

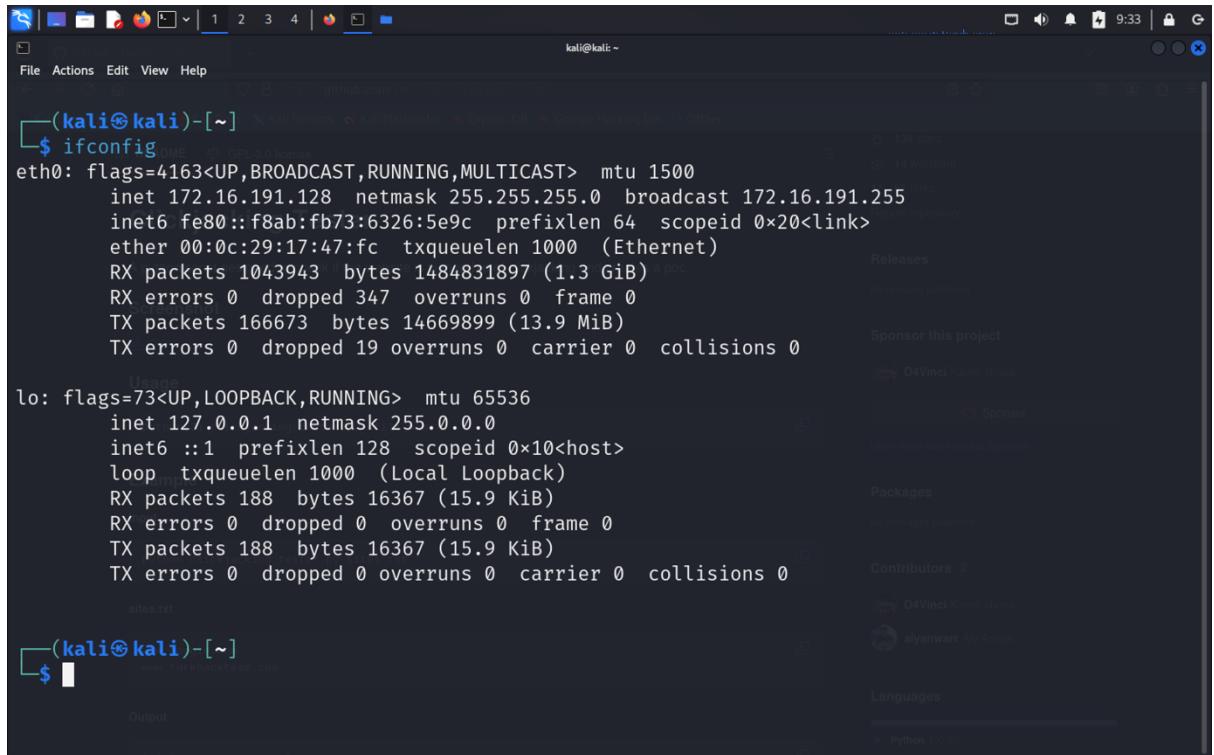
Week 3: Network Scanning, Footprinting, and Enumeration

Network Scanning and Analysis Report

Task 1: Identify Target IP Range

1. Checked the IP range of the local network using `ifconfig`:

```
ifconfig
```



```
kali@kali: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.16.191.128 netmask 255.255.255.0 broadcast 172.16.191.255
              inet6 fe80::f8ab:fb73:6326:5e9c prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:17:47:fc txqueuelen 1000 (Ethernet)
                  RX packets 1043943 bytes 1484831897 (1.3 GiB)
                  RX errors 0 dropped 347 overruns 0 frame 0
                  TX packets 166673 bytes 14669899 (13.9 MiB)
                  TX errors 0 dropped 19 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 prefixlen 128 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 188 bytes 16367 (15.9 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 188 bytes 16367 (15.9 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali: ~
```

Output:

```
inet 172.18.191.128 netmask 255.255.255.0 broadcast 172.16.191.255
```

- Target IP Range: 172.16.191.0/24

2. Verified active IP ranges using a ping sweep:

```
nmap -sn 172.16.191.0/24
```

Output:

```
(kali㉿kali)-[~]
$ nmap -sn 172.16.191.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 10:24 EST
Nmap scan report for 172.16.191.1
Host is up (0.00083s latency).
MAC Address: 3A:F9:D3:F5:EC:65 (Unknown)
Nmap scan report for 172.16.191.2
Host is up (0.0014s latency).
MAC Address: 00:50:56:E7:24:EC (VMware)
Nmap scan report for 172.16.191.130
Host is up (0.0024s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 172.16.191.254
Host is up (0.00083s latency).
MAC Address: 00:50:56:F0:01:AC (VMware)
Nmap scan report for 172.16.191.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds

(kali㉿kali)-[~]
```

Task 2: Perform Ping Scan

- Identified active hosts:

```
nmap -sn 172.16.191.0/24
```

Output:

```
(kali㉿kali)-[~]
$ nmap -sn 172.16.191.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 10:24 EST
Nmap scan report for 172.16.191.1
Host is up (0.00083s latency).
MAC Address: 3A:F9:D3:F5:EC:65 (Unknown)
Nmap scan report for 172.16.191.2
Host is up (0.0014s latency).
MAC Address: 00:50:56:E7:24:EC (VMware)
Nmap scan report for 172.16.191.130
Host is up (0.0024s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 172.16.191.254
Host is up (0.00083s latency).
MAC Address: 00:50:56:F0:01:AC (VMware)
Nmap scan report for 172.16.191.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.06 seconds

(kali㉿kali)-[~]
```

Task 3: Port Scanning

1. Performed a comprehensive port scan on the Metasploitable machine and other active hosts:

```
nmap -p- 172.16.191.130
```

Output:

```
File Actions Edit View Help
└ $ nmap -p- 172.16.191.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 10:28 EST
Nmap scan report for 172.16.191.130
Host is up (0.00017s latency).
Not shown: 65505 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
513/tcp   open  exec
514/tcp   open  rlogin
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
1434/tcp  open  unknown
46600/tcp open  unknown
47342/tcp open  unknown
48461/tcp open  unknown
MAC Address: 00:0c:29:fa:dd:2a (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.70 seconds
└ [kali㉿kali]:~
```

```
File Actions Edit View Help
└ PS> nmap -p- 172.16.191.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 11:22 EST
Nmap scan report for 172.16.191.2
Host is up (0.00073s latency).
All 65535 scanned ports on 172.16.191.2 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 00:50:56:E7:24:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.46 seconds
└ [kali㉿kali]:~/[home/kali]
└ PS> nmap -p- 172.16.191.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 11:22 EST
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.14% done; ETC: 11:44 (0:21:34 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.14% done; ETC: 11:44 (0:21:34 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.15% done; ETC: 11:45 (0:22:02 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.15% done; ETC: 11:45 (0:22:01 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.16% done; ETC: 11:45 (0:21:59 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.16% done; ETC: 11:45 (0:21:58 remaining)
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.16% done; ETC: 11:45 (0:21:58 remaining)
Nmap scan report for 172.16.191.254
Host is up (0.00051s latency).
All 65535 scanned ports on 172.16.191.254 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:F0:01:AC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1329.37 seconds
└ [kali㉿kali]:~/[home/kali]
```

```

PS> nmap -p- 172.16.191.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 13:13 EST
Nmap scan report for 172.16.191.128
Host is up (0.0000040s latency).
All 65535 scanned ports on 172.16.191.128 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-17 06:06 EST
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds

```

Task 4: Service Enumeration

1. Enumerated services on open ports using Nmap's service detection:

```
nmap -sV 172.16.191.130
```

Output:

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 12:25 EST
Nmap scan report for 172.16.191.130
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd 2.0.0
35/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-remntr 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)
6872/tcp  open  unknown      Unknown
8009/tcp  open  dpp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:FA:D0:2A (VMware)

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 13.54 seconds

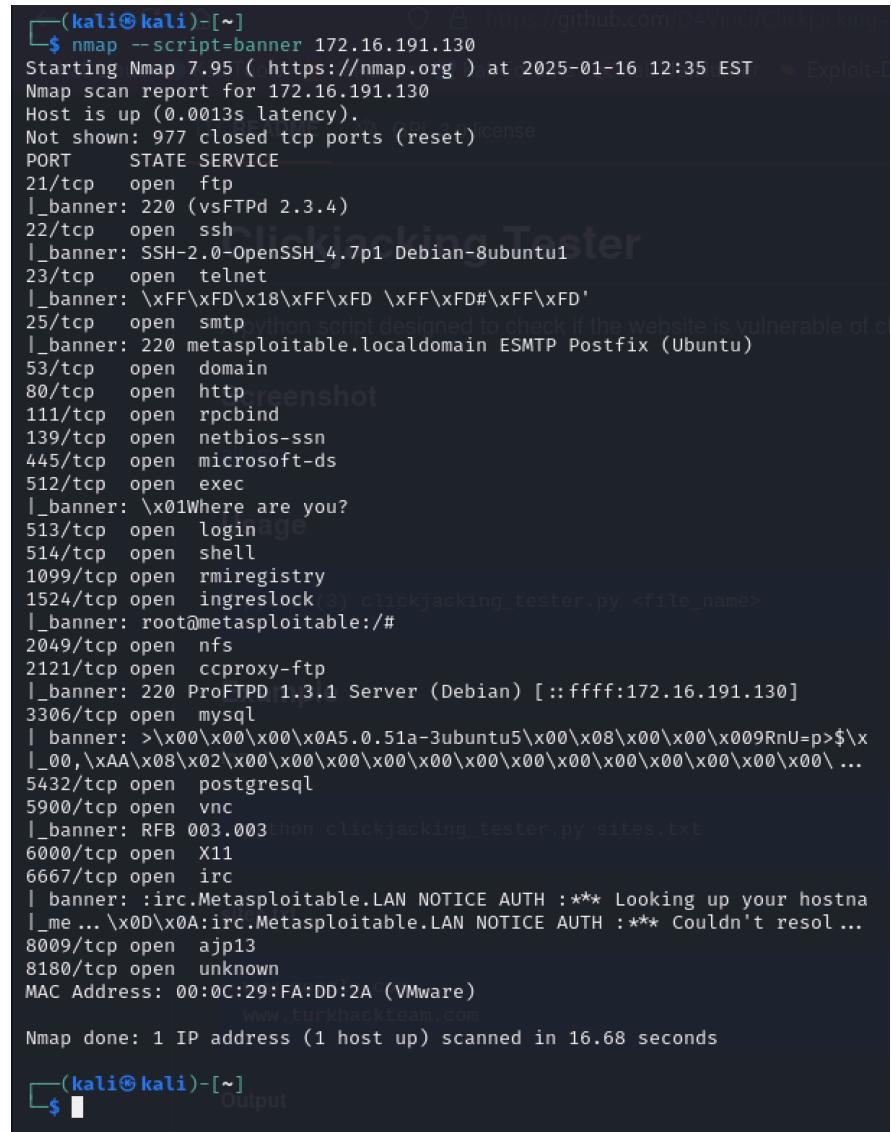
```

Task 5: Banner Grabbing

1. Performed banner grabbing using Nmap and Netcat:

- Using Nmap:

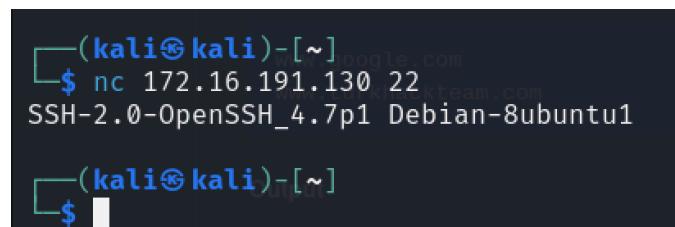
```
nmap --script=banner 172.16.191.130
```



```
(kali㉿kali)-[~] $ nmap --script=banner 172.16.191.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 12:35 EST
Nmap scan report for 172.16.191.130
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_banner: 220 (vsFTPd 2.3.4)
22/tcp    open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
23/tcp    open  telnet
|_banner: \xFF\xFD\x18\xFF\xFD \xFF\xFD#\xFF\xFD'
25/tcp    open  smtp
|_banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
53/tcp    open  domain
80/tcp    open  http
|_banner: HTTP/1.1 200 OK
|_banner: Clickjacking Tester
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
|_banner: \x01Where are you?
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
|_banner: 3) clickjacking_tester.py <file_name>
|_banner: root@metasploitable:/# 
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
|_banner: 220 ProFTPD 1.3.1 Server (Debian) [::ffff:172.16.191.130]
3306/tcp  open  mysql
|_banner: >\x00\x00\x00\x0A\x05.0.51a-3ubuntu5\x00\x08\x00\x00\x00\x009RnU=p>$\x
|_me ... \x0D\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostna...
|_me ... \x0D\x0A:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resol ...
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)
www.turkhackteam.com
Nmap done: 1 IP address (1 host up) scanned in 16.68 seconds
(kali㉿kali)-[~] $
```

- o Using Netcat:

```
nc 172.16.191.130 22
```



```
(kali㉿kali)-[~] $ nc 172.16.191.130 22
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
(kali㉿kali)-[~] $
```

Task 6: OS Fingerprinting

1. Performed OS fingerprinting to identify the target OS:

```
nmap -O 172.16.191.130
```

Output:

```
$ nmap -O 172.16.191.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 12:42 EST [Google Hacking DB]
Nmap scan report for 172.16.191.130
Host is up (0.0014s 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:F4:DD:2A (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

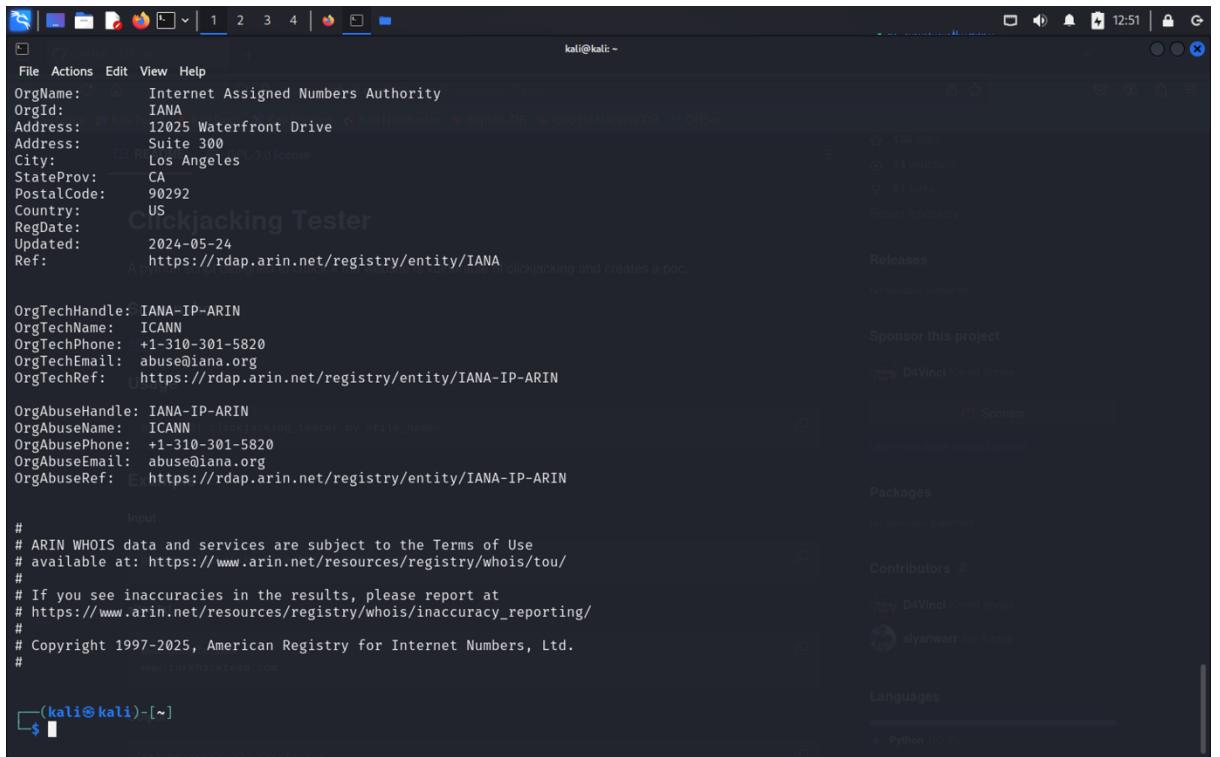
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.93 seconds
```

Task 7: Footprinting

1. Used whois to gather domain information:

```
whois 172.16.191.130
```

```
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
# Screenshot
NetRange: 172.16.0.0 - 172.31.255.255
CIDR: 172.16.0.0/12
NetName: PRIVATE-ADDRESS-BBLK-RFC1918-IANA-RESERVED
NetHandle: NET-172-16-0-0-1
Parent: NET172 (NET-172-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/172.16.0.0
```



A screenshot of a terminal window titled "Clickjacking Tester". The window shows WHOIS data for the Internet Assigned Numbers Authority (IANA). The data includes:

- OrgName: Internet Assigned Numbers Authority
- OrgId: IANA
- Address: 12025 Waterfront Drive
- Address: Suite 300
- City: Los Angeles
- StateProv: CA
- PostalCode: 90292
- Country: US
- RegDate: 2024-05-24
- Updated: 2024-05-24
- Ref: https://rdap.arin.net/registry/entity/IANA

The terminal also displays a note about clickjacking and creating a poc.

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

Input
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/resources/registry/whois/tou/

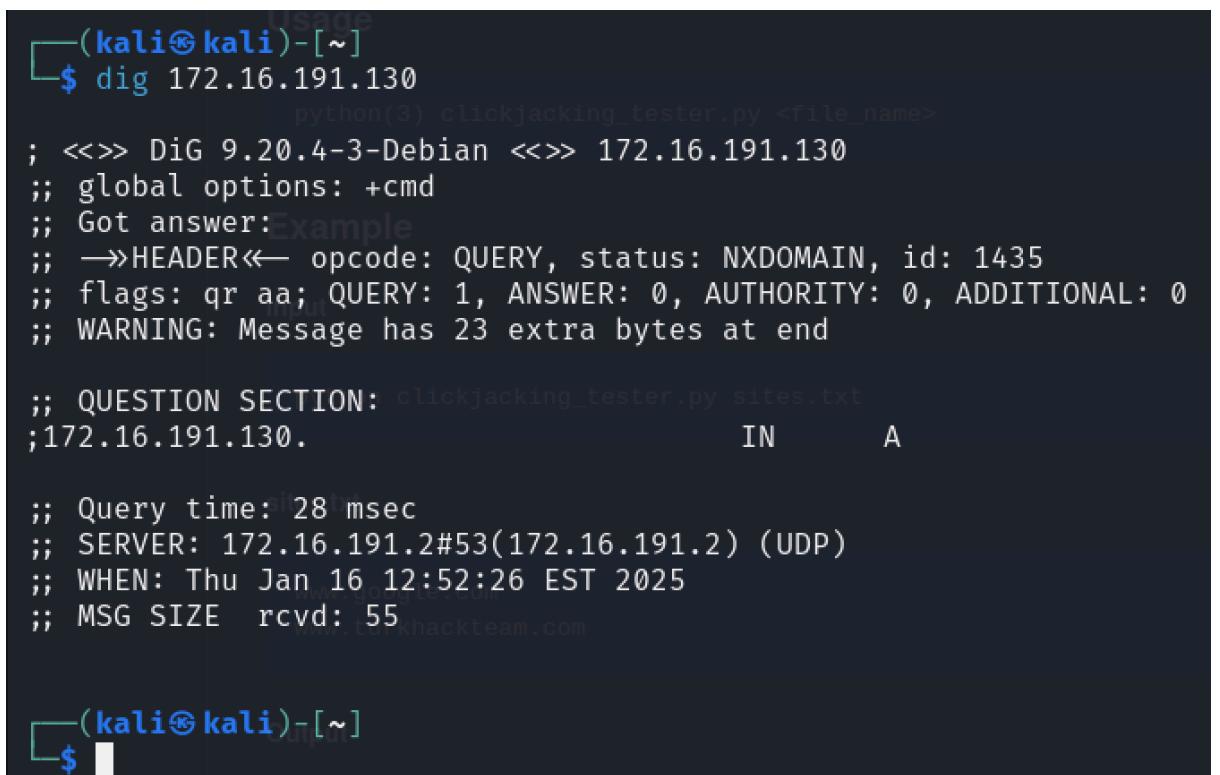
If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/

Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

(kali㉿kali)-[~]

2. Used dig to query DNS records:

```
dig 172.16.191.130
```



```
(kali㉿kali)-[~]
$ dig 172.16.191.130
    python(3) clickjacking_tester.py <file_name>
; <>>> DiG 9.20.4-3-Debian <>>> 172.16.191.130
;; global options: +cmd
;; Got answer:
Example
;; →HEADER← opcode: QUERY, status: NXDOMAIN, id: 1435
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: Message has 23 extra bytes at end

;; QUESTION SECTION: clickjacking_tester.py sites.txt
172.16.191.130.          IN      A

;; Query time: 28 msec
;; SERVER: 172.16.191.2#53(172.16.191.2) (UDP)
;; WHEN: Thu Jan 16 12:52:26 EST 2025
;; MSG SIZE  rcvd: 55

(kali㉿kali)-[~]
```

3. Performed DNS lookup using nslookup:

```
nslookup 172.16.191.130
```

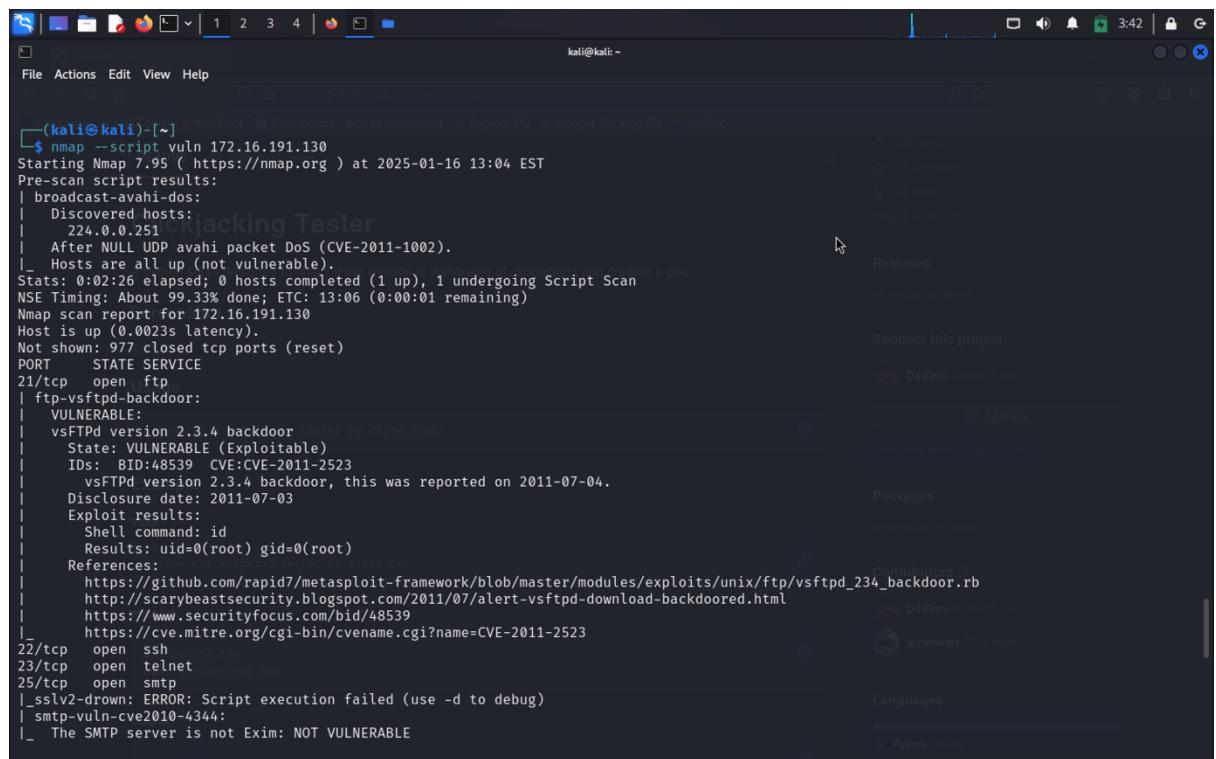
```
(kali㉿kali)-[~]nshot
$ nslookup 172.16.191.130
;; Got recursion not available from 172.16.191.2
** server can't find 130.191.16.172.in-addr.arpa: NXDOMAIN
```

Task 8: Vulnerability Assessment

1. Performed a vulnerability scan using Nmap's vulnerability scripts:

```
nmap --script vuln 172.16.191.130
```

Output:



The screenshot shows a web browser window displaying the output of an Nmap vulnerability scan. The URL in the address bar is <https://github.com/nmap/nmap-vulnerability-Tester>. The page content is a terminal session showing the command `nmap --script vuln 172.16.191.130` and its output. The output indicates that port 21/tcp (FTP) is open and vulnerable to a vsFTPD backdoor exploit, which was reported on July 4, 2011. Other ports listed include 22/tcp (SSH), 23/tcp (telnet), and 25/tcp (SMTP). The page also includes links to GitHub repository information and a 'Sponsor this project' button.

```
(kali㉿kali)-[~]$ nmap --script vuln 172.16.191.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 13:04 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
Stats: 0:02:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.33% done; ETC: 13:06 (0:00:01 remaining)
Nmap scan report for 172.16.191.130
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|  ftp-vsftpd-backdoor:
|    VULNERABLE:
|      vsFTPD version 2.3.4 backdoor (vsftpd.py vsftpd names)
|        State: VULNERABLE (Exploitable)
|        IDs:  BID:48539  CVE: CVE-2011-2523
|          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://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
|          https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
|_ _sslv2-drown: ERROR: Script execution failed (use -d to debug)
|_ smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
```

```

File Actions Edit View Help
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
| The SMTP server is not Exim: NOT VULNERABLE
53/tcp open domain
80/tcp open http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-CSRF: Couldn't find any CSRF vulnerabilities.
|_http-aspnets-debug: ERROR: Script execution failed (use -d to debug)
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec_ishot
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
|rmi-vuln-classloader:
| VULNERABLE:
| RMI registry default configuration remote code execution vulnerability
| State: VULNERABLE
| Clickjacking tester by STATE.m4v
| Default configuration of RMI registry allows loading classes from remote URLs which can 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
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
| http-cookie-flags:
| /admin/:
| JSESSIONID:

```

```

File Actions Edit View Help
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
| http-cookie-flags:
| /admin/:
| JSESSIONID:
|     httponly flag not set
| /admin/cp.html:ishot
| JSESSIONID:
|     httponly flag not set
| http-enum:
| /admin/: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin/account.html: Possible admin folder
| /admin/admin_login.html: Possible admin folder
| /admin/home.html: Possible admin folder
| /admin/admin-login.html: Possible admin folder
| /admin/adminLogin.html: Possible admin folder
| /admin/controlpanel.html: Possible admin folder
| /admin/cp.html: Possible admin folder
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 34284.80 seconds

```

Task 9: Comparison of Tools

- **Performed scans with additional open-source tools:**
 - Compared results of service enumeration and vulnerability assessment with Nmap.

Identify Target IP Range

With ip (Linux command):

```
ip a
```

- This command provides the IP address and subnet mask of the target machine. I used this to identify the IP range, 172.16.191.0/24.

With netdiscover:

```
netdiscover -r 172.16.191.0/24
```

- netdiscover scans the network and lists all live hosts.

Comparison:

- ip only identifies the IP range; netdiscover is quicker for identifying live hosts in the range compared to nmap's -sn ping scan.

The screenshot shows a terminal window with the following content:

```
root@kali: /home/kali
7 Captured ARP Req/Rep packets, from 4 hosts.  Total size: 420
Nmap scan report for 172.16.191.2
Nmap done: 1 IP address (1 host up) scanned in 11.46 seconds
[root@kali]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:17:47:fc brd ff:ff:ff:ff:ff:ff
    inet 172.16.191.128/24 brd 172.16.191.255 scope global dynamic noprefixroute eth0
        valid_lft 1223sec preferred_lft 1223sec
    inet6 fe80::f8ab:fb73:6326:5e9c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@kali]#
```

Perform Ping Scan

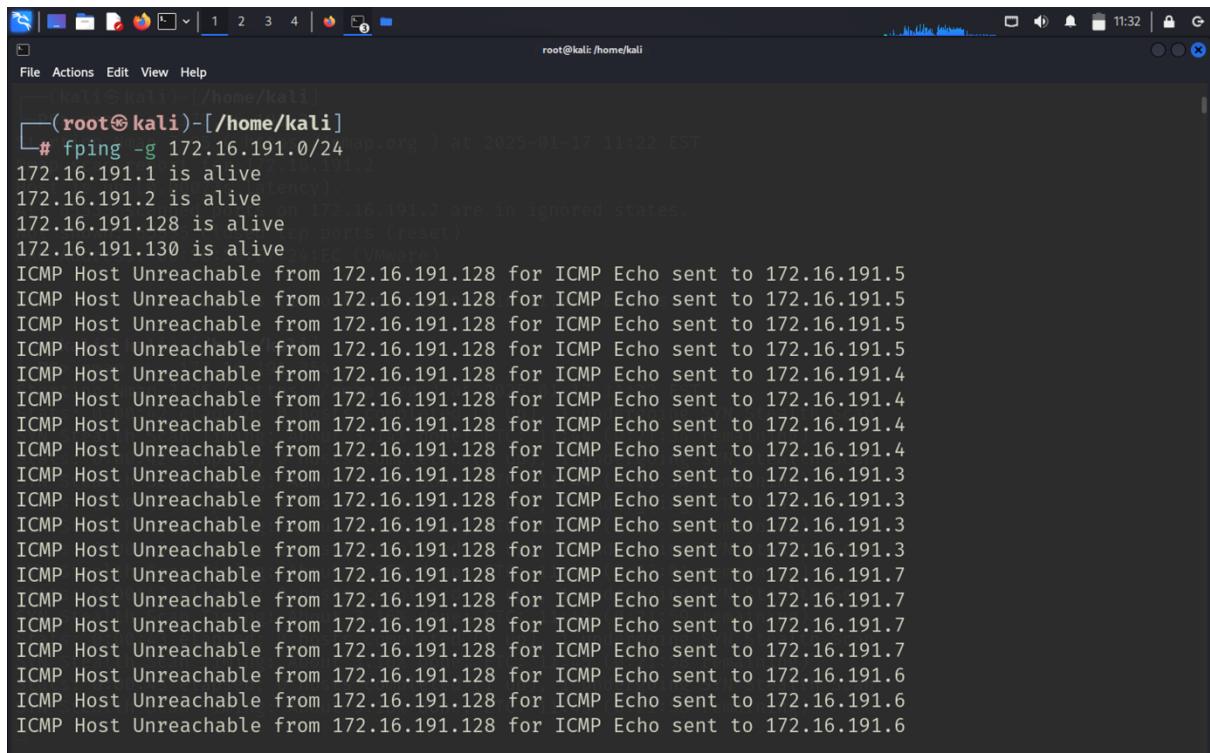
With fping:

```
fping -g 172.16.191.0/24
```

- fping sends ICMP echo requests to the specified range to find active hosts.

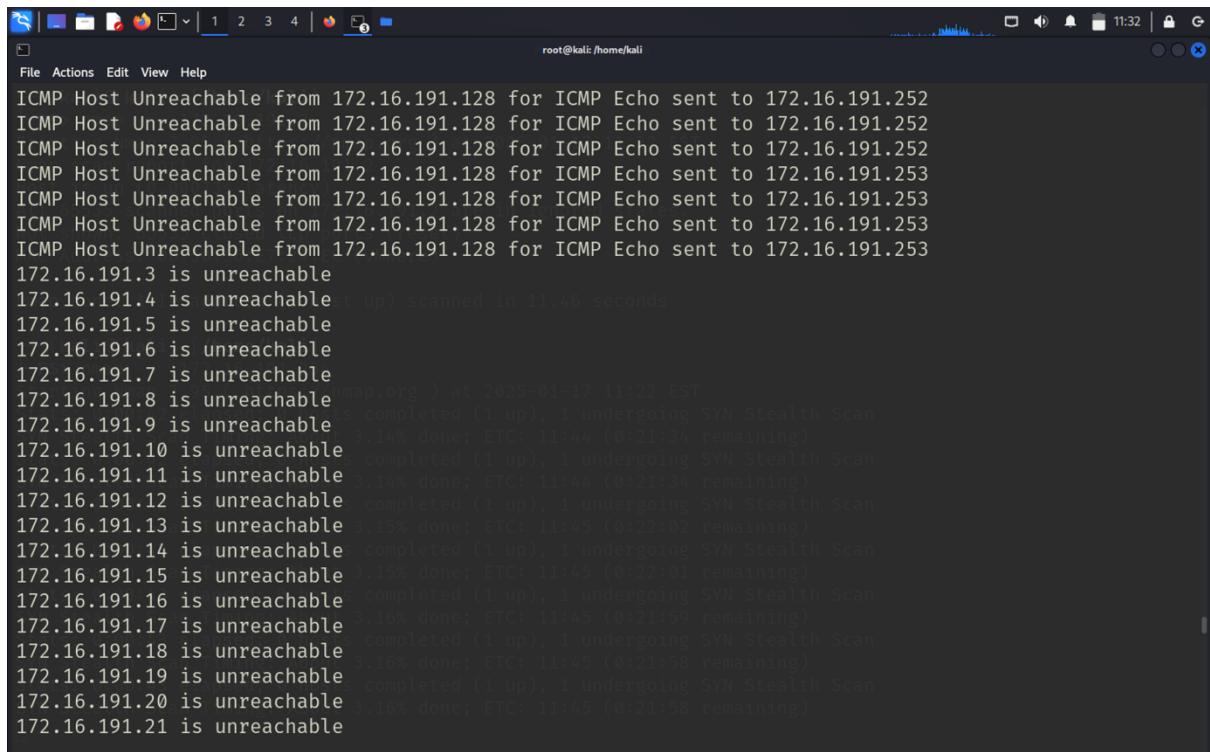
Comparison:

- fping is faster and more lightweight than nmap -sn, but it doesn't provide additional details like hostnames that nmap can.



```
(root㉿kali)-[~/home/kali]
└─# fping -g 172.16.191.0/24
  nmap.org ) at 2025-01-17 11:22 EST
172.16.191.1 is alive (latency)
172.16.191.2 is alive (latency)
172.16.191.128 is alive (tcp ports (reset))
172.16.191.130 is alive (2456C (VMware))

ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.5
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.5
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.5
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.5
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.4
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
ICMP Host Unreachable from 172.16.191.128 for ICMP Echo sent to 172.16.191.3
```



```
root@kali:~/home/kali
└─# nmap -sn 172.16.191.0/24
  nmap.org ) at 2025-01-17 11:22 EST
172.16.191.3 is unreachable
172.16.191.4 is unreachable (1 up) scanned in 11.46 seconds
172.16.191.5 is unreachable
172.16.191.6 is unreachable
172.16.191.7 is unreachable
172.16.191.8 is unreachable
172.16.191.9 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.10 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.11 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.12 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.13 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.14 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.15 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.16 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.17 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.18 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.19 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.20 is unreachable (1 up) completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.21 is unreachable (1 up)
```

```
172.16.191.232 is unreachable
172.16.191.233 is unreachable
172.16.191.234 is unreachable (org.) at 2025-01-17 11:22 EST
172.16.191.235 is unreachable2
172.16.191.236 is unreachable 172.16.191.2 are in ignored states.
172.16.191.237 is unreachable (reset)
172.16.191.238 is unreachable (VMware)
172.16.191.239 is unreachable
172.16.191.240 is unreachable (up) scanned in 11.46 seconds
172.16.191.241 is unreachable
172.16.191.242 is unreachable
172.16.191.243 is unreachable
172.16.191.244 is unreachable (org.) at 2025-01-17 11:22 EST
172.16.191.245 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.246 is unreachable 14% done; ETC: 11:44 (0:21:34 remaining)
172.16.191.247 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.248 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.249 is unreachable 15% done; ETC: 11:45 (0:22:02 remaining)
172.16.191.250 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.251 is unreachable 13% done; ETC: 11:45 (0:22:01 remaining)
172.16.191.252 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.253 is unreachable 10% done; ETC: 11:45 (0:21:59 remaining)
172.16.191.254 is unreachable completed (1 up), 1 undergoing SYN Stealth Scan
172.16.191.255 is unreachable 16% done; ETC: 11:45 (0:21:58 remaining)
[root@kali]-[/home/kali] #
```

Port Scanning

With masscan:

```
masscan -p 1-65535 172.16.191.130 --rate=1000
```

- masscan performs ultra-fast port scanning.

Comparison:

- masscan is faster than nmap for large-scale port scans but lacks the service detection and OS fingerprinting features.

```
172.16.191.254 is unreachable (kali)
[root@kali]-[/home/kali] # masscan -p 1-65535 172.16.191.130 --rate=1000 at 2025-01-17 11:22 EST
Starting masscan 1.3.2 (http://bit.ly/14GZcT) at 2025-01-17 16:37:10 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 1524/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 6667/tcp on 172.16.191.130
Discovered open port 445/tcp on 172.16.191.130
Discovered open port 8009/tcp on 172.16.191.130
Discovered open port 2049/tcp on 172.16.191.130 scanned in 11.46 seconds
Discovered open port 47342/tcp on 172.16.191.130
Discovered open port 8787/tcp on 172.16.191.130
Discovered open port 80/tcp on 172.16.191.130
Discovered open port 3632/tcp on 172.16.191.130
Discovered open port 6000/tcp on 172.16.191.130 at 2025-01-17 11:22 EST
Discovered open port 139/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 5432/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 5900/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 1099/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 48461/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 23/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 8180/tcp on 172.16.191.130
Discovered open port 25/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 2121/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 41388/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 46600/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 6697/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 512/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 513/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 22/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 514/tcp on 172.16.191.130 completed (1 up), 1 undergoing SYN Stealth Scan
Discovered open port 21/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
Discovered open port 53/tcp on 172.16.191.130 172.16.191.2 are in ignored states.
```

Service Enumeration

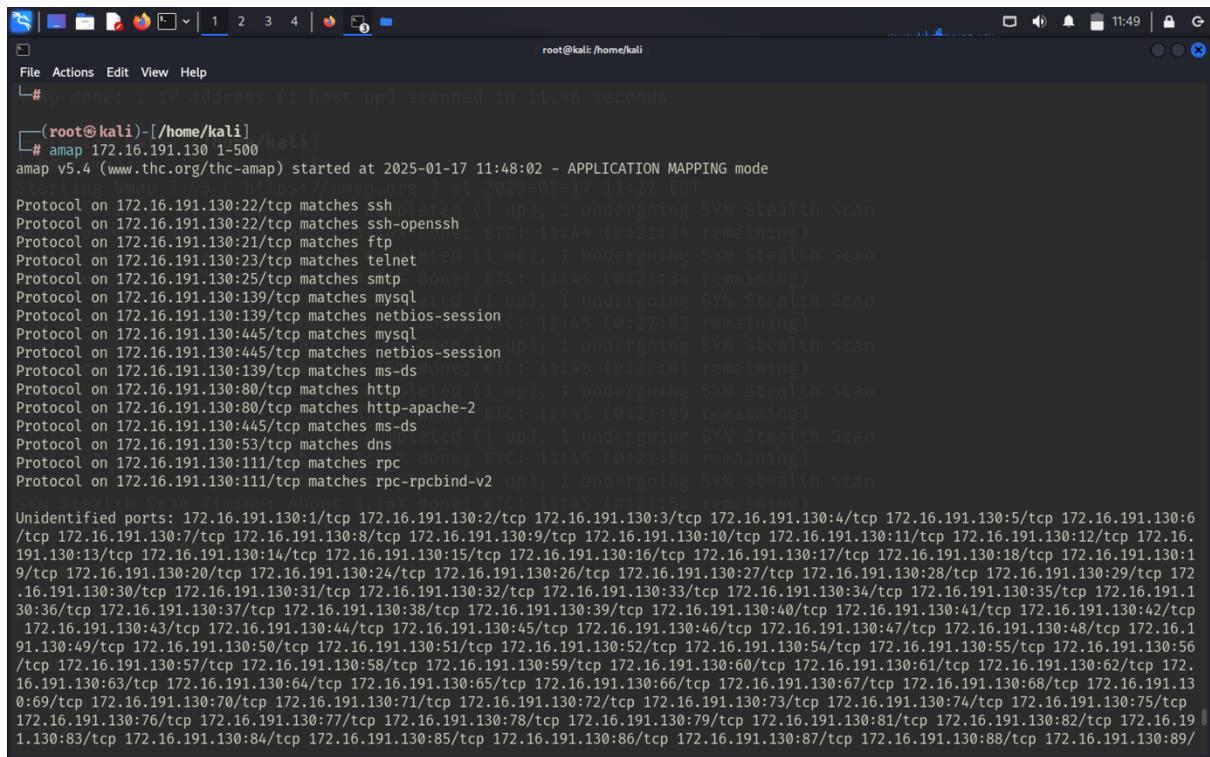
With amap:

```
amap 172.16.191.130 1-500
```

- amap identifies the services running on open ports.

Comparison:

- amap provides similar service version details but is less comprehensive than nmap -sV.



```
root@kali: /home/kali
# done 1 IP address (1 host up) scanned in 11.46 seconds
[root@kali]# amap 172.16.191.130 1-500
amap v5.4 (www.thc.org/thc-amap) started at 2025-01-17 11:48:02 - APPLICATION MAPPING mode
Protocol on 172.16.191.130:22/tcp matches ssh
Protocol on 172.16.191.130:22/tcp matches ssh-openssh
Protocol on 172.16.191.130:21/tcp matches ftp
Protocol on 172.16.191.130:23/tcp matches telnet
Protocol on 172.16.191.130:25/tcp matches smtp
Protocol on 172.16.191.130:139/tcp matches mysql
Protocol on 172.16.191.130:139/tcp matches netbios-session
Protocol on 172.16.191.130:445/tcp matches mysql
Protocol on 172.16.191.130:445/tcp matches netbios-session
Protocol on 172.16.191.130:80/tcp matches ms-ds
Protocol on 172.16.191.130:80/tcp matches http
Protocol on 172.16.191.130:80/tcp matches http-apache-2
Protocol on 172.16.191.130:445/tcp matches ms-ds
Protocol on 172.16.191.130:53/tcp matches dns
Protocol on 172.16.191.130:111/tcp matches rpc
Protocol on 172.16.191.130:111/tcp matches rpc-rpcbind-v2
Unidentified ports: 172.16.191.130:1/tcp 172.16.191.130:2/tcp 172.16.191.130:3/tcp 172.16.191.130:4/tcp 172.16.191.130:5/tcp 172.16.191.130:6/tcp 172.16.191.130:7/tcp 172.16.191.130:8/tcp 172.16.191.130:9/tcp 172.16.191.130:10/tcp 172.16.191.130:11/tcp 172.16.191.130:12/tcp 172.16.191.130:13/tcp 172.16.191.130:14/tcp 172.16.191.130:15/tcp 172.16.191.130:16/tcp 172.16.191.130:17/tcp 172.16.191.130:18/tcp 172.16.191.130:19/tcp 172.16.191.130:20/tcp 172.16.191.130:24/tcp 172.16.191.130:26/tcp 172.16.191.130:27/tcp 172.16.191.130:28/tcp 172.16.191.130:29/tcp 172.16.191.130:30/tcp 172.16.191.130:31/tcp 172.16.191.130:32/tcp 172.16.191.130:33/tcp 172.16.191.130:34/tcp 172.16.191.130:35/tcp 172.16.191.130:36/tcp 172.16.191.130:37/tcp 172.16.191.130:38/tcp 172.16.191.130:39/tcp 172.16.191.130:40/tcp 172.16.191.130:41/tcp 172.16.191.130:42/tcp 172.16.191.130:43/tcp 172.16.191.130:44/tcp 172.16.191.130:45/tcp 172.16.191.130:46/tcp 172.16.191.130:47/tcp 172.16.191.130:48/tcp 172.16.191.130:49/tcp 172.16.191.130:50/tcp 172.16.191.130:51/tcp 172.16.191.130:52/tcp 172.16.191.130:54/tcp 172.16.191.130:55/tcp 172.16.191.130:56/tcp 172.16.191.130:57/tcp 172.16.191.130:58/tcp 172.16.191.130:59/tcp 172.16.191.130:60/tcp 172.16.191.130:61/tcp 172.16.191.130:62/tcp 172.16.191.130:63/tcp 172.16.191.130:64/tcp 172.16.191.130:65/tcp 172.16.191.130:66/tcp 172.16.191.130:67/tcp 172.16.191.130:68/tcp 172.16.191.130:69/tcp 172.16.191.130:70/tcp 172.16.191.130:71/tcp 172.16.191.130:72/tcp 172.16.191.130:73/tcp 172.16.191.130:74/tcp 172.16.191.130:75/tcp 172.16.191.130:76/tcp 172.16.191.130:77/tcp 172.16.191.130:78/tcp 172.16.191.130:79/tcp 172.16.191.130:81/tcp 172.16.191.130:82/tcp 172.16.191.130:83/tcp 172.16.191.130:84/tcp 172.16.191.130:85/tcp 172.16.191.130:86/tcp 172.16.191.130:87/tcp 172.16.191.130:88/tcp 172.16.191.130:89/
```

Banner Grabbing

With Netcat:

```
nc -v 172.16.191.130 80
```

- Manually connect to an open port to retrieve service information.

With telnet:

```
telnet 172.16.191.130 80
```

Comparison:

- Both Netcat and telnet require manual interaction but can sometimes provide more detailed or raw service banners compared to nmap --script=banner.

```
Stats: 0:00:13 elapsed; 0 hosts completed (1 up)
SYN Scan: About 3.16% done; 1 hosts up
(UNKNOWN) [172.16.191.130] 80 (http) open
# nc -v 172.16.191.130 80
172.16.191.130: inverse host lookup failed: Unknown host
(running)
```

```
(root㉿kali)-[~/home/kali]
# nc -v 172.16.191.130 80
172.16.191.130: inverse host lookup failed: Unknown host
(UNKNOWN) [172.16.191.130] 80 (http) open
root@kali:~# telnet 172.16.191.130
Trying 172.16.191.130 ...
Connected to 172.16.191.130.
Escape character is '^]'.
msfadmin@metasploitable:~$ hping3 -c 1 -n -p 80 --script banner 172.16.191.130
Hping3 v3.0-dev ( http://www.hping.org ) -- (Linux: i386:pcap )
Hping3 is a user-friendly and automated tool for OS fingerprinting, providing accurate results by
comparing responses against its extensive OS signature database with commands like nmap -O
It is faster and ideal for quick reconnaissance tasks, presenting clean, structured
outputs that include OS details, open ports, and services. In contrast, hping3 is a more advanced and
flexible tool, allowing users to craft custom packets and analyze raw responses such as TTL, window
size, and TCP/IP behavior. However, hping3 requires detailed knowledge of networking and manual
interpretation, making it less accessible but highly valuable for specialized or bypass scenarios where
it should be for only 1 paragraph

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Wed Jan 15 05:07:20 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
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:
```

```
(root㉿kali)-[~/home/kali]
# nc -v 172.16.191.130 80
172.16.191.130: inverse host lookup failed: Unknown host
(UNKNOWN) [172.16.191.130] 80 (http) open
root@kali:~# telnet 172.16.191.130
Trying 172.16.191.130 ...
Connected to 172.16.191.130.
Escape character is '^]'.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:fa:dd:2a
          inet addr:172.16.191.130  Bcast:172.16.191.255  Mask:255.255.255.0
          inet6 addr: fd62:f079:e174:1:20c:29ff:fe:fa:dd2a/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:225311 errors:215 dropped:281 overruns:0 frame:0
          TX packets:154844 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16373177 (15.6 MB)  TX bytes:15851923 (15.1 MB)
          Interrupt:17 Base address:0x2000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:7502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7502 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3707661 (3.5 MB)  TX bytes:3707661 (3.5 MB)
msfadmin@metasploitable:~$
```

OS Fingerprinting

With hping3:

```
hping3 --icmp 172.16.191.130
```

- hping3 performs OS fingerprinting using ICMP responses and other network behaviors.

Comparison:

- Nmap is a user-friendly and automated tool for OS fingerprinting, providing accurate results by comparing responses against its extensive OS signature database with commands like nmap -O <target-IP>. It is faster and ideal for quick reconnaissance tasks, presenting clean, structured outputs that include OS details, open ports, and services. In contrast, hping3 is a more advanced and flexible tool, allowing users to craft custom packets and analyze raw responses such as TTL, window size, and TCP/IP behavior. However, hping3 requires detailed knowledge of networking and manual interpretation, making it less accessible but highly valuable for specialized or bypass scenarios where custom packet manipulation is needed.

```
root@kali: ~
└─# hping3 --icmp 172.16.191.130
HPING 172.16.191.130 (eth0 172.16.191.130): icmp mode set, 28 headers + 0 data bytes
len=46 ip=172.16.191.130 ttl=64 id=30556 icmp_seq=0 rtt=3.5 ms
len=46 ip=172.16.191.130 ttl=64 id=30557 icmp_seq=1 rtt=3.1 ms
len=46 ip=172.16.191.130 ttl=64 id=30558 icmp_seq=2 rtt=6.4 ms
len=46 ip=172.16.191.130 ttl=64 id=30559 icmp_seq=3 rtt=1.6 ms
len=46 ip=172.16.191.130 ttl=64 id=30560 icmp_seq=4 rtt=4.9 ms
len=46 ip=172.16.191.130 ttl=64 id=30561 icmp_seq=5 rtt=11.5 ms
len=46 ip=172.16.191.130 ttl=64 id=30562 icmp_seq=6 rtt=7.0 ms
len=46 ip=172.16.191.130 ttl=64 id=30563 icmp_seq=7 rtt=1.3 ms
len=46 ip=172.16.191.130 ttl=64 id=30564 icmp_seq=8 rtt=8.1 ms
len=46 ip=172.16.191.130 ttl=64 id=30565 icmp_seq=9 rtt=3.0 ms
len=46 ip=172.16.191.130 ttl=64 id=30566 icmp_seq=10 rtt=1.5 ms
len=46 ip=172.16.191.130 ttl=64 id=30567 icmp_seq=11 rtt=5.6 ms
len=46 ip=172.16.191.130 ttl=64 id=30568 icmp_seq=12 rtt=4.6 ms
len=46 ip=172.16.191.130 ttl=64 id=30569 icmp_seq=13 rtt=11.6 ms
len=46 ip=172.16.191.130 ttl=64 id=30570 icmp_seq=14 rtt=7.2 ms
len=46 ip=172.16.191.130 ttl=64 id=30571 icmp_seq=15 rtt=6.9 ms
len=46 ip=172.16.191.130 ttl=64 id=30572 icmp_seq=16 rtt=9.4 ms
len=46 ip=172.16.191.130 ttl=64 id=30573 icmp_seq=17 rtt=8.5 ms
len=46 ip=172.16.191.130 ttl=64 id=30574 icmp_seq=18 rtt=7.6 ms
len=46 ip=172.16.191.130 ttl=64 id=30575 icmp_seq=19 rtt=7.5 ms
^C
— 172.16.191.130 hping statistic —
20 packets transmitted, 20 packets received, 0% packet loss
round-trip min/avg/max = 1.3/6.0/11.6 ms
root@kali: ~
```

Footprinting

1. IP Tools Suite (ipcalc or arp-scan)

arp-scan:

- **Purpose:** Scan the local network and list all active IP addresses.
- **Command:**

```
sudo arp-scan -l
```

- **Output:**
 - Identifies all active IP addresses on the subnet, including device MAC addresses.

ipcalc:

- **Purpose:** Calculates and validates the IP address range, helping in identifying the network scope.
- **Command:**
- `ipcalc 172.16.191.130`
- **Output:**
 - Provides details about the subnet and broadcast IP.

```
(root㉿kali)-[~]
└─# sudo arp-scan -l
Nmap is a user-friendly and automated tool for OS fingerprinting, providing accurate results by
ARP scanning. It can also be used for port scanning with commands like nmap -sS
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
Interface: eth0, type: EN10MB, MAC: 00:0c:29:17:47:fc, IPv4: 172.16.191.128
172.16.191.1 3a:f9:d3:f5:ec:65 (Unknown: locally administered)
172.16.191.2 00:50:56:e7:24:ec (VMware, Inc.)
172.16.191.130 00:0c:29:fa:dd:2a (VMware, Inc.)
172.16.191.254 00:50:56:f0:01:ac (VMware, Inc.)
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.123 seconds (120.58 hosts/sec). 4 responded
```

```
(root㉿kali)-[~]
└─# ipcalc 172.16.191.130
Address: 172.16.191.130
Netmask: 255.255.255.0 = 24
Wildcard: 0.0.0.255
⇒
Network: 172.16.191.0/24
HostMin: 172.16.191.1
HostMax: 172.16.191.254
Broadcast: 172.16.191.255
Hosts/Net: 254
          comparing responses against its extensive OS signature database
          <target-IP>. It is faster and ideal for quick reconnaissance
          10101100.00010000.10111111.en. 10000010
          11111111.11111111.11111111. 00000000
          00000000.00000000.00000000. h. 11111111
          interpretation, making it less accessible but highly valuable
          10101100.00010000.10111111.de. 00000000
          10101100.00010000.10111111. 00000001
          10101100.00010000.10111111. 11111110
          10101100.00010000.10111111. 11111111
          Class B, Private Internet
```

2. Nikto for Web Servers

- **Purpose:** Scans for vulnerabilities on web servers accessible via IP address.
 - **Command:**
- ```
nikto -h http://172.16.191.130
```
- **Output:**
    - Lists web server vulnerabilities, outdated software, and potential configuration issues.
  - **Use Case:** Useful if the Metasploitable machine has a web server running (usually port 80).

```

File Actions Edit View Help
-(root@kali)-[~]
nikto -h http://172.16.191.130
- Nikto v2.5.0

+ Target IP: 172.16.191.130
+ Target Hostname: 172.16.191.130
+ Target Port: 80
+ Start Time: 2025-01-17 14:21:30 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

```

```

File Actions Edit View Help
requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to a unauthorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icons/readme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to a
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-01-17 14:21:52 (GMT-5) (22 seconds)

+ 1 host(s) tested
-(root@kali)-[~]


```

### 3. Enum4linux for SMB Services

- Purpose:** Enumerates information from SMB shares and services running on the target IP.
- Command:**

```
enum4linux -a 172.16.191.130
```

- **Output:**
  - Provides usernames, shared folders, and policies for the target machine.
- **Use Case:** Ideal for machines running SMB services (e.g., Windows or Samba servers).

```

root@kali: ~
enum4linux -a 172.16.191.130
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Fri Jan 17 14:24:58 2025

[+] Got domain/workgroup name: WORKGROUP
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

[+] Got OS info for 172.16.191.130 from srvinfo: SMB2.1+ (Windows 10 Pro)
platform_id : 500
os_version : 4.9
server type : 0x9a03

[+] Users on 172.16.191.130
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)

```

```

root@kali: ~
File Actions Edit View Help
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, and custom Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name:,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0xfc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]

root@kali: ~
File Actions Edit View Help
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[ssh] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]

```

```

root@kali: ~
File Actions Edit View Help
user:[uucp] rid:[0x3fc]
(Share Enumeration on 172.16.191.130)
Share

Shares:
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.

Server Comment
Workgroup Master
WORKGROUP METASPOITABLE

[+] Attempting to map shares on 172.16.191.130
//172.16.191.130/print$ Mapping: DENIED Listing: N/A Writing: N/A
//172.16.191.130/tmp Mapping: OK Listing: OK Writing: N/A
//172.16.191.130/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing *
//172.16.191.130/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//172.16.191.130/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

[+] Attaching to 172.16.191.130 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
 [+] METASPOITABLE
 [+] Builtin
[+] Password Info for Domain: METASPOITABLE
 [+] Minimum password length: 5
 [+] Password history length: None
 [+] Maximum password age: Not Set
 [+] Password Complexity Flags: 000000
 [+] Domain Refuse Password Change: 0
 [+] Domain Password Store Cleartext: 0
 [+] Domain Password Lockout Admins: 0
 [+] Domain Password No Clear Change: 0
 [+] Domain Password No Anon Change: 0
 [+] Domain Password Complex: 0
 [+] Minimum password age: None
 [+] Reset Account Lockout Counter: 30 minutes
 [+] Locked Account Duration: 30 minutes
 [+] Account Lockout Threshold: None
 [+] Forced Log off Time: Not Set

```

```

[+] Retrieved partial password policy with rpcclient:
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
[+] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)

```

```

File Actions Edit View Help
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)

(Getting printer info for 172.16.191.130)

No printers returned.

enum4linux complete on Fri Jan 17 14:25:08 2025
```

## Comparison with nmap

| Tool       | Functionality                            | Comparison to nmap                                     |
|------------|------------------------------------------|--------------------------------------------------------|
| arp-scan   | Discovers IPs and MACs in local subnet.  | Simpler and faster than nmap for network scans.        |
| Nikto      | Detects web server vulnerabilities.      | More focused on web vulnerabilities than nmap.         |
| Enum4linux | Enumerates SMB shares and user accounts. | SMB-focused, complements nmap for service enumeration. |

## Vulnerability Assessment

### With Nikto:

```
nikto -h http:// 172.16.191.130
```

- Nikto scans for known vulnerabilities on web servers.

### Comparison:

- Nikto is more thorough for web and system vulnerabilities compared to nmap --script=vuln. However, nmap is faster for basic vulnerability checks.

```
File Actions Edit View Help
[root@kali] ~
nikto -h http://172.16.191.130
- Nikto v2.5.0

+ Target IP: 172.16.191.130
+ Target Hostname: 172.16.191.130
+ Target Port: 80
+ Start Time: 2025-01-17 14:21:30 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

File Actions Edit View Help
root@kali: ~
requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /?phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /?phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to unauthorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /?phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icons/readme/
+ /?phpMyAdmin/: phpMyAdmin directory found.
+ /?phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to a
+ /?phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time: 2025-01-17 14:21:52 (GMT-5) (22 seconds)

+ 1 host(s) tested
[root@kali] ~
#
```

## Task 10: Conducted 5 More Active Scans with Nmap

- Analyzed specific findings and recorded results for different scan types:
  - SYN scan (-sS)

The screenshot shows a terminal window titled 'root@kali: ~'. The command entered is '# nmap -sS 172.16.191.130'. The output displays the Nmap scan report for the target host. It lists various open ports and services, including 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), 514/tcp (shell), 1099/tcp (rmiregistry), 1524/tcp (ingreslock), 2049/tcp (nfs), 2121/tcp (ccproxy-ftp), 3306/tcp (mysql), 5432/tcp (postgresql), 5900/tcp (vnc), 6000/tcp (X11), 6667/tcp (irc), 8009/tcp (ajp13), and 8180/tcp (unknown). The MAC address of the host is listed as 00:0C:29:FA:DD:2A (VMware). The scan completed in 1.51 seconds.

```
nmap -sS 172.16.191.130
Starting Nmap 7.95 (https://nmap.org) at 2025-01-17 14:39 EST
Nmap scan report for 172.16.191.130
Host is up (0.0063s 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:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

- UDP scan (-sU)

The screenshot shows a terminal window titled 'root@kali: ~'. The command entered is '# nmap -sU 172.16.191.130'. The output displays the Nmap scan report for the target host. It lists various open ports and services, including 53/udp (domain), 68/udps (dhcpc), 69/udp (tftp), 111/udp (rpcbind), 137/udp (netbios-ns), 138/udp (netbios-dgm), and 2049/udp (nfs). The MAC address of the host is listed as 00:0C:29:FA:DD:2A (VMware). The scan completed in 1077.69 seconds.

```
nmap -sU 172.16.191.130
Starting Nmap 7.95 (https://nmap.org) at 2025-01-17 14:39 EST
Nmap scan report for 172.16.191.130
Host is up (0.0013s latency).

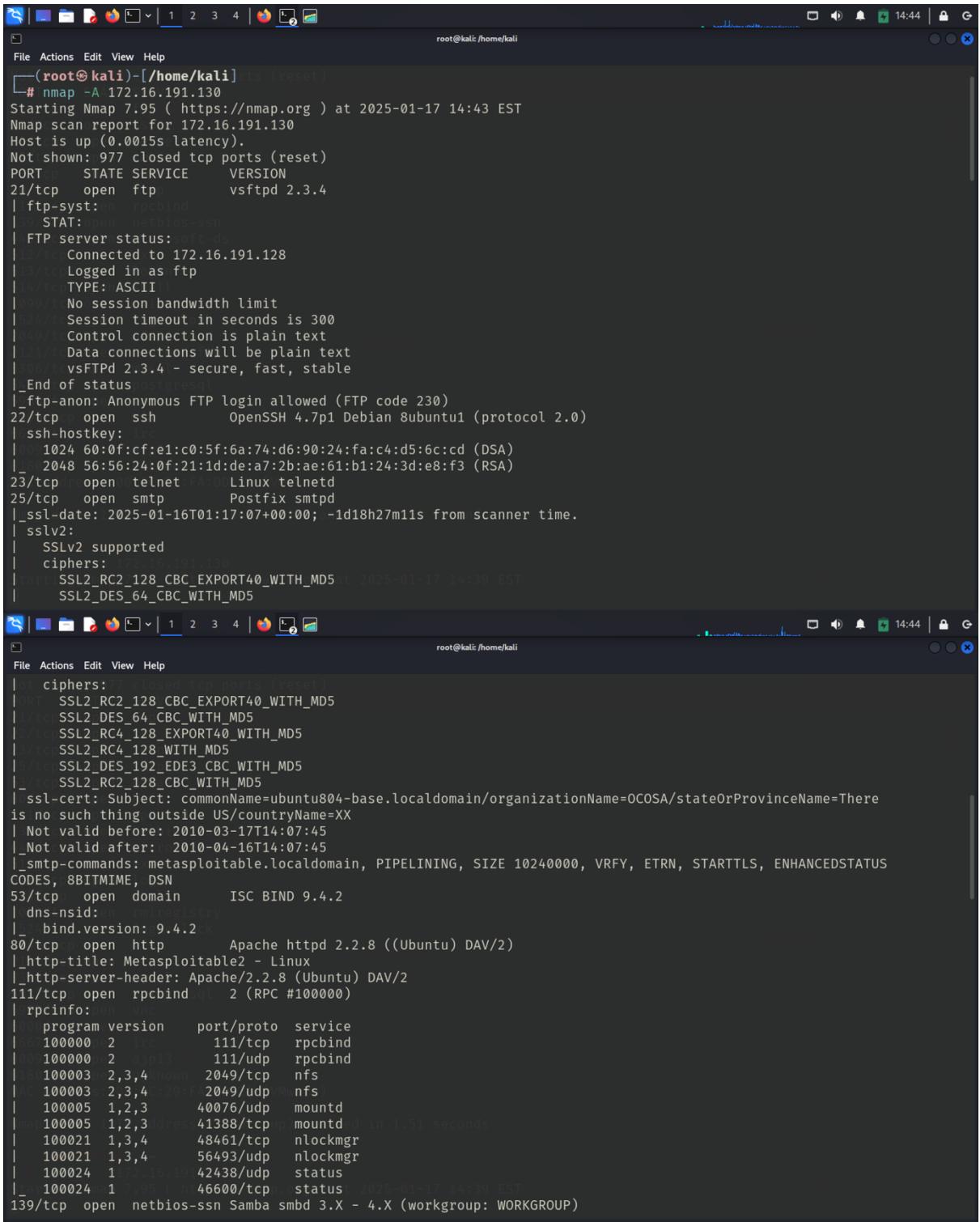
Not shown: 993 closed udp ports (port-unreach)

PORT STATE SERVICE
53/udp open domain
68/udps open | filtered dhcpc
69/udp open | filtered tftp
111/udp open | filtered rpcbind
137/udp open | filtered netbios-ns
138/udp open | filtered netbios-dgm
2049/udp open | filtered nfs

MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1077.69 seconds
```

### 3. Aggressive scan (-A)



The image shows two terminal windows side-by-side, both titled "root@kali:/home/kali". The top window displays the output of an aggressive Nmap scan (-A) against the host 172.16.191.130. The bottom window shows the detailed SSL/TLS cipher suite information for the same host.

```
nmap -A 172.16.191.130
Starting Nmap 7.95 (https://nmap.org) at 2025-01-17 14:43 EST
Nmap scan report for 172.16.191.130
Host is up (0.0015s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-syst:en
| STAT:
|_ FTP server status: soft-ds
| Connected to 172.16.191.128
| 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 statuspostgres
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: 2025-01-16T01:17:07+00:00; -1d18h27m11s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers: / 172.16.191.130
|_tanc SSL2_RC2_128_CBC_EXPORT40_WITH_MD5 at 2025-01-17 14:39 EST
|_SSL2_DES_64_CBC_WITH_MD5

ciphers: 77 closed ten ports (reset)
|_ORIG SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_1/1 SSL2_DES_64_CBC_WITH_MD5
|_2/2 SSL2_RC4_128_EXPORT40_WITH_MD5
|_3/3 SSL2_RC4_128_WITH_MD5
|_5/5 SSL2_DES_192_EDE3_CBC_WITH_MD5
|_7/7 SSL2_RC2_128_CBC_WITH_MD5
| 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, ENHANCEDSTATUS
CODES, 8BITMIME, DSN
53/tcp open domain ISC BIND 9.4.2
| dns-nsid: en
| dns-registry:
| 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
| 100003 2,3,4 2049/tcp nfs
| AC 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 40076/udp mountd
| map 100005 1,2,3 41388/tcp mounted in 1.51 seconds
| 100021 1,3,4 48461/tcp nlockmgr
| 100021 1,3,4 56493/udp nlockmgr
| 100024 1,2,3,4 42438/udp status
|_100024 1,2,3,4 46600/tcp status 2025-01-17 14:39 EST
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

```

root@kali:~/home/kali
File Actions Edit View Help
| 100024 1 closed 42438/udp status
| 100024 1 SERVICE 46600/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 OpenBSD or Solaris rlogin
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs log-ssn 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 77
| Capabilities flags: 43564
| Some Capabilities: ConnectWithDatabase, Support41Auth, SupportsTransactions, SupportsCompression, Speaks41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake
| Status: Autocommit
| Salt: ^_Dt%xx'Xvh%|eeK'!m'
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2025-01-16T01:17:07+00:00; -1d18h27m11s 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 vncress (1 VNC (protocol 3.3)) 1.51 seconds
| vnc-info:
| Protocol version: 3.3
| Security types: 101,130
|_ VNC Authentication (2) (nmap.org) at 2025-01-17 14:39 EST
6000/tcp open X11 (access denied)
root@kali:~/home/kali
File Actions Edit View Help
| Security types:ed tcp ports (reset)
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
| irc-info:en telnet
|5/users: 1 smtp
|3/servers: 1 domain
|0/lusers: 1 http
|1/lservers: 0 rpcbind
|3/server: irc.Metasploitable.LAN
|4/version: Unreal3.2.8.1. irc.Metasploitable.LAN
|2/uptime: 0 days, 15:09:40
|3/source ident: nmap
|4/source host: 6F9BB140.856A3A34.168799A3.IP
|error: Closing Link: ztovnzbir[172.16.191.128] (Quit: ztovnzbir)
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
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:FA:DD:2A (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 (VMware)
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel

Host script results: 191.130
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:

```

```
File Actions Edit View Help
MAC Address: 00:0C:29:FA:DD:2A (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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linu
x:linux_kernel http
|_ http open rpcbind
Host script results:
|_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: 2025-01-15T20:16:55-05:00
|_| smb-security-mode:
|_| account_used: <blank>
|_| authentication_level: user
|_| challenge_response: supported
|_| message_signing: disabled (dangerous, but default)
|_| smb2-time: Protocol negotiation failed (SMB2)
|_| clock-skew: mean: -1d17h12m10s, deviation: 2h30m00s, median: -1d18h27m11s
MAC Address: 00:0C:29:FA:DD:2A (VMware)
TRACEROUTE
HOP RTT e: ADDRESSress (1 host up) scanned in 1.51 seconds
1 1.48 ms 172.16.191.130

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 27.96 seconds
```

#### 4. Timing optimization scan (-T4)

```
File Actions Edit View Help
[root@kali]-[/home/kali]
nmap -T4 172.16.191.130
Starting Nmap 7.95 (https://nmap.org) at 2025-01-17 14:58 EST
Nmap scan report for 172.16.191.130
Host is up (0.0019s 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
519/tcp open dup_ports (port-unreach)
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open cccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc-red
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

5. Scan for specific ports (-p 21,22,80)

```
[root@kali]# nmap -p21,22,80 172.16.191.130
Starting Nmap 7.95 (https://nmap.org) at 2025-01-17 15:02 EST
Nmap scan report for 172.16.191.130
Host is up (0.0010s latency).
PORT STATE SERVICE
21/tcp open netbios-ns
22/tcp open netbios-dgm
80/tcp open http
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.297 seconds
```