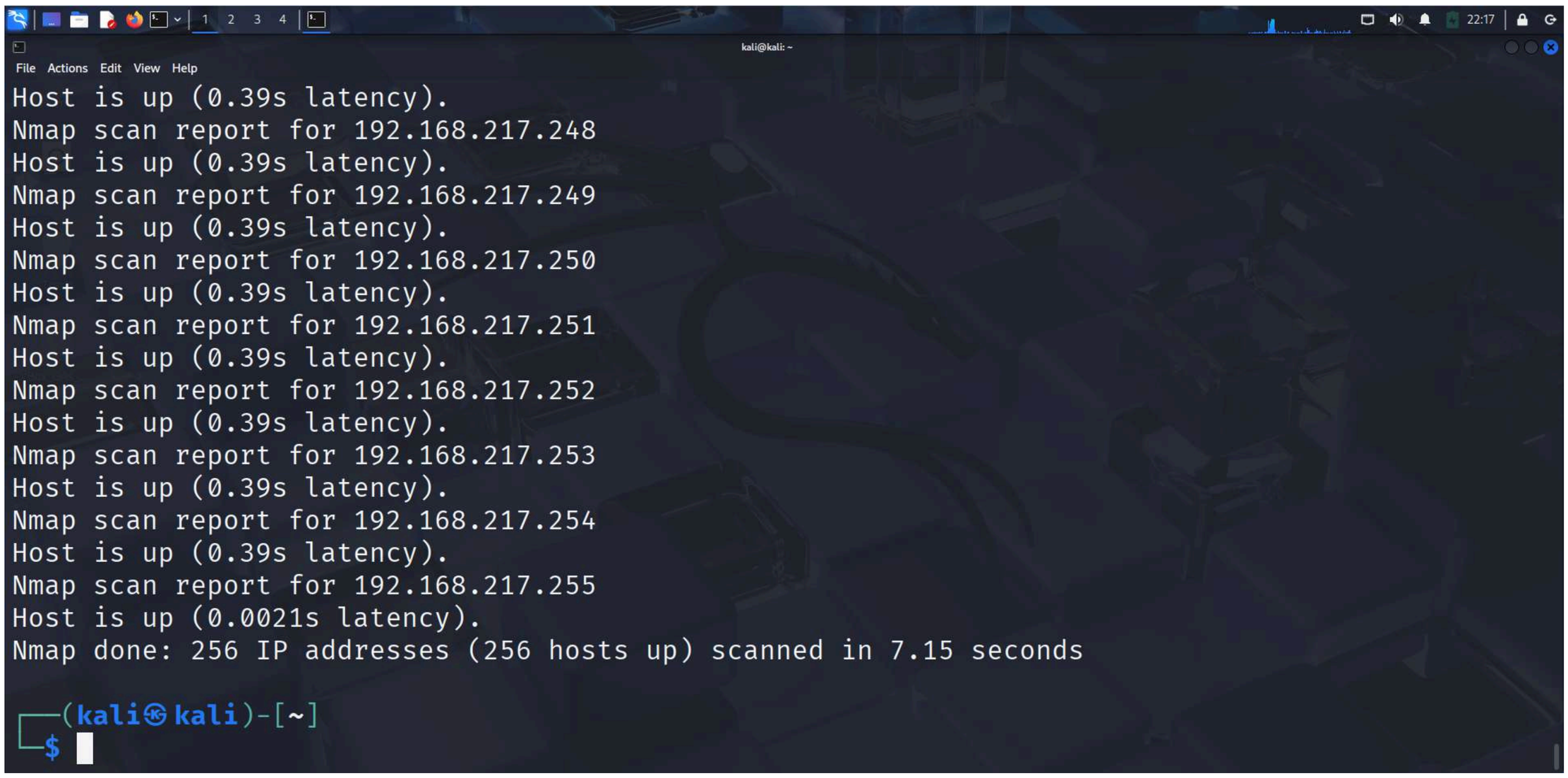


IP Address of metasploitable machine is :

192.168.217.56/24

To find IP we use command: ip





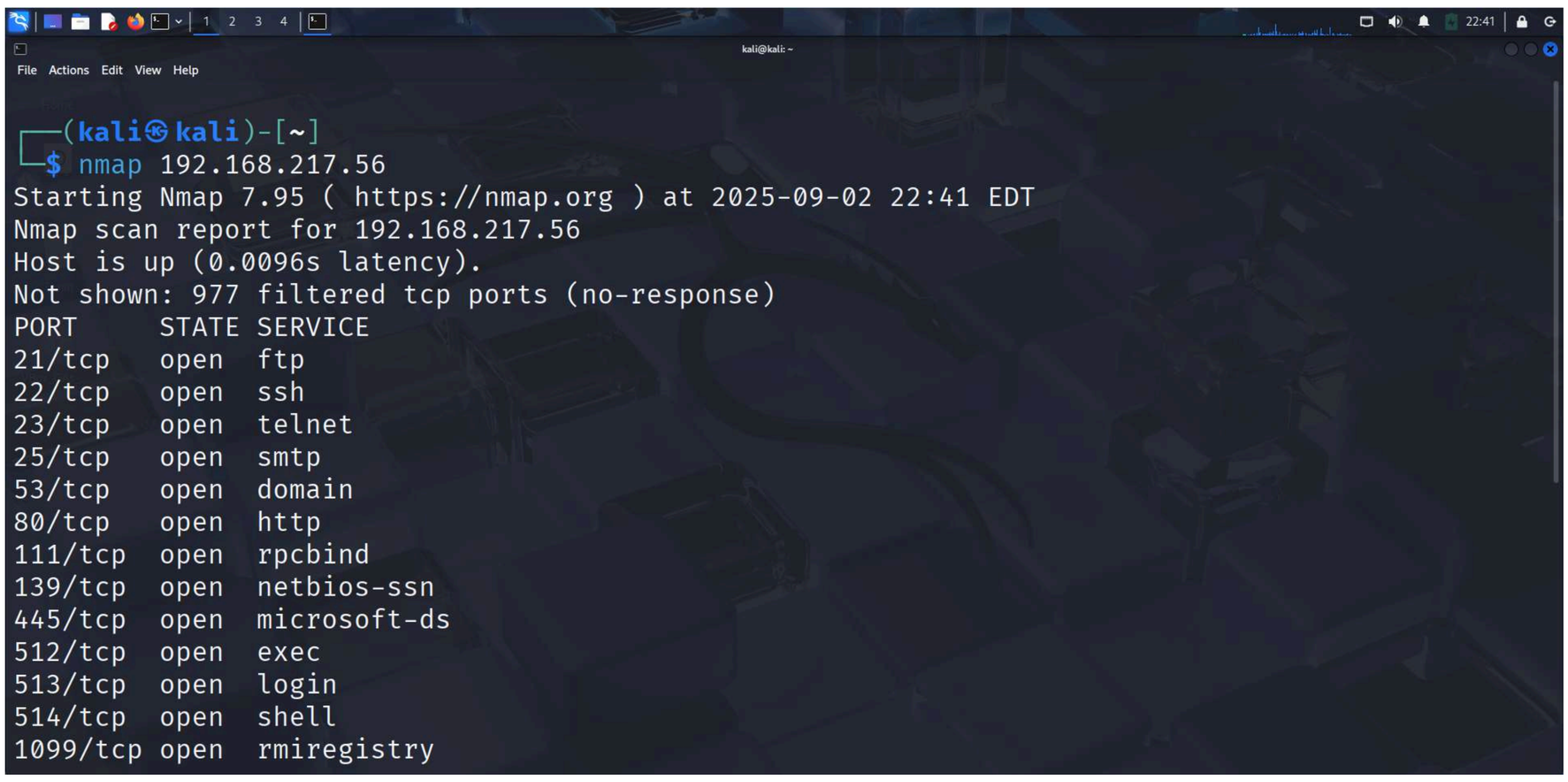
“Host is up” shows that machine is live

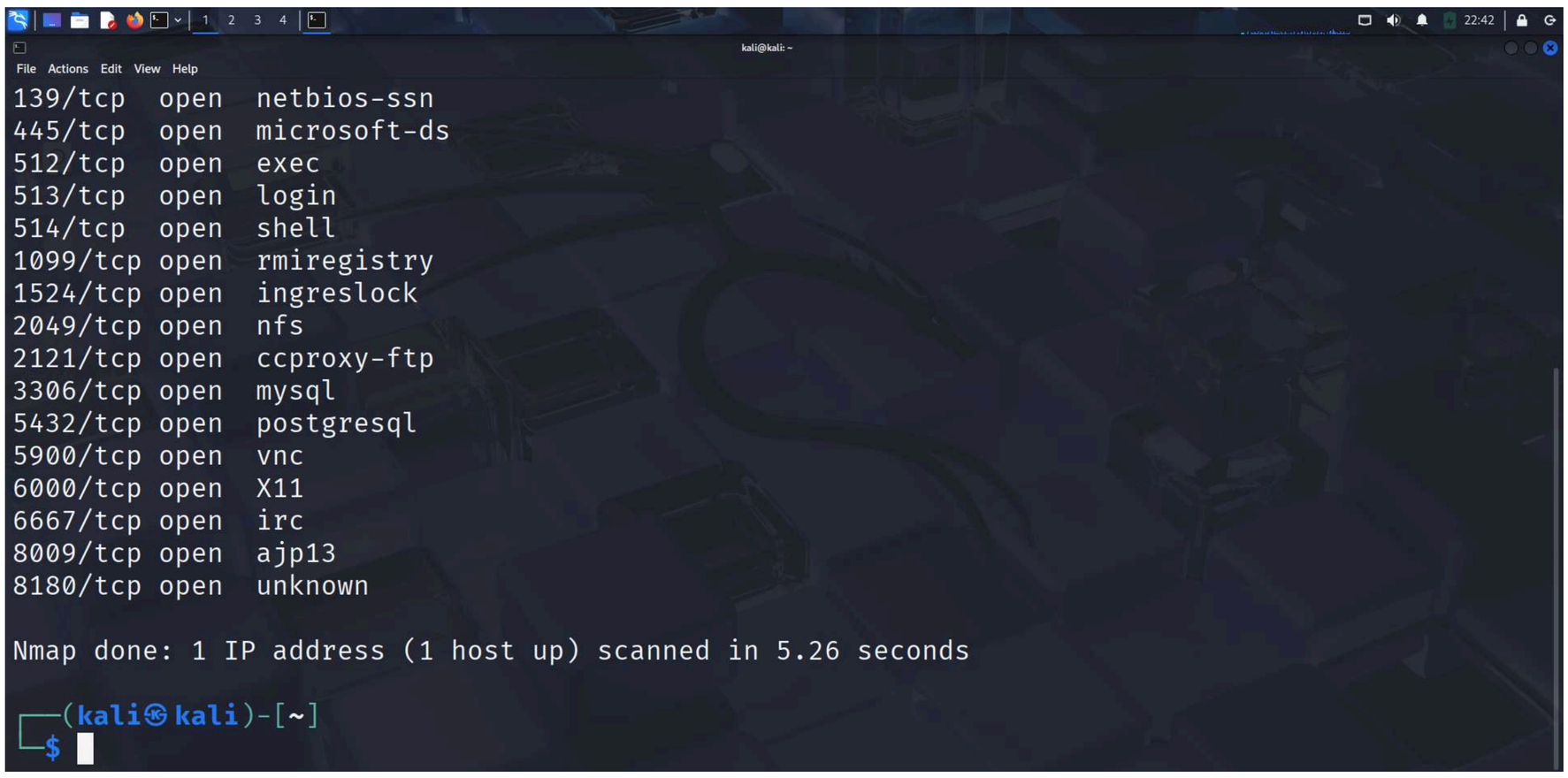
Practical 3: Default Port Scan

Command:

nmap <target-ip>

Explanation: Scans the most common 1000 TCP ports.



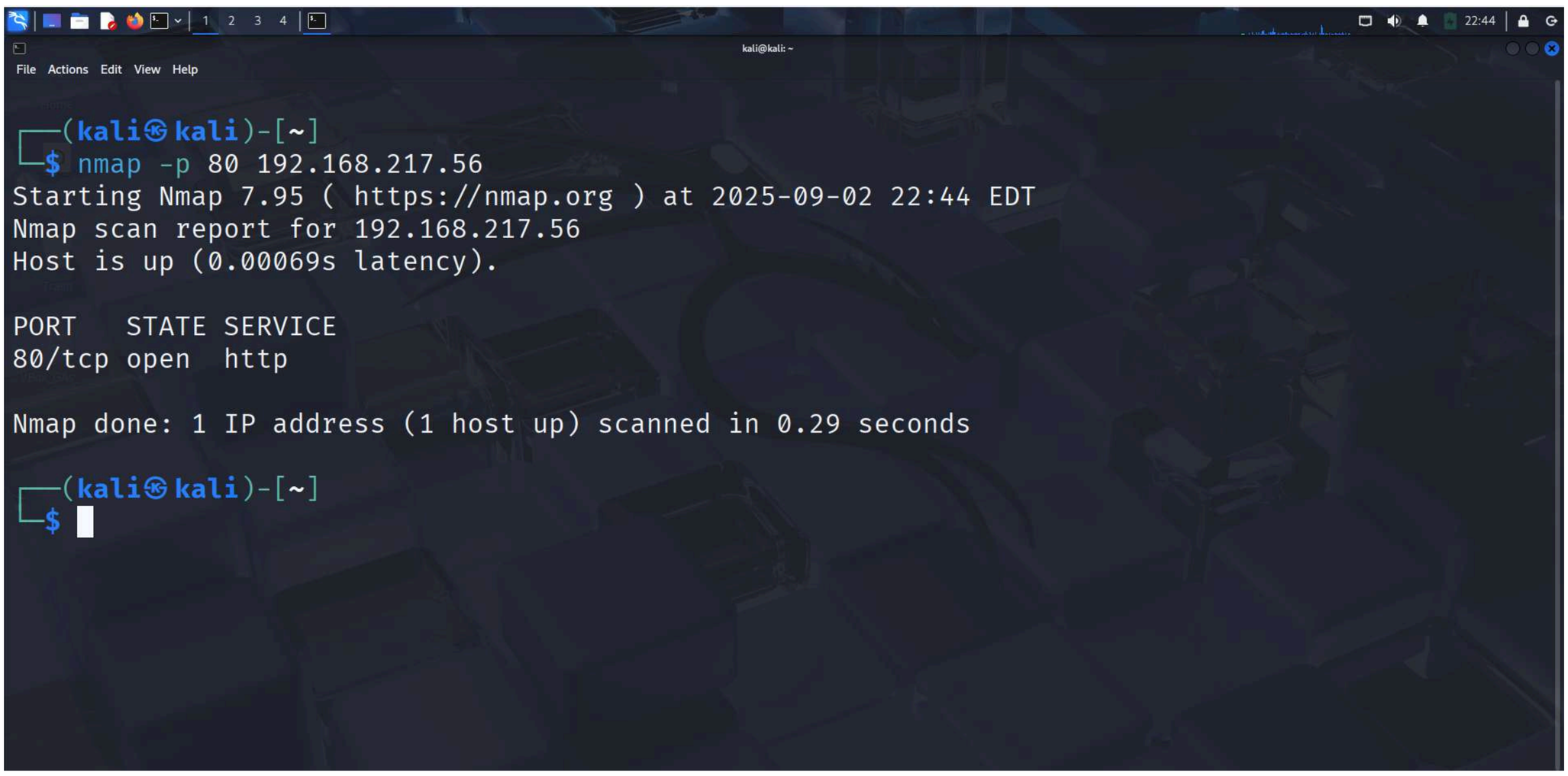


Practical 4: Scan Specific Port

Command:

nmap -p 80 <target-ip>

Explanation: Scans only port 80 on the target

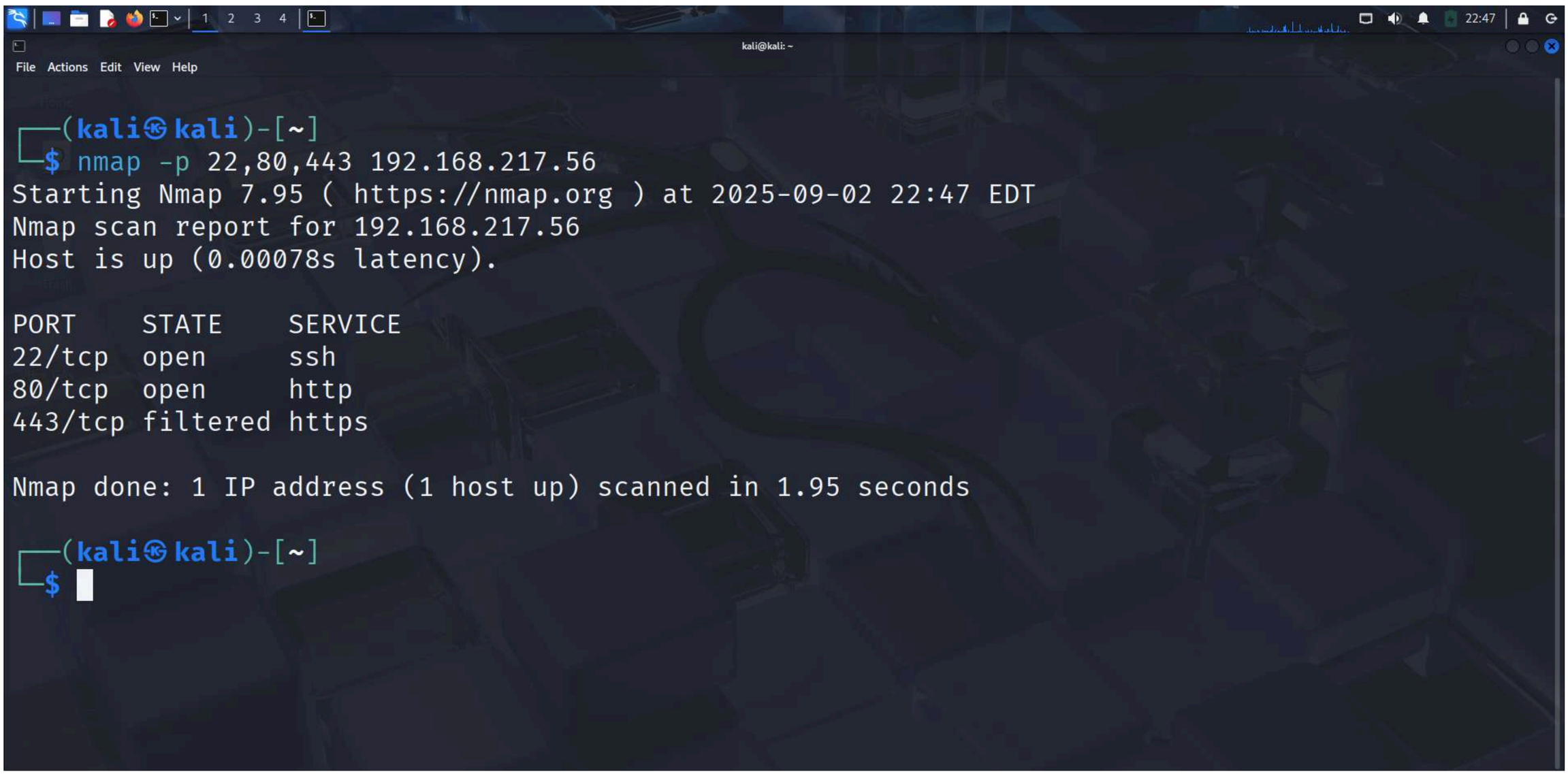


Practical 5: Scan Multiple Ports

Command:

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

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

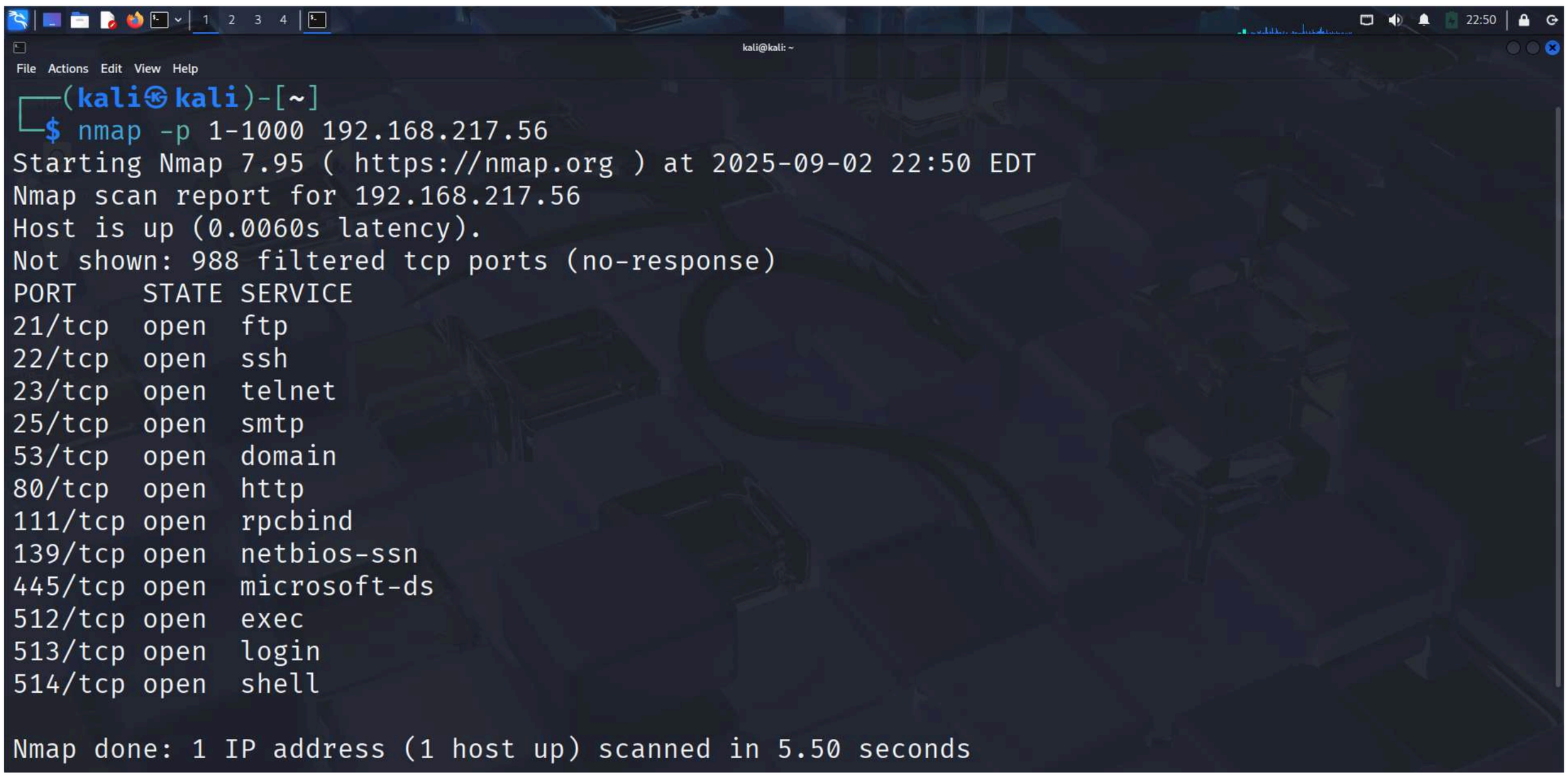


Practical 6: Scan Port Range

Command:

nmap -p 1-1000 <target-ip>

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

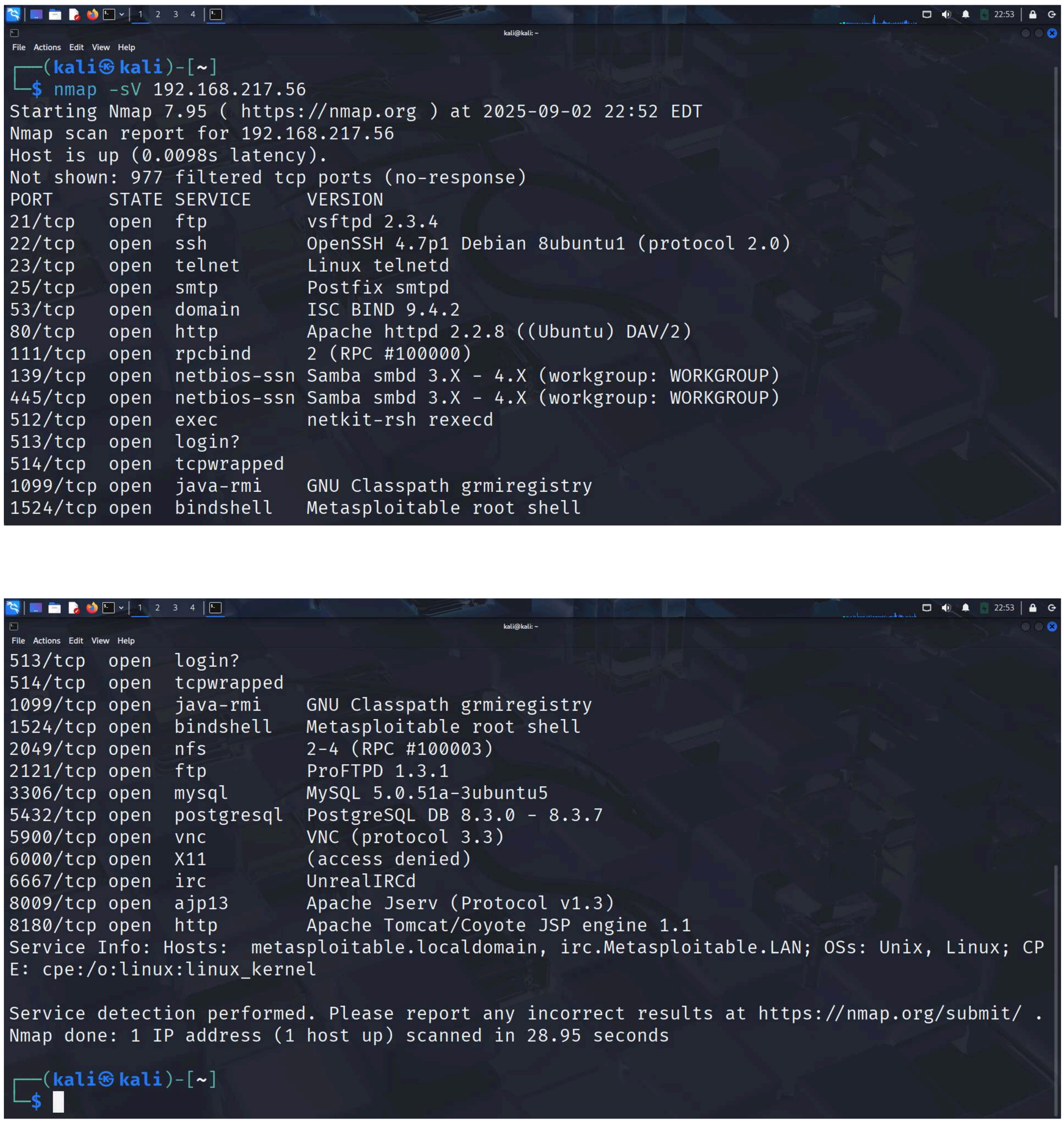


Practical 7: Service Version Detection

Command:

nmap -sV <target-ip>

Explanation: Detects the service and version running on open ports

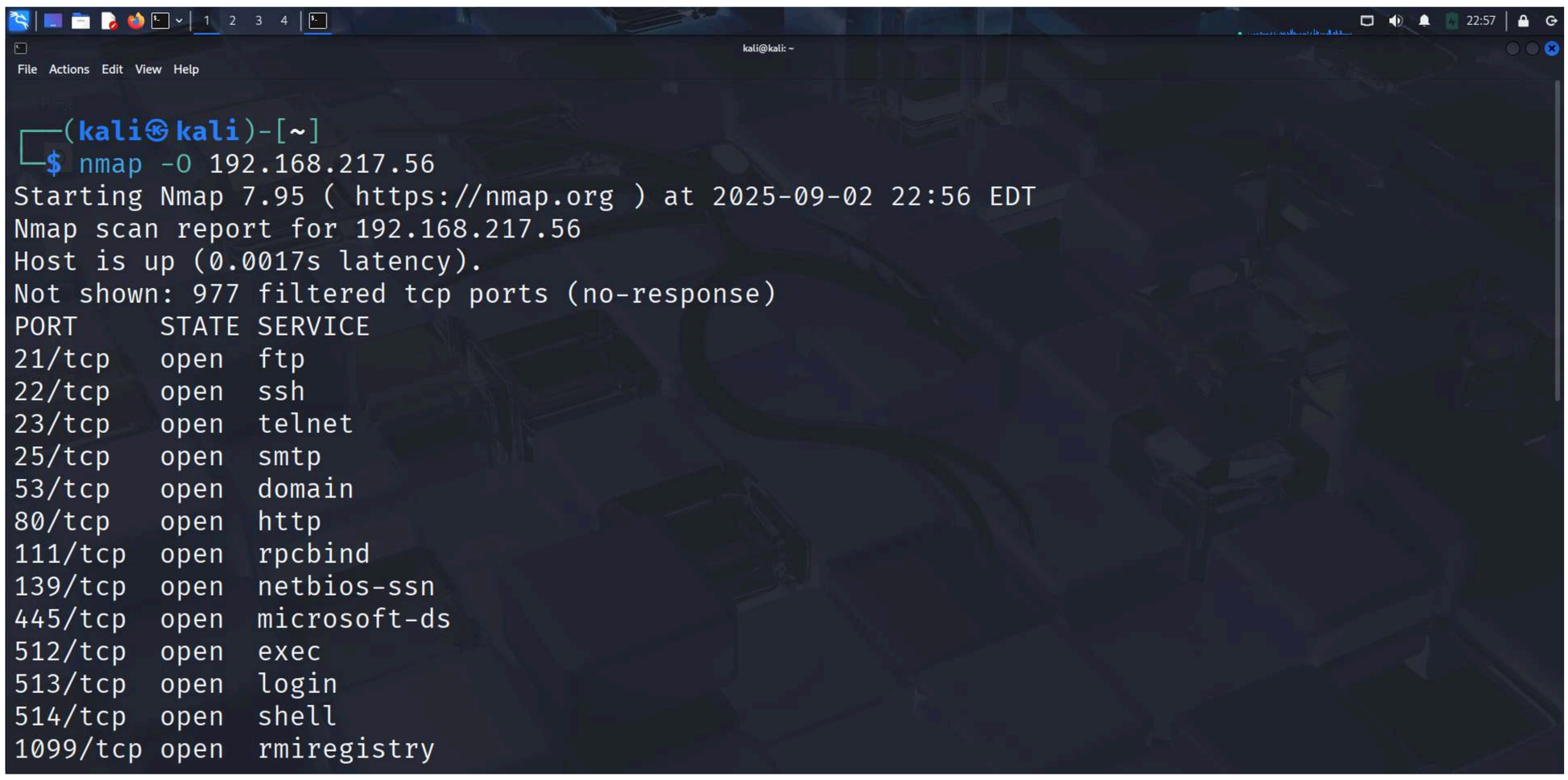


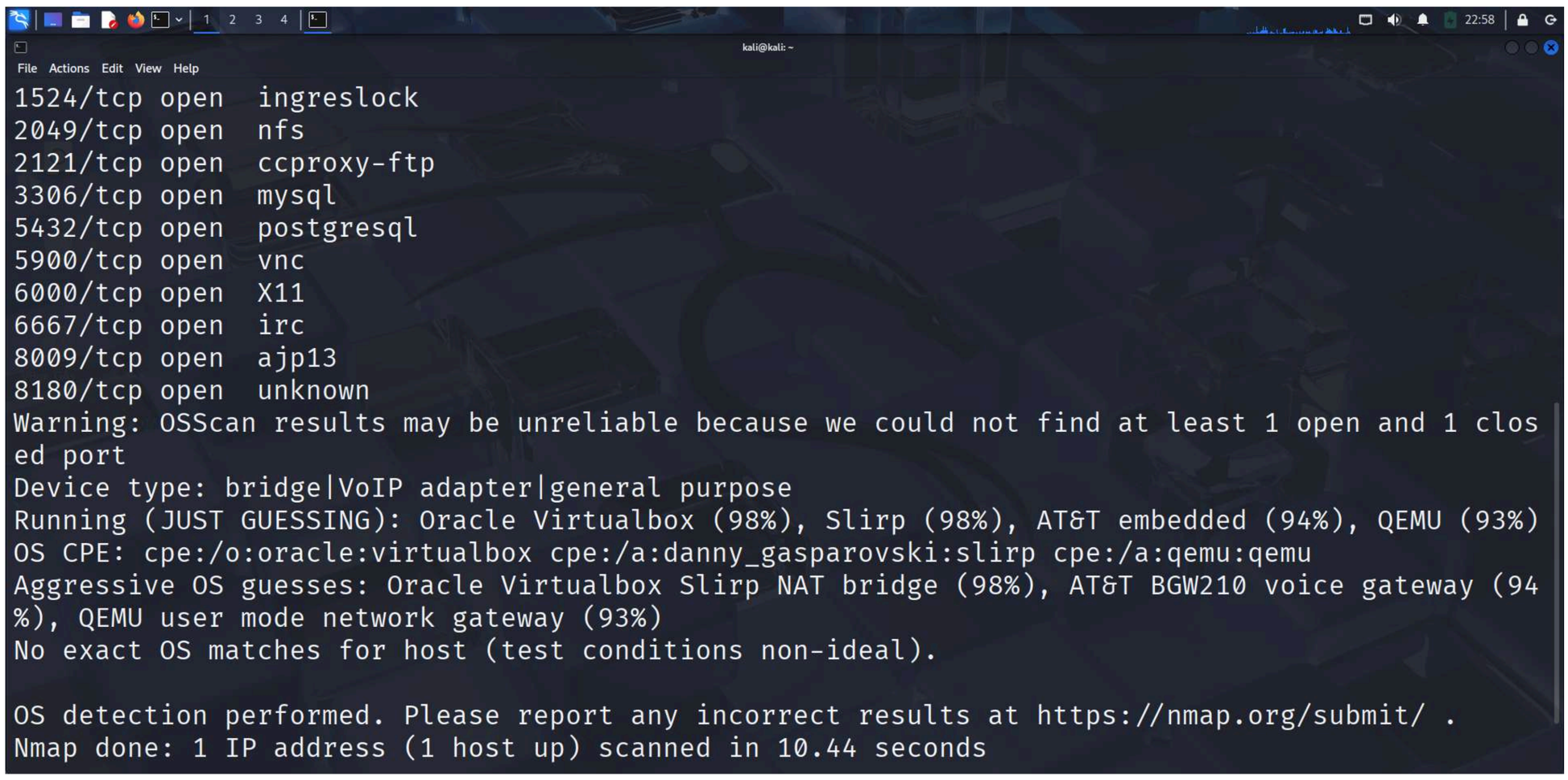
Practical 8: Operating System Detection

Command:

nmap -O <target-ip>

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



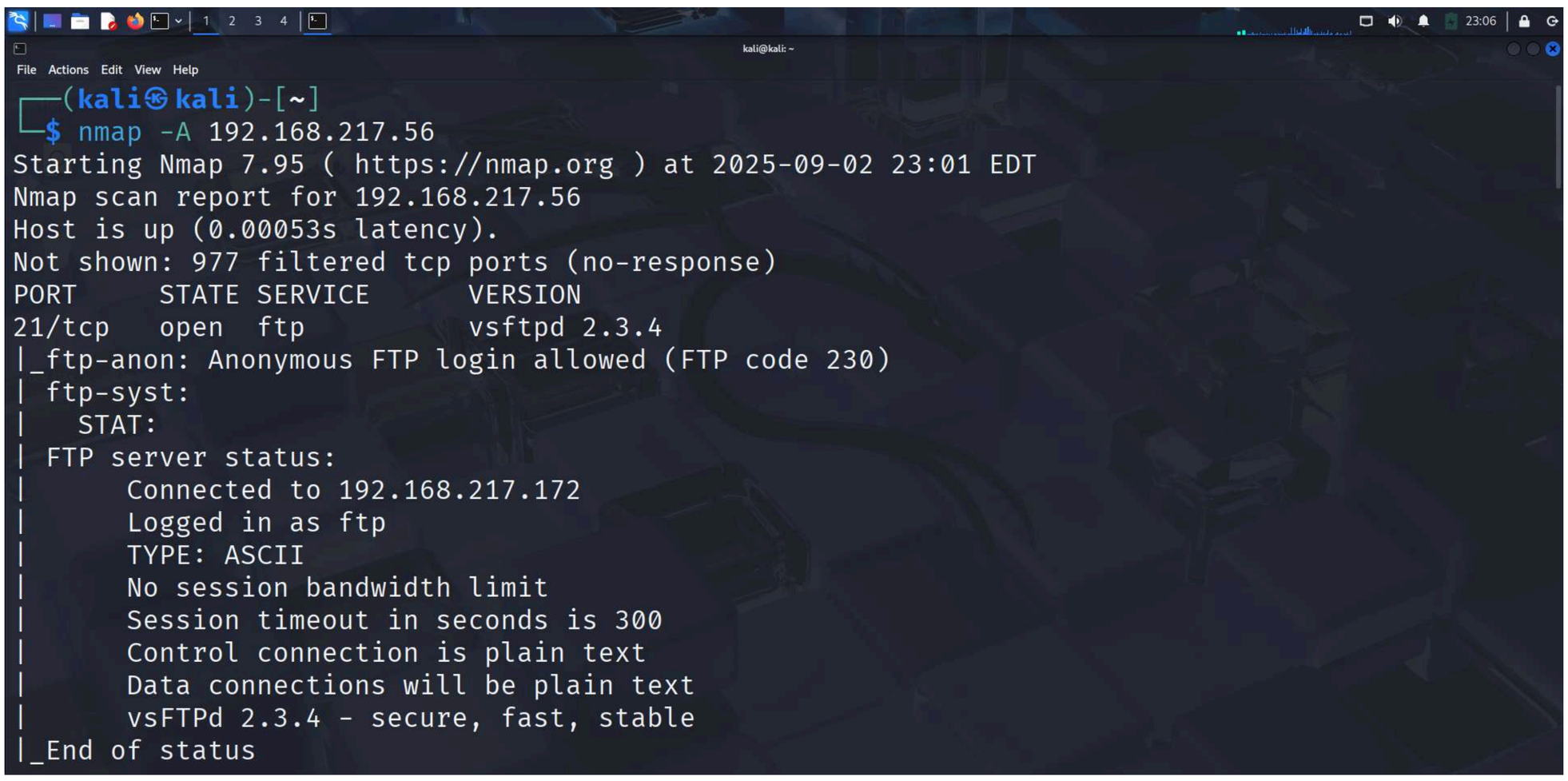


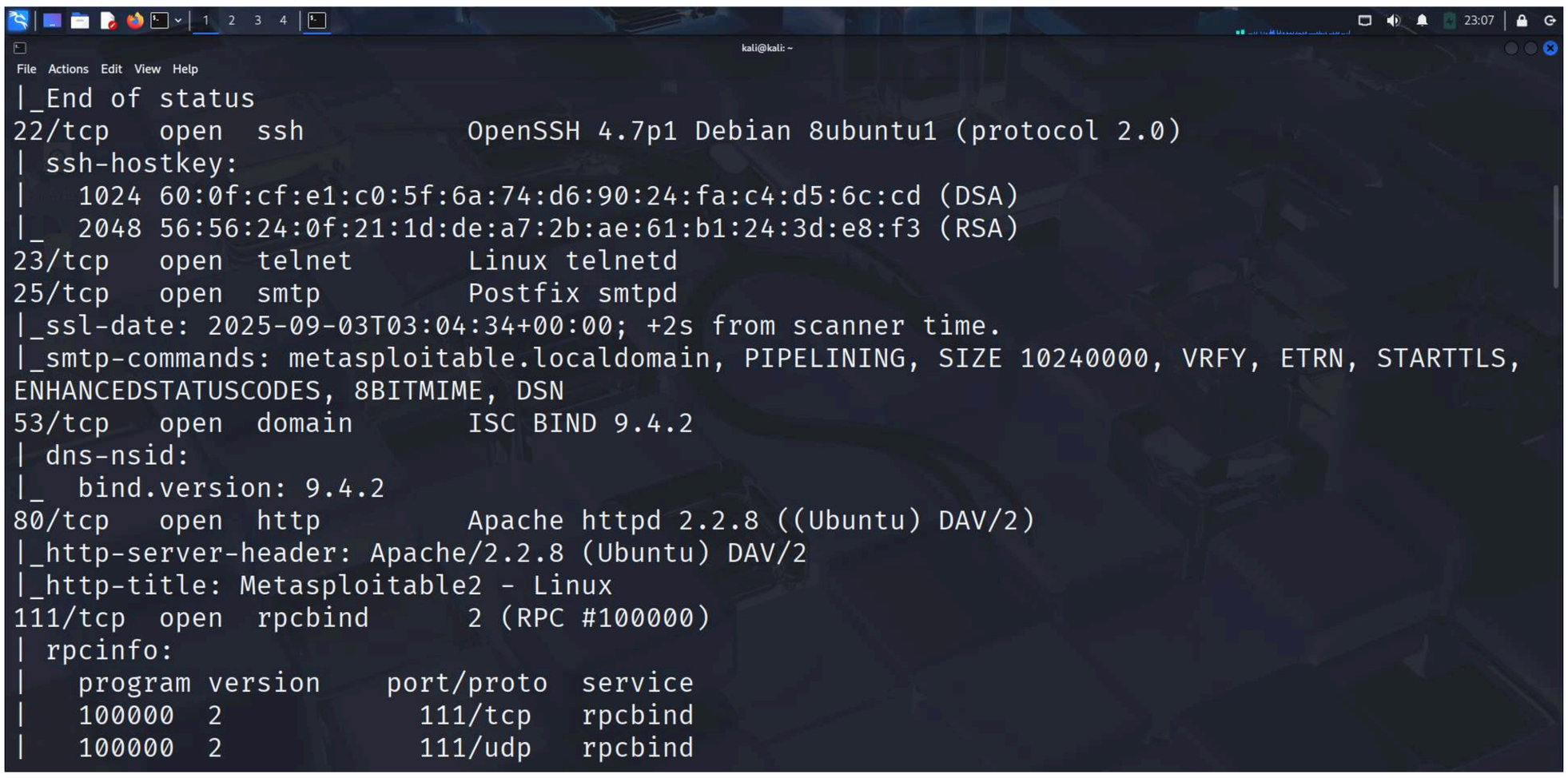
Practical 9: Aggressive Scan (All-in-One)

Command:

nmap -A <target-ip>

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

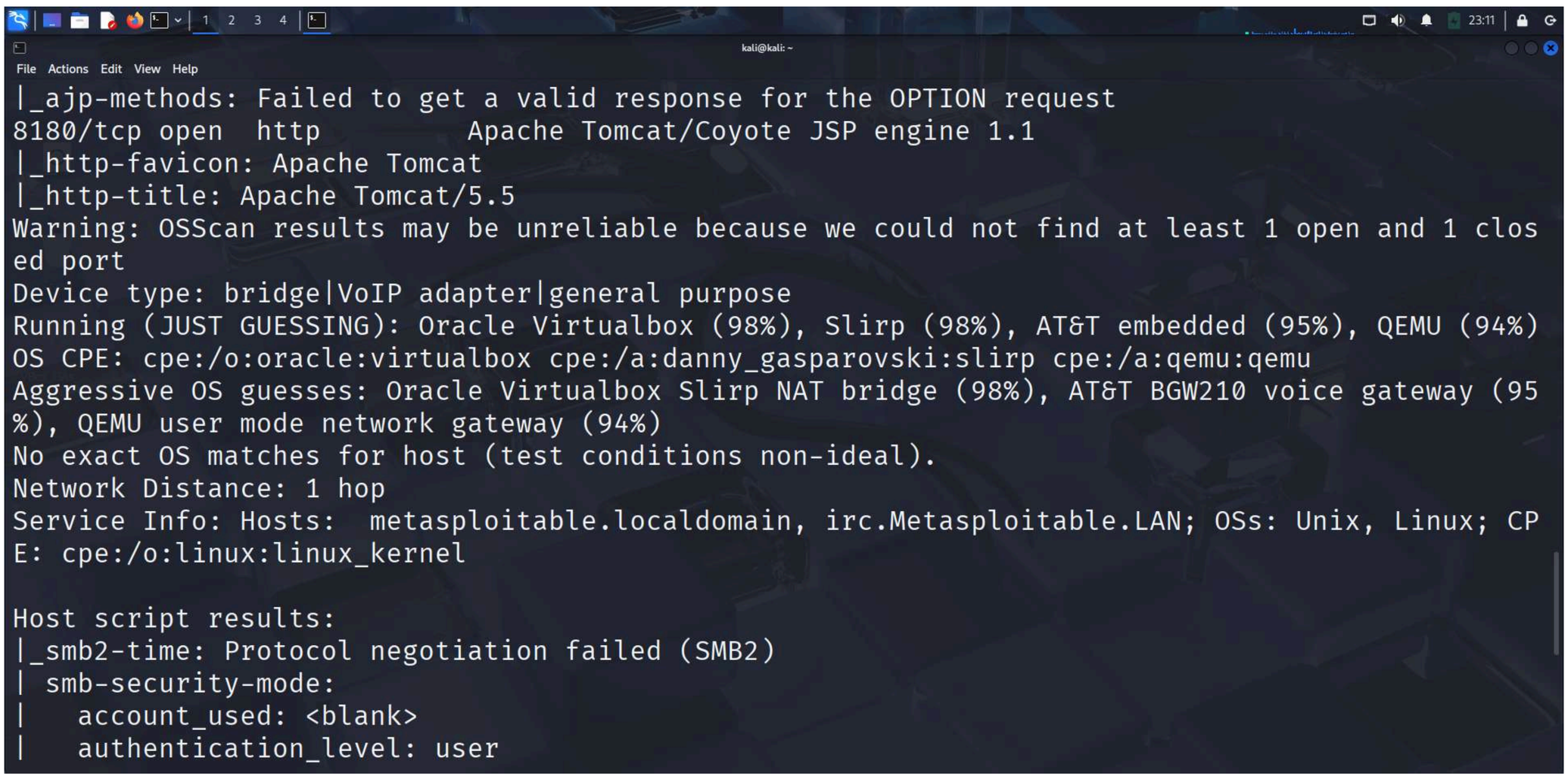


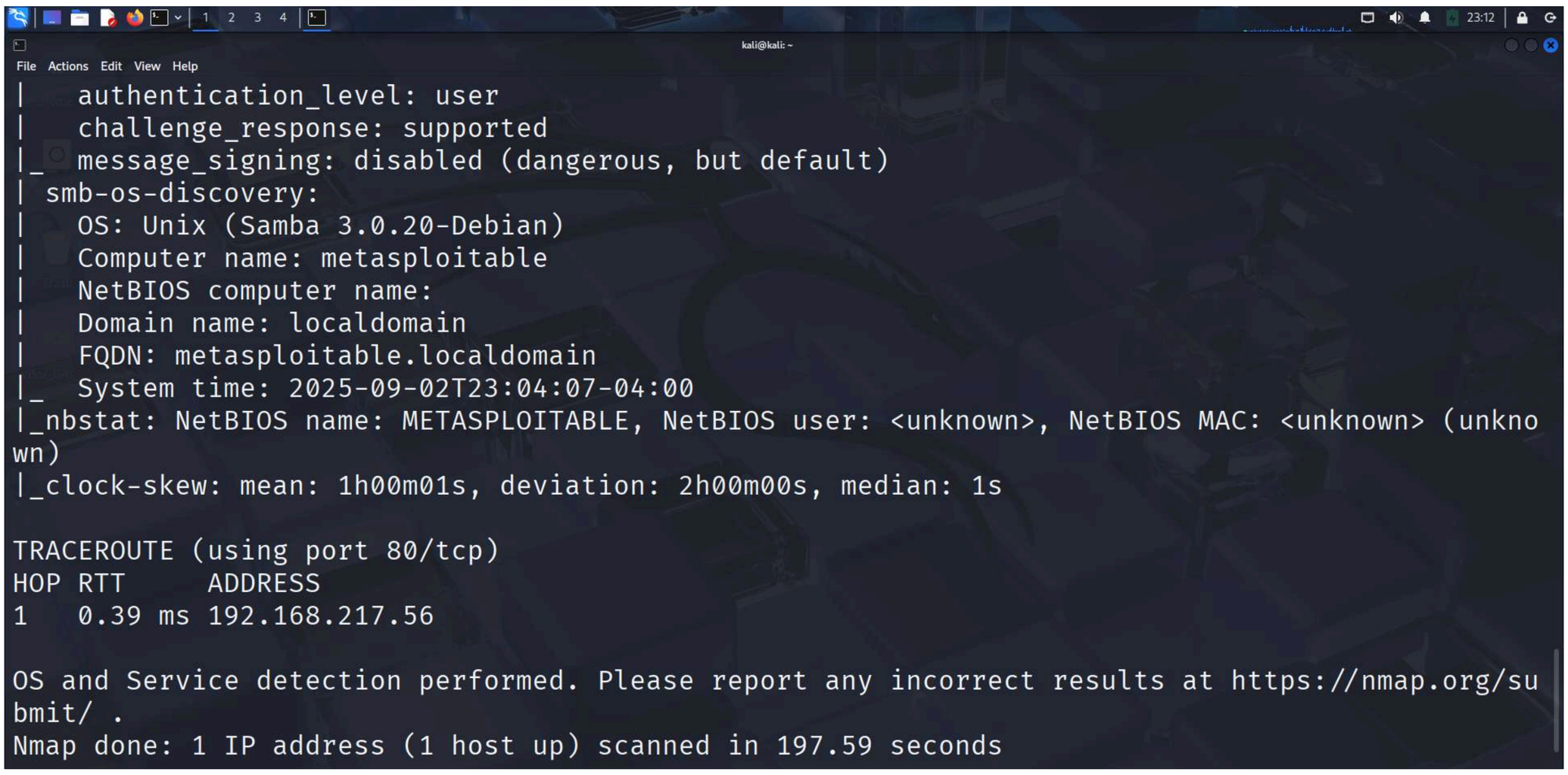


```
111/tcp  open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      42615/udp   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)
```

```
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, SwitchToSSLAf
terHandshake, 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/stateOrProvi
nceName=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:
```

```
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
```


kali@kali: ~
File Actions Edit View Help
|_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 clos
ed 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

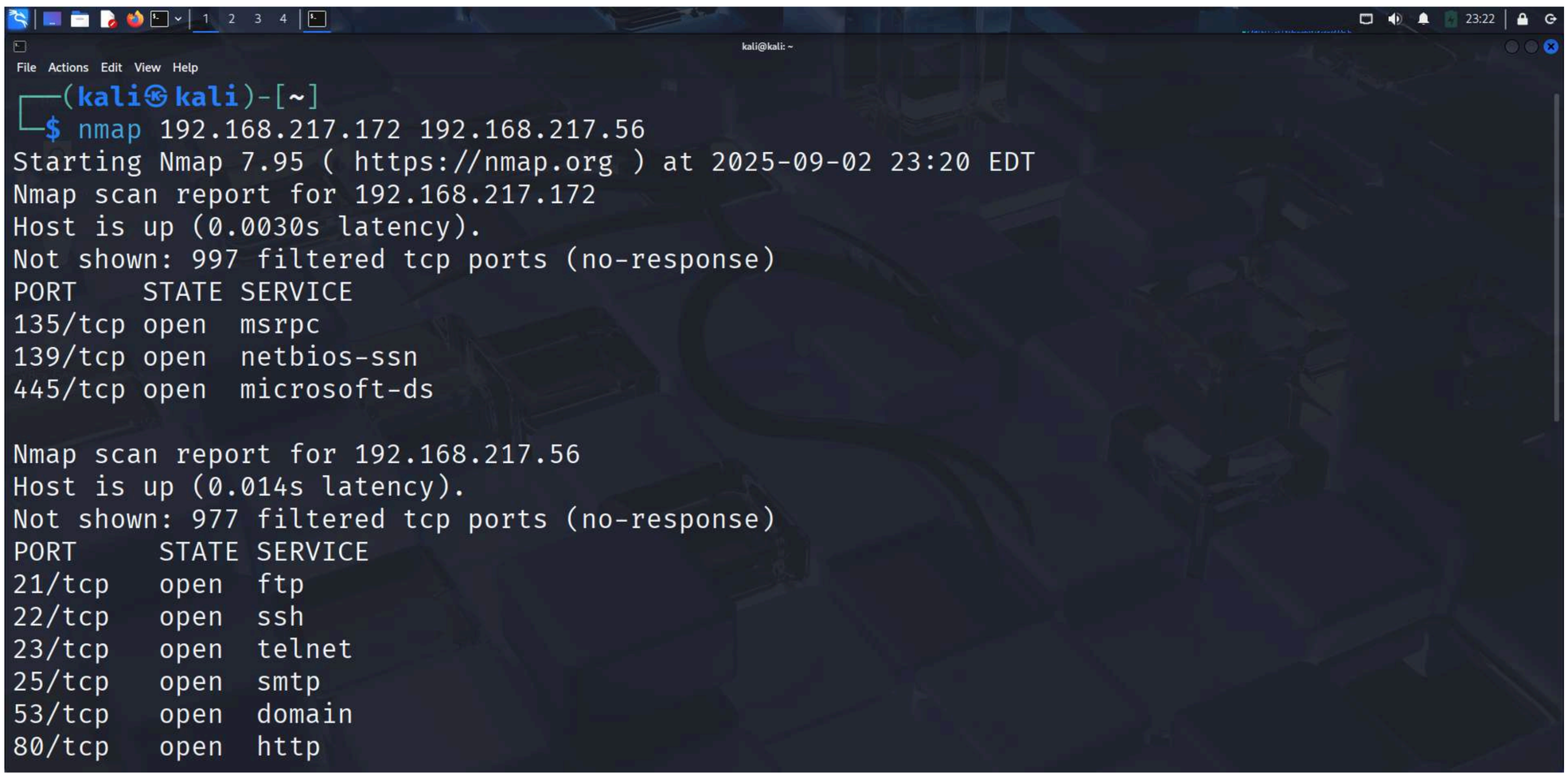

kali@kali: ~
File Actions Edit View Help
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2025-09-02T23:04:07-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkno
wn)
|_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/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.59 seconds

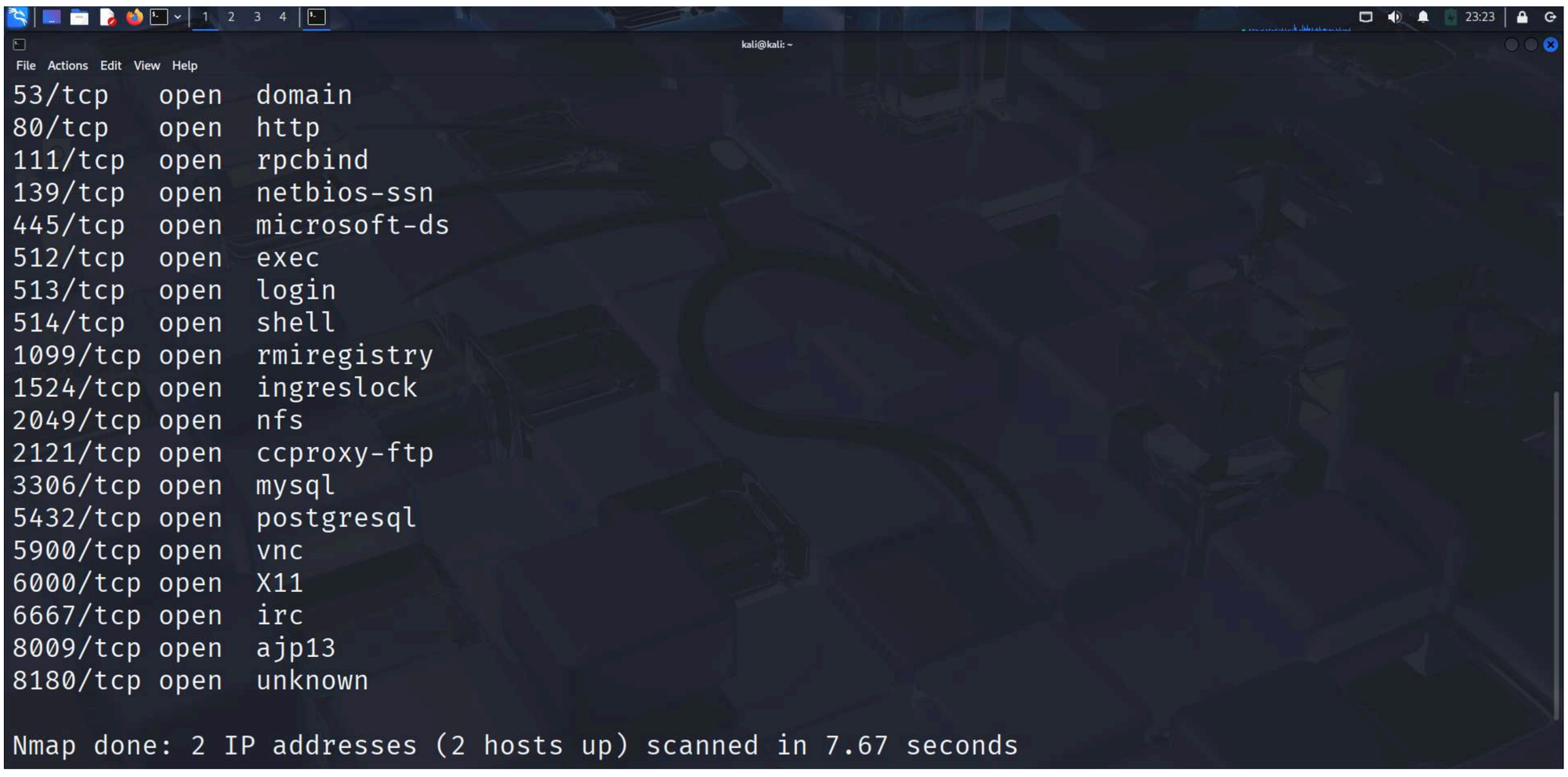
Practical 10: Scan Multiple IPs

Command:

nmap <ip1> <ip2>

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



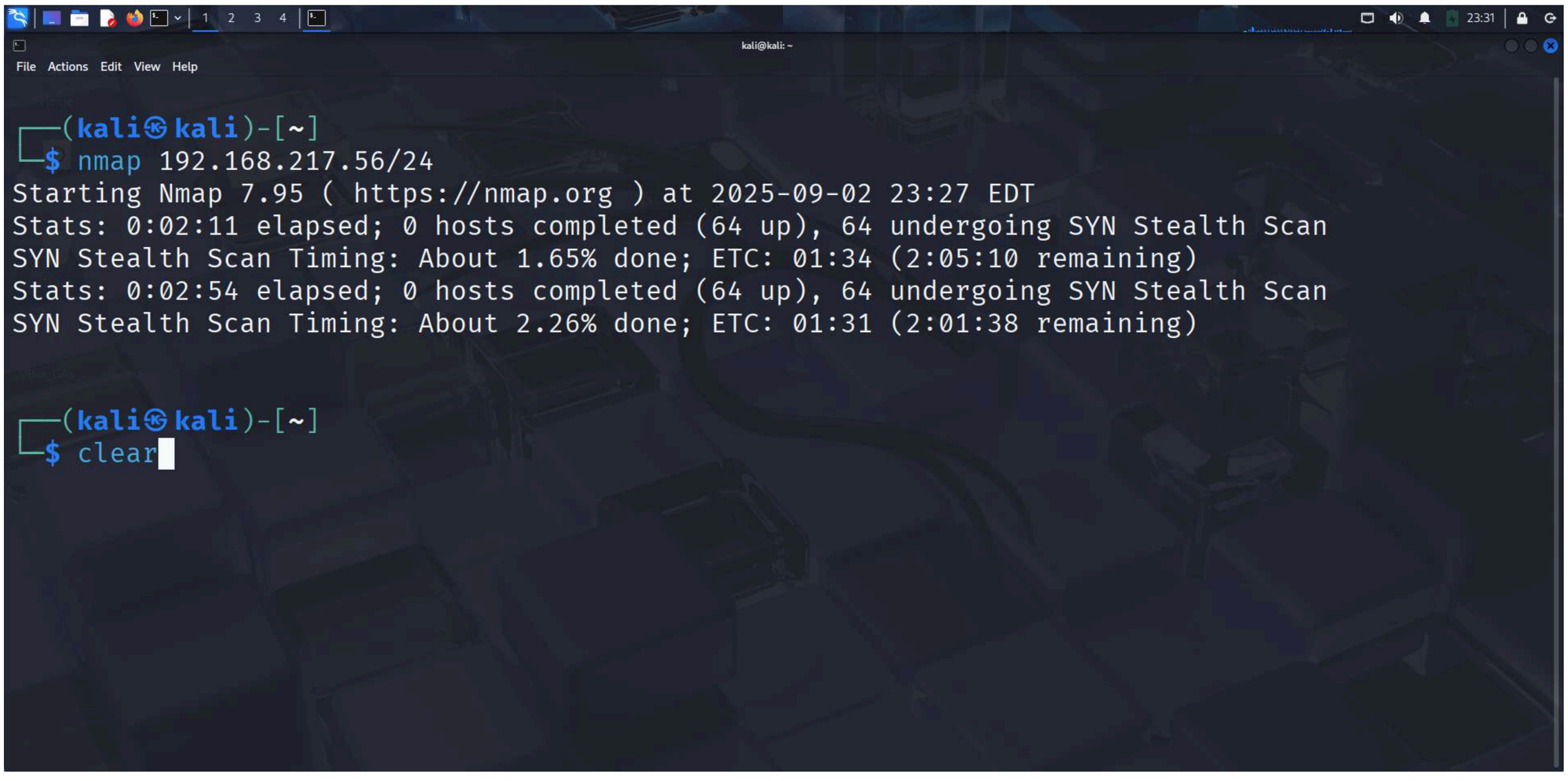


Practical 11: Scan Entire Subnet

Command:

nmap 192.168.1.0/24

Explanation: Scans all devices in the given subnet.



It will take approximately 1 – 2 hours to complete scan the entire subnet,

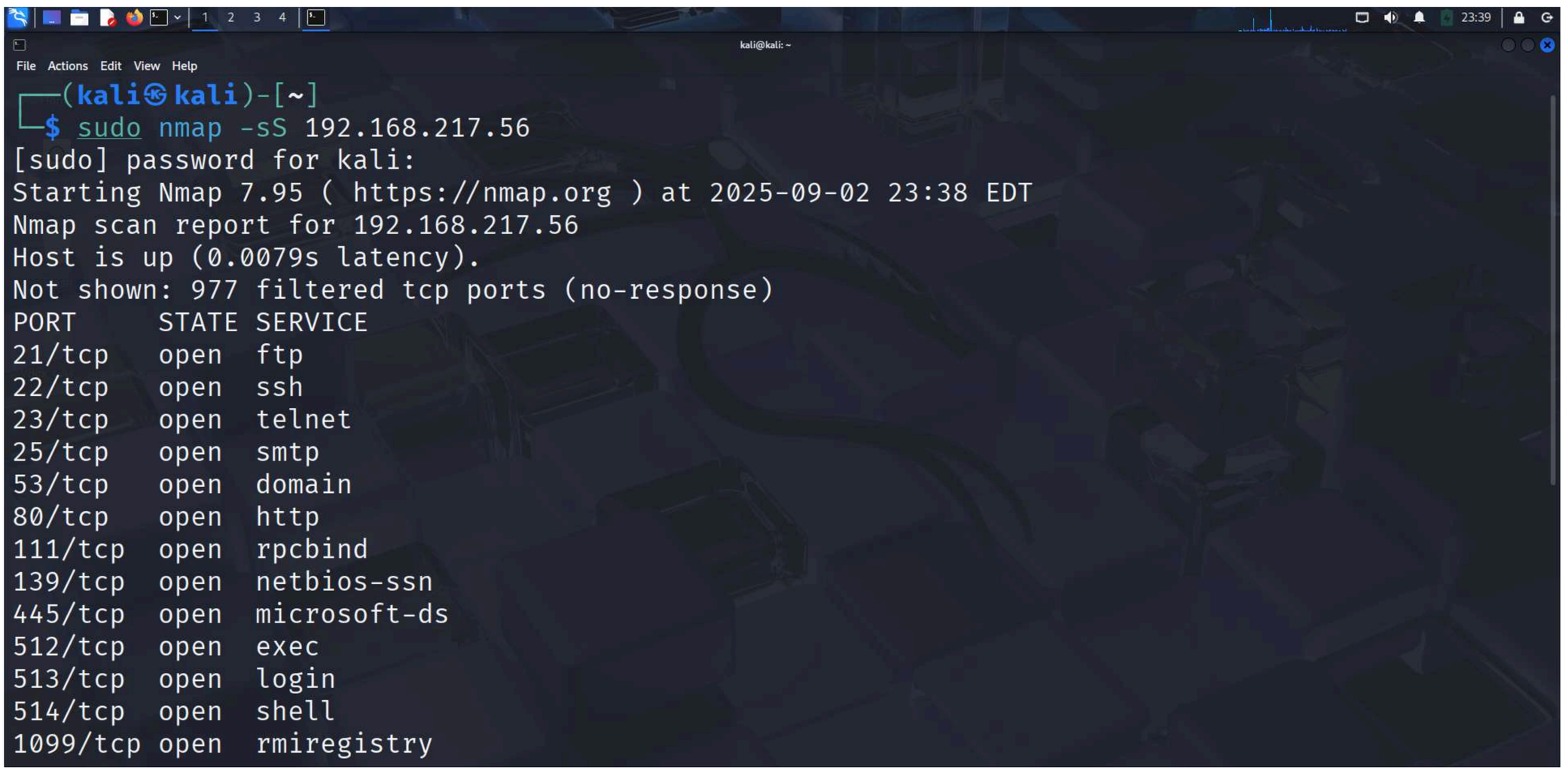
We can check the progress by pressing “space” key

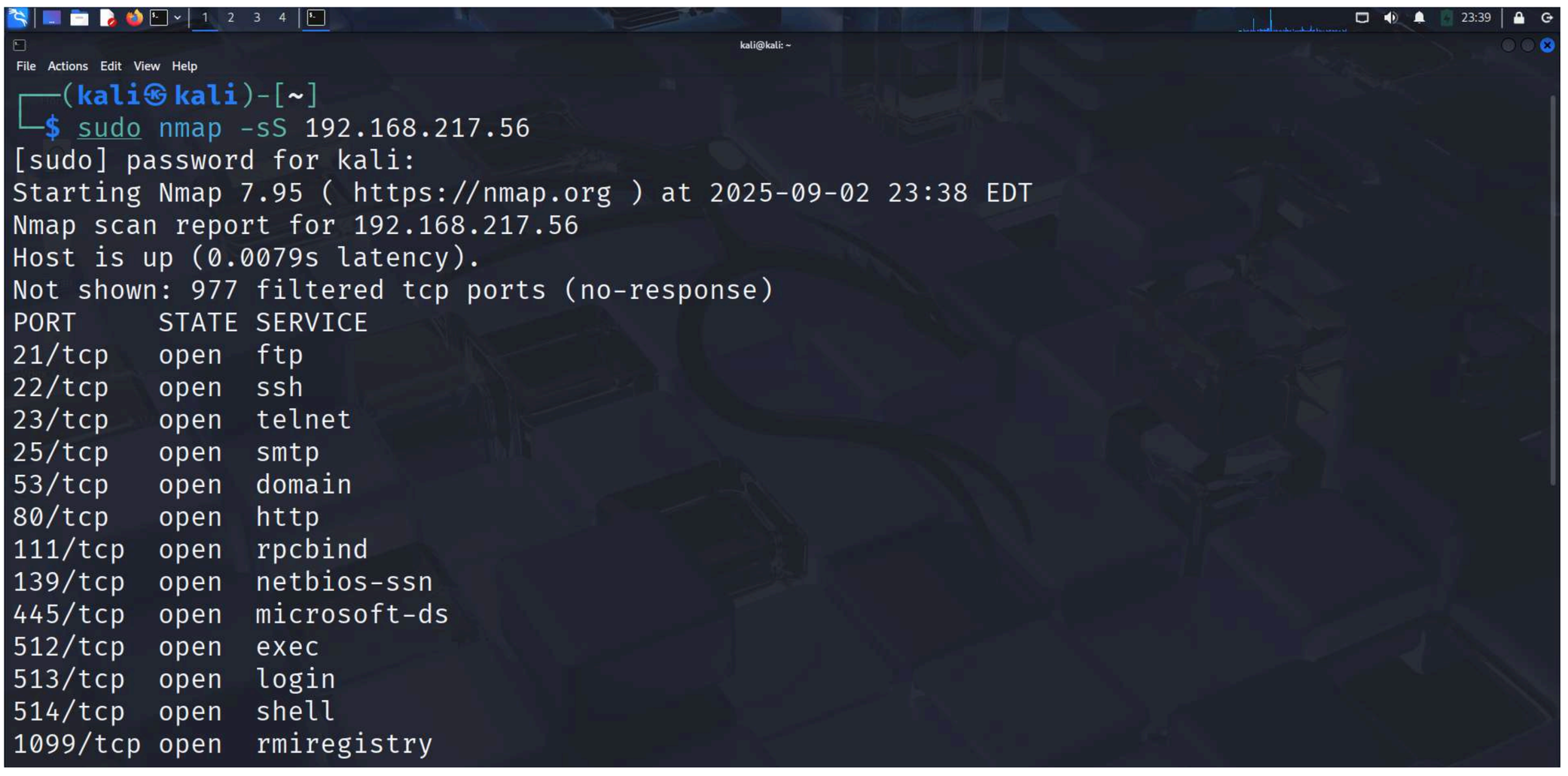
Practical 12: Stealth Scan (SYN Scan)

Command:

sudo nmap -sS <target-ip>

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



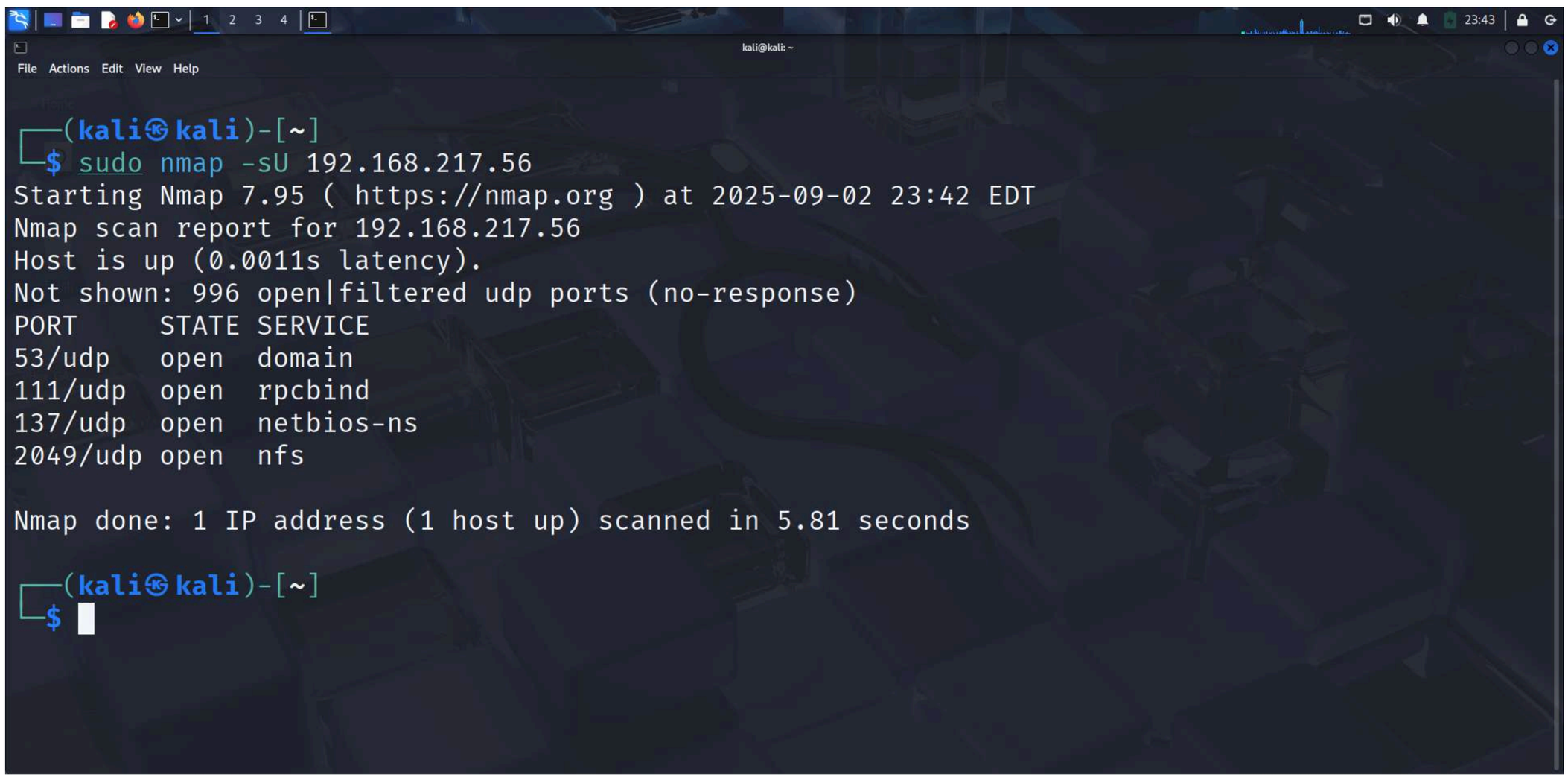


Practical 13: UDP Scan

Command:

sudo nmap -sU <target-ip>

Explanation: Scans for open UDP ports.

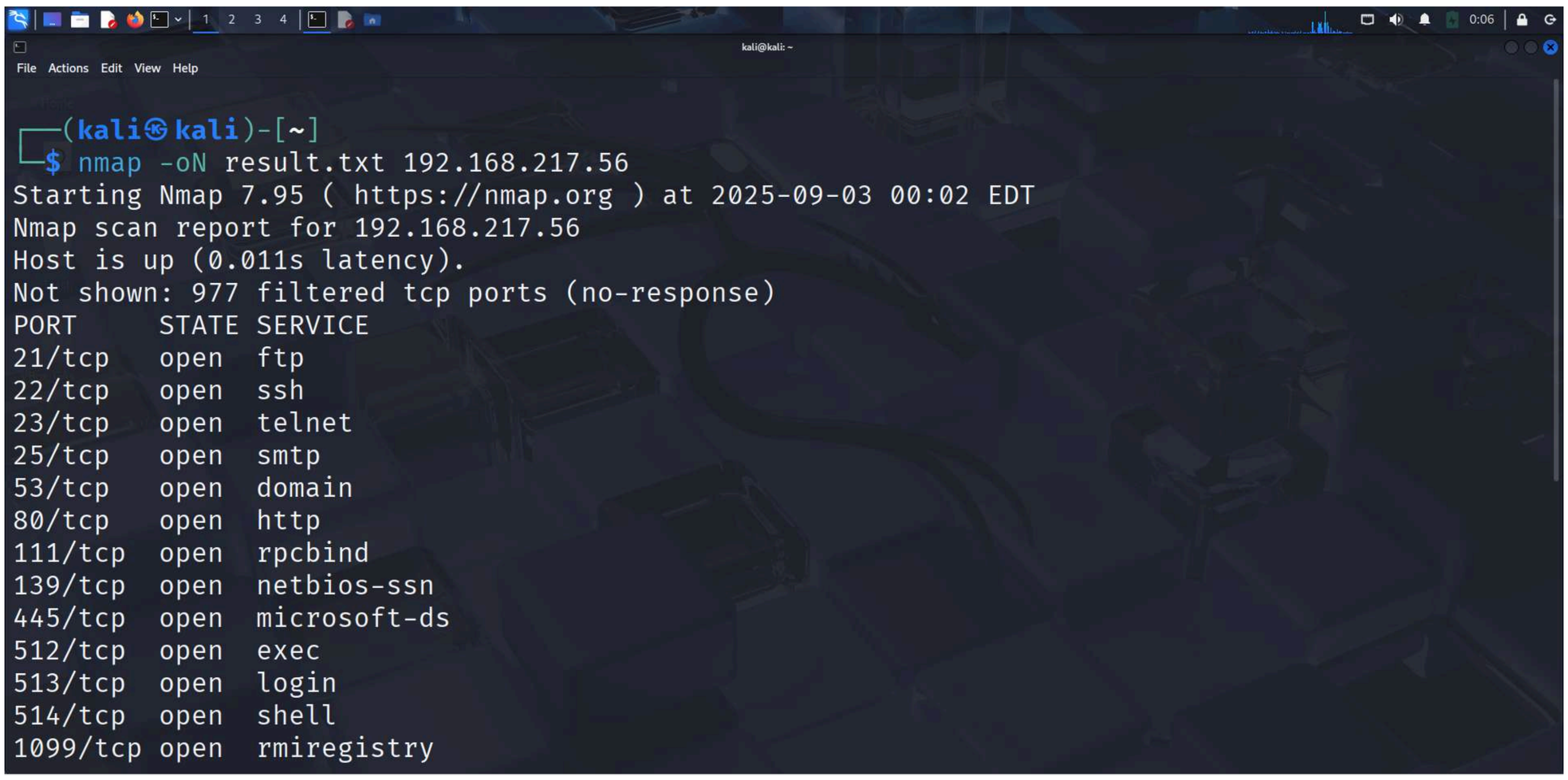


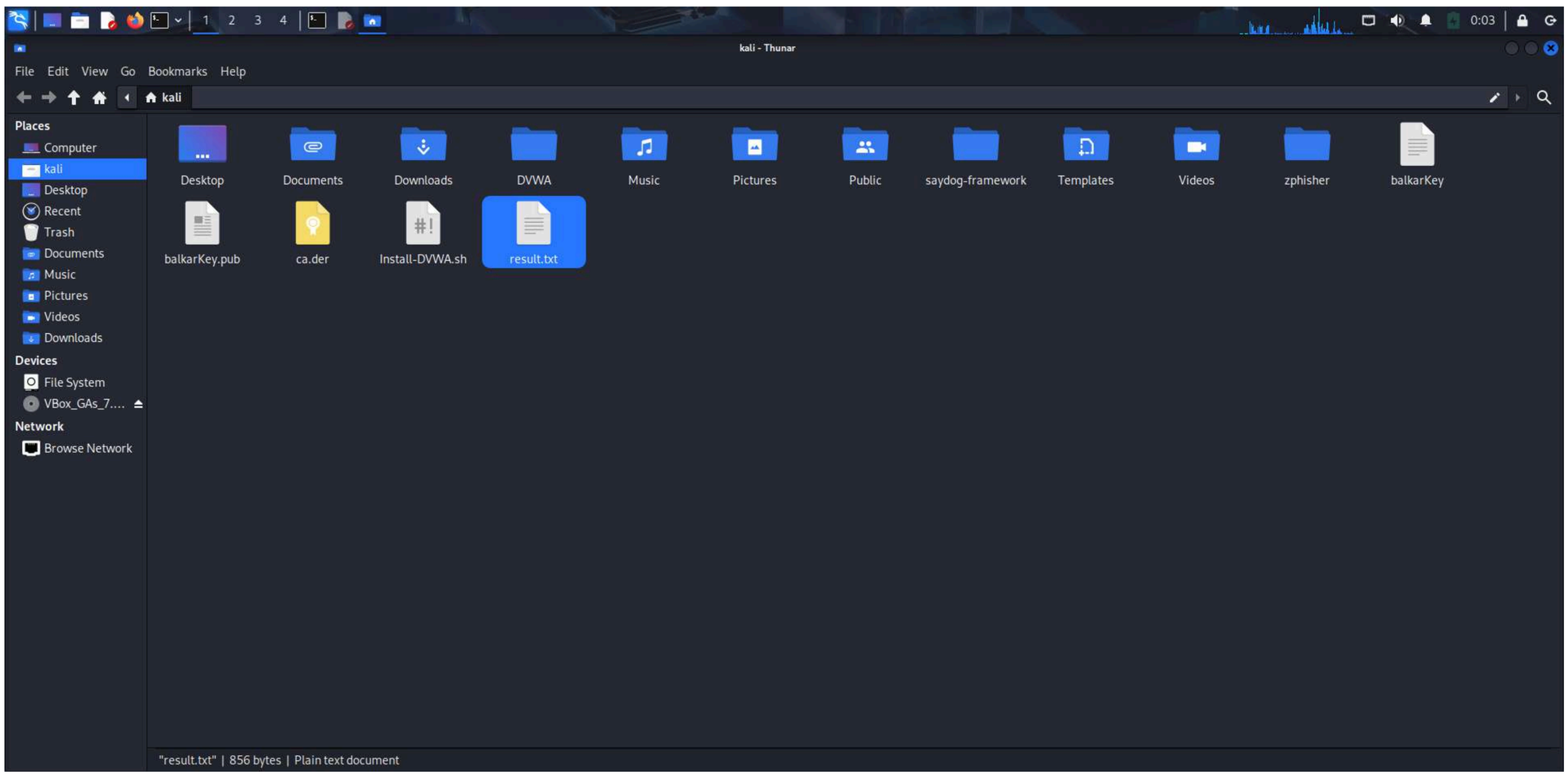
Practical 14: Save Output to File

Command:

nmap -oN result.txt <target-ip>

Explanation: Saves the scan results into a text file.



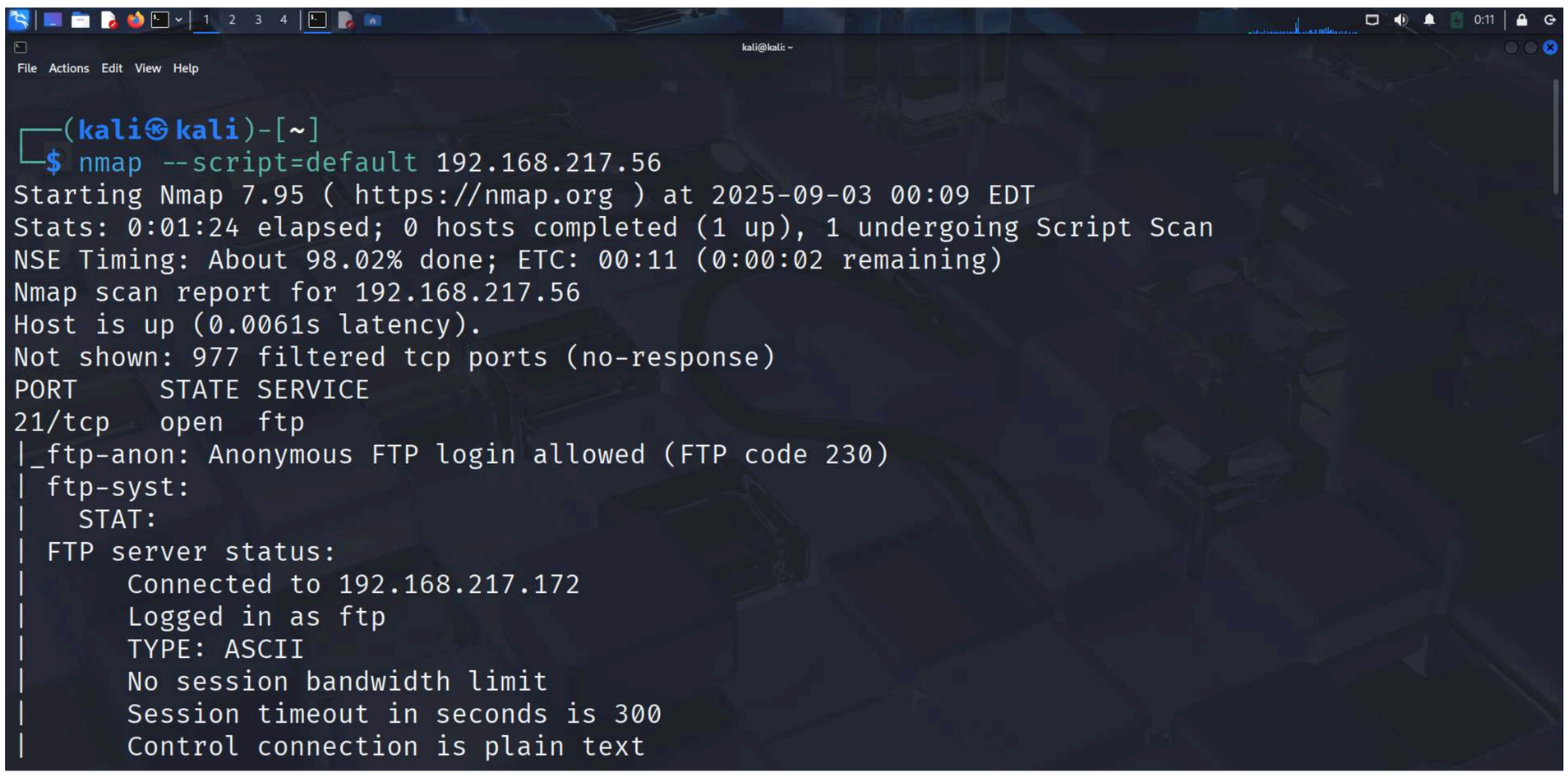


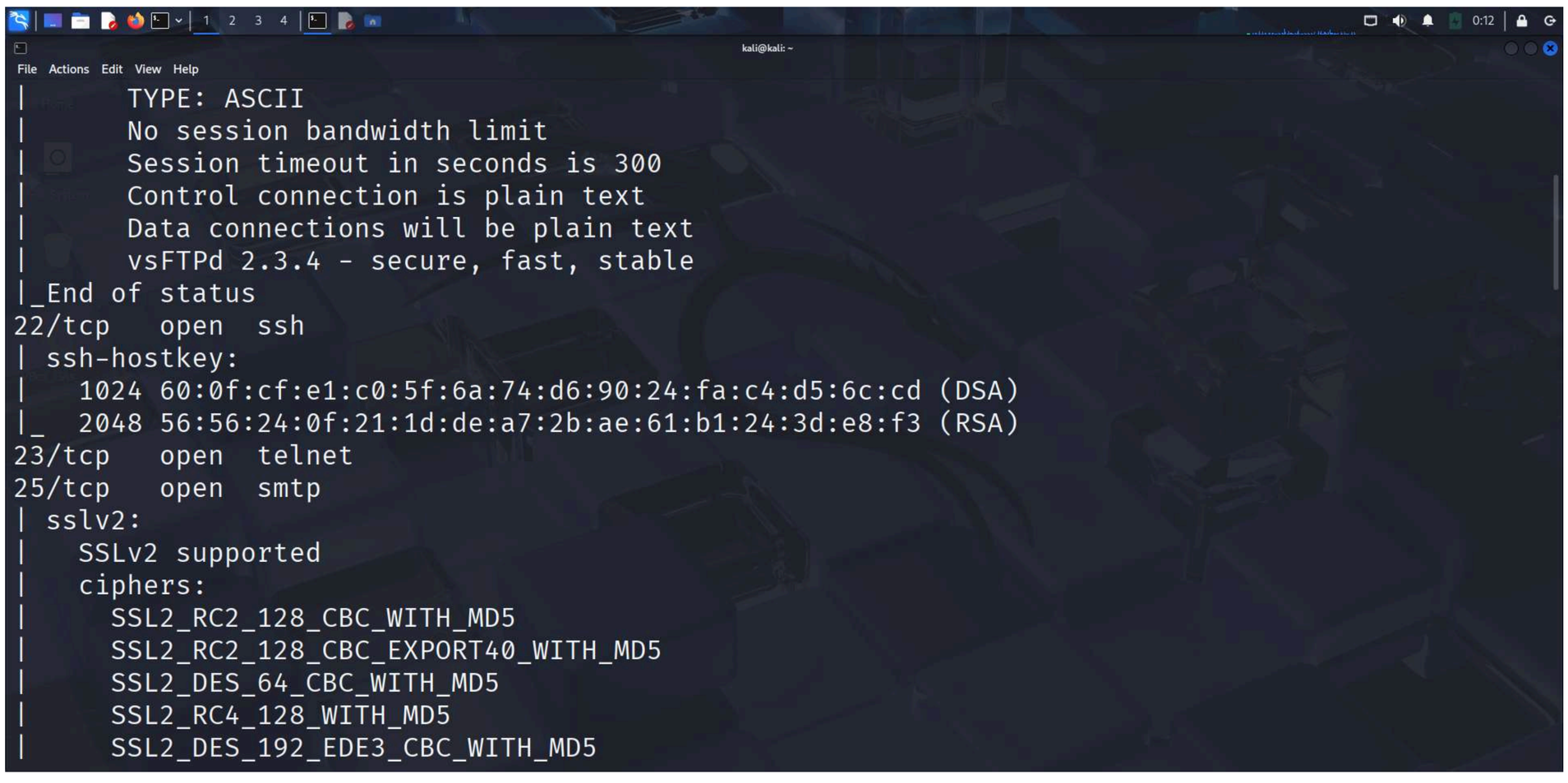
Practical 15: Script Scan (NSE)

Command:

nmap --script=default <target-ip>

Explanation: Runs default Nmap scripts for detailed scanning.

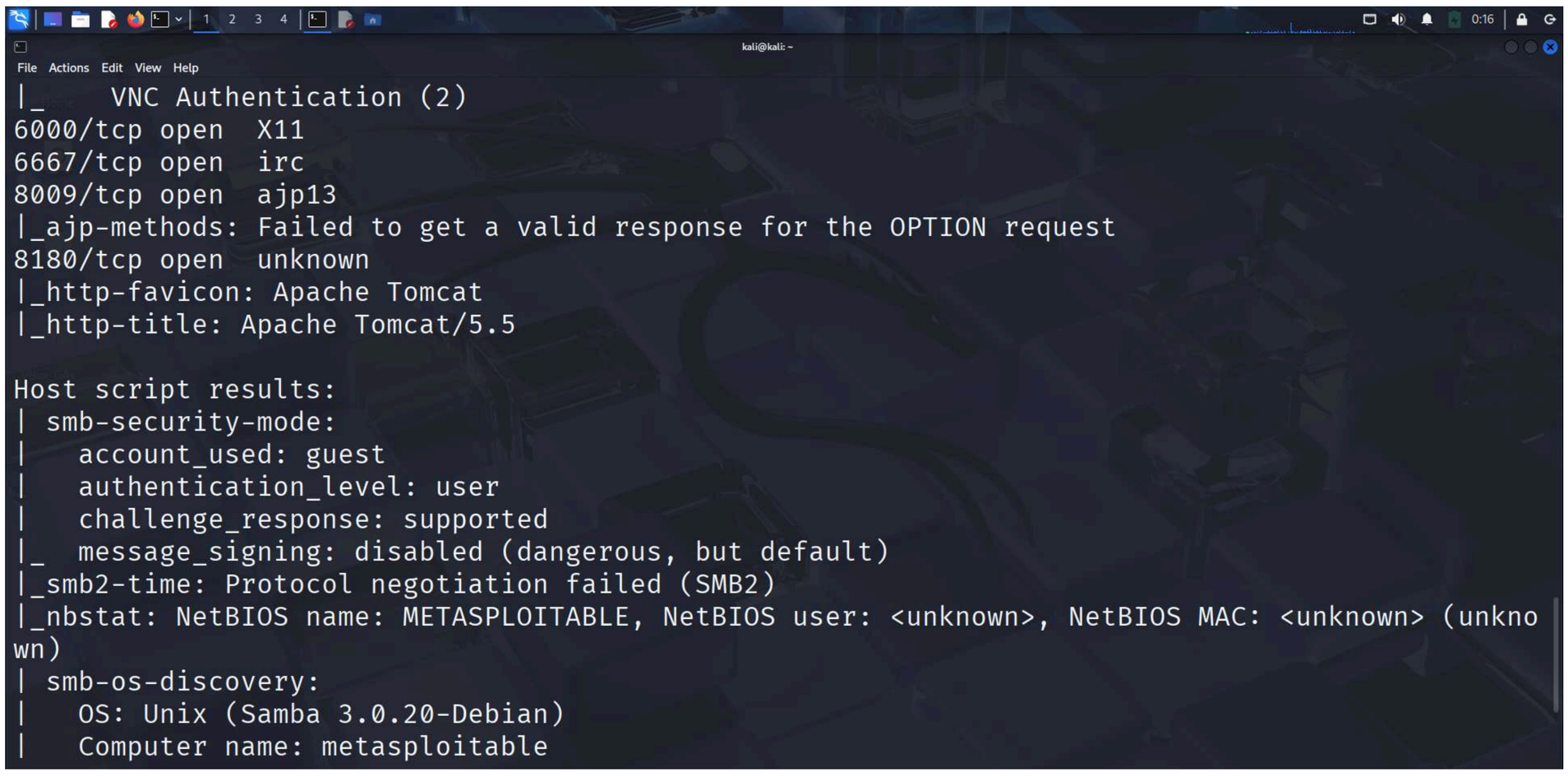


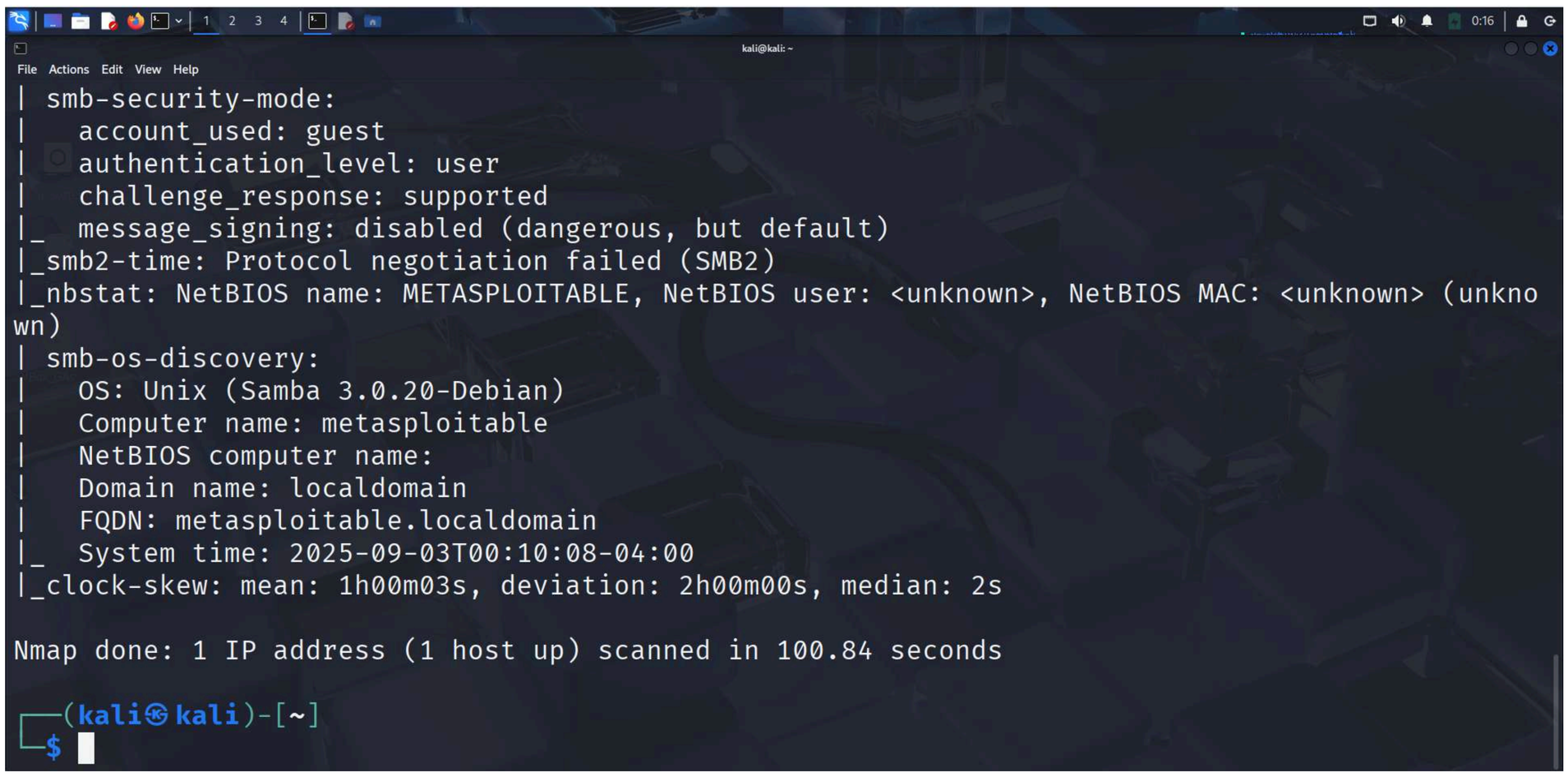


```
|      SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_ssl-date: 2025-09-03T04:10:44+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvi
nceName=There is no such thing outside US/countryName=XX
| Not valid 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
```

```
|   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
```

```
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 31
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase, SupportsCompression, SupportsTransa
ctions, SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew
|   Status: Autocommit
|_  Salt: v~9=ddI!cQOt}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/stateOrProvi
nceName=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
```

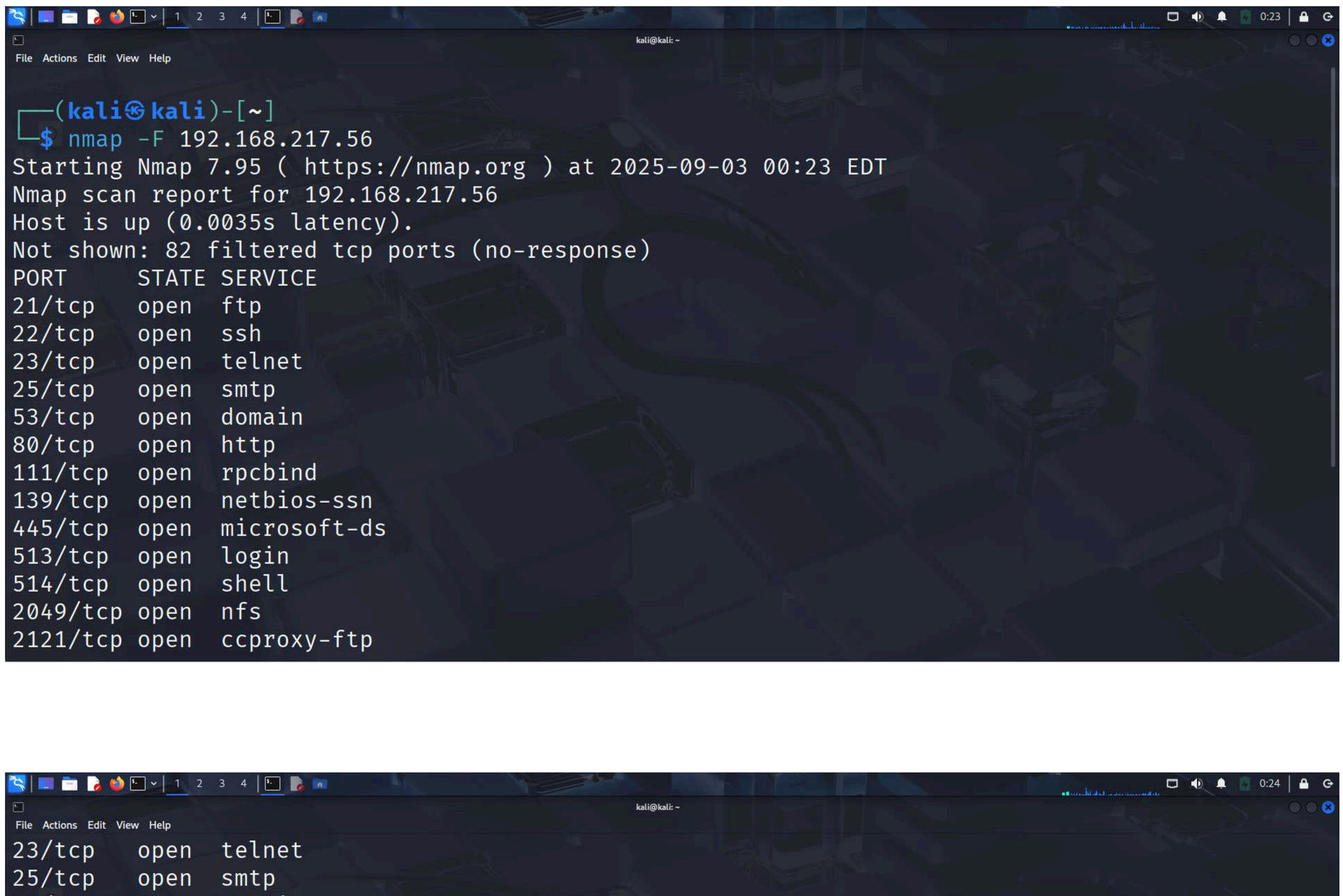

kali@kali: ~
File Actions Edit View Help
|_ VNC Authentication (2)
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
Host script results:
| smb-security-mode: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

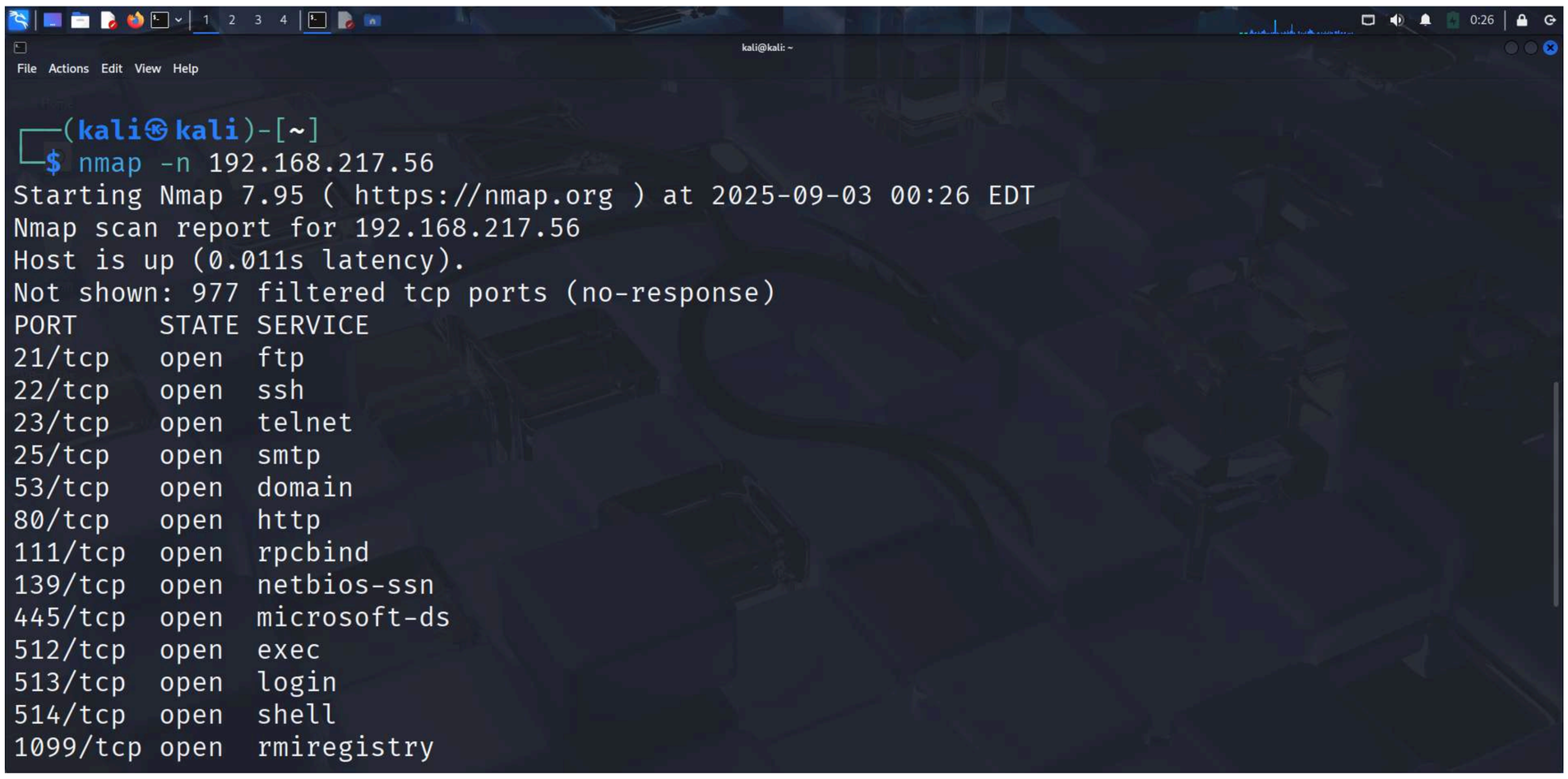
👉 **Scans the top 100 most common ports (faster than normal scan).**

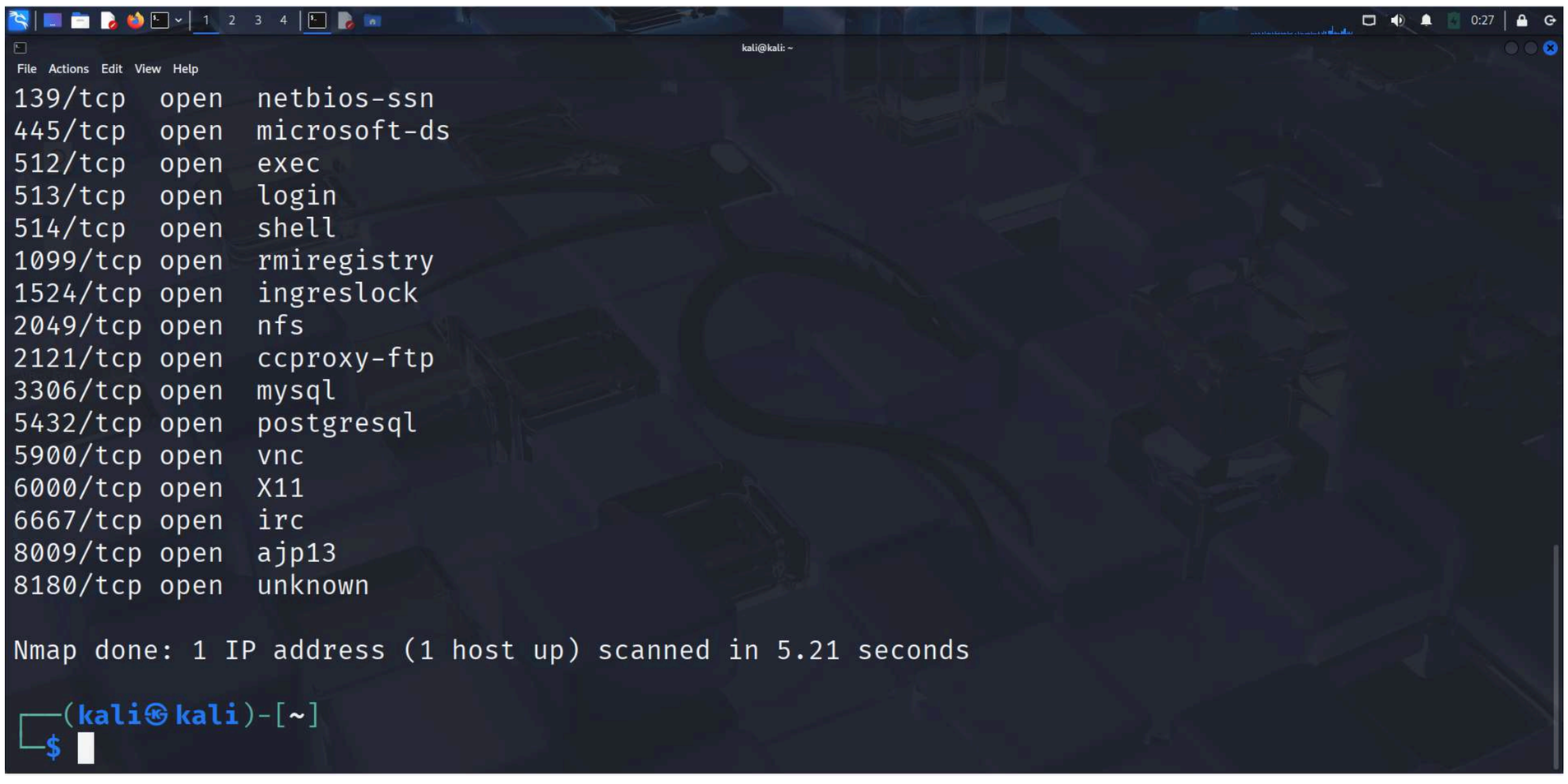


Practical-17: Scan Without DNS Resolution

nmap -n <target-ip>

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

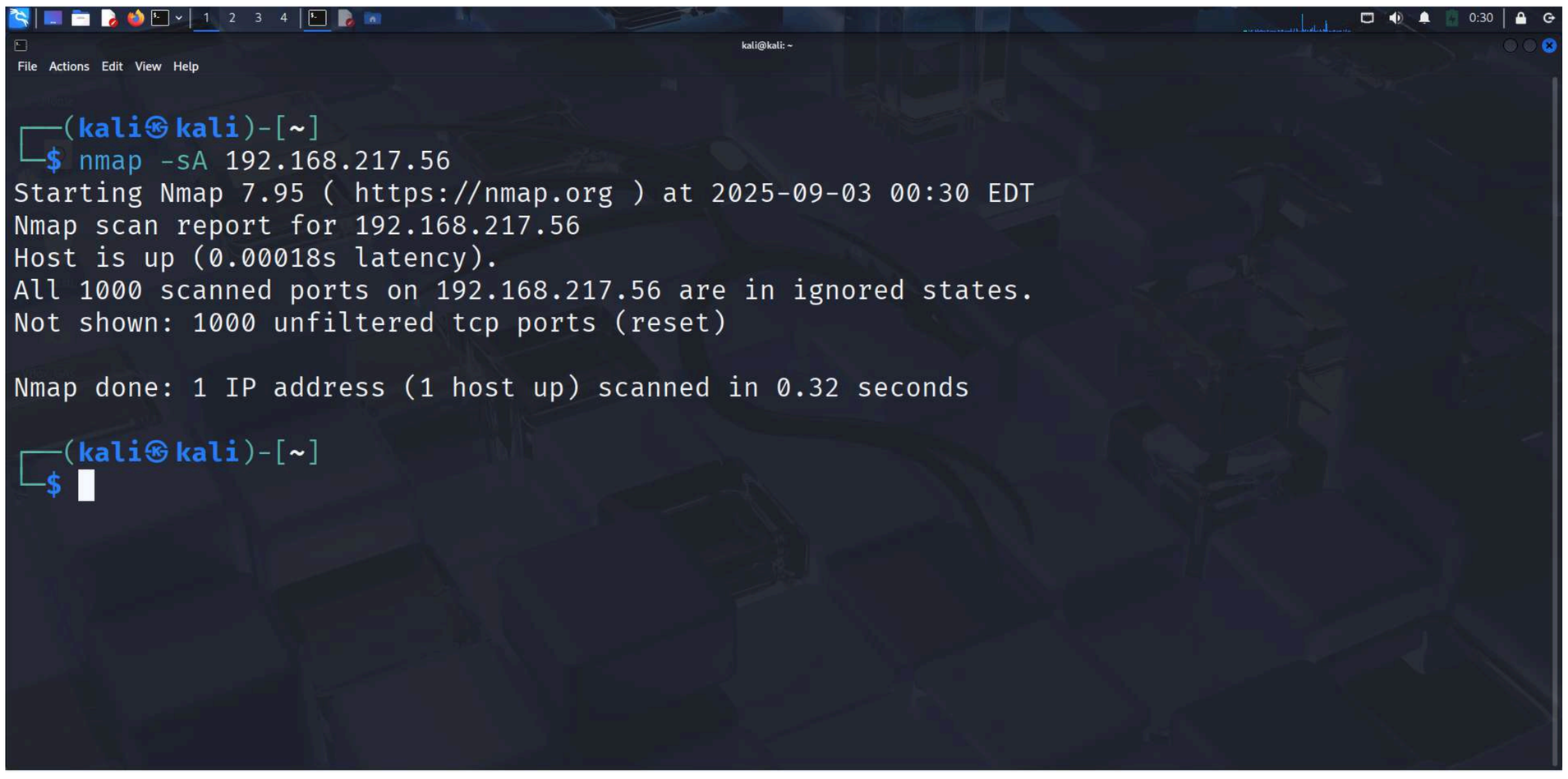




Practical-18: Detect Firewall/Packet Filters

nmap -sA <target-ip>

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



- ● 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.

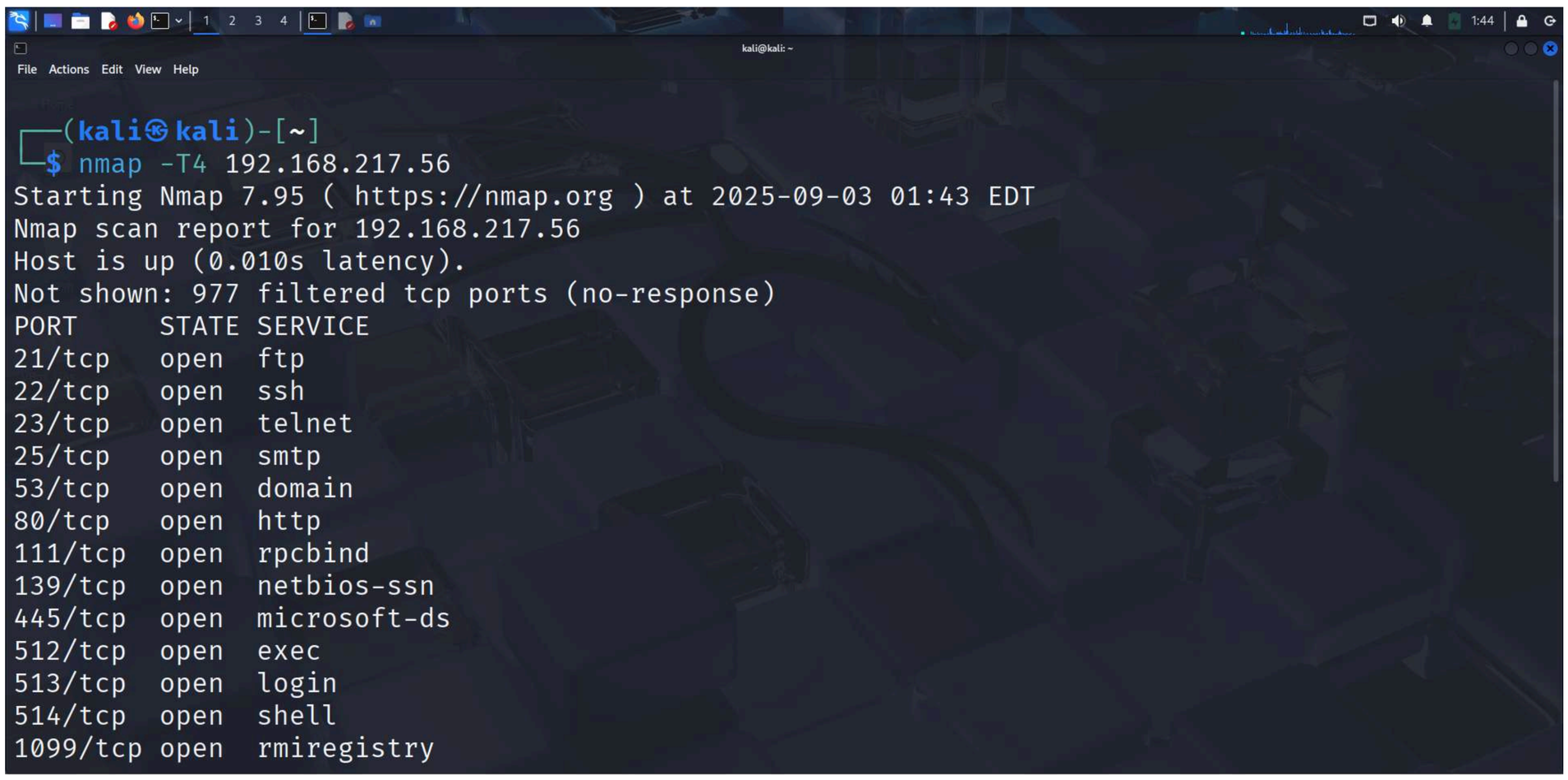
- Practical-19: Idle Scan (Anonymous Scan)
- nmap -sI <zombie-ip> <target-ip>
- 👉 Uses a “zombie” machine to scan another target without revealing your IP.
- What is an Idle Scan?
- ● Idle Scan is a stealth technique in Nmap.
- ● Instead of scanning the target directly from your IP, you use a third machine (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 -sI <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 -sI 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

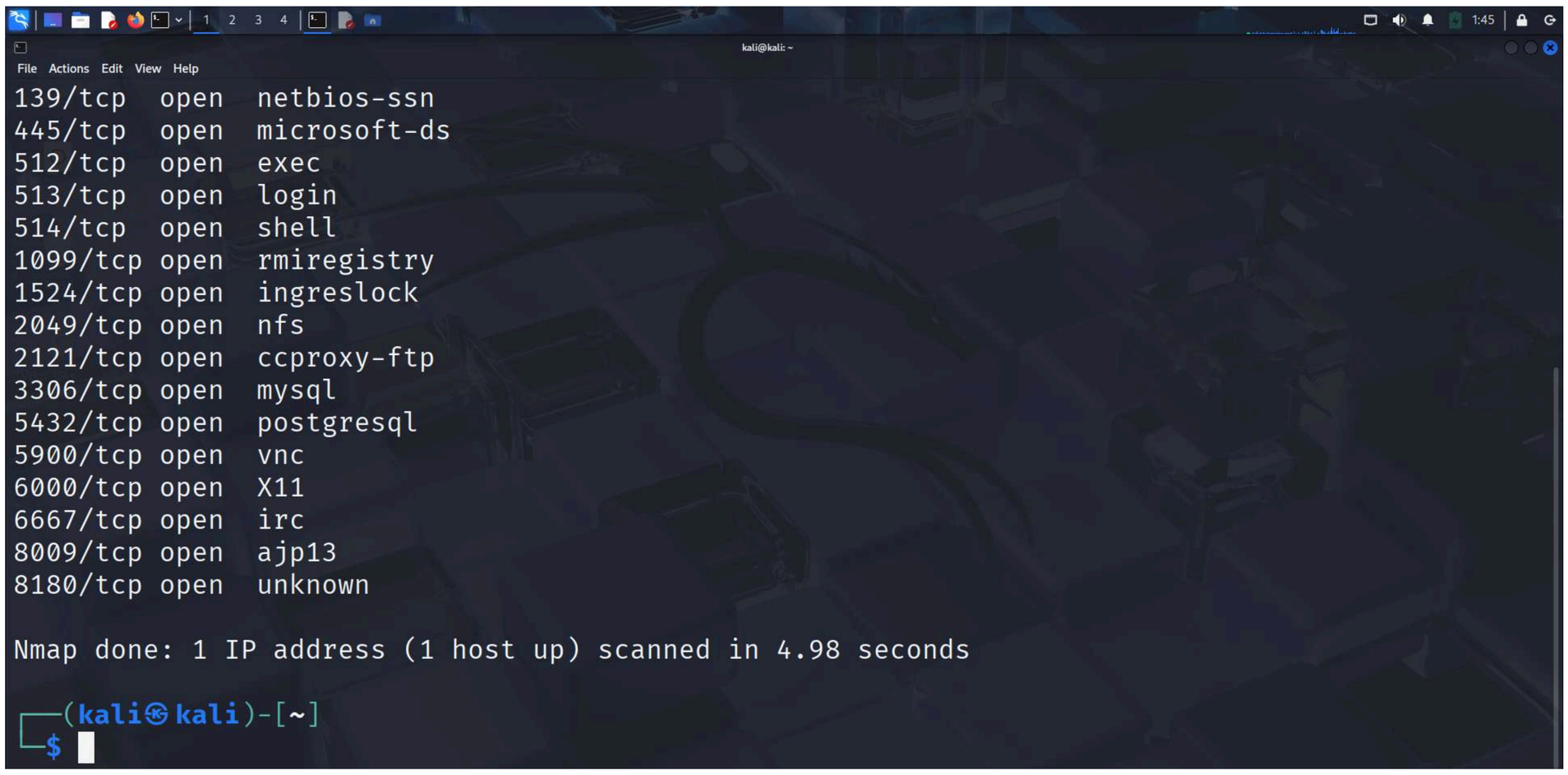
If the scan works, it will show open/closed ports on the target, but the scan will appear to come from the zombie host.

Practical-20: Timing Templates

nmap -T4 <target-ip>

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

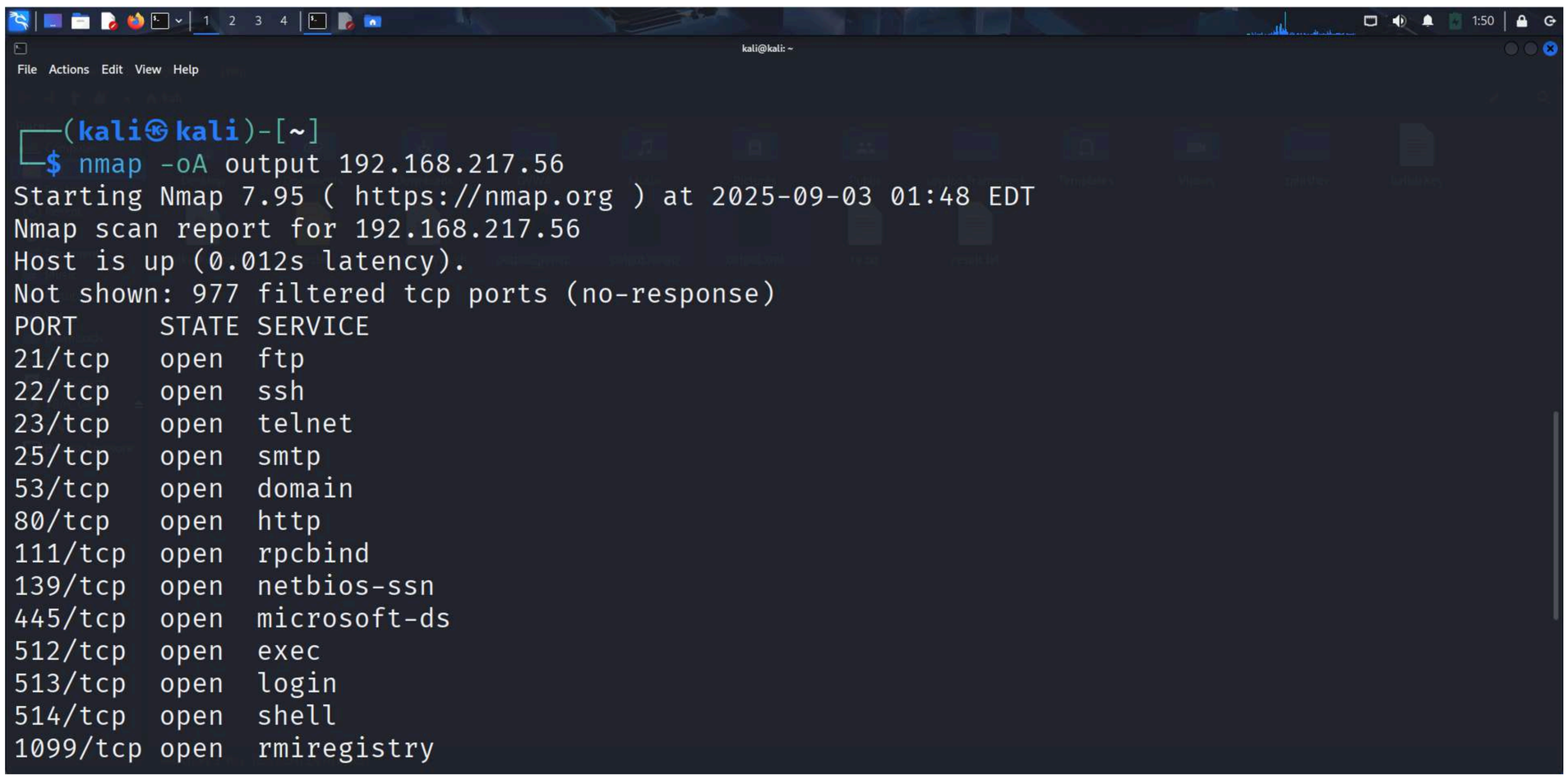


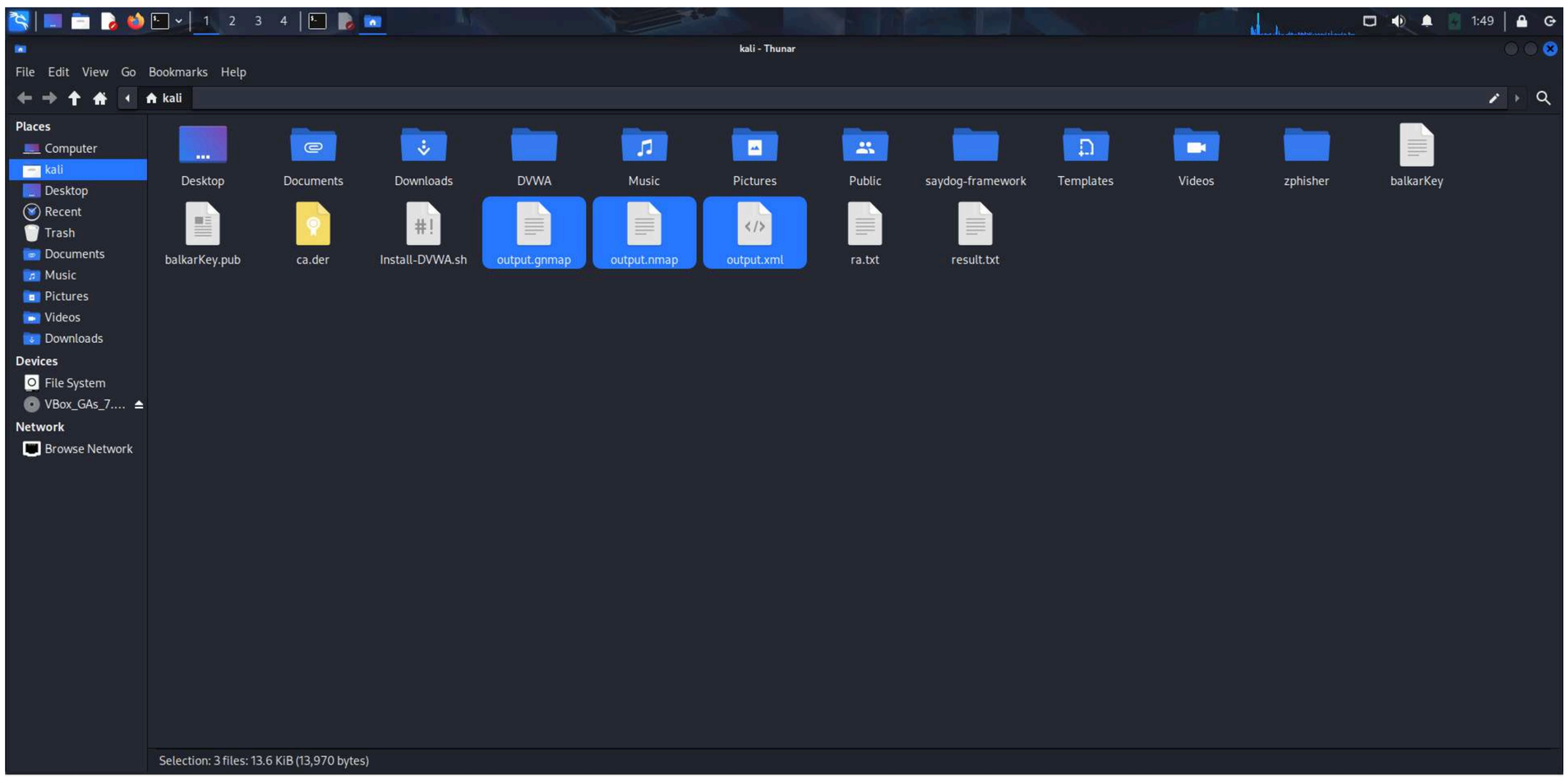


Practical-21: Scan and Save Output in All Formats

nmap -oA output <target-ip>

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

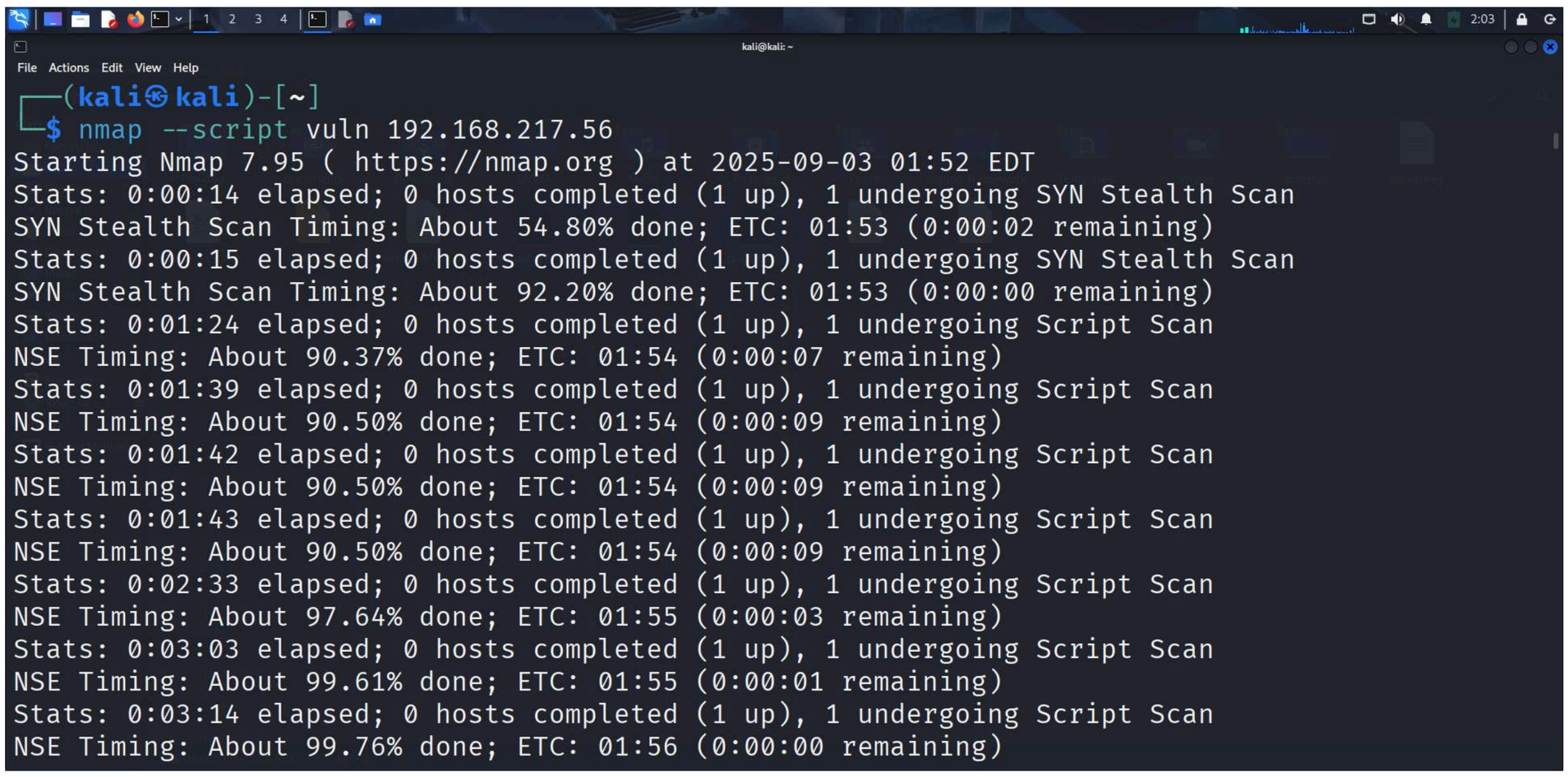


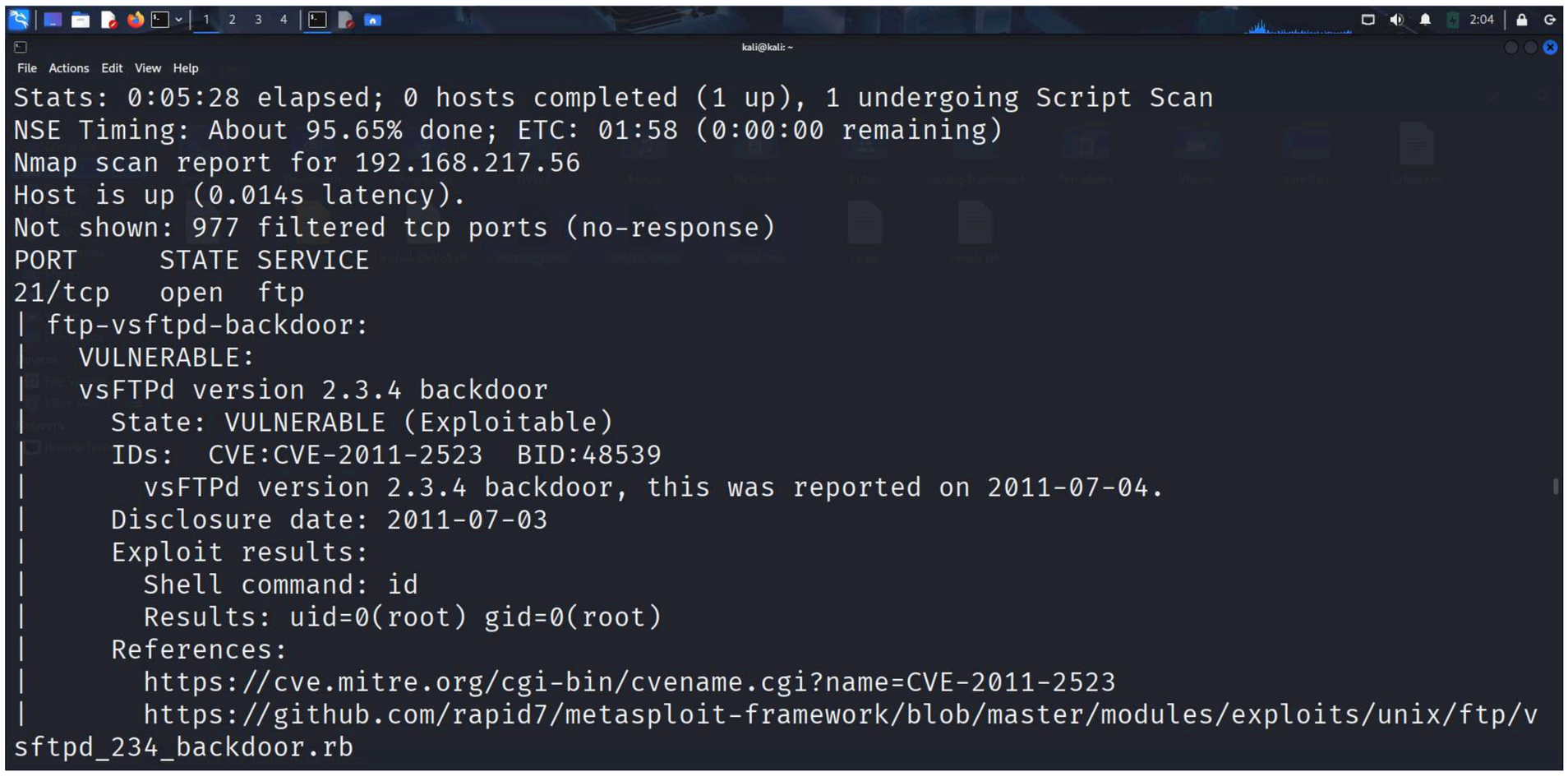


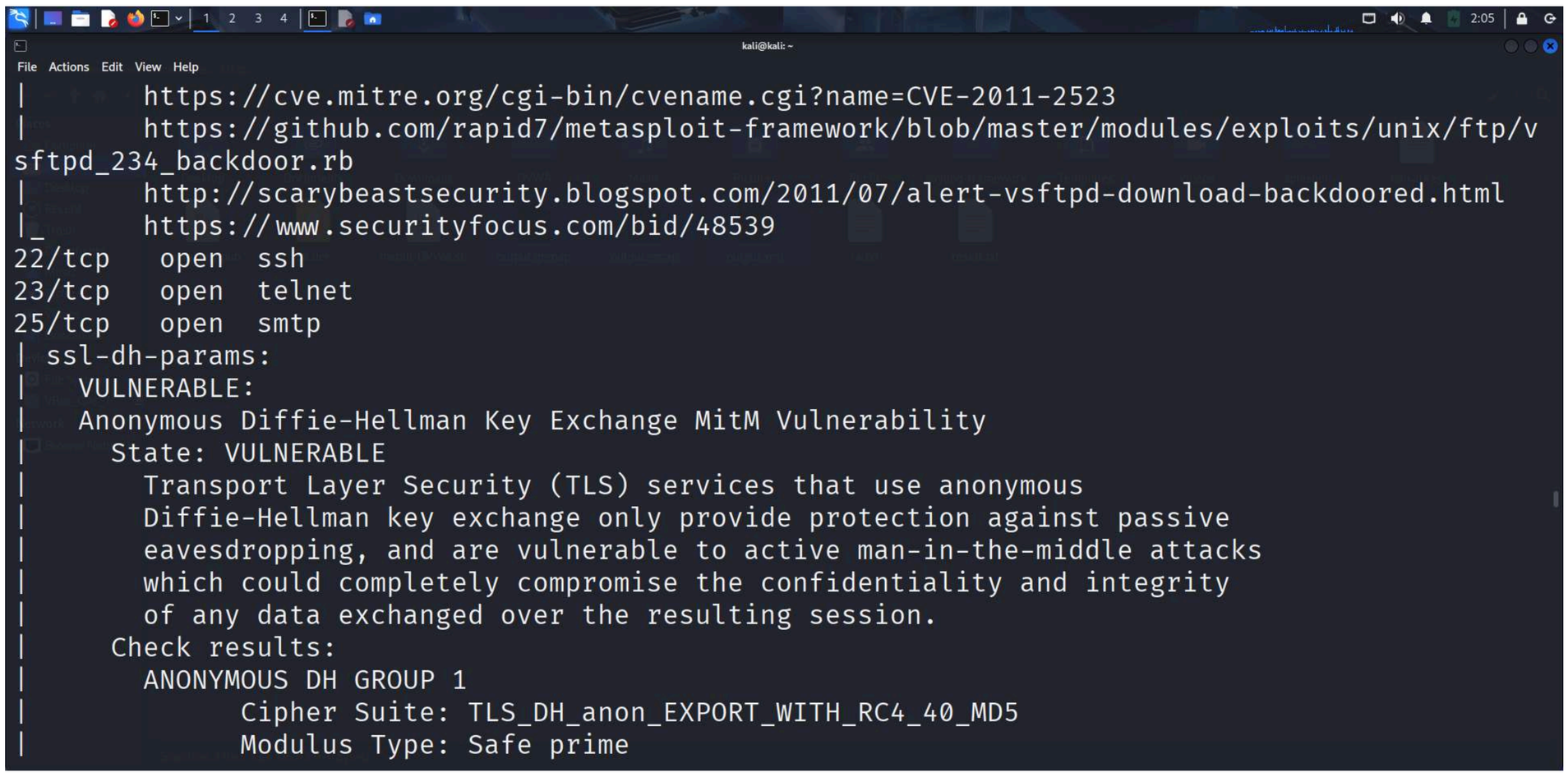
Practical-22: Detect Vulnerabilities (NSE Scripts)

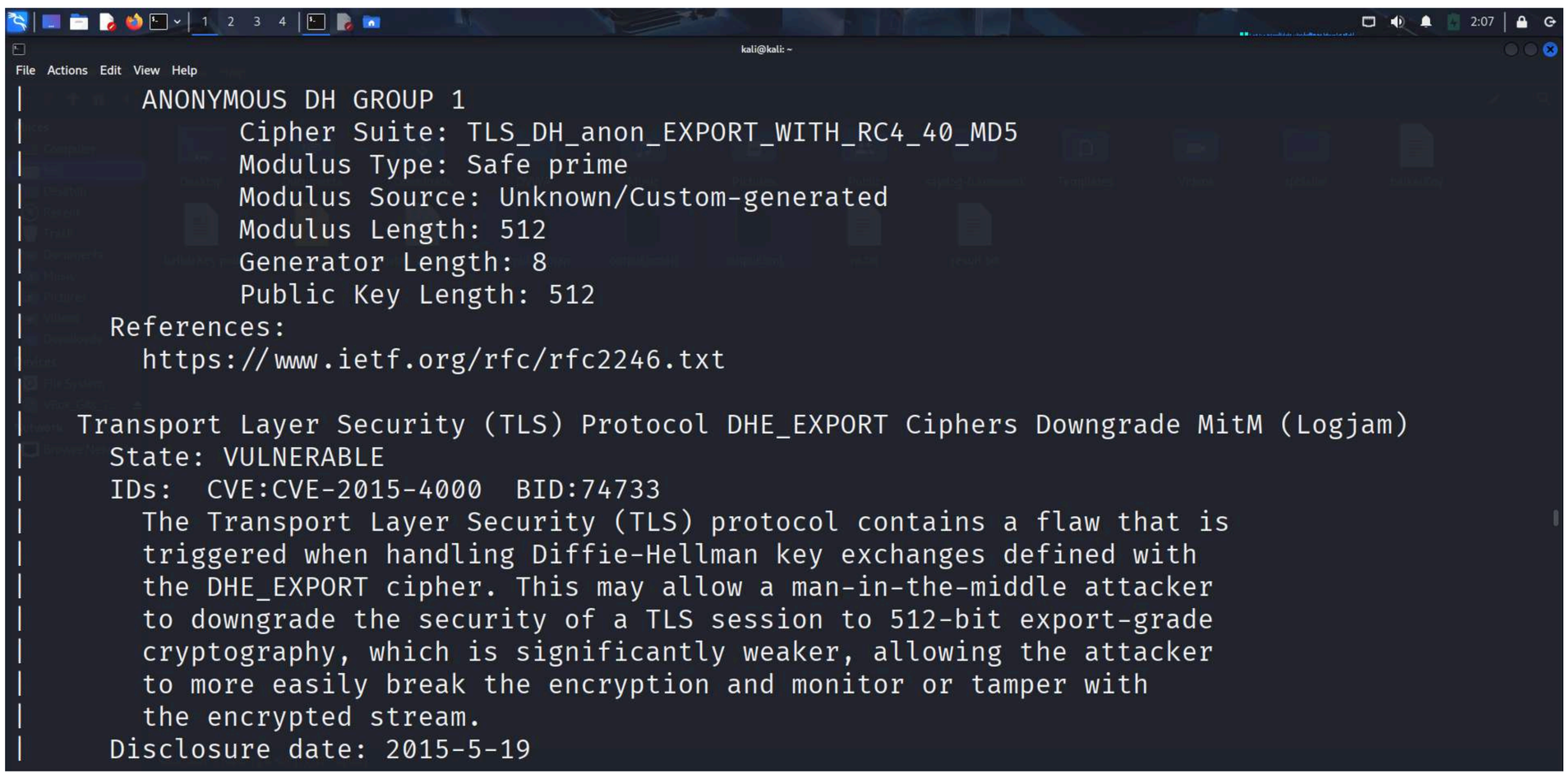
nmap --script vuln <target-ip>

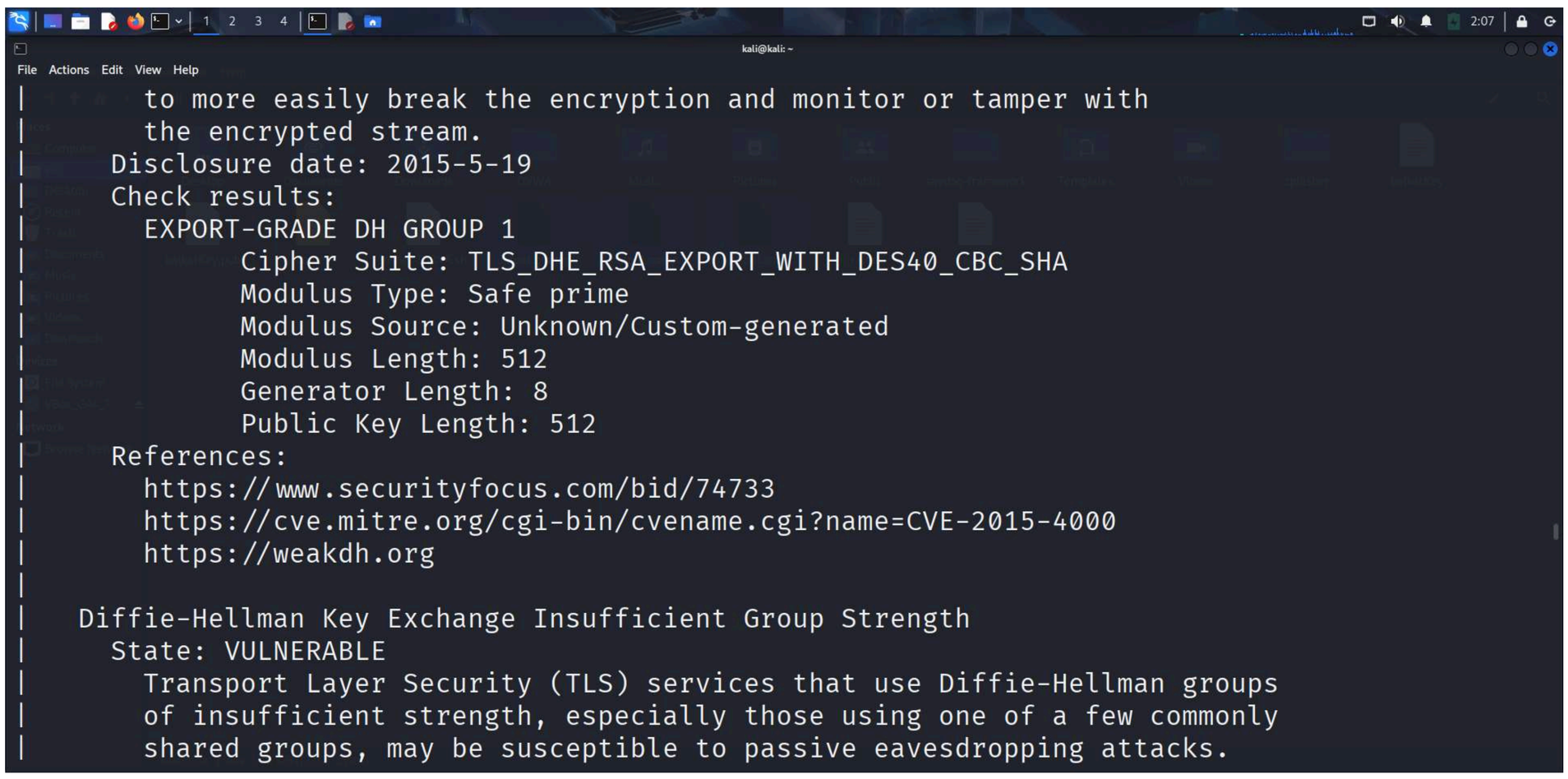
👉 Runs vulnerability detection scripts.






kali@kali: ~
File Actions Edit View Help
| 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
| 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

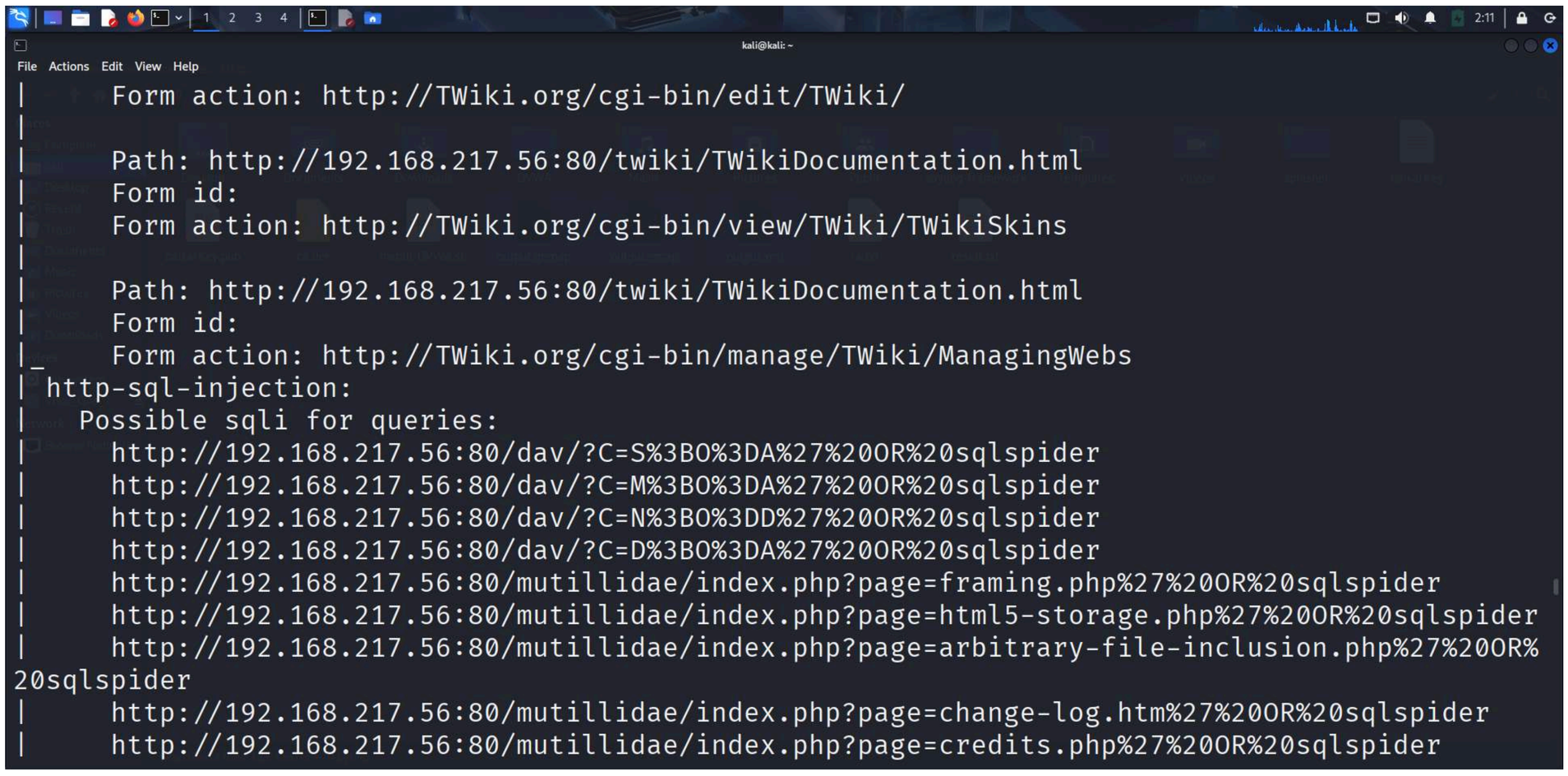

kali@kali: ~
File Actions Edit View Help
| ANONYMOUS DH GROUP 1
| Cipher Suite: TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 512
| Generator Length: 8
| Public Key Length: 512
| References:
| https://www.ietf.org/rfc/rfc2246.txt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

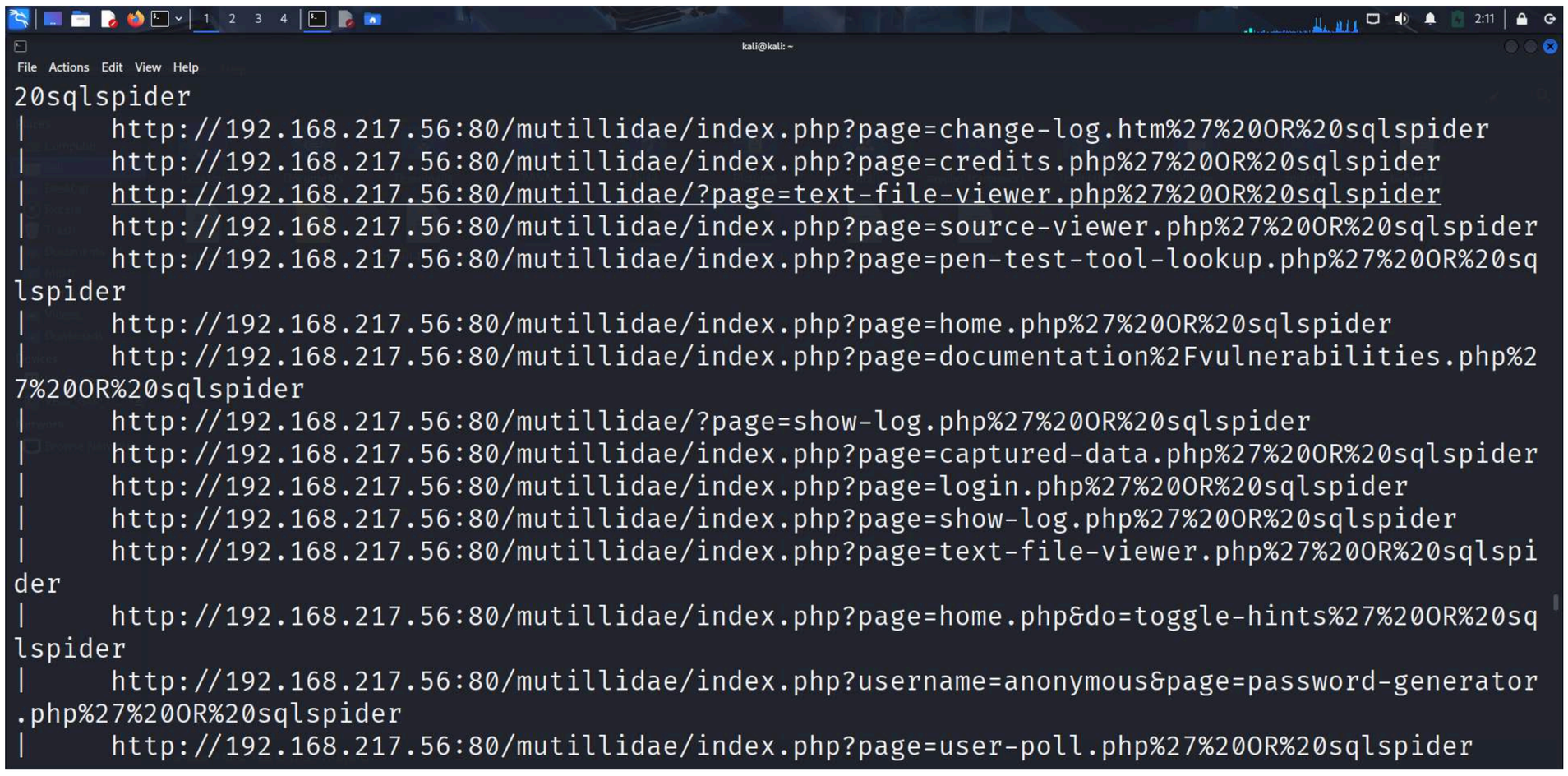

kali@kali: ~
File Actions Edit View Help
| to more easily break the encryption and monitor or tamper with
| the encrypted stream.
| Disclosure date: 2015-5-19
| Check results:
| EXPORT-GRADE DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
| Modulus Type: Safe prime
| Modulus Source: 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.

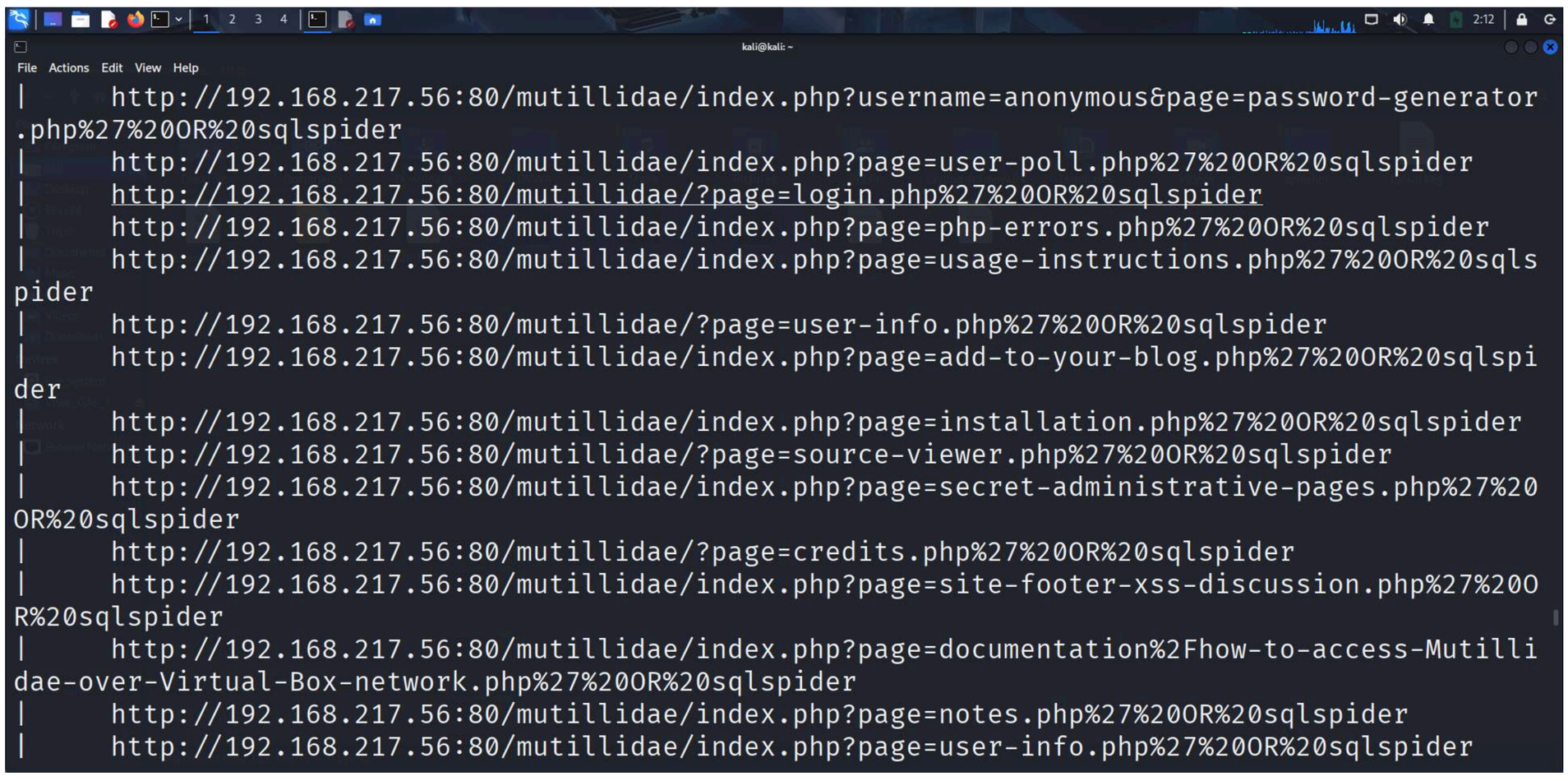
```
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher 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
```

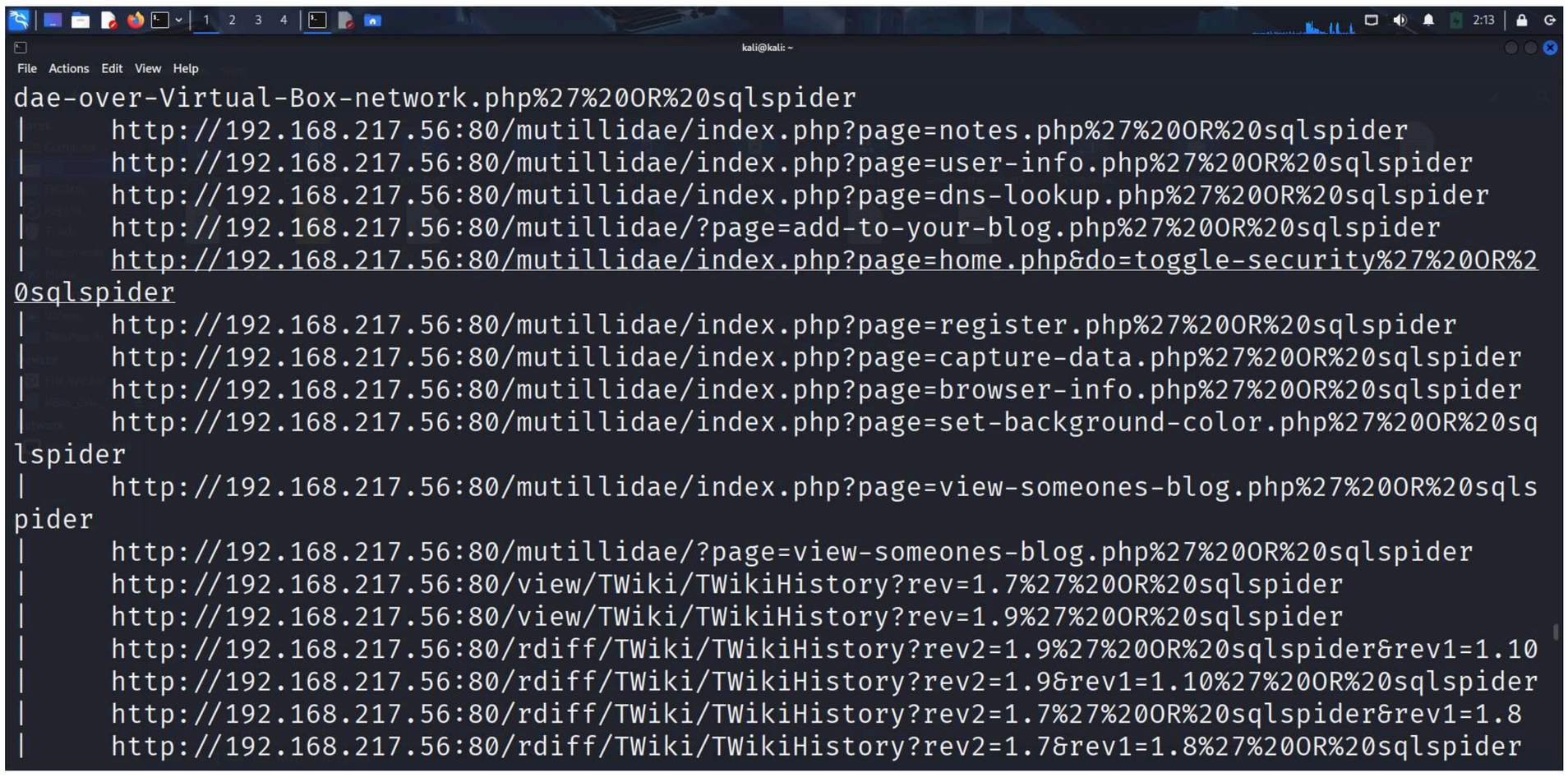
```
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.217.56
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.217.56:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
|     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
```

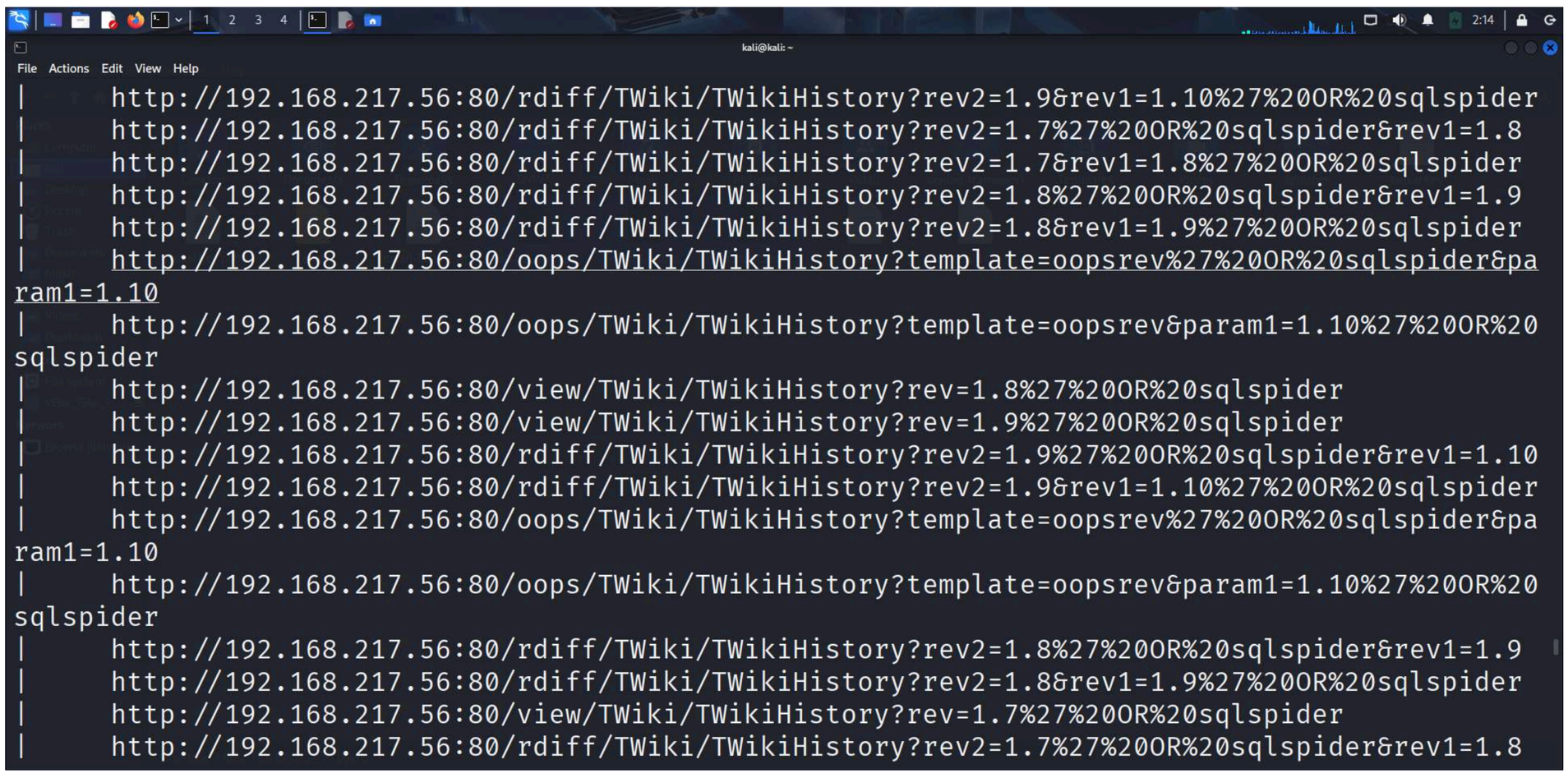
```
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           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:
```

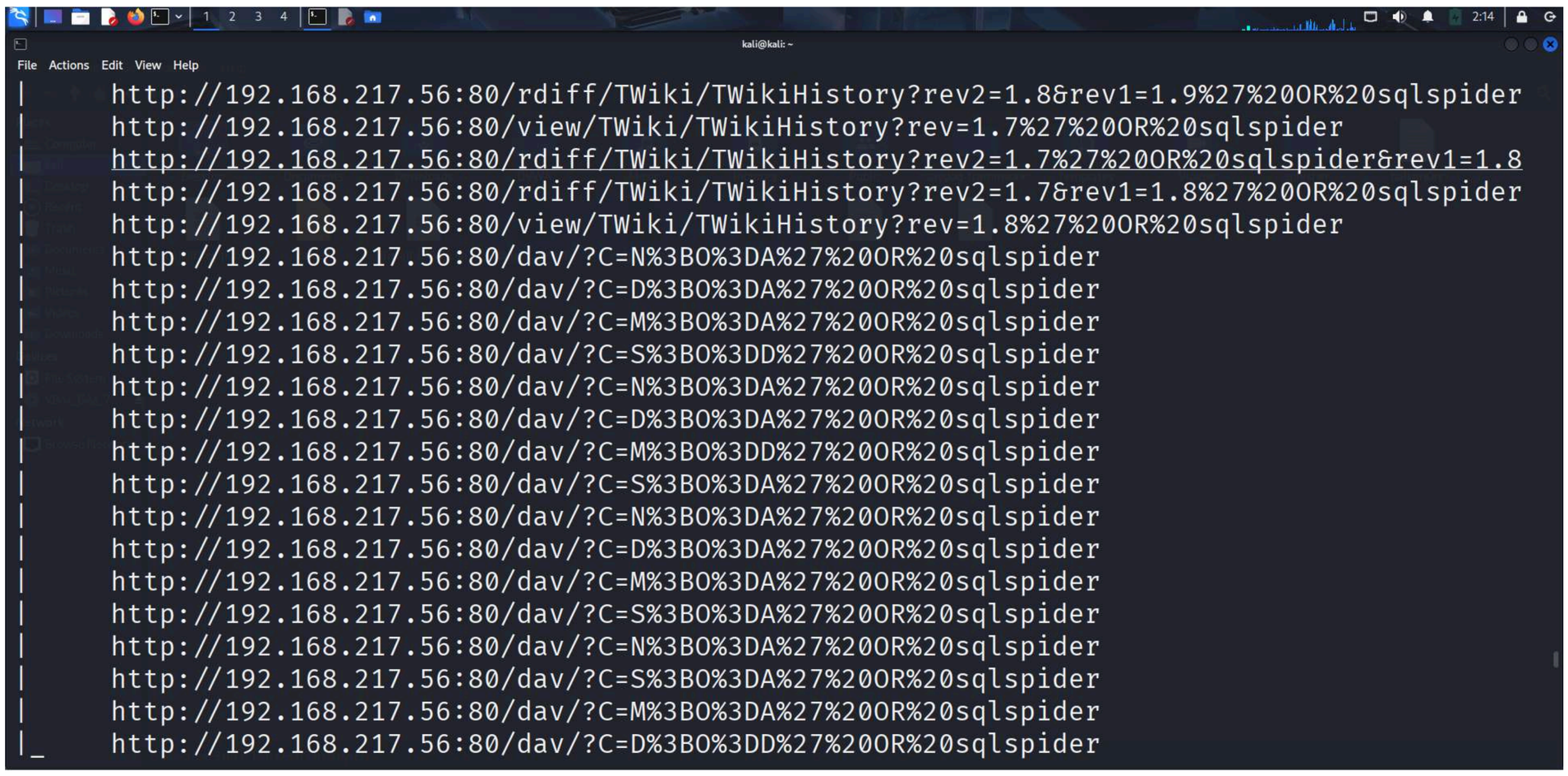

kali@kali: ~
File Actions Edit View Help
| Form action: http://TWiki.org/cgi-bin/edit/TWiki/
|
| Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
| Form id:
| Form action: http://TWiki.org/cgi-bin/view/TWiki/TWikiSkins
|
| Path: http://192.168.217.56:80/twiki/TWikiDocumentation.html
| Form id:
|_ Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
| http-sql-injection:
| Possible sqli for queries:
| http://192.168.217.56:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3BO%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


kali@kali: ~
File Actions Edit View Help
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%20sq
lspider
| 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%2
7%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%20sqlspi
der
| http://192.168.217.56:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sq
lspider
| 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


kali@kali: ~
File Actions Edit View Help
| 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%20sqls
pider
| 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%20sqlspi
der
| 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%20
OR%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%20O
R%20sqlspider
| http://192.168.217.56:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutilli
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


kali@kali: ~
File Actions Edit View Help
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


kali@kali: ~
File Actions Edit View Help
| 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


kali@kali: ~
File Actions Edit View Help
| 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%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=S%3BO%3DD%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3BO%3DD%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=N%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
| http://192.168.217.56:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|_ http://192.168.217.56:80/dav/?C=D%3BO%3DD%27%20OR%20sqlspider

```
|     http://192.168.217.56:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.217.56:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.217.56:80/dav/?C=D%3BO%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-cve2017-1001000: 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:
```

```
|_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:
|
|_    Couldn'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:
```

```
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
```

```
| 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
```

```
|   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
```

```
|     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.**

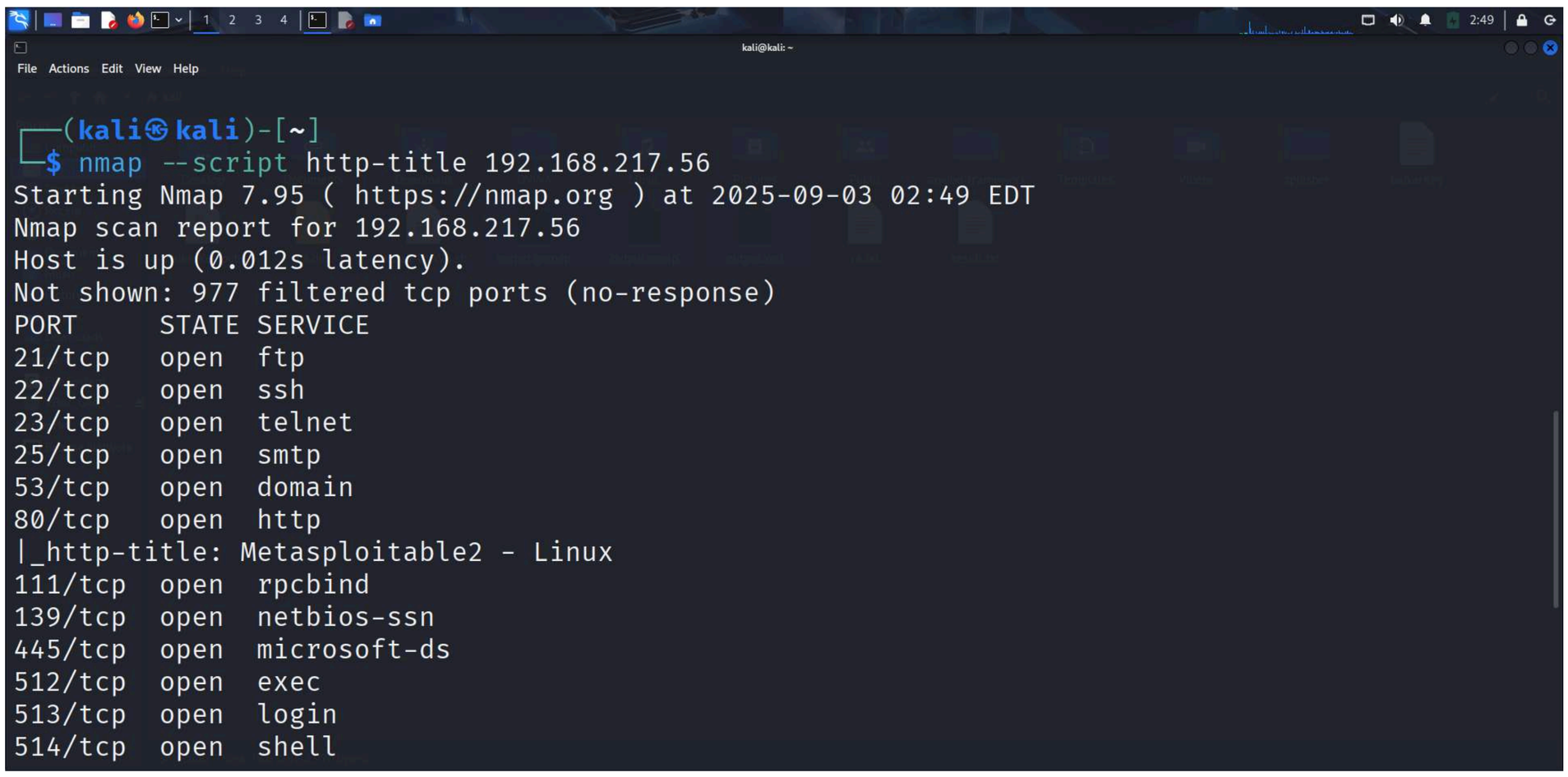
```
┌──(kali㉿kali)-[~]
└─$ nmap --script malware 192.168.217.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-03 02:43 EDT
Nmap scan report for 192.168.217.56
Host is up (0.0096s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh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

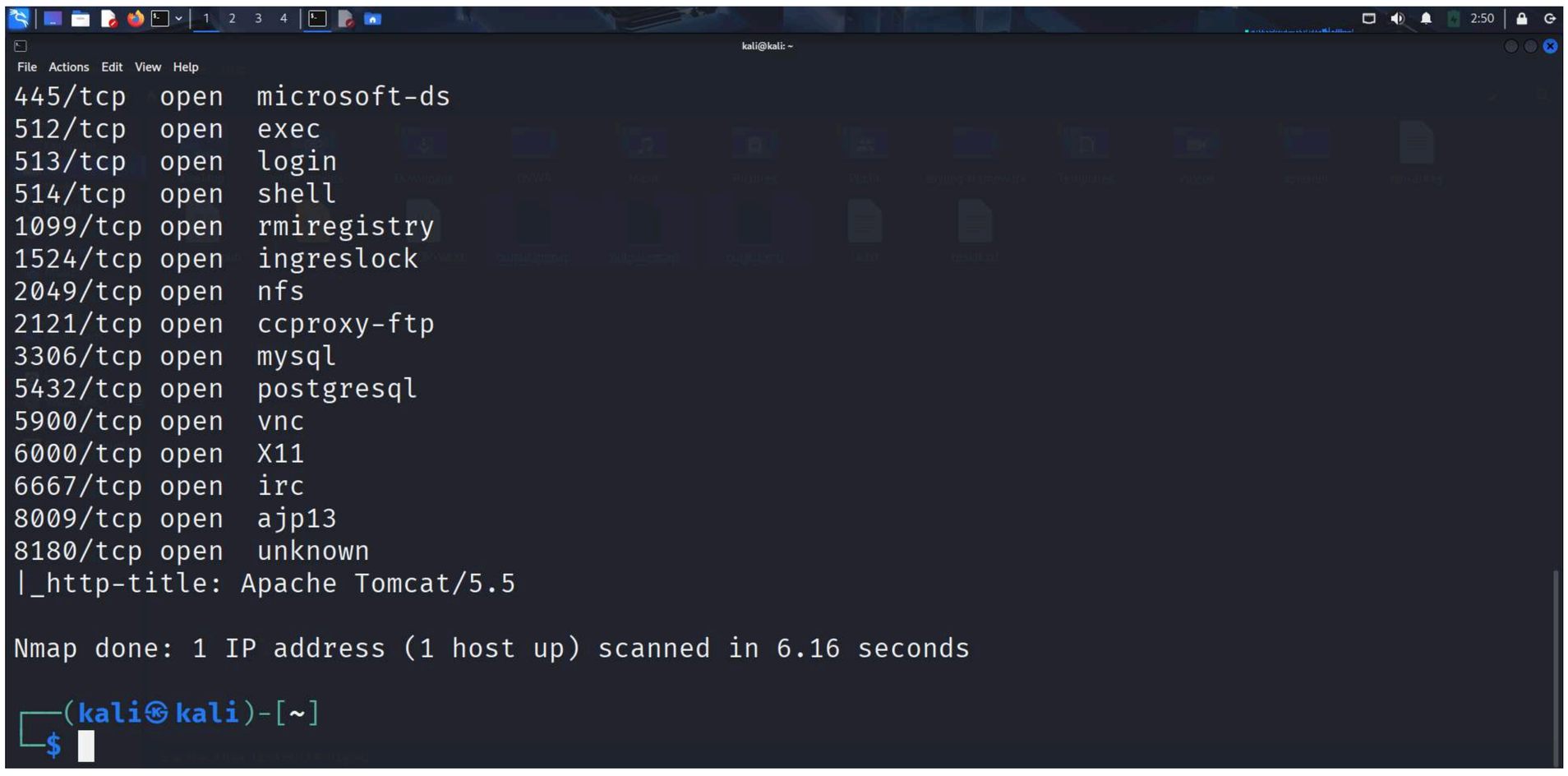
```
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks 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.

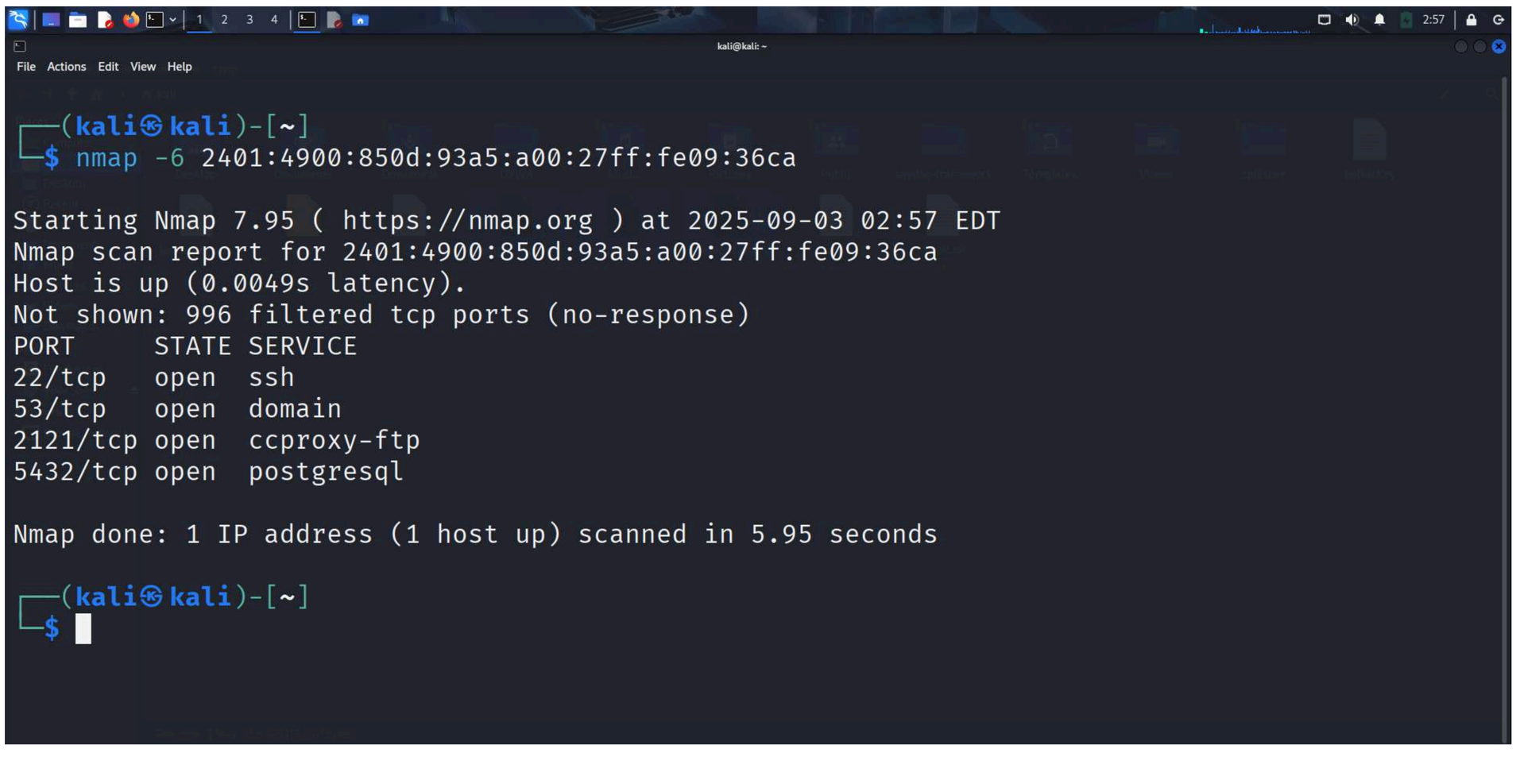




Practical-25: Scan IPv6 Targets

nmap -6 <ipv6-address>

👉 Performs scanning on IPv6 addresses.



✅ 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.