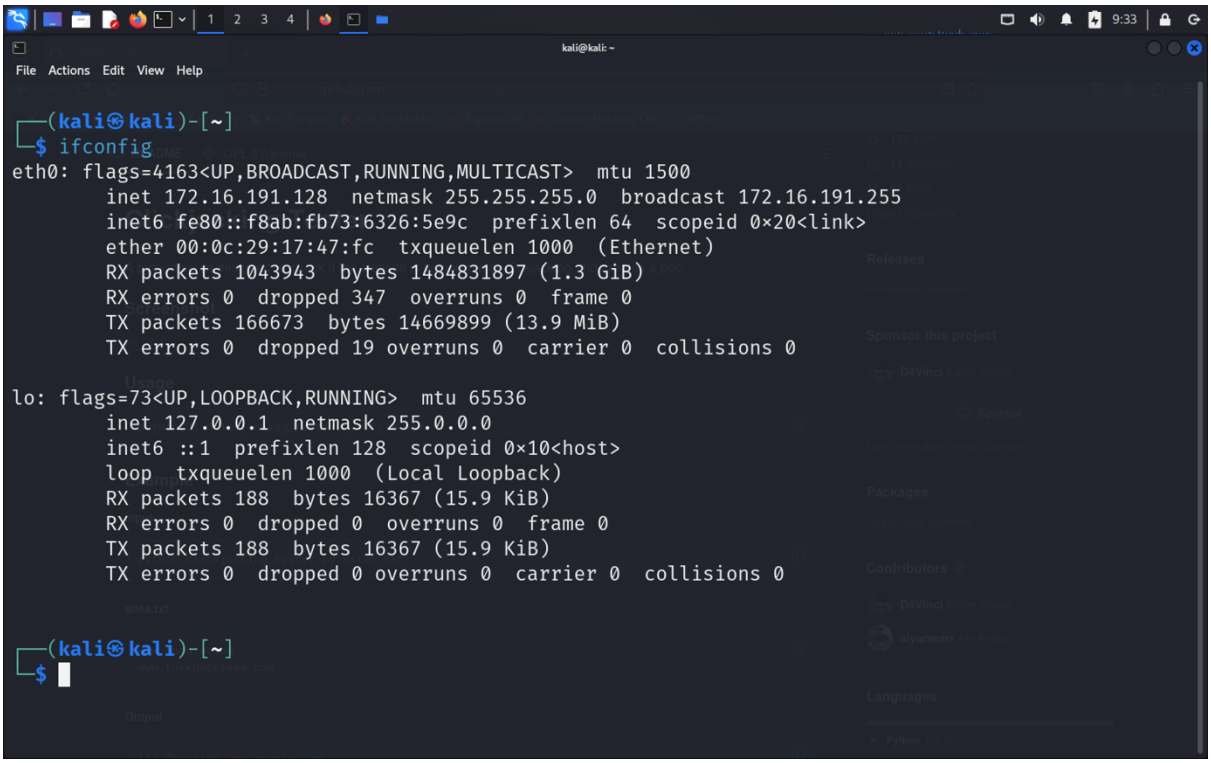
Week 3: Network Scanning, Footprinting, and Enumeration

Network Scanning and Analysis Report

Task 1: Identify Target IP Range

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

   `ifconfig`



   Output:

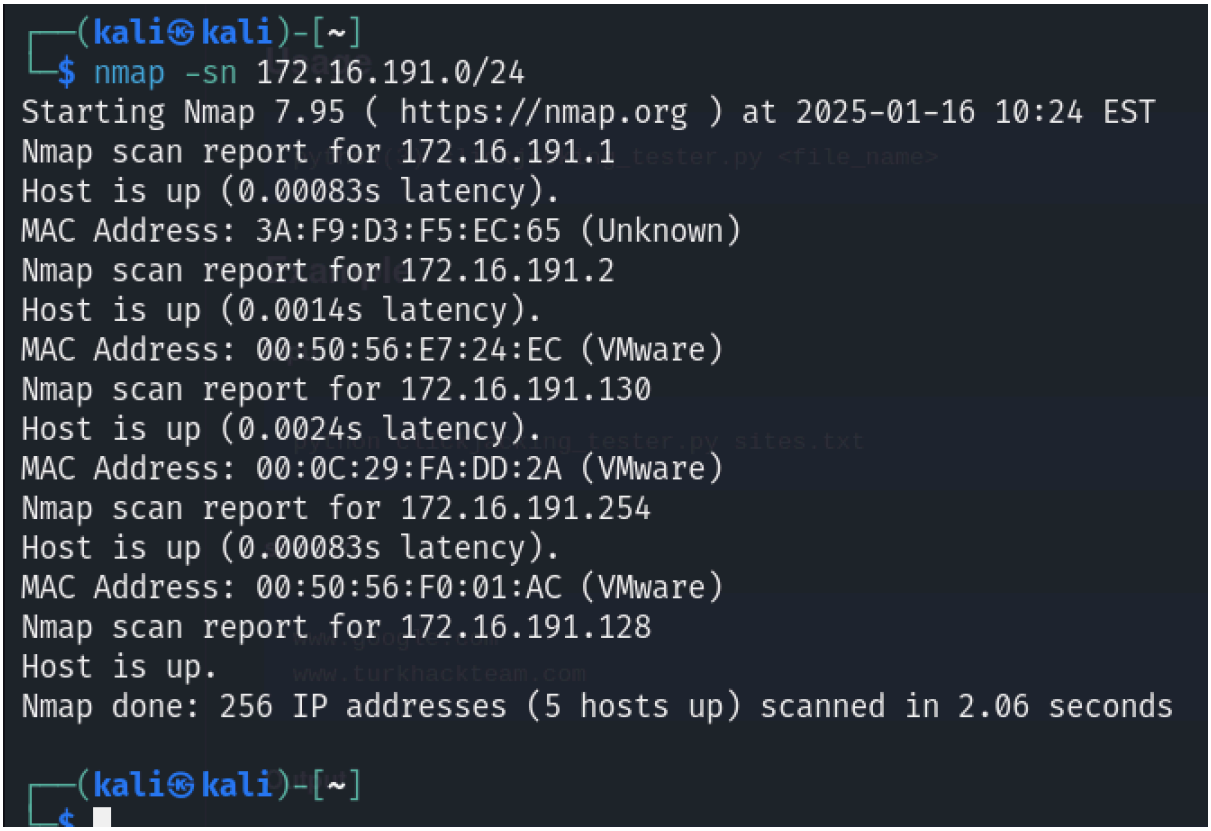
   `inet 172.18.191.128  netmask 255.255.255.0  broadcast 172.16.191.255`

   - 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:

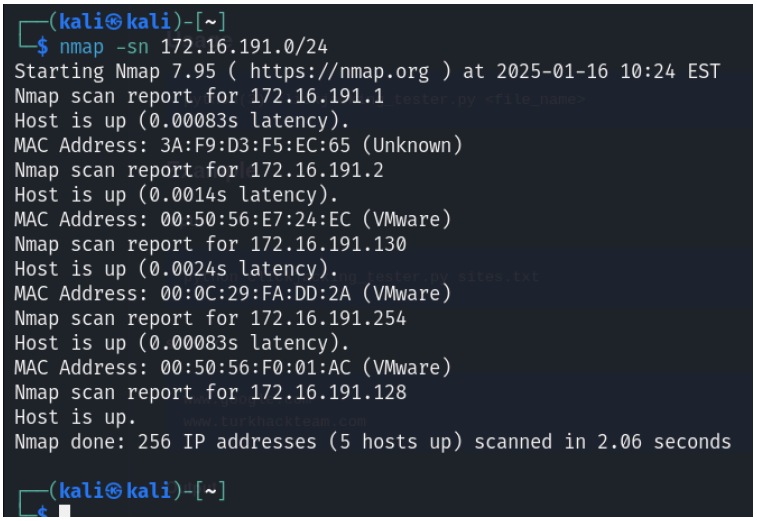


Task 2: Perform Ping Scan

- **Identified active hosts:**

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

Output:

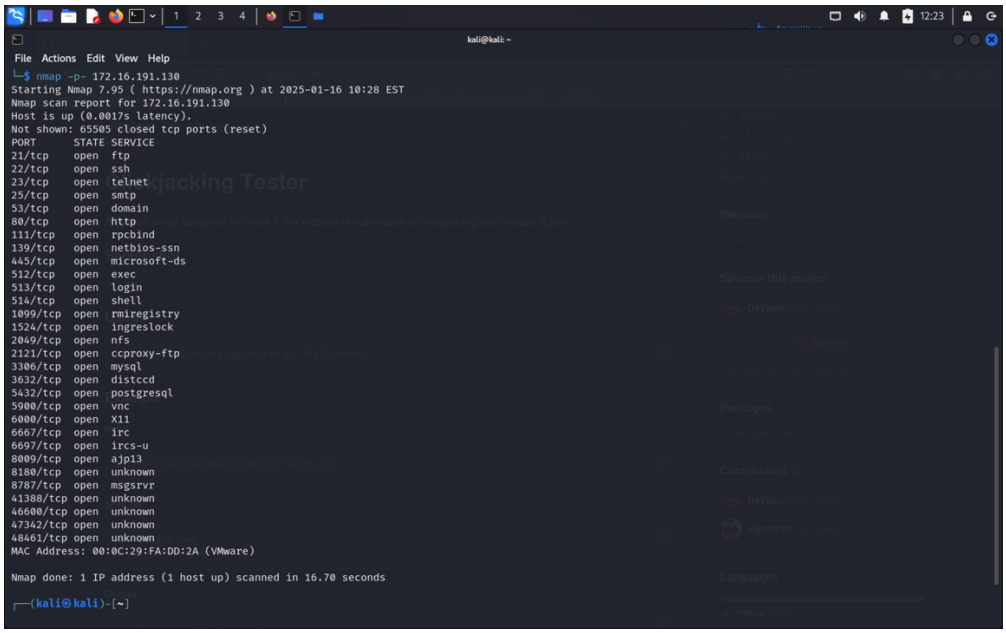


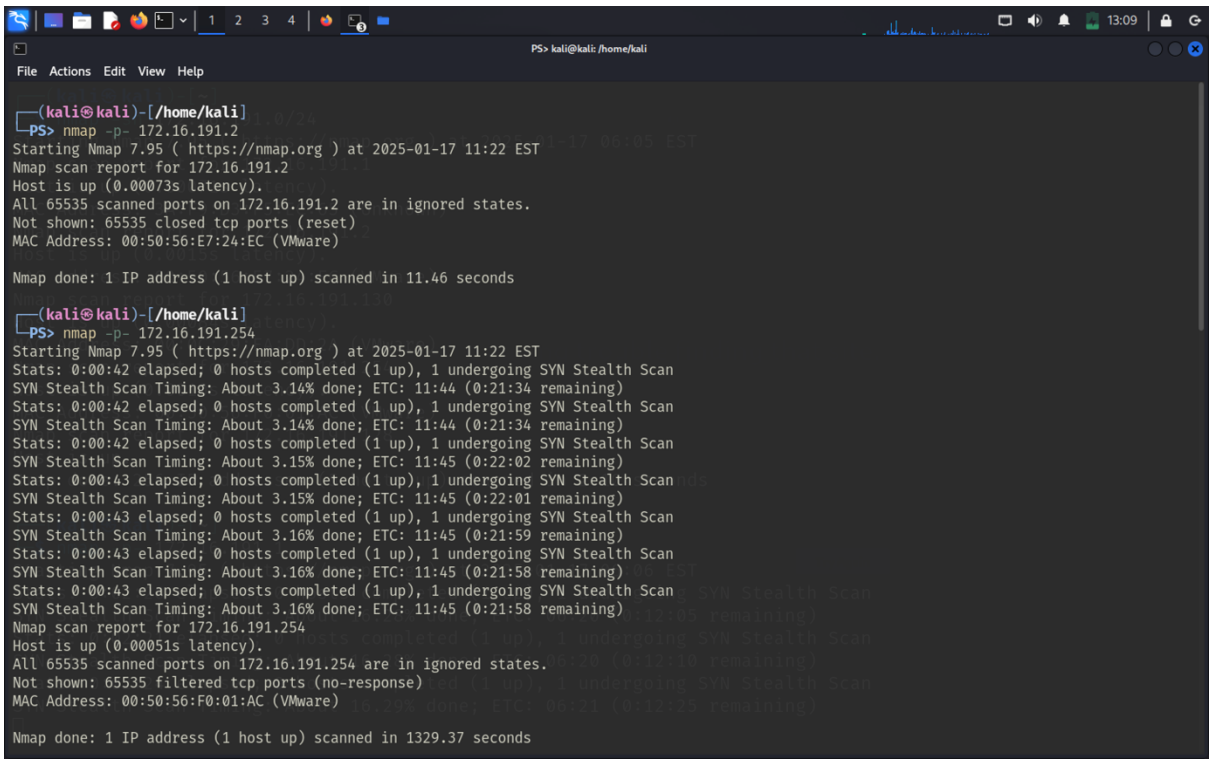
Task 3: Port Scanning

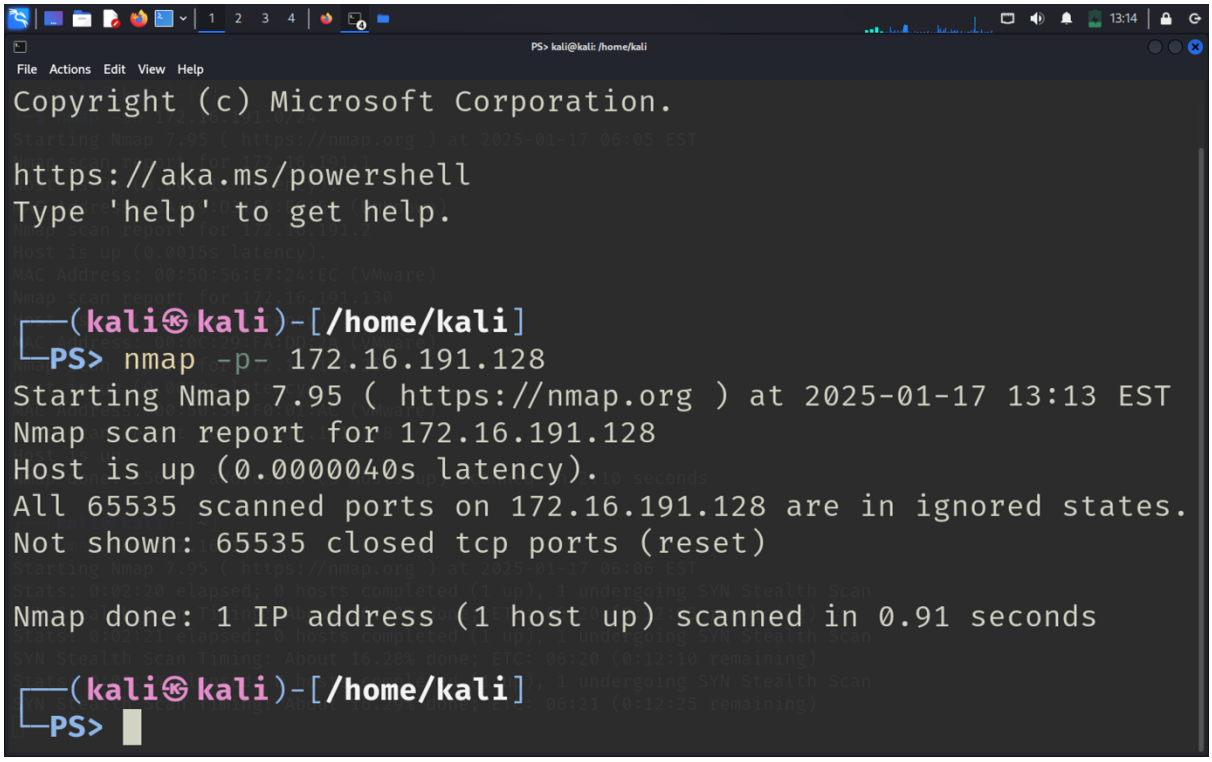
1. **Performed a comprehensive port scan on the Metasploitable machine and other active hosts:**

   ```
   nmap -p- 172.16.191.130
   ```

   Output:





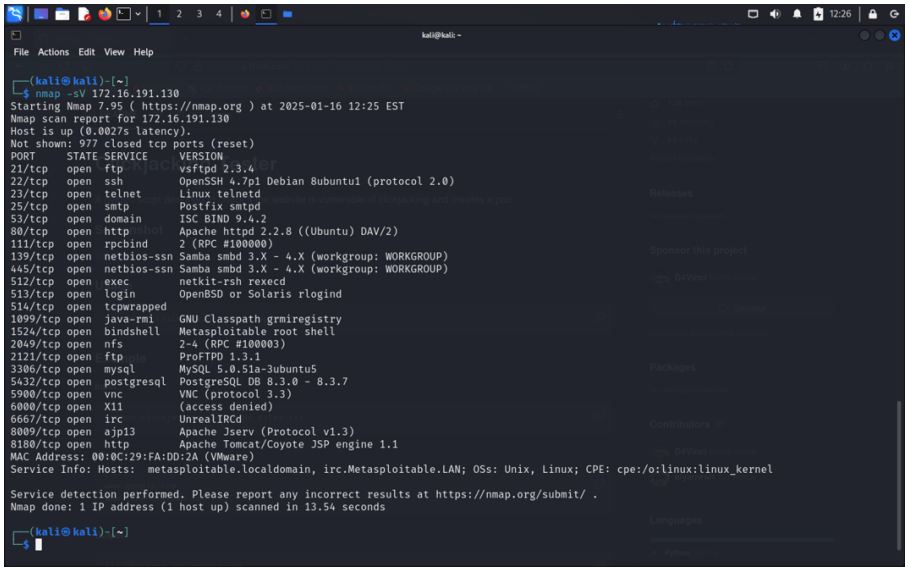


Task 4: Service Enumeration

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

   `nmap -sV 172.16.191.130`

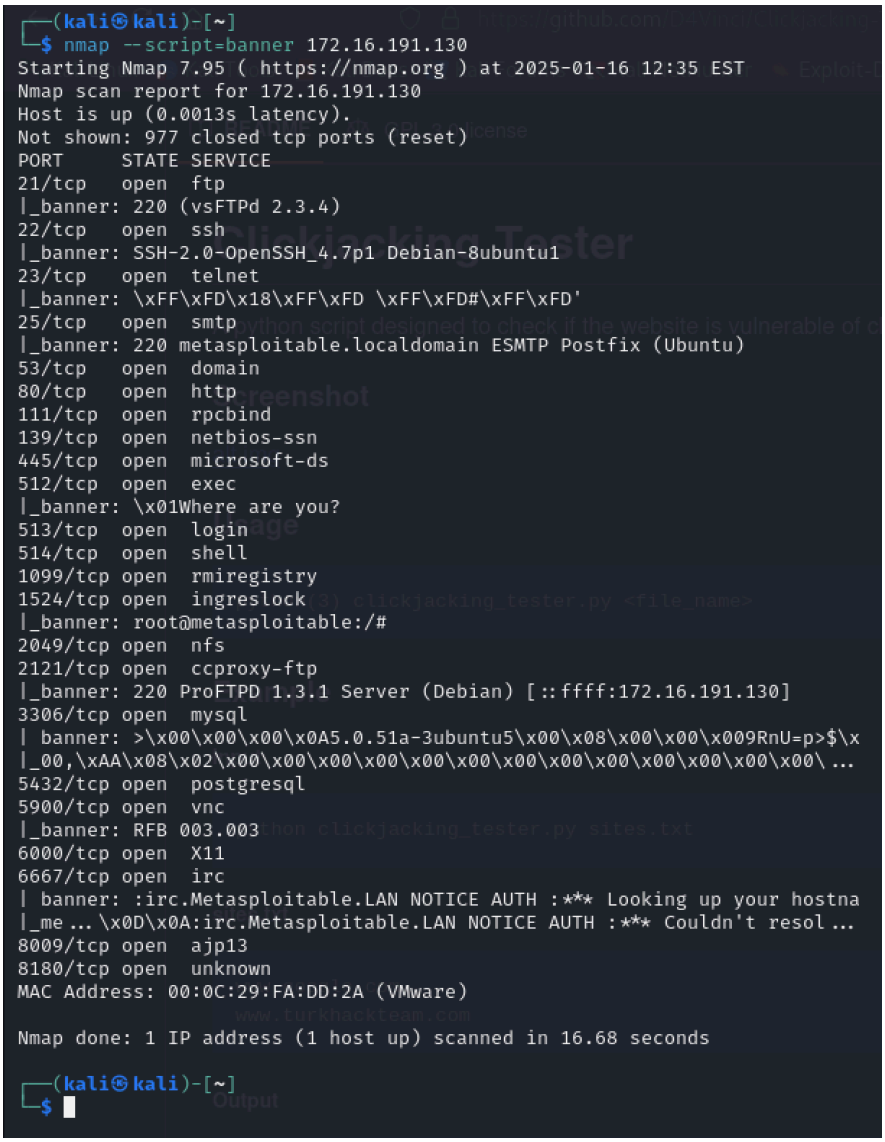
   Output:



Task 5: Banner Grabbing

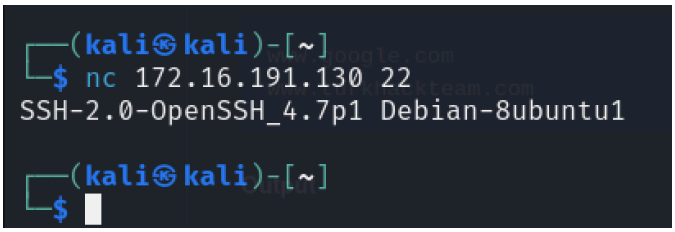
1. **Performed banner grabbing using Nmap and Netcat:**
   - Using Nmap:

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



- Using Netcat:

```
nc 172.16.191.130 22
```

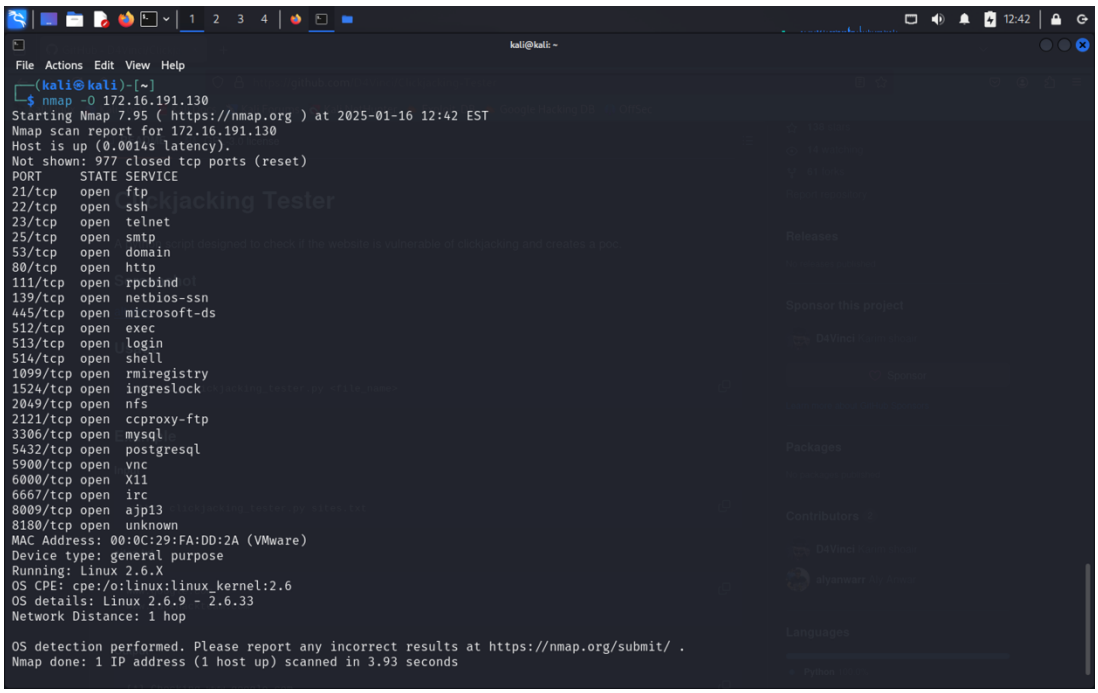


Task 6: OS Fingerprinting

1. **Performed OS fingerprinting to identify the target OS:**

```
nmap -O 172.16.191.130
```

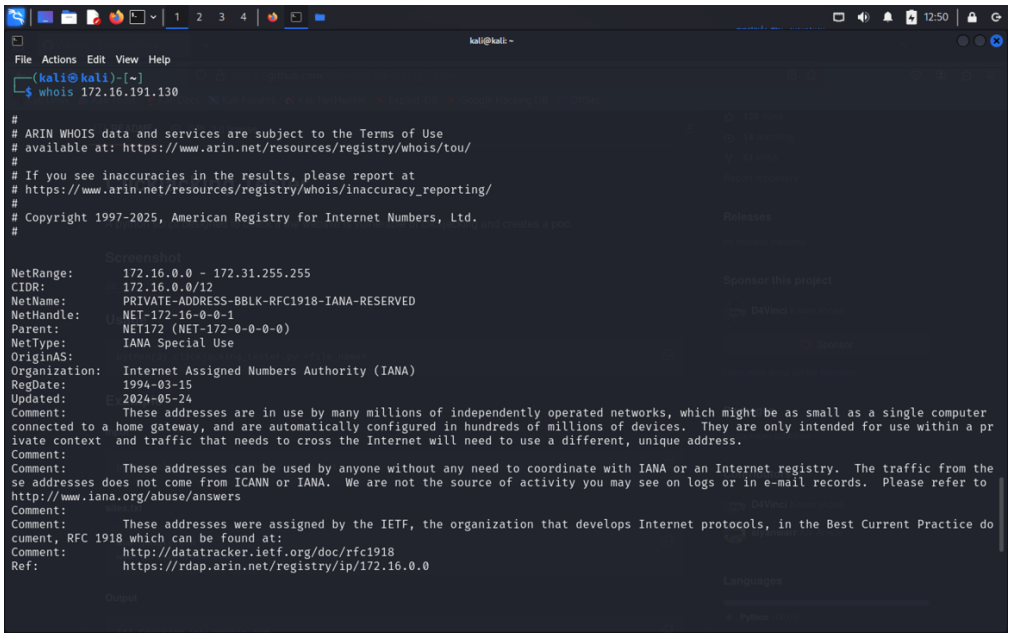
Output:

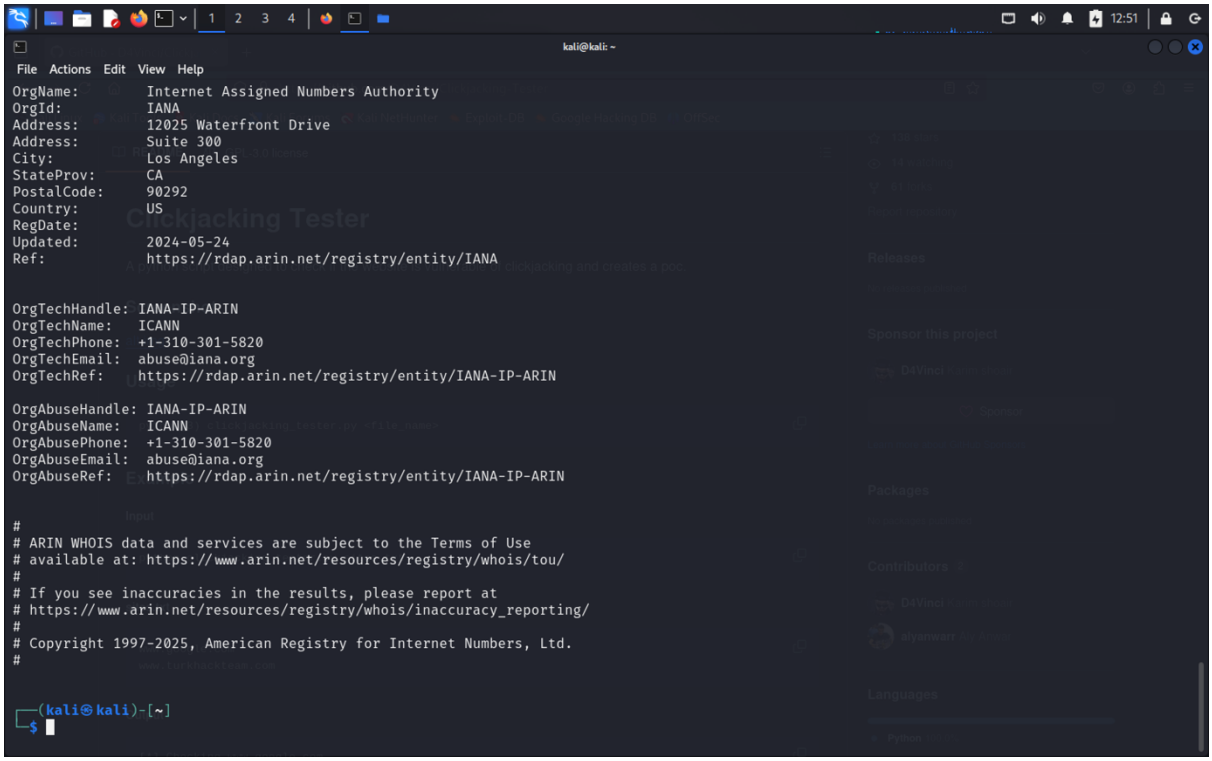


Task 7: Footprinting

1. **Used `whois` to gather domain information:**

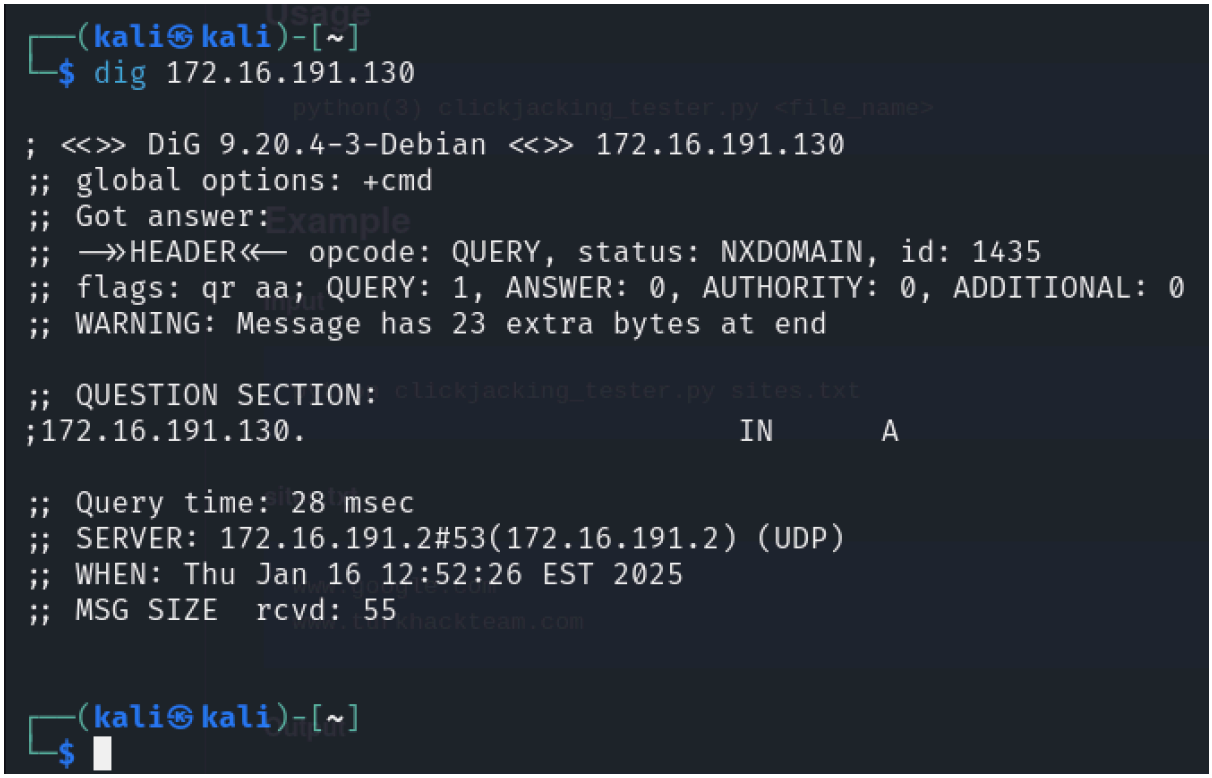
```
whois 172.16.191.130
```





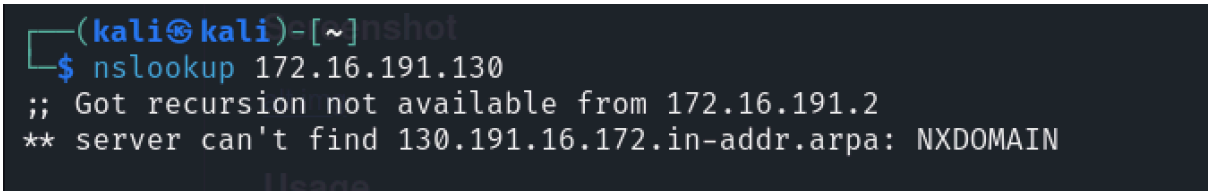
2. **Used `dig` to query DNS records:**

```
dig 172.16.191.130
```



3. **Performed DNS lookup using `nslookup`:**

   `nslookup 172.16.191.130`

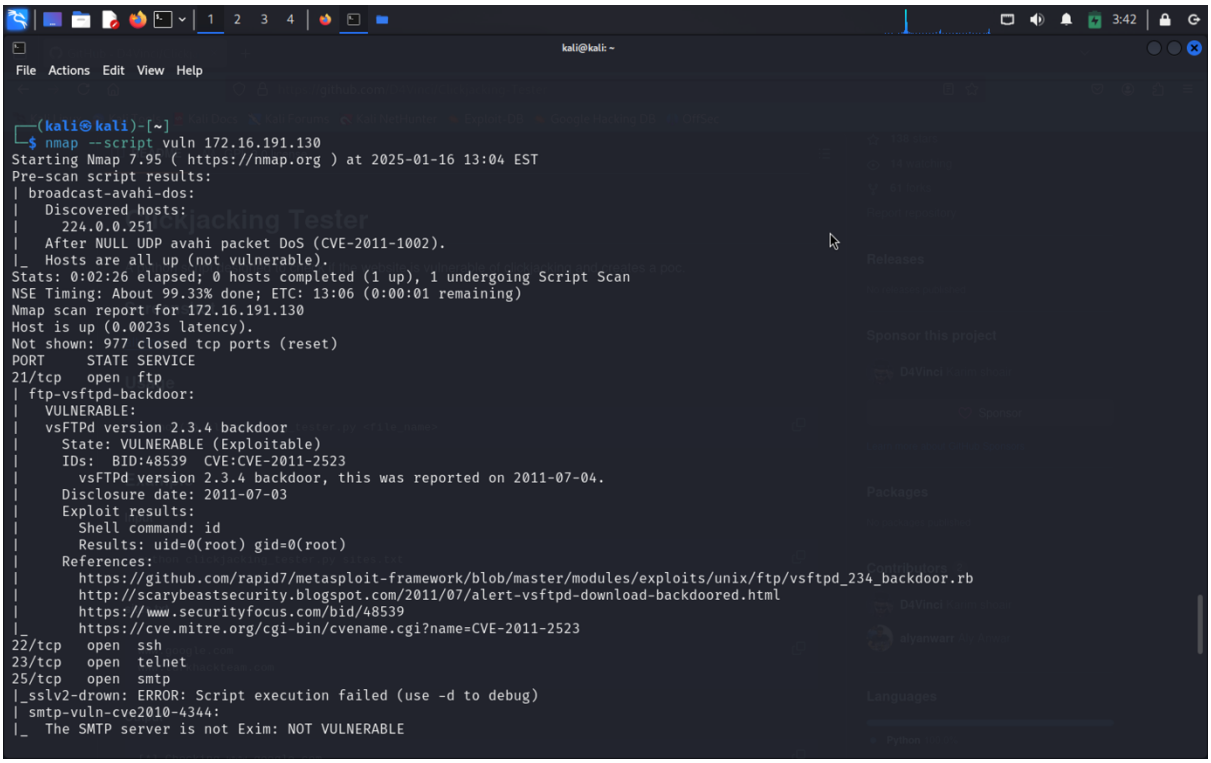


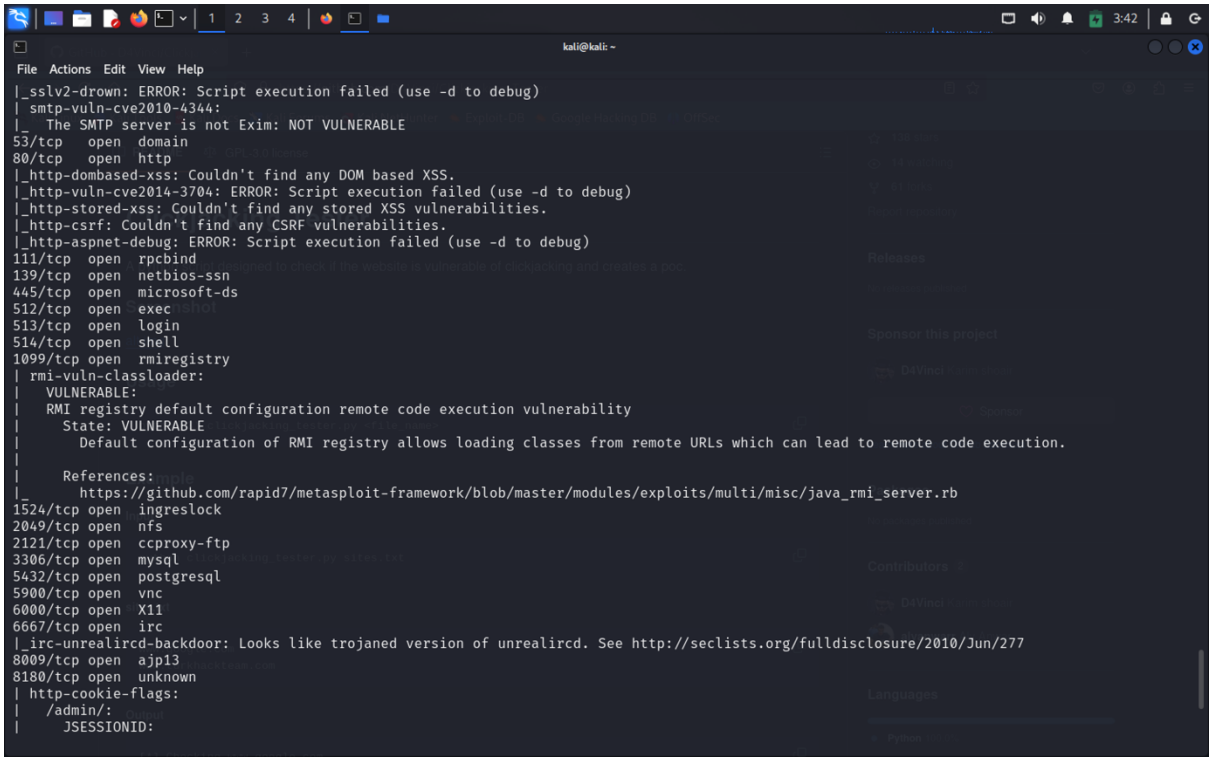
Task 8: Vulnerability Assessment

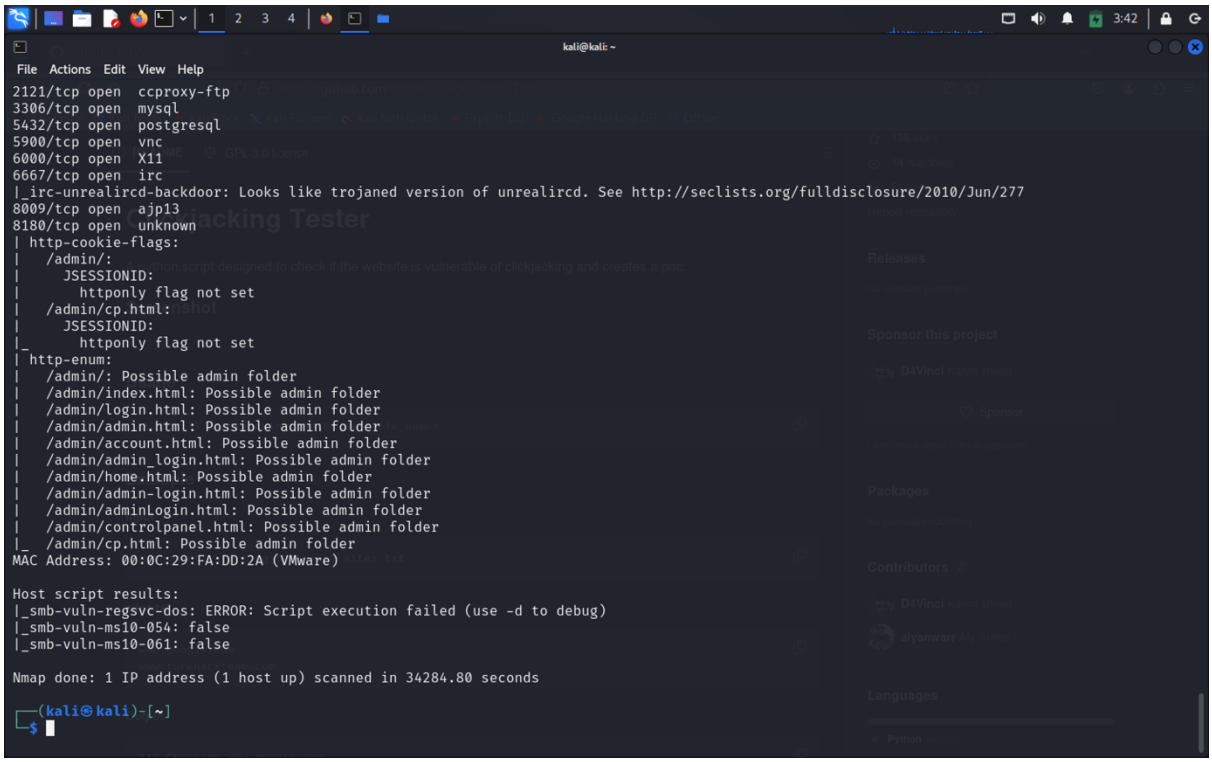
1. **Performed a vulnerability scan using Nmap's vulnerability scripts:**

   `nmap --script vuln 172.16.191.130`

   Output:







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`.

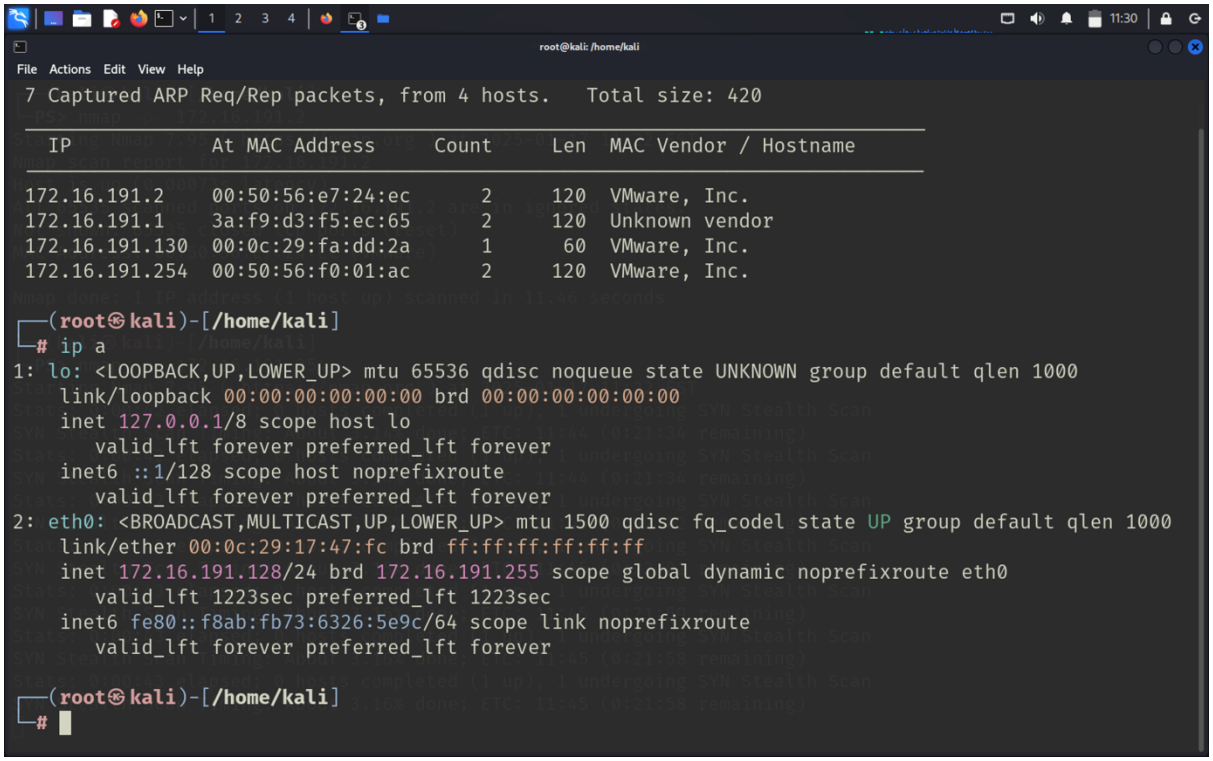
With `netdiscover`:

```
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.



Perform Ping Scan

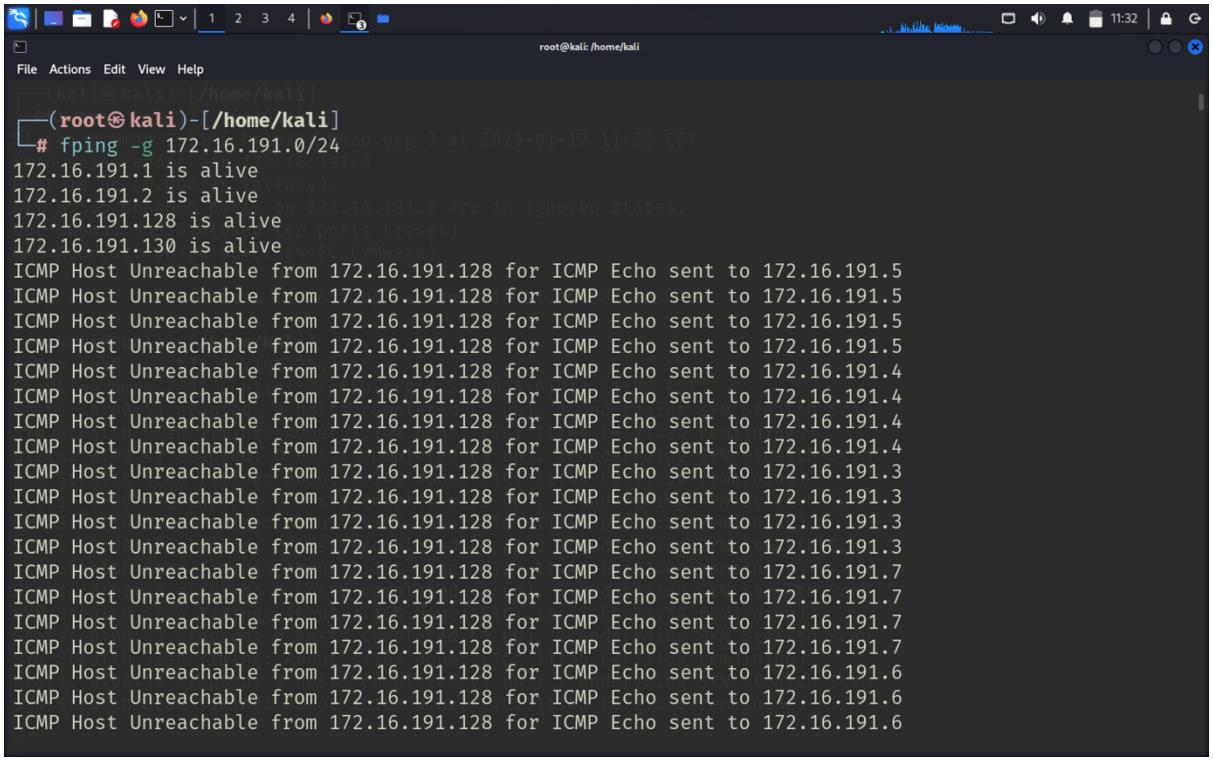
With `fping`:

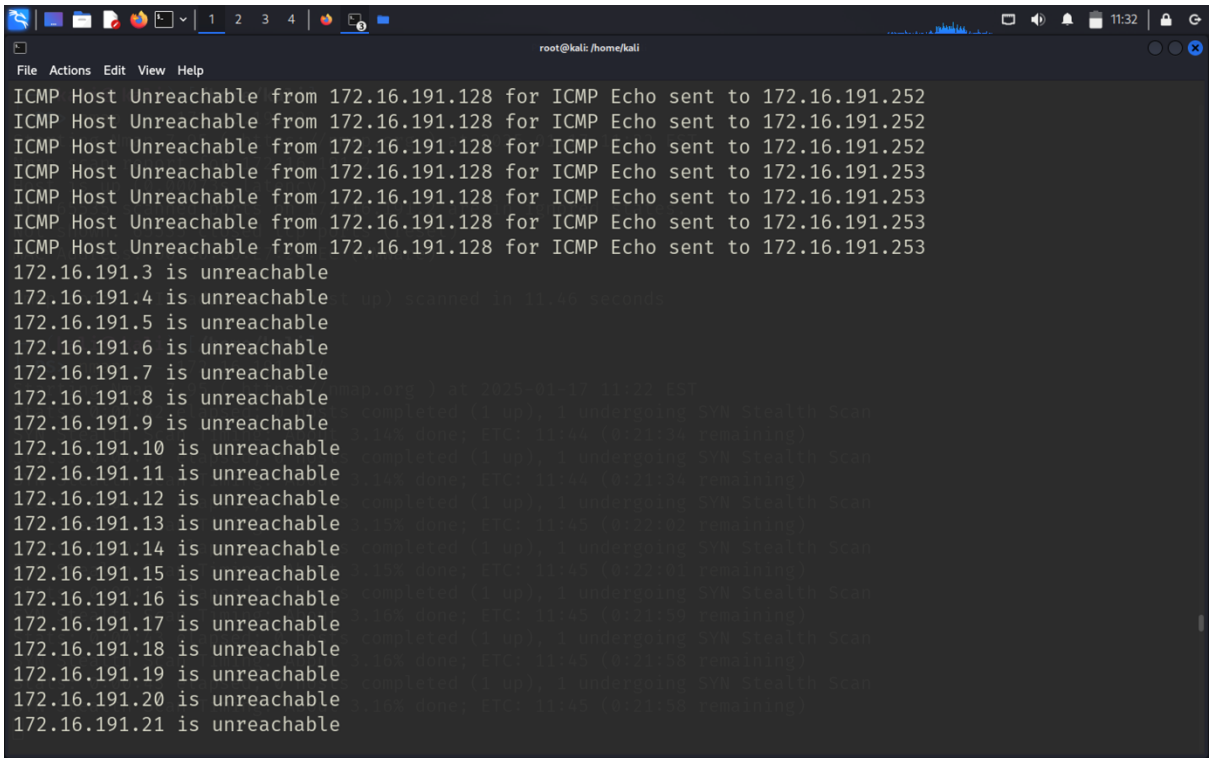
```
fping -g 172.16.191.0/24
```

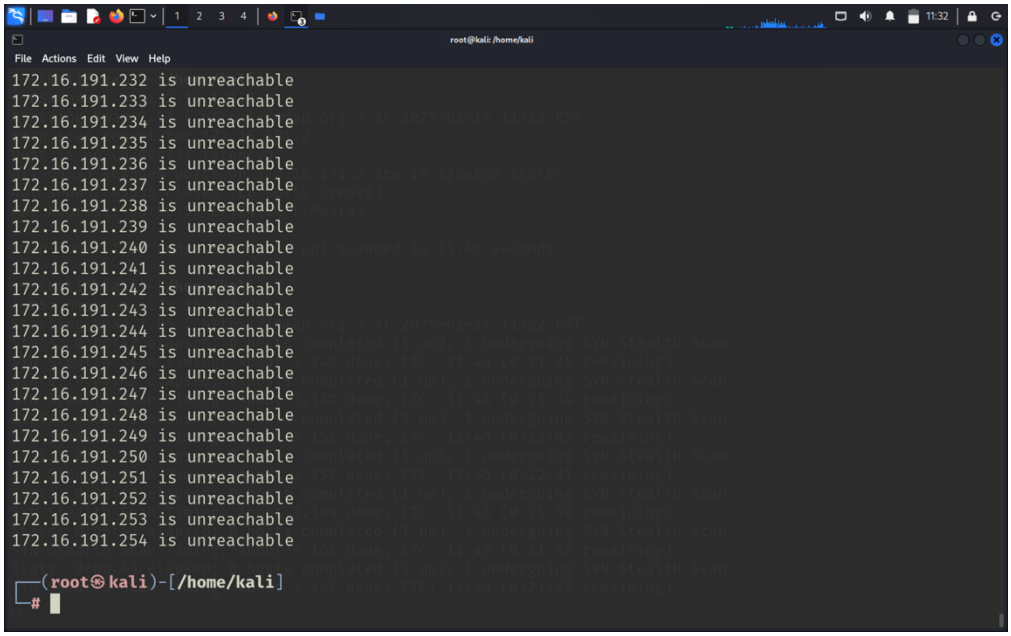
- `fping` sends ICMP echo requests to the specified range to find active hosts.

Comparison:

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







Port Scanning

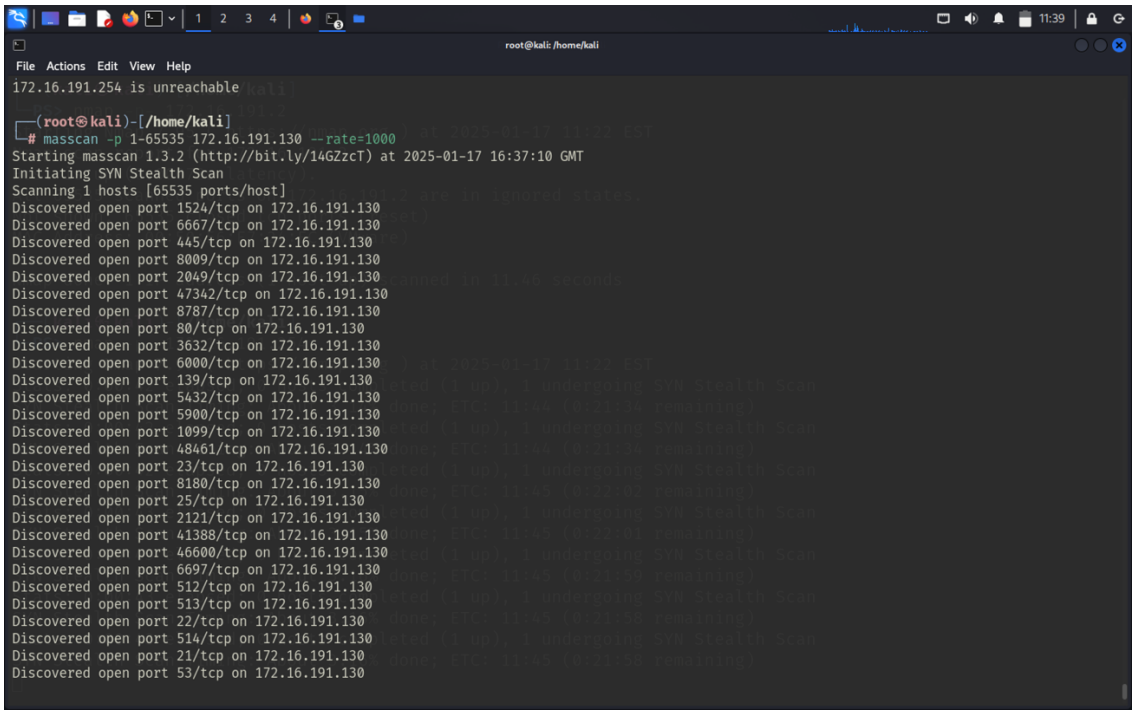
With `masscan`:

```
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.



Service Enumeration

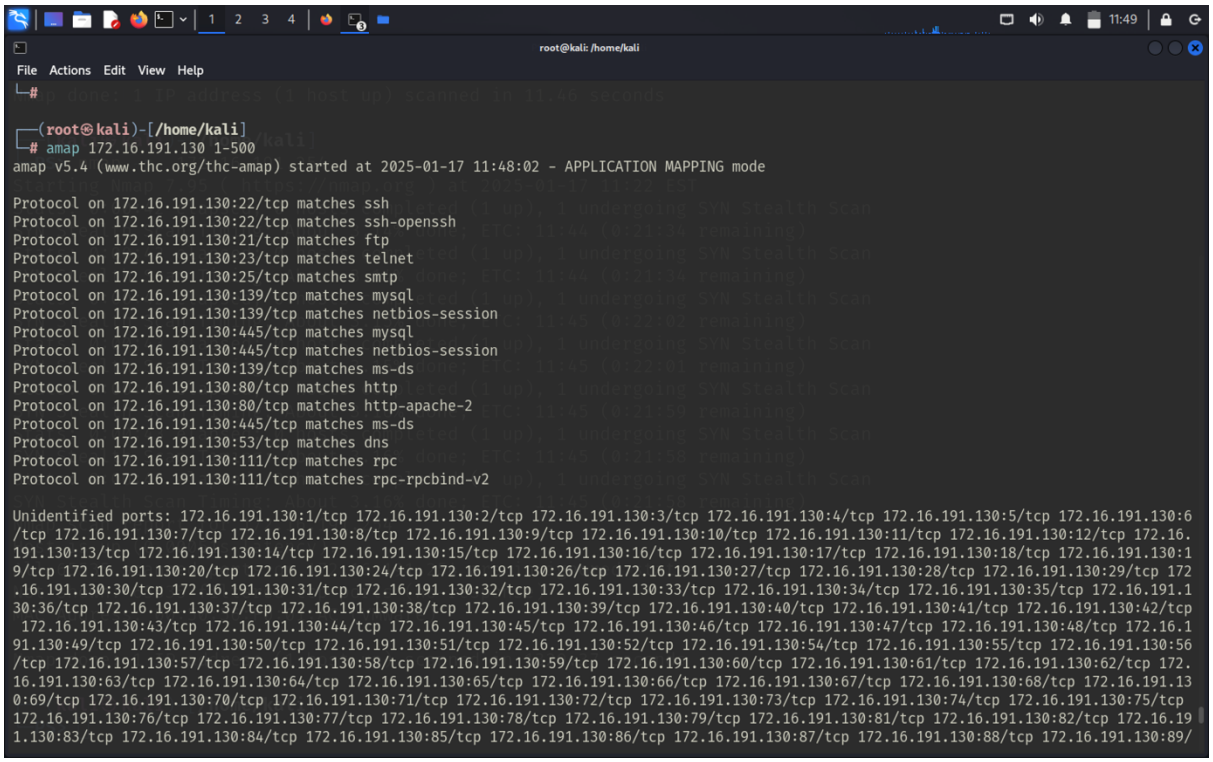
With `amap`:

```
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`.



Banner Grabbing

With `Netcat`:

```
nc -v 172.16.191.130 80
```

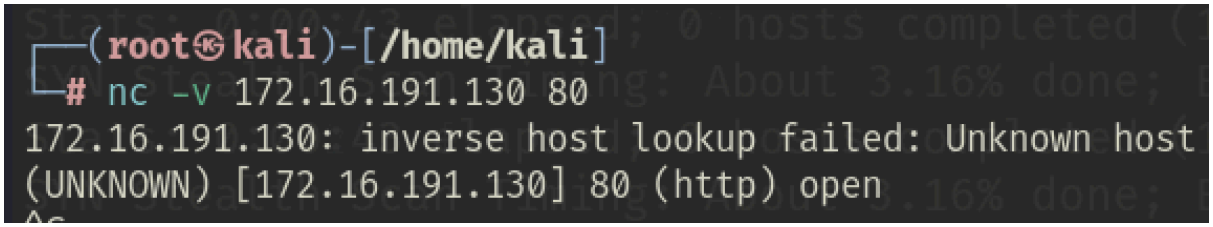
- Manually connect to an open port to retrieve service information.

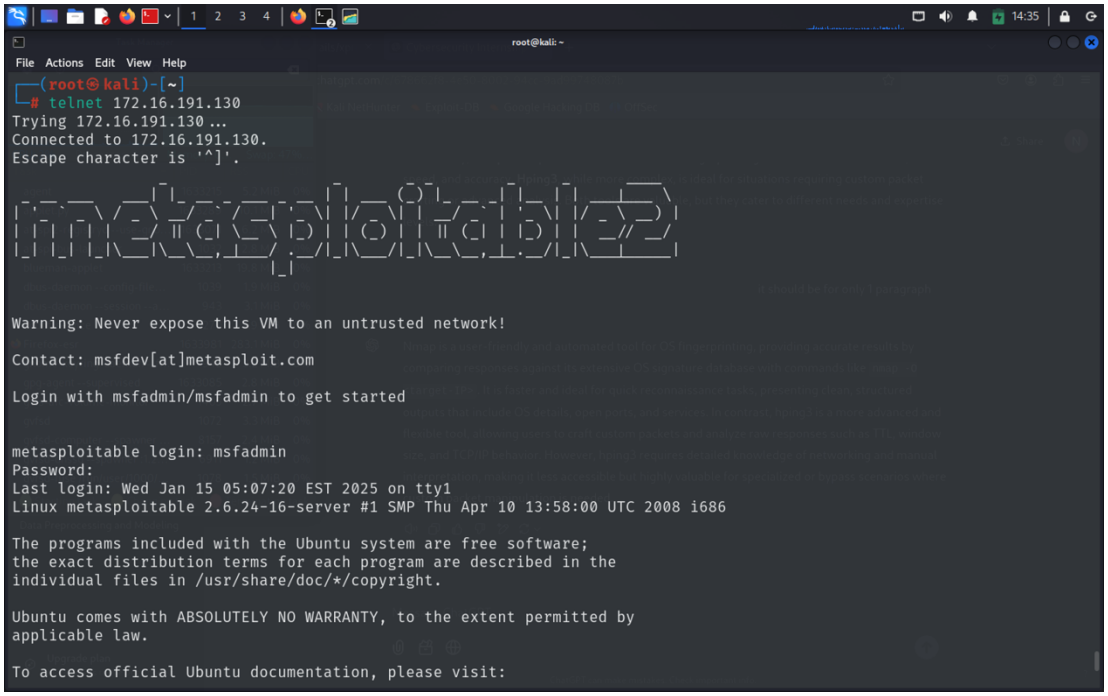
With `telnet`:

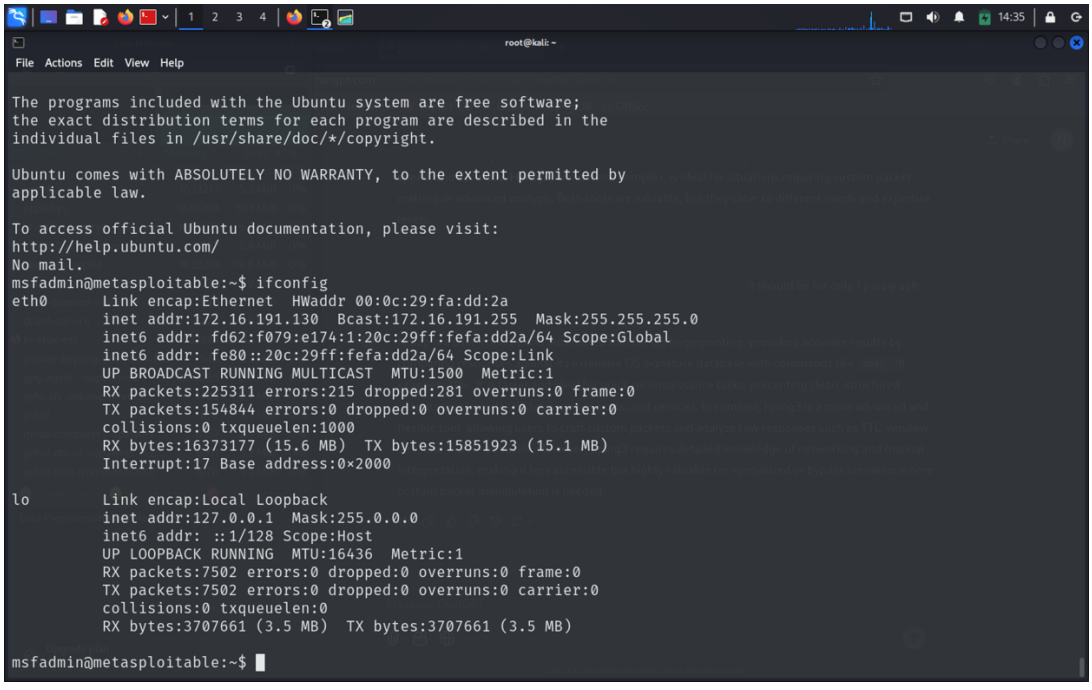
```
telnet 172.16.191.130 80
```

Comparison:

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







OS Fingerprinting

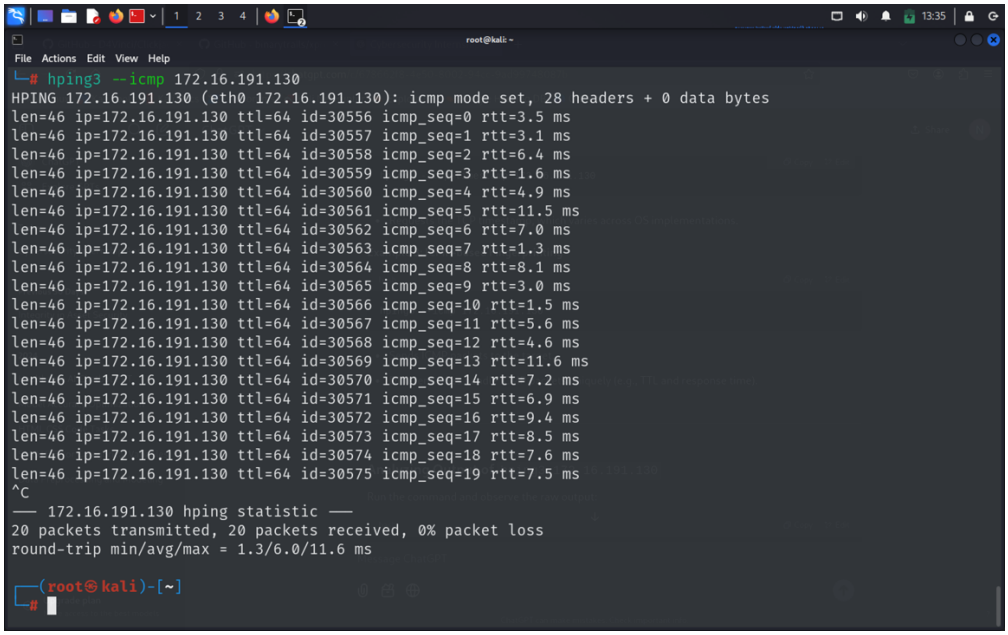
With `hping3`:

```
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.



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
Interface: eth0, type: EN10MB, MAC: 00:0c:29:17:47:fc, IPv4: 172.16.191.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
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
```

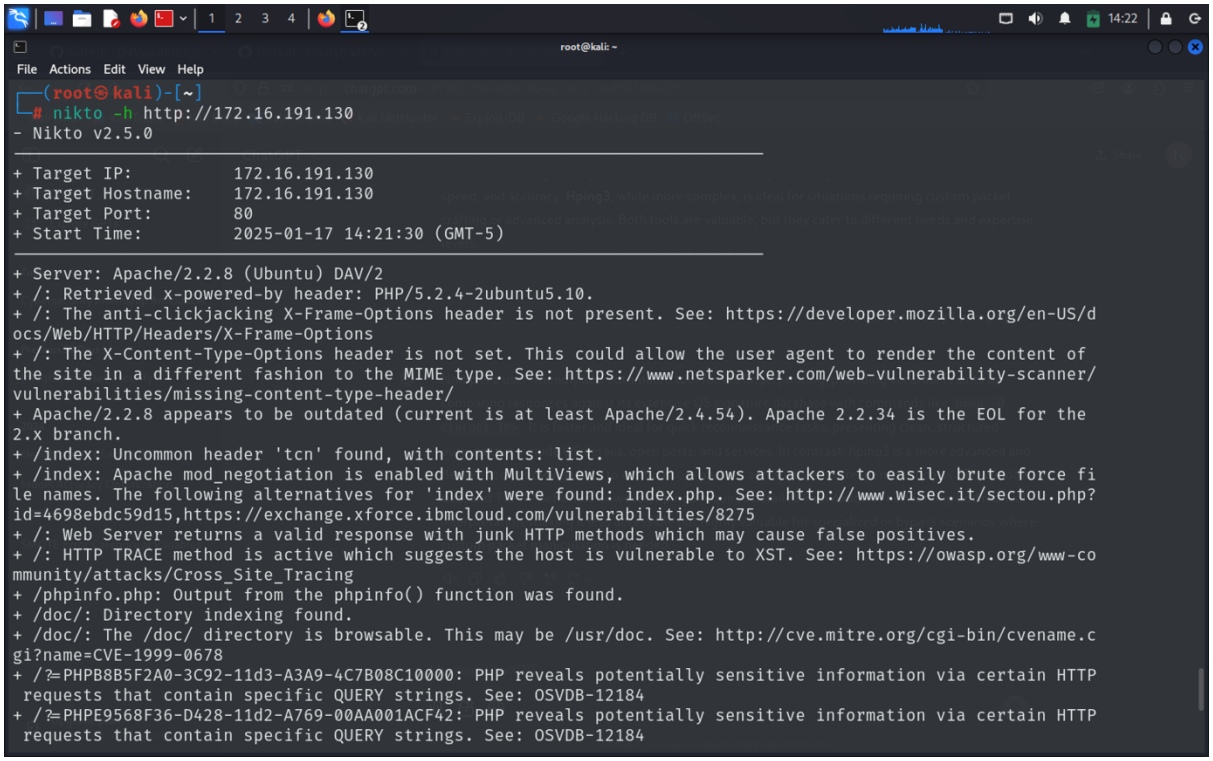
```
┌──(root㉿kali)-[~]
└─# ipcalc 172.16.191.130
Address:   172.16.191.130       10101100.00010000.10111111. 10000010
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
⇒
Network:   172.16.191.0/24      10101100.00010000.10111111. 00000000
HostMin:   172.16.191.1         10101100.00010000.10111111. 00000001
HostMax:   172.16.191.254       10101100.00010000.10111111. 11111110
Broadcast: 172.16.191.255       10101100.00010000.10111111. 11111111
Hosts/Net: 254                   Class B, Private Internet
```

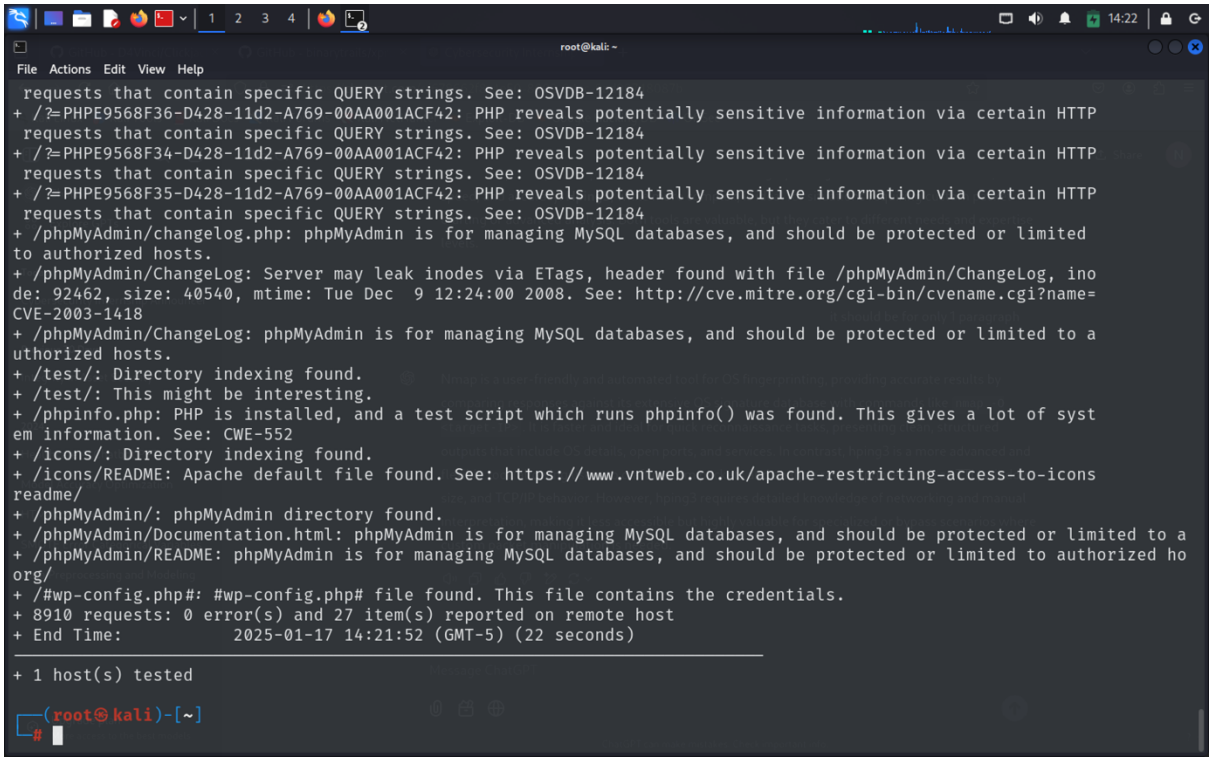
2. `Nikto` for Web Servers

- **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).



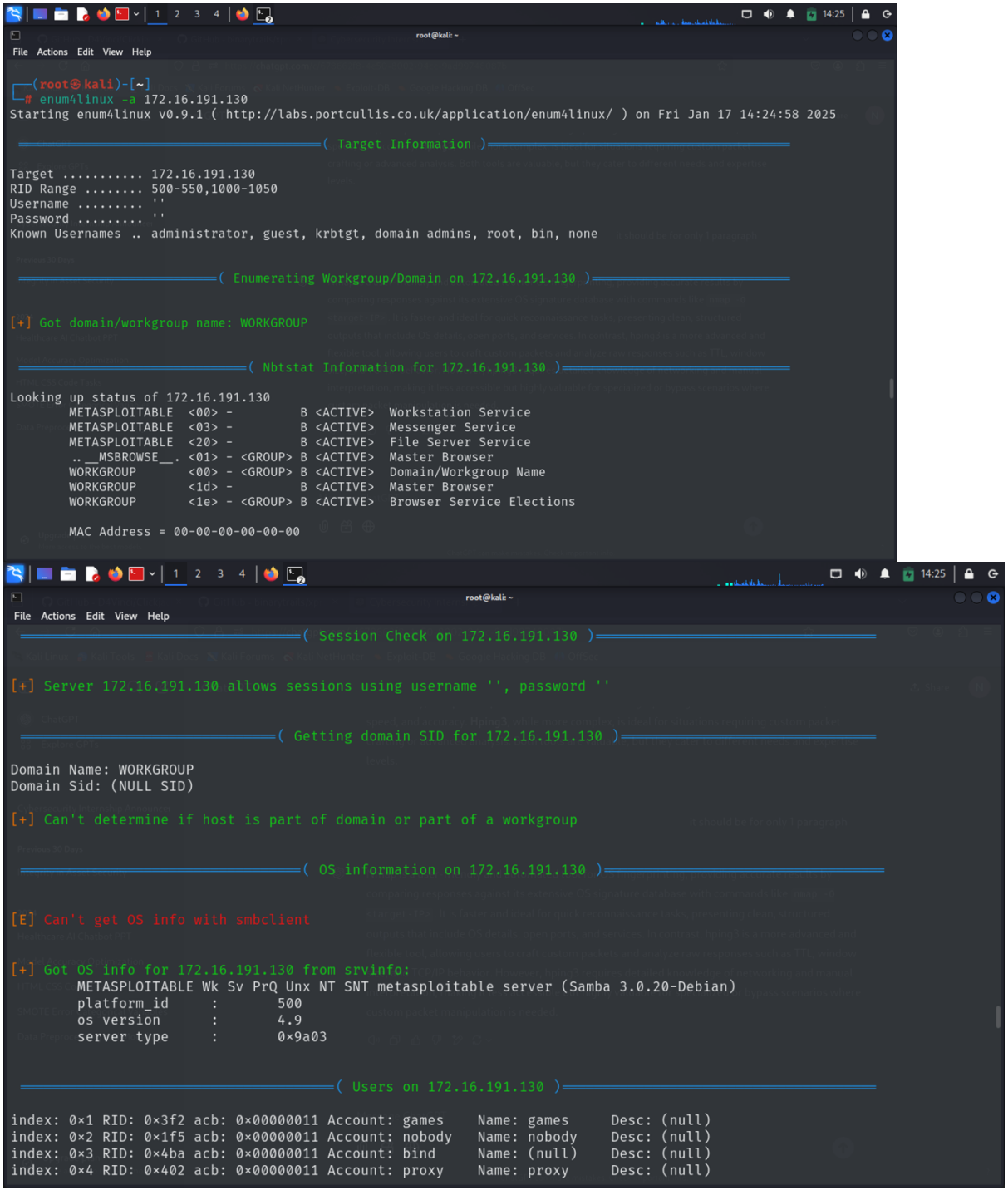


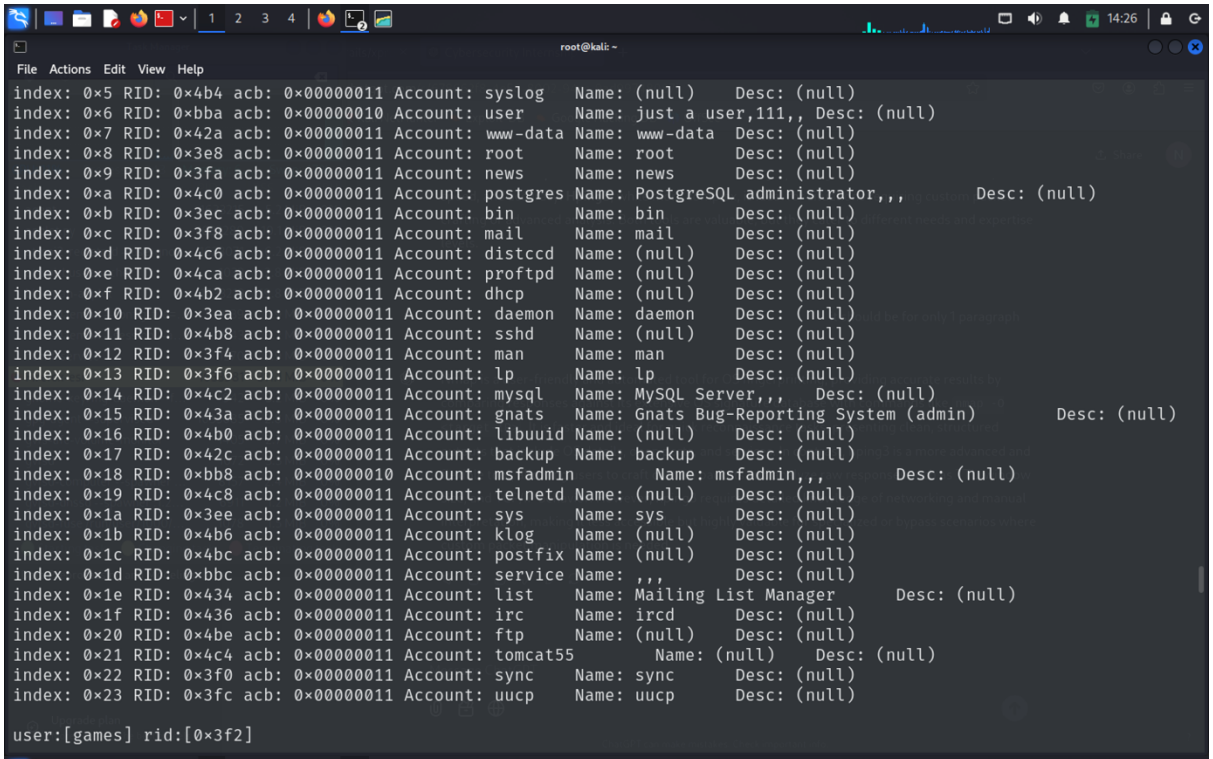
3. `Enum4linux` for SMB Services

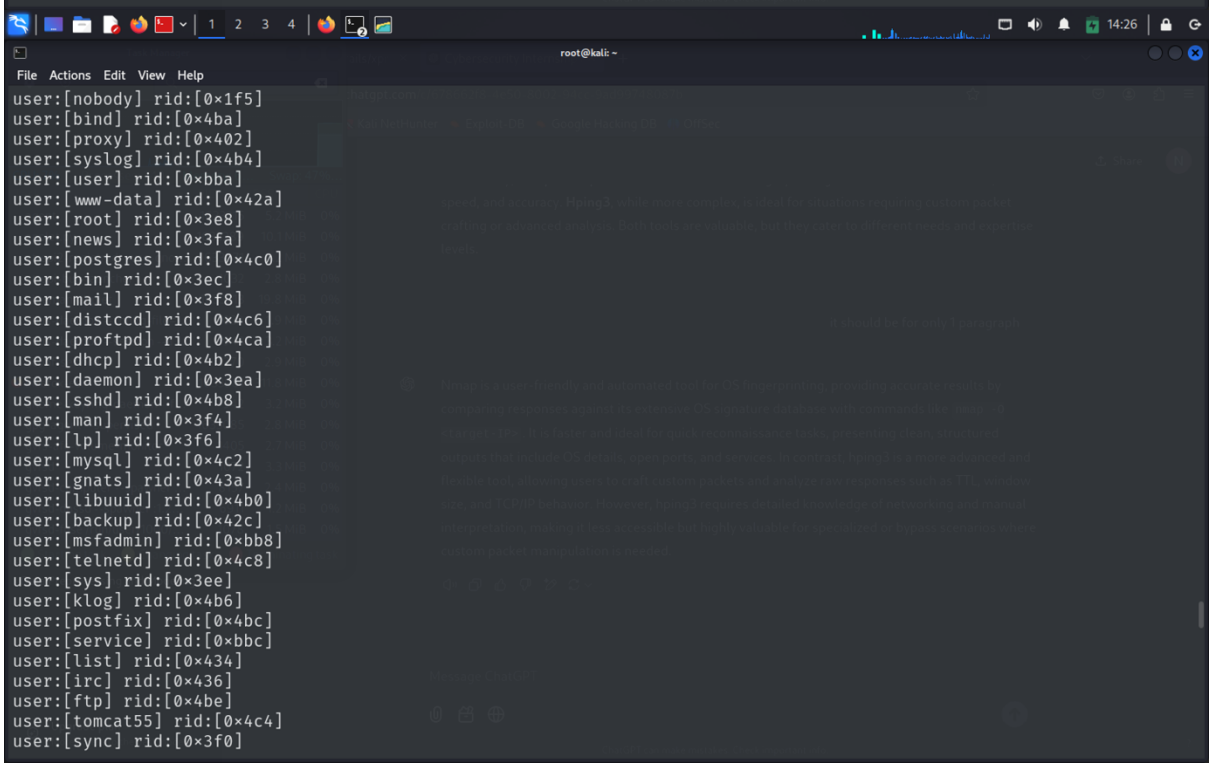
- **Purpose:** Enumerates information from SMB shares and services running on the target IP.
- **Command:**

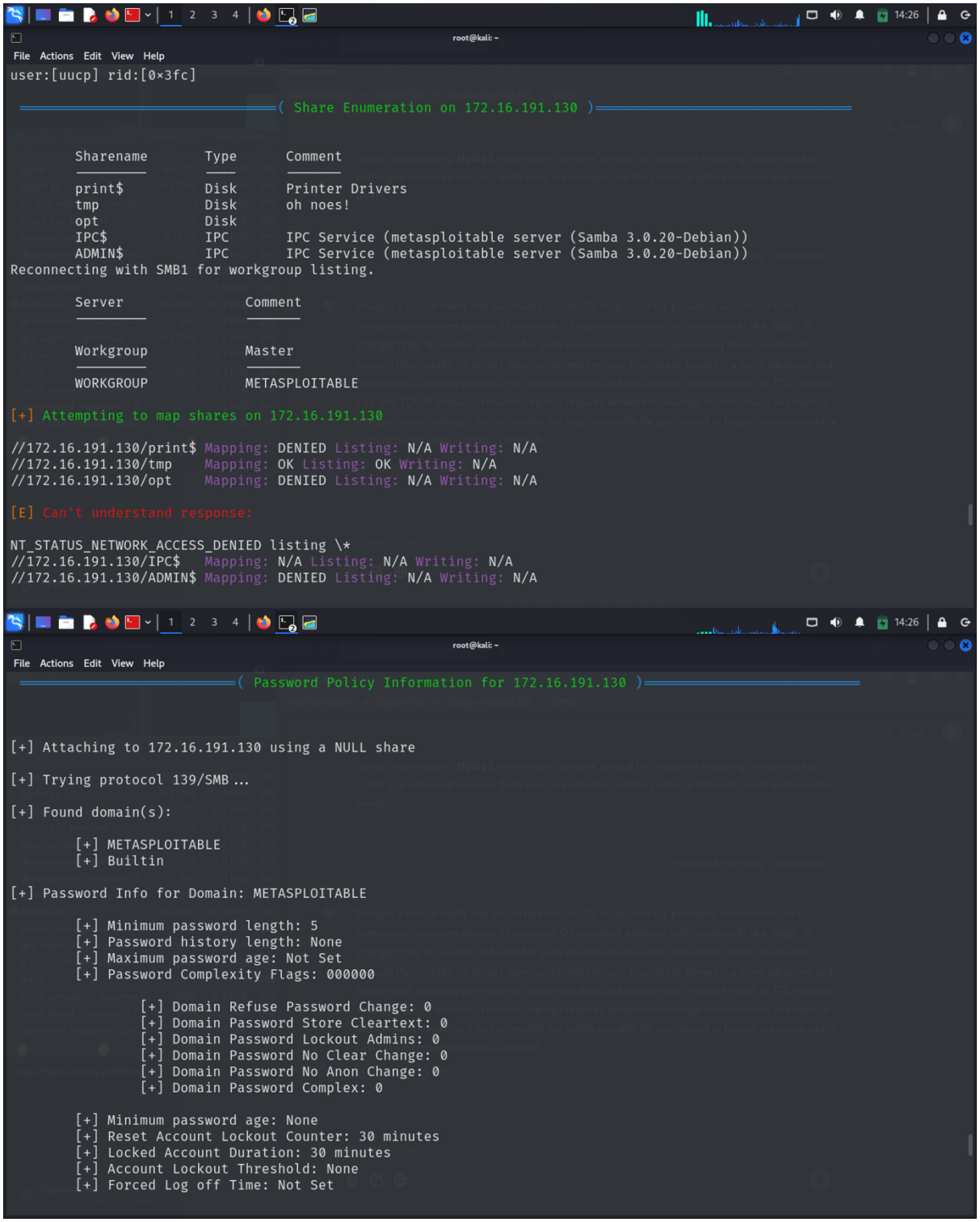
```
enum4linux -a 172.16.191.130
```

- **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).

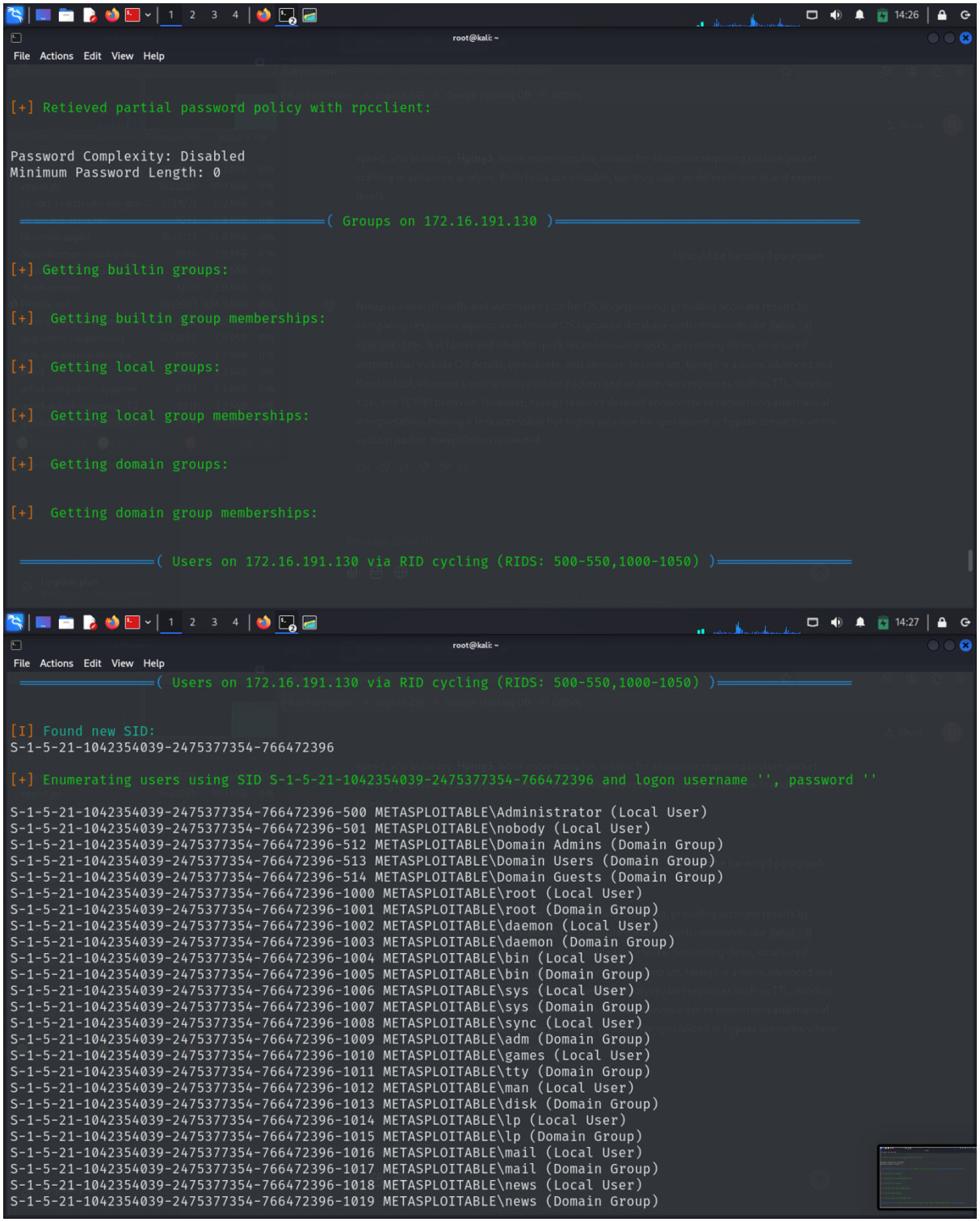


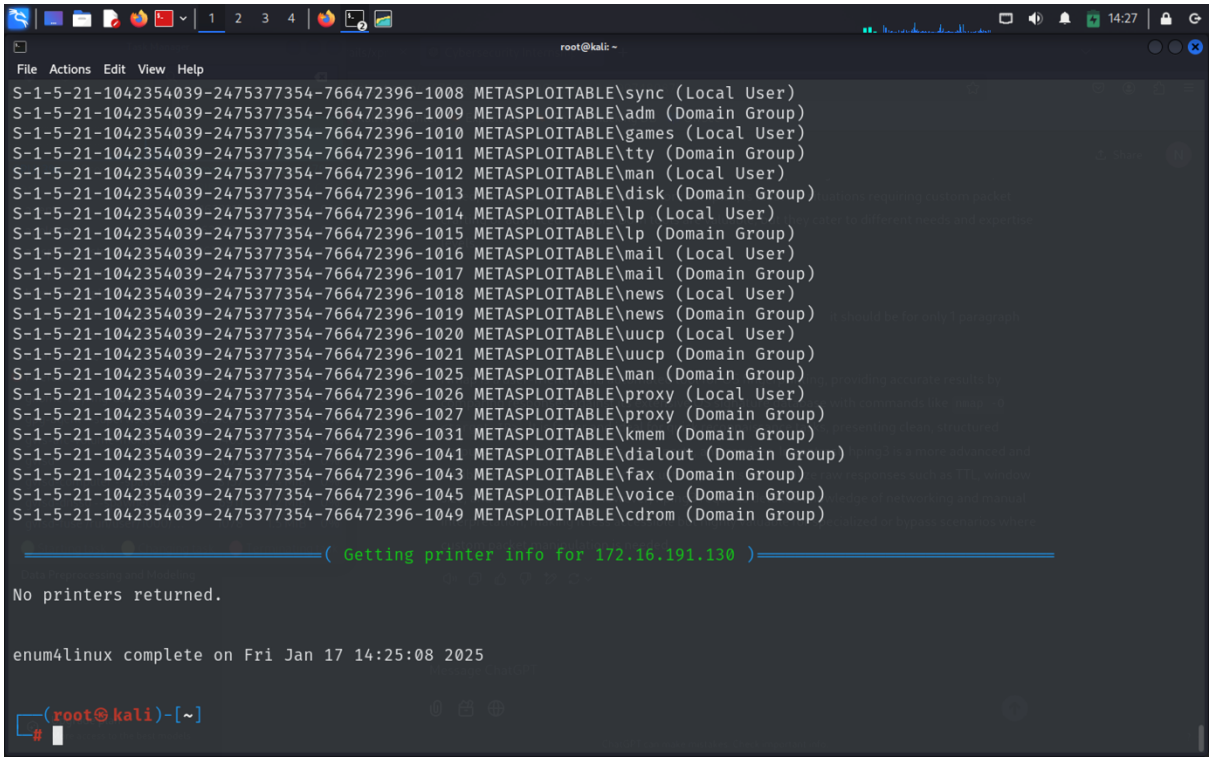

root@kali: ~
File Actions Edit View Help
index: 0×5 RID: 0×4b4 acb: 0×00000011 Account: syslog Name: (null) Desc: (null)
index: 0×6 RID: 0×bba acb: 0×00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0×7 RID: 0×42a acb: 0×00000011 Account: www-data Name: www-data Desc: (null)
index: 0×8 RID: 0×3e8 acb: 0×00000011 Account: root Name: root Desc: (null)
index: 0×9 RID: 0×3fa acb: 0×00000011 Account: news Name: news Desc: (null)
index: 0×a RID: 0×4c0 acb: 0×00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0×b RID: 0×3ec acb: 0×00000011 Account: bin Name: bin Desc: (null)
index: 0×c RID: 0×3f8 acb: 0×00000011 Account: mail Name: mail Desc: (null)
index: 0×d RID: 0×4c6 acb: 0×00000011 Account: distccd Name: (null) Desc: (null)
index: 0×e RID: 0×4ca acb: 0×00000011 Account: proftpd Name: (null) Desc: (null)
index: 0×f RID: 0×4b2 acb: 0×00000011 Account: dhcp Name: (null) Desc: (null)
index: 0×10 RID: 0×3ea acb: 0×00000011 Account: daemon Name: daemon Desc: (null)
index: 0×11 RID: 0×4b8 acb: 0×00000011 Account: sshd Name: (null) Desc: (null)
index: 0×12 RID: 0×3f4 acb: 0×00000011 Account: man Name: man Desc: (null)
index: 0×13 RID: 0×3f6 acb: 0×00000011 Account: lp Name: lp Desc: (null)
index: 0×14 RID: 0×4c2 acb: 0×00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0×15 RID: 0×43a acb: 0×00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0×16 RID: 0×4b0 acb: 0×00000011 Account: libuuid Name: (null) Desc: (null)
index: 0×17 RID: 0×42c acb: 0×00000011 Account: backup Name: backup Desc: (null)
index: 0×18 RID: 0×bb8 acb: 0×00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0×19 RID: 0×4c8 acb: 0×00000011 Account: telnetd Name: (null) Desc: (null)
index: 0×1a RID: 0×3ee acb: 0×00000011 Account: sys Name: sys Desc: (null)
index: 0×1b RID: 0×4b6 acb: 0×00000011 Account: klog Name: (null) Desc: (null)
index: 0×1c RID: 0×4bc acb: 0×00000011 Account: postfix Name: (null) Desc: (null)
index: 0×1d RID: 0×bbc acb: 0×00000011 Account: service Name: ,,, Desc: (null)
index: 0×1e RID: 0×434 acb: 0×00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0×1f RID: 0×436 acb: 0×00000011 Account: irc Name: ircd Desc: (null)
index: 0×20 RID: 0×4be acb: 0×00000011 Account: ftp Name: (null) Desc: (null)
index: 0×21 RID: 0×4c4 acb: 0×00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0×22 RID: 0×3f0 acb: 0×00000011 Account: sync Name: sync Desc: (null)
index: 0×23 RID: 0×3fc acb: 0×00000011 Account: uucp Name: uucp Desc: (null)
user:[games] rid:[0×3f2]


root@kali: ~
File Actions Edit View Help
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]


root@kali: ~
File Actions Edit View Help
user:[uucp] rid:[0×3fc]
(Share Enumeration on 172.16.191.130)
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 METASPLOITABLE
[+] 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

root@kali: ~
File Actions Edit View Help
(Password Policy Information for 172.16.191.130)
[+] Attaching to 172.16.191.130 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE
[+] 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


root@kali: ~
File Actions Edit View Help
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
(Groups on 172.16.191.130)
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
(Users on 172.16.191.130 via RID cycling (RIDS: 500-550,1000-1050))
root@kali: ~
File Actions Edit View Help
(Users on 172.16.191.130 via RID cycling (RIDS: 500-550,1000-1050))
[I] 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)



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

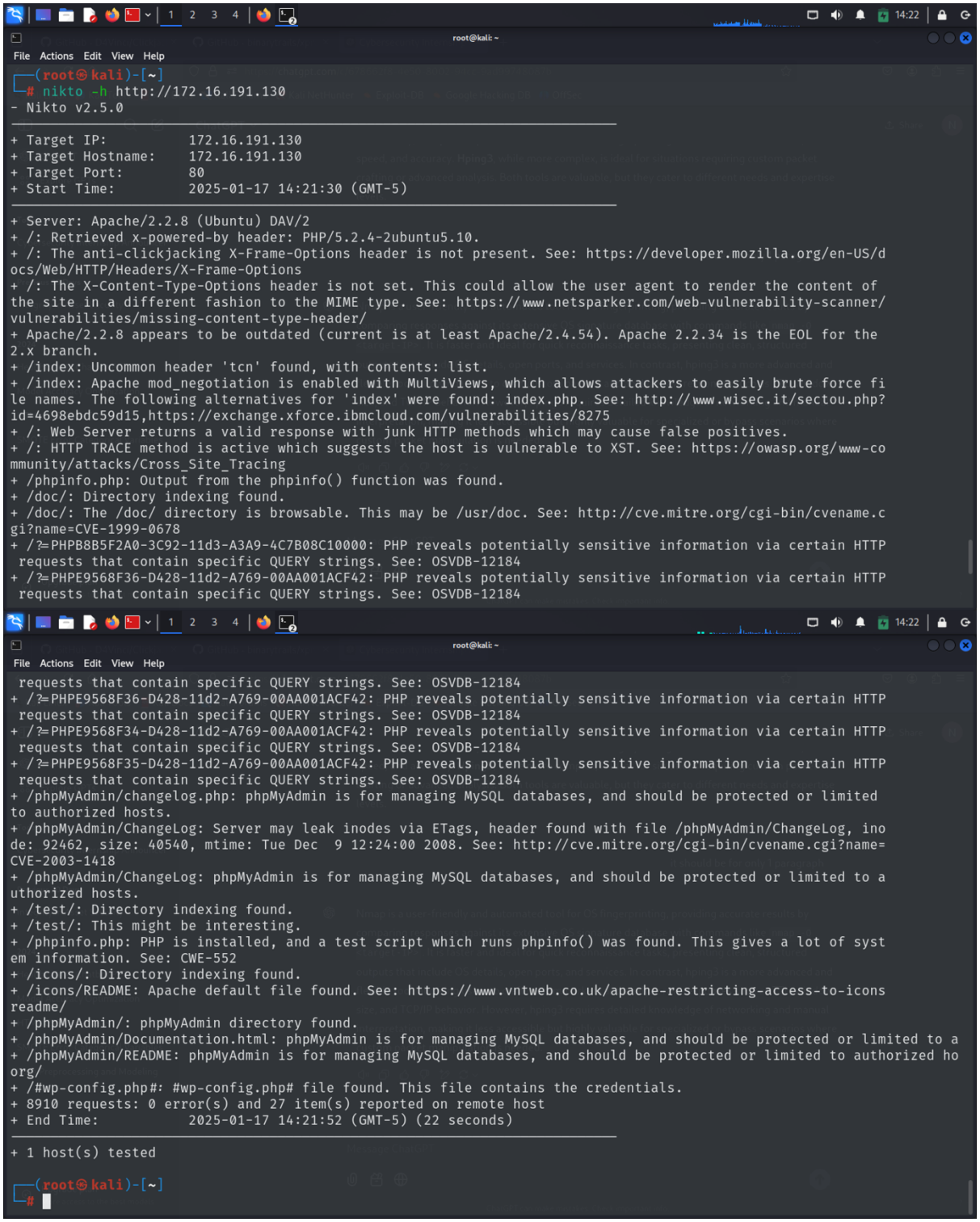
With `Nikto`:

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

- `Nikto` scans for known vulnerabilities on web servers.

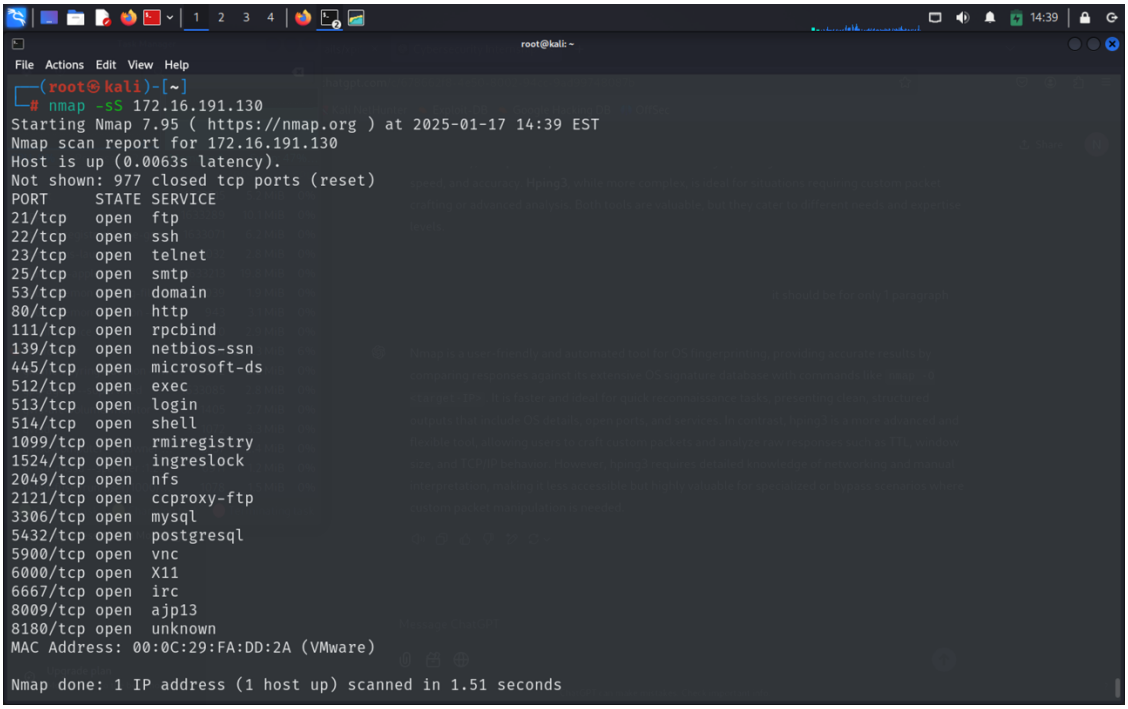
Comparison:

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

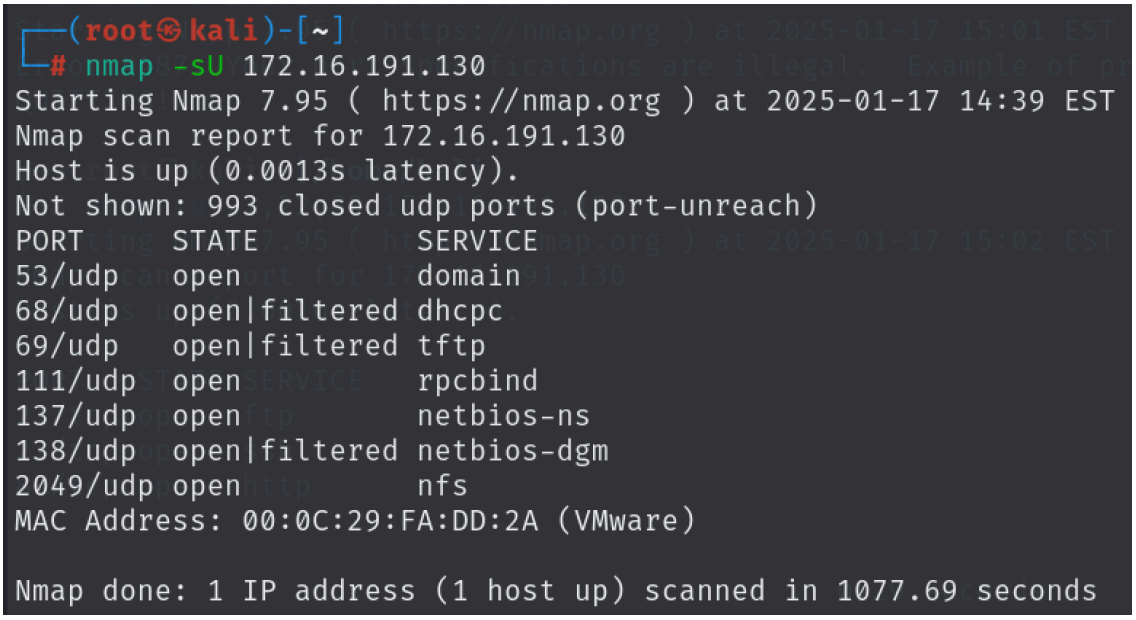

root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
nikto -h http://172.16.191.130
- Nikto v2.5.0
+ Target IP: 172.16.191.130
+ Target Hostname: 172.16.191.130
+ Target Port: 80
+ Start Time: 2025-01-17 14:21:30 (GMT-5)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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
root@kali: ~
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 authorized 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-iconsreadme/
+ /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 hoorg/
+ /#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

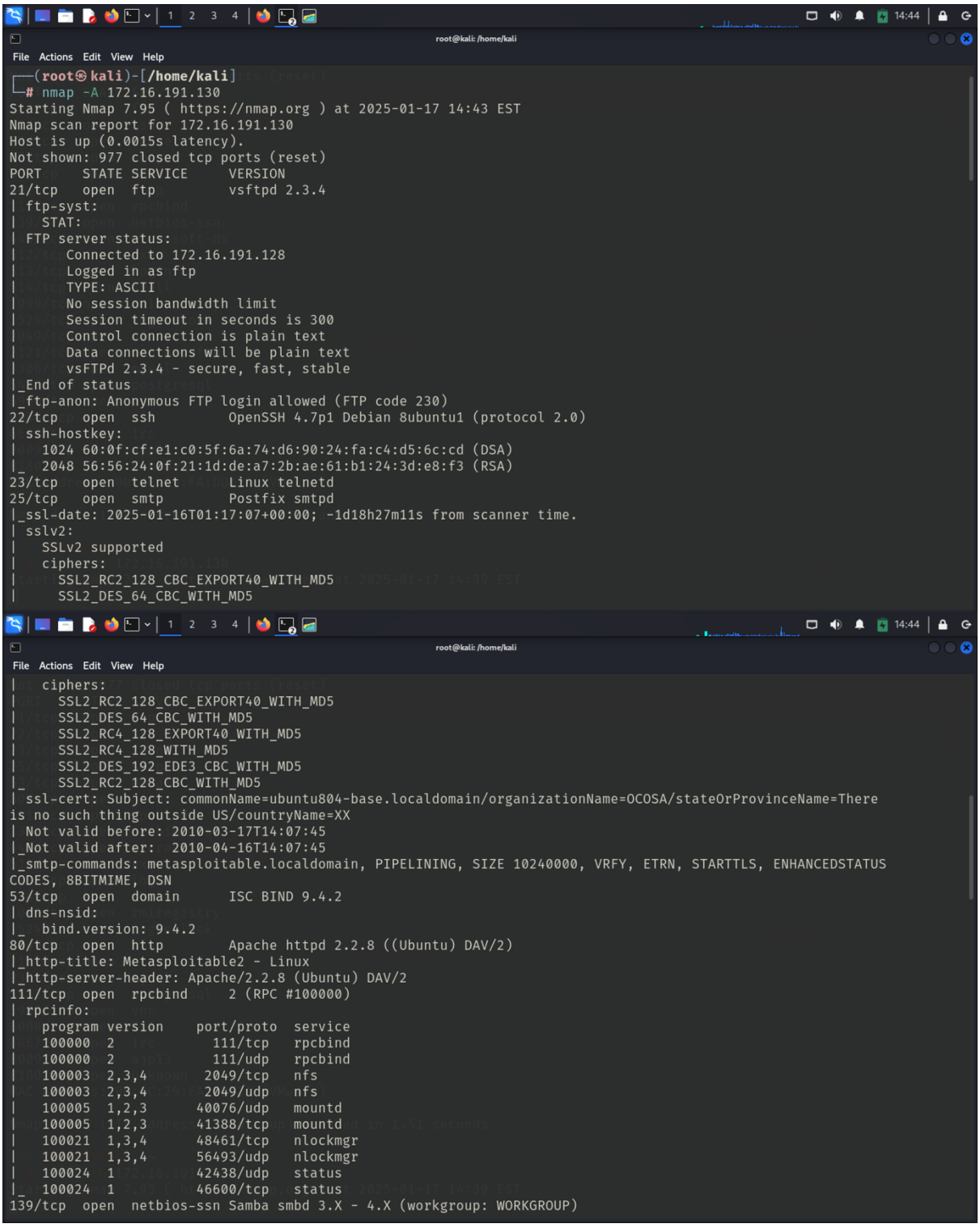
- **Analyzed specific findings and recorded results for different scan types:**
    1. SYN scan (`-sS`)

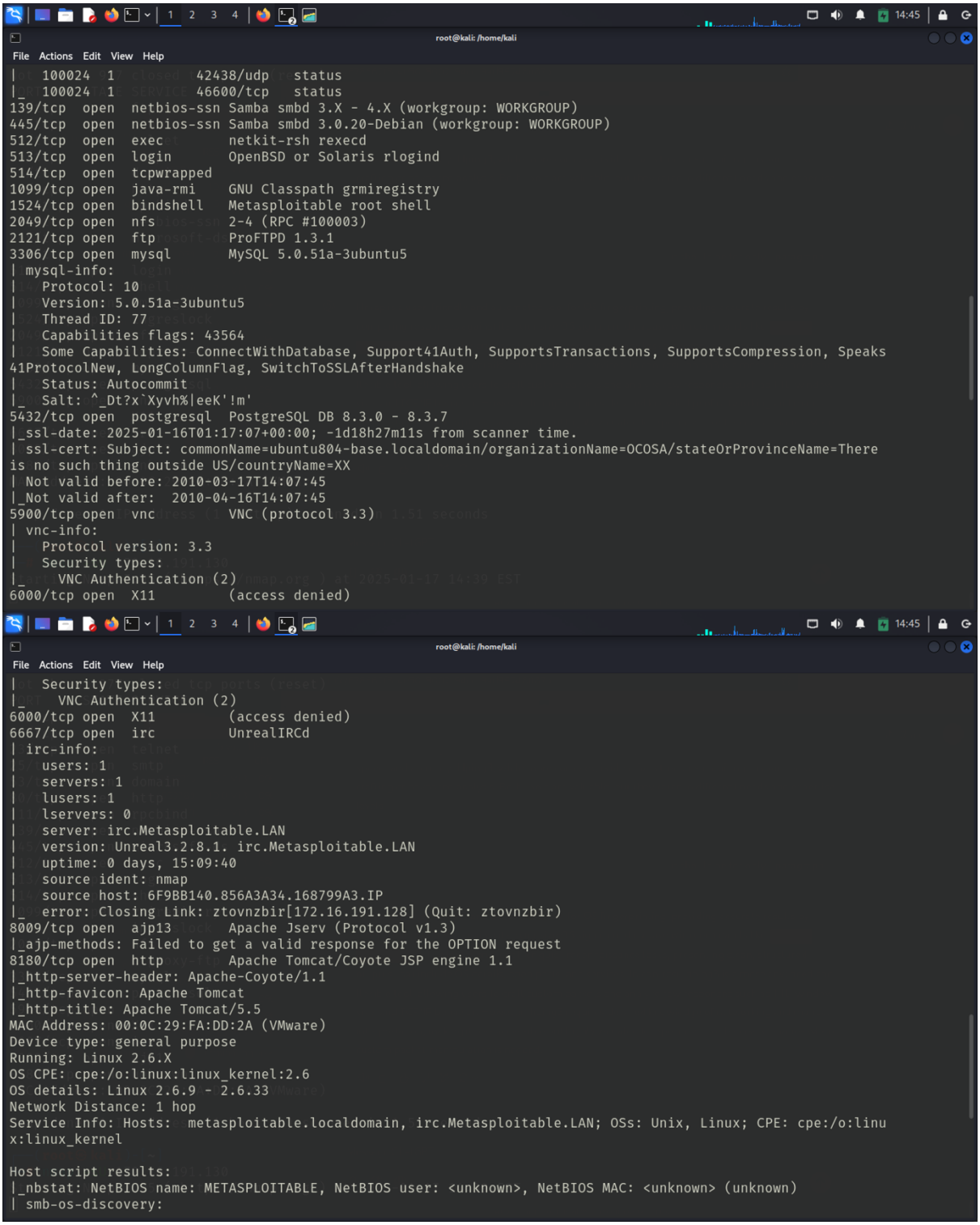


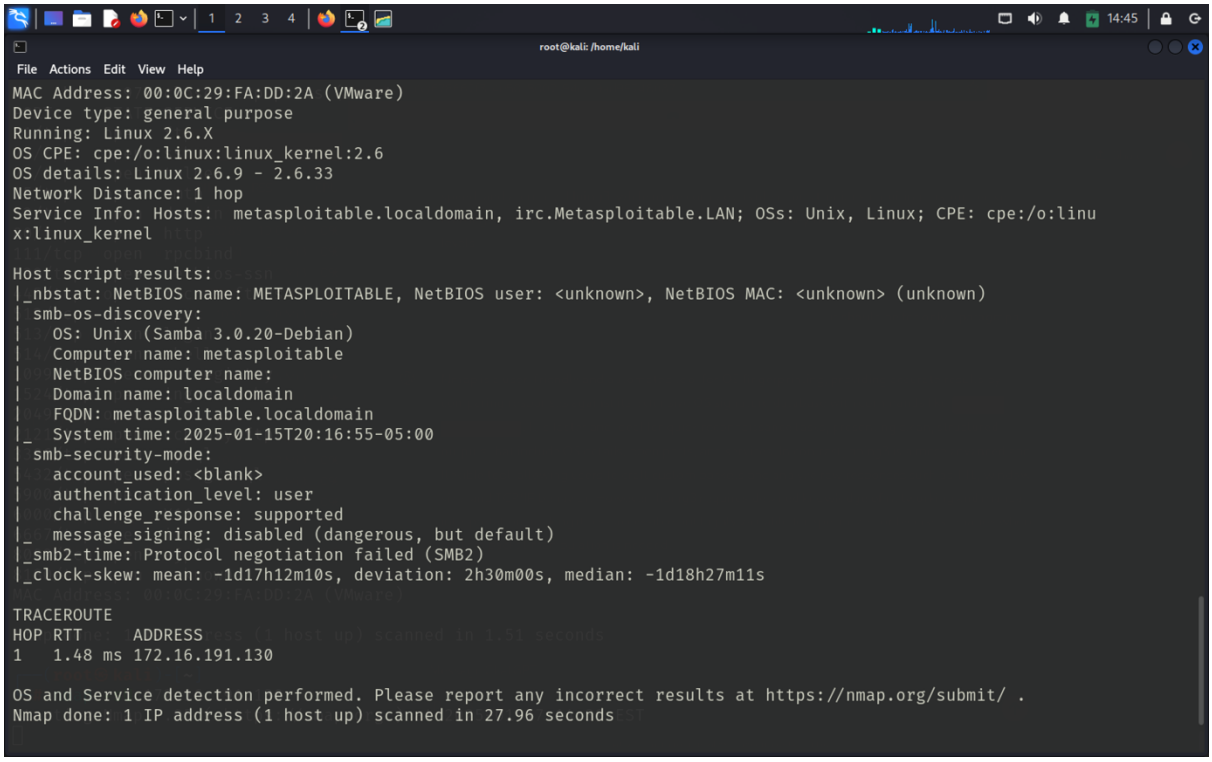
    2. UDP scan (`-sU`)



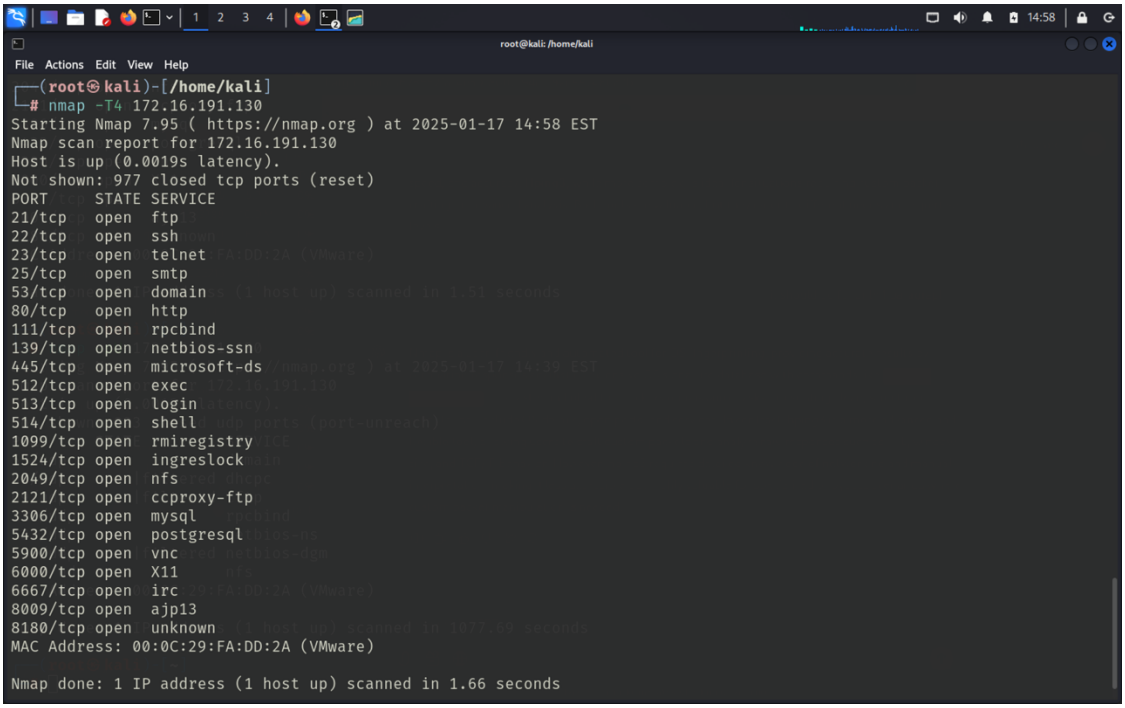
3. Aggressive scan (`-A`)




root@kali: /home/kali
File Actions Edit View Help
| 100024 1 42438/udp status
|_ 100024 1 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 rlogind
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
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 77
| Capabilities flags: 43564
| Some Capabilities: ConnectWithDatabase, Support41Auth, SupportsTransactions, SupportsCompression, Speaks
41ProtocolNew, LongColumnFlag, SwitchToSSLAfterHandshake
| Status: Autocommit
|_ Salt: ^_Dt?x`Xyvh%|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 vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11 (access denied)
root@kali: /home/kali
File Actions Edit View Help
| 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, 15:09:40
| source ident: nmap
| 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
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:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:



4. Timing optimization scan (`-T4`)



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