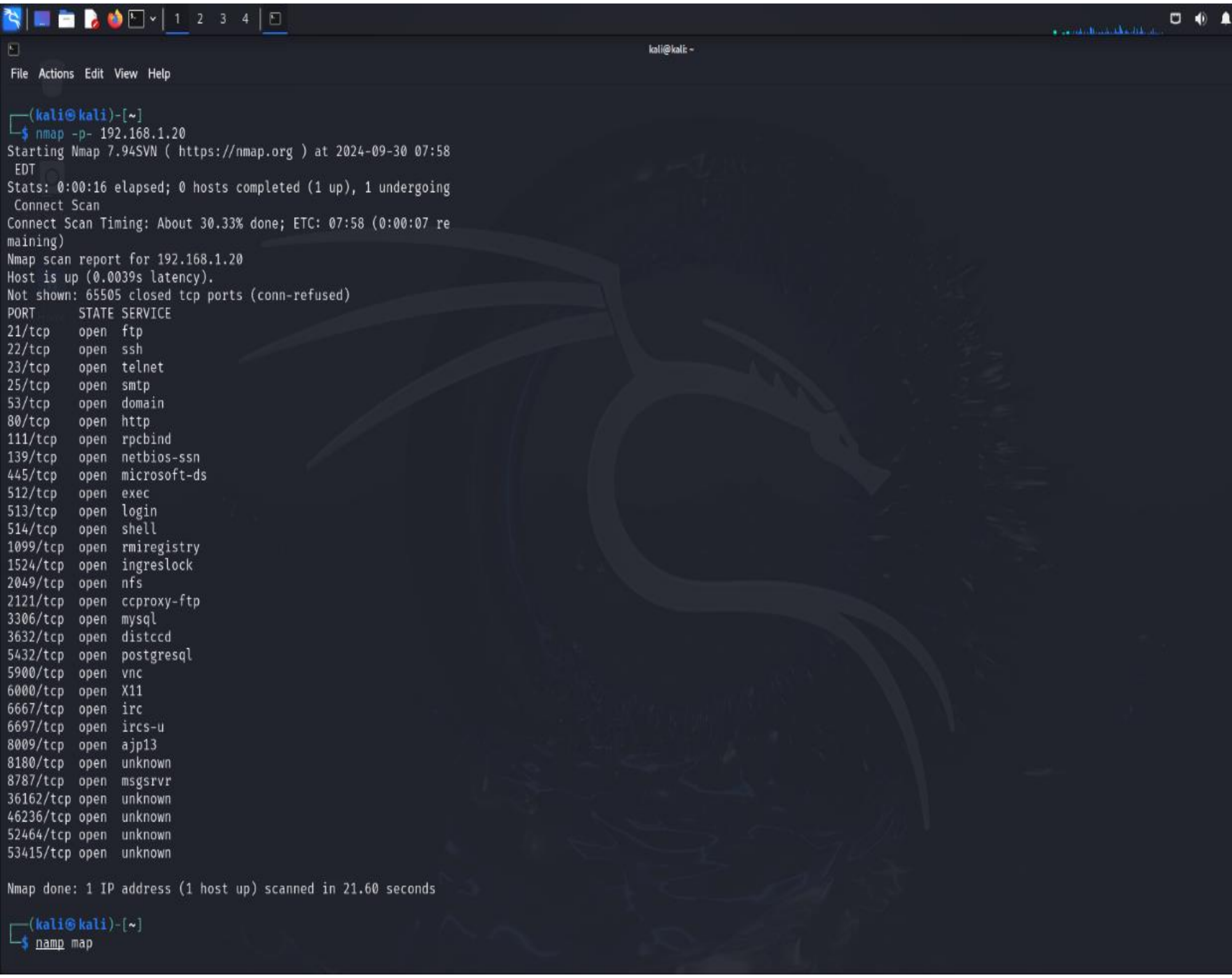
Nmap Reference Guide

- ## Commands –

1)namp -p-

The command `nmap -p-` tells Nmap to scan all 65,535 TCP ports on the target host. The `-p-` option specifies that every port should be included in the scan, making it a comprehensive check for open ports.

Example: nmap -p- 192.168.1.20



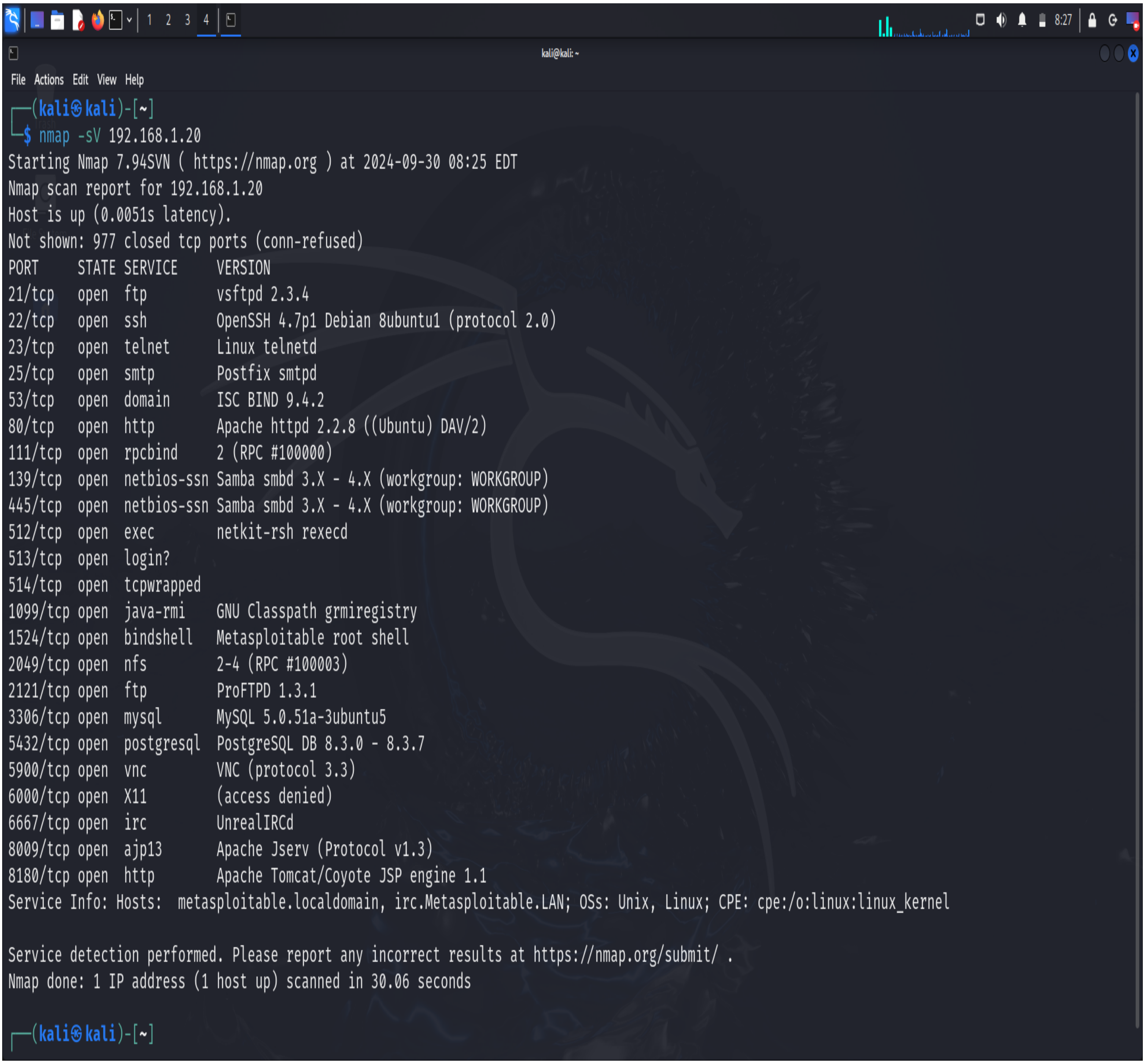
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 07:58
 EDT
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing
 Connect Scan
Connect Scan Timing: About 30.33% done; ETC: 07:58 (0:00:07 re
maining)
Nmap scan report for 192.168.1.20
Host is up (0.0039s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36162/tcp open  unknown
46236/tcp open  unknown
52464/tcp open  unknown
53415/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds

┌──(kali㉿kali)-[~]
└─$ namp map
```

Nmap Reference Guide

2) nmap -sV

The command `nmap -sV` enables service version detection during the scan, allowing Nmap to identify the versions of services running on open ports. This helps gather more detailed information about the target system's software and can aid in vulnerability assessments.

Example: nmap -sV 192.168.1.20



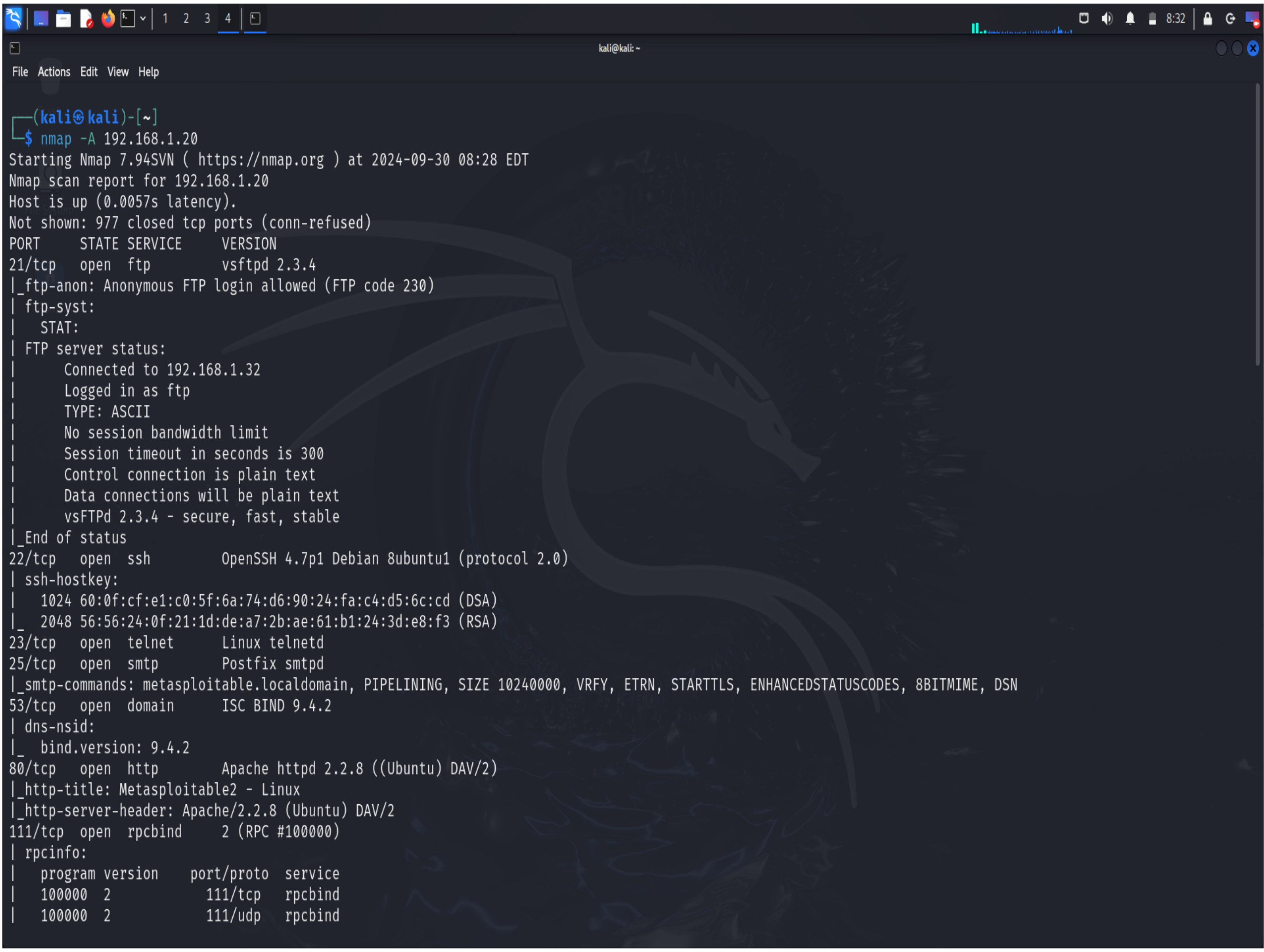
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:25 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0051s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  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; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.06 seconds

┌──(kali㉿kali)-[~]
```

Nmap Reference Guide

3) nmap -A

The command `nmap -A` enables aggressive scanning, which includes service version detection, OS detection, script scanning, and traceroute. This comprehensive approach provides detailed information about the target system, including the services running, their versions, and potential vulnerabilities.

Example: nmap -A 192.168.1.20

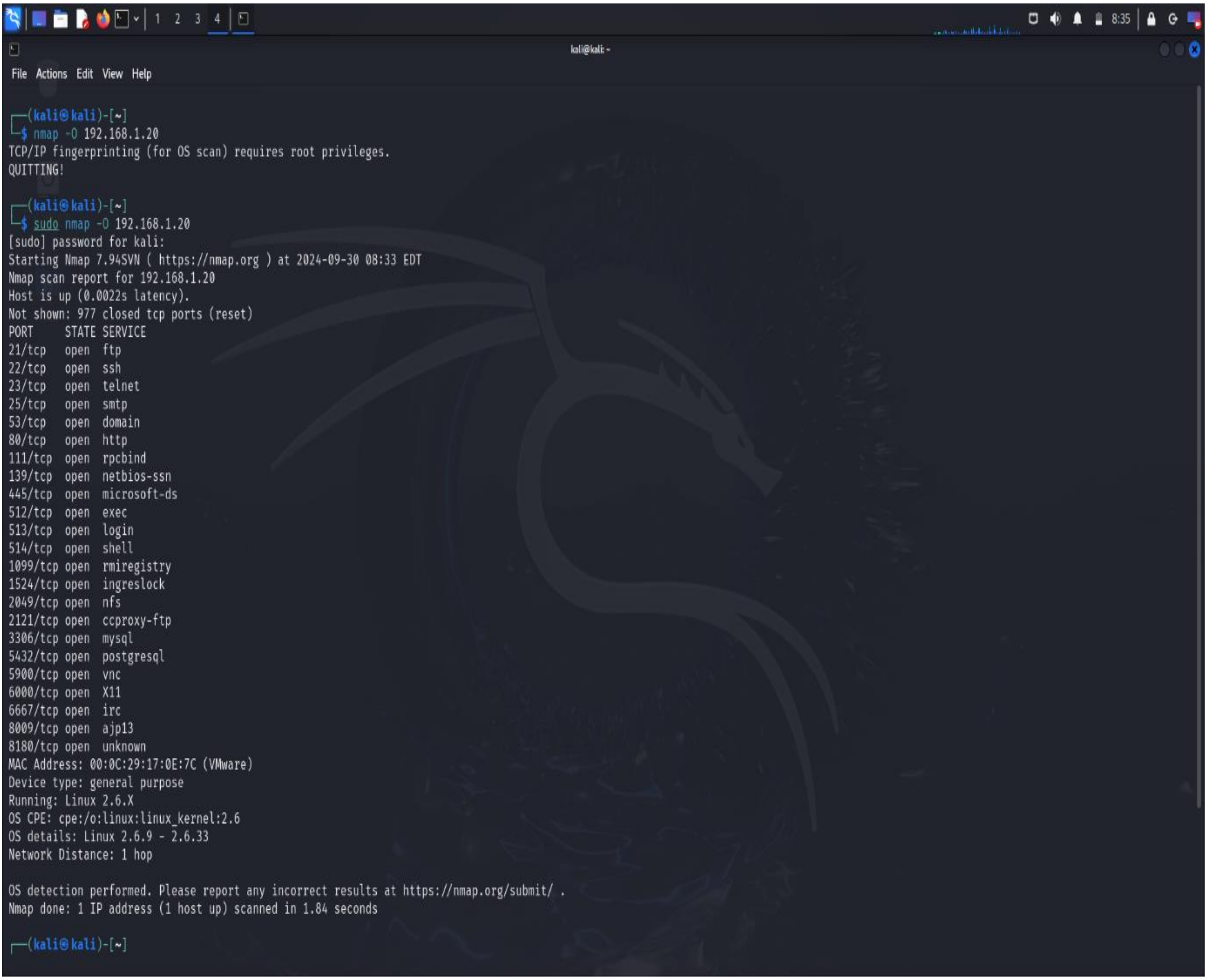


```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:28 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0057s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.32
|      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
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
|_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-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
```

Nmap Reference Guide

4) nmap -O

The command `nmap -O` enables operating system detection, allowing Nmap to identify the OS of the target host based on network responses and other characteristics. This can help in understanding the target's environment and potential vulnerabilities related to the specific operating system.
Example: nmap -O 192.168.1.20



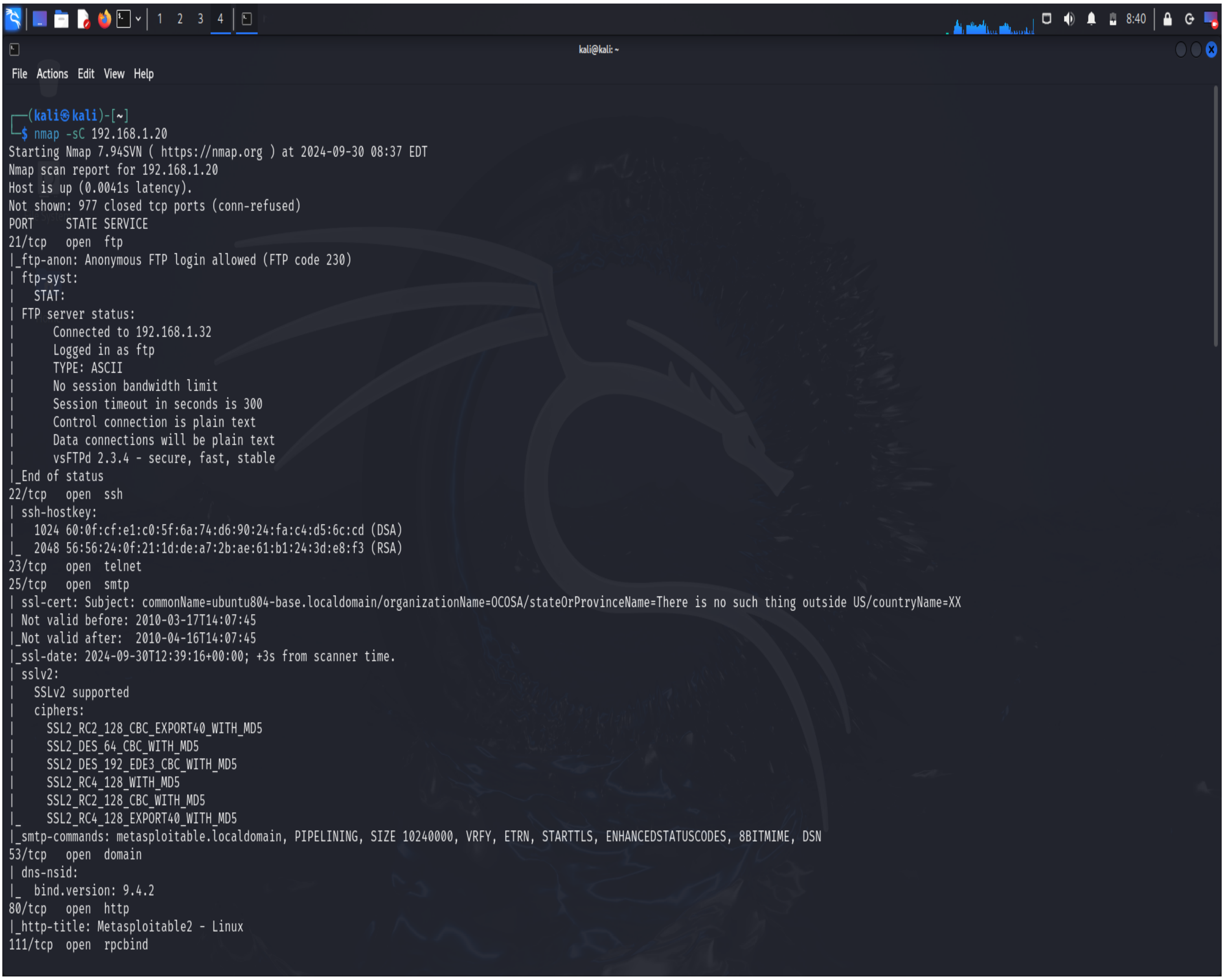
```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.1.20
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.1.20
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:33 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:17:0E:7C (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.84 seconds

┌──(kali㉿kali)-[~]
```

Nmap Reference Guide

5) nmap -sC

The command `nmap -sC` runs a set of default scripts against the target during the scan. These scripts perform various tasks, such as gathering additional information about services, checking for vulnerabilities, and assessing security configurations, enhancing the overall reconnaissance process.

Example: nmap -sC 192.168.1.20



```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-30 08:37 EDT
Nmap scan report for 192.168.1.20
Host is up (0.0041s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.32
|      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
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
| 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: 2024-09-30T12:39:16+00:00; +3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_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
```

Nmap Reference Guide

Nmap Reference Guide