Practical 3:

Aim: Practical on enumerating host, port, and service scanning

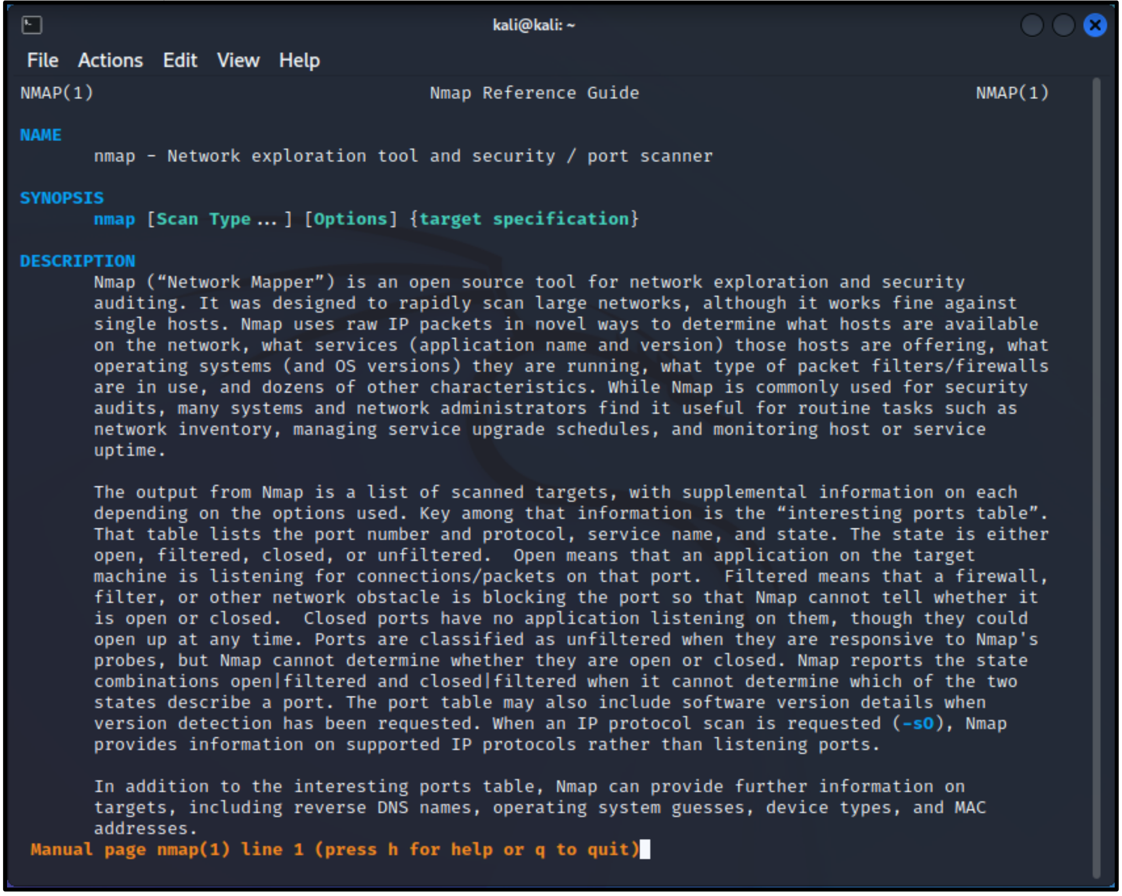
Note:

- The tool being used for port scanning, data enumeration, and service scanning is NMAP.
- Nmap is a network scanner created by Gordon Lyon.
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
- Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

Port Scanning:

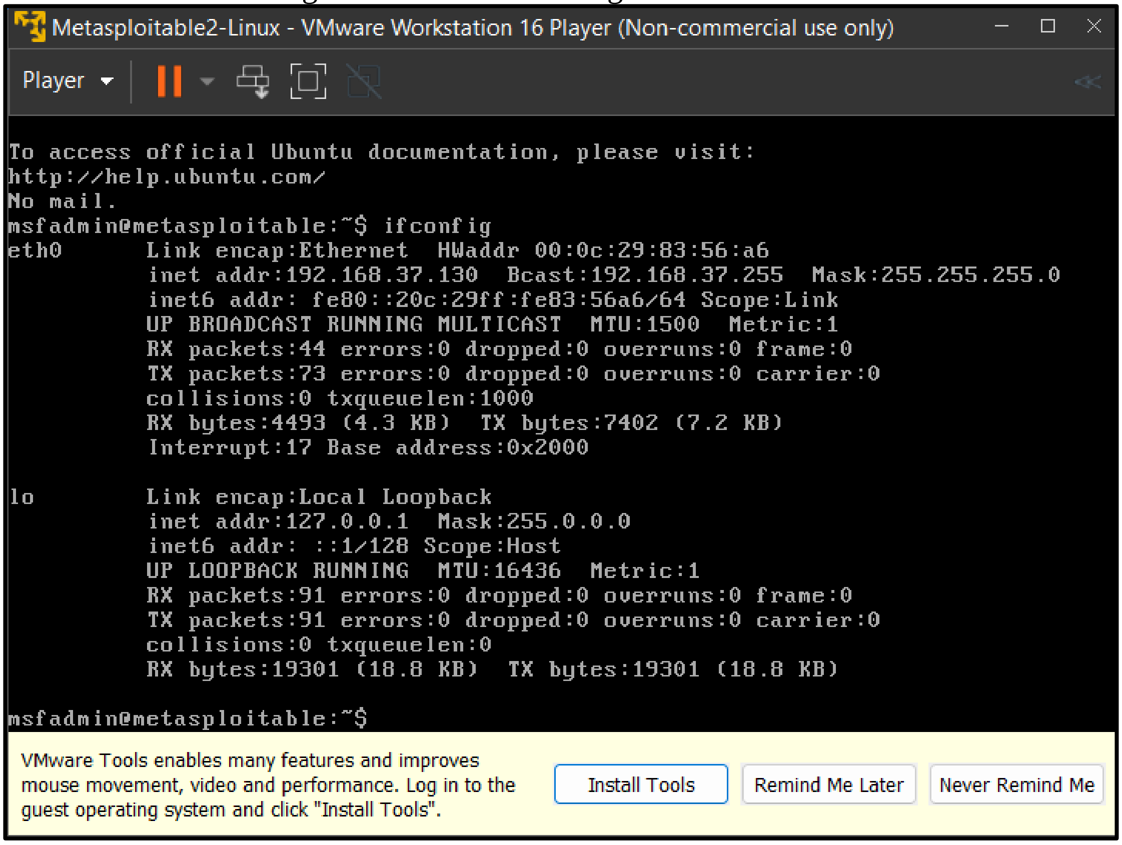
- A port scanner is an application designed to probe a server or host for open ports.
- Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

1. To see the help/ manual of Nmap we can use the command "man nmap" (OS used kali linux).



```
NMAP(1)                        Nmap Reference Guide                       NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type ... ] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration and security
       auditing. It was designed to rapidly scan large networks, although it works fine against
       single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available
       on the network, what services (application name and version) those hosts are offering, what
       operating systems (and OS versions) they are running, what type of packet filters/firewalls
       are in use, and dozens of other characteristics. While Nmap is commonly used for security
       audits, many systems and network administrators find it useful for routine tasks such as
       network inventory, managing service upgrade schedules, and monitoring host or service
       uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on each
       depending on the options used. Key among that information is the "interesting ports table".
       That table lists the port number and protocol, service name, and state. The state is either
       open, filtered, closed, or unfiltered.  Open means that an application on the target
       machine is listening for connections/packets on that port.  Filtered means that a firewall,
       filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it
       is open or closed.  Closed ports have no application listening on them, though they could
       open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's
       probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state
       combinations open|filtered and closed|filtered when it cannot determine which of the two
       states describe a port. The port table may also include software version details when
       version detection has been requested. When an IP protocol scan is requested (-sO), Nmap
       provides information on supported IP protocols rather than listening ports.

       In addition to the interesting ports table, Nmap can provide further information on
       targets, including reverse DNS names, operating system guesses, device types, and MAC
       addresses.
 Manual page nmap(1) line 1 (press h for help or q to quit)
```

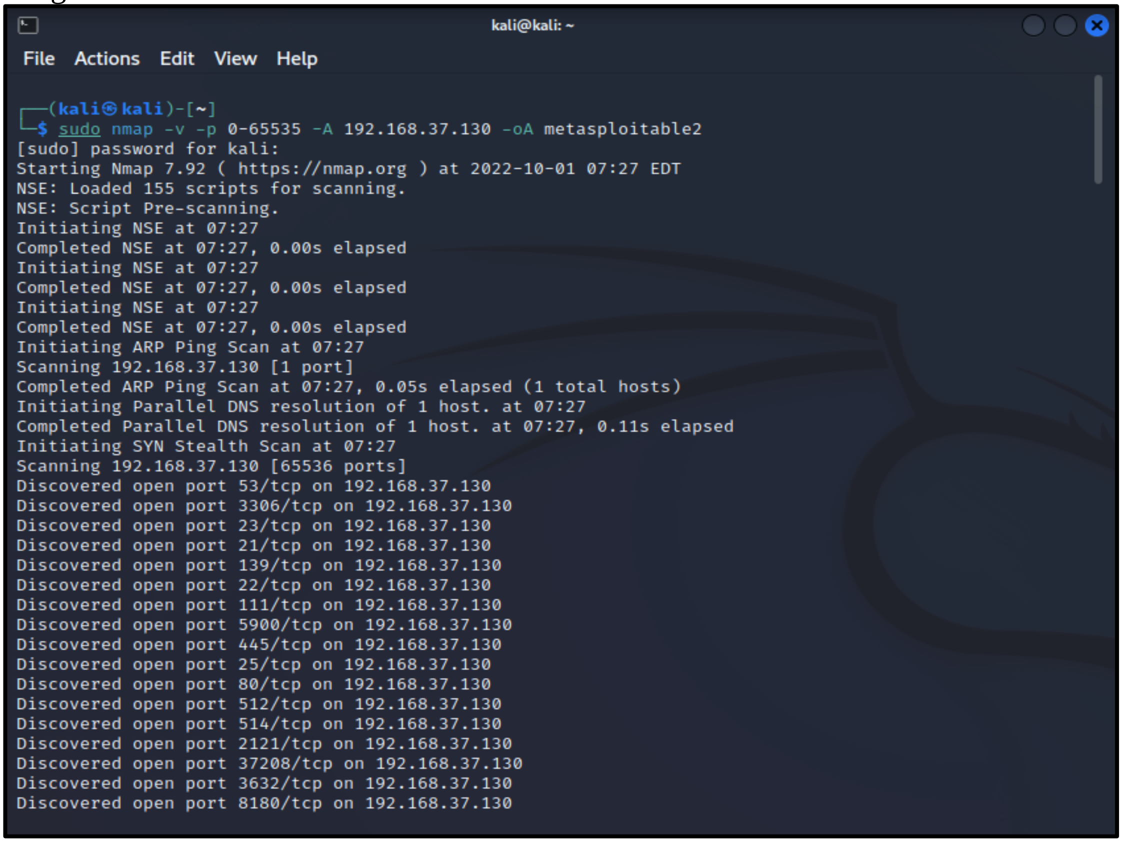
2. You will need to run the target machine metasploitable2 and check the ip address of the machine using the command “ifconfig”.


Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player

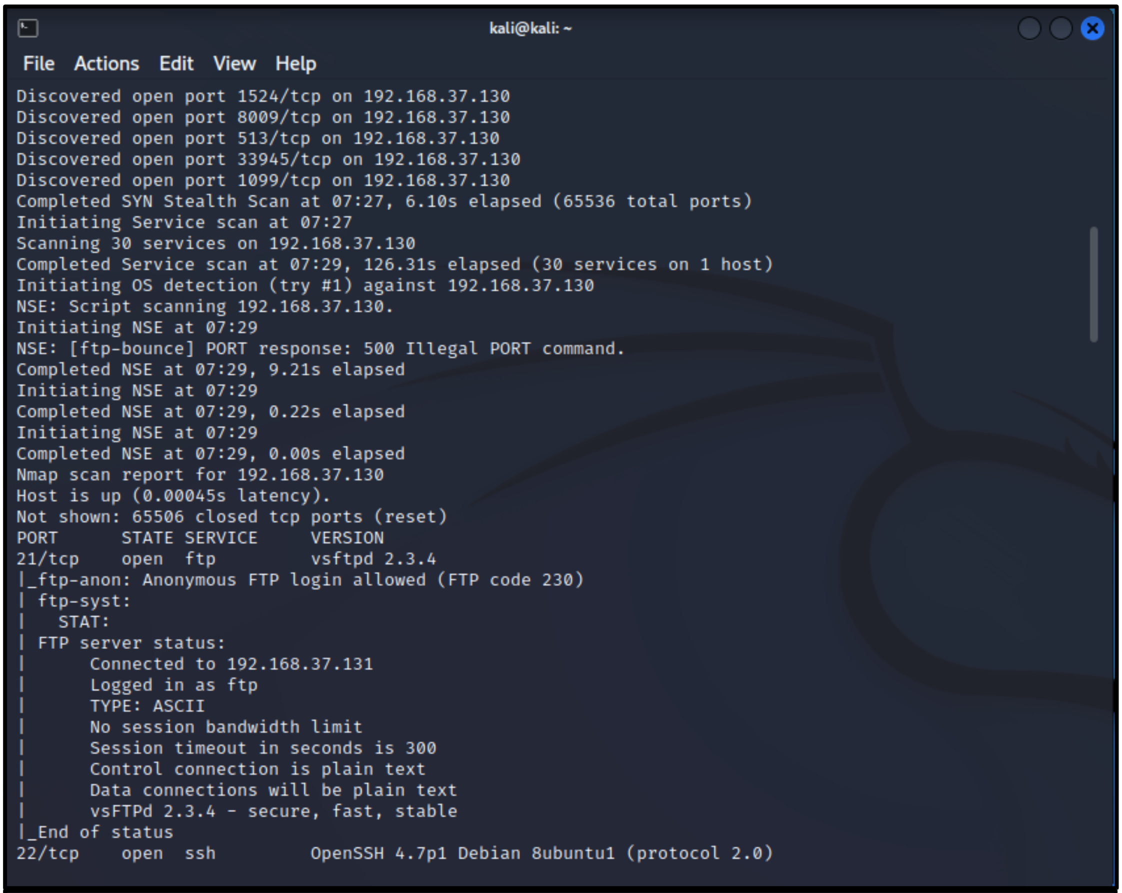
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:83:56:a6
          inet addr:192.168.37.130  Bcast:192.168.37.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe83:56a6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:44 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4493 (4.3 KB)  TX bytes:7402 (7.2 KB)
          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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

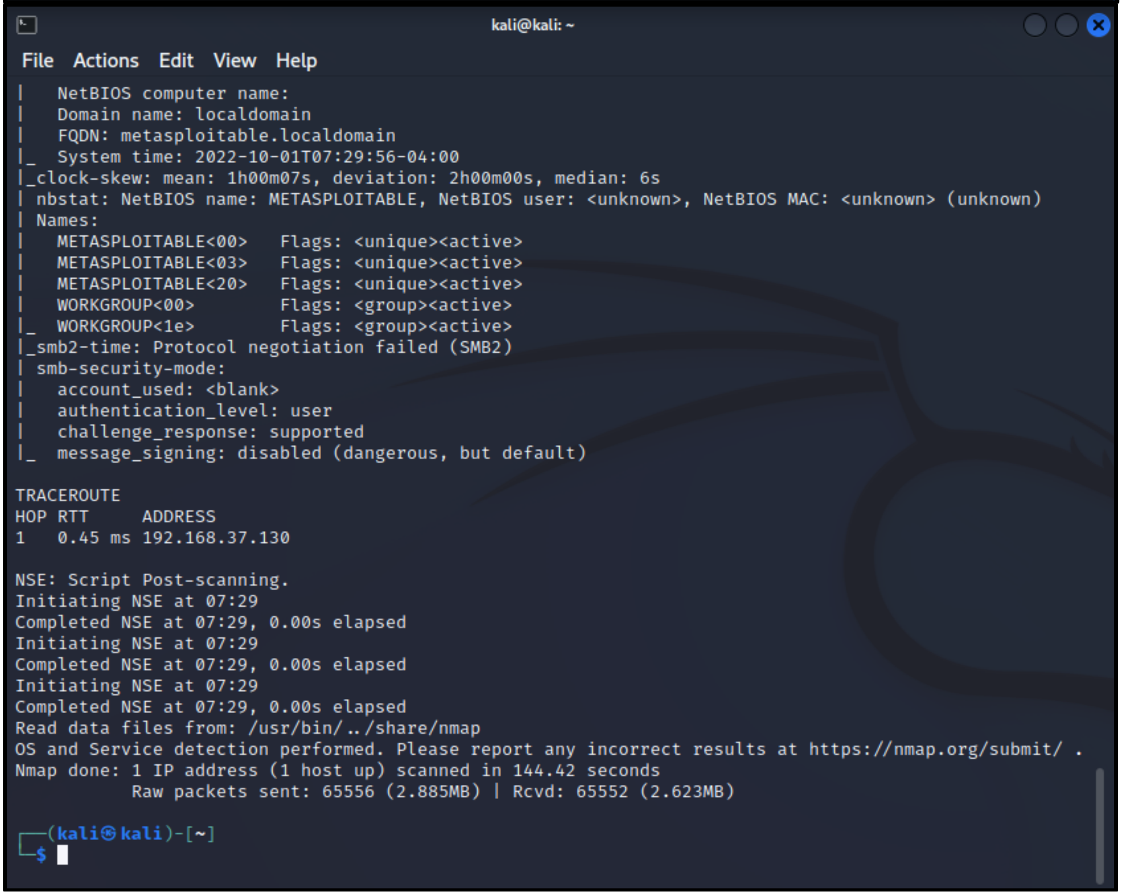
3. Using Kali perform port scanning using nmap on the target machine by running the given command shown below.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -p 0-65535 -A 192.168.37.130 -oA metasploitable2
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:27 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating NSE at 07:27
Completed NSE at 07:27, 0.00s elapsed
Initiating ARP Ping Scan at 07:27
Scanning 192.168.37.130 [1 port]
Completed ARP Ping Scan at 07:27, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:27
Completed Parallel DNS resolution of 1 host. at 07:27, 0.11s elapsed
Initiating SYN Stealth Scan at 07:27
Scanning 192.168.37.130 [65536 ports]
Discovered open port 53/tcp on 192.168.37.130
Discovered open port 3306/tcp on 192.168.37.130
Discovered open port 23/tcp on 192.168.37.130
Discovered open port 21/tcp on 192.168.37.130
Discovered open port 139/tcp on 192.168.37.130
Discovered open port 22/tcp on 192.168.37.130
Discovered open port 111/tcp on 192.168.37.130
Discovered open port 5900/tcp on 192.168.37.130
Discovered open port 445/tcp on 192.168.37.130
Discovered open port 25/tcp on 192.168.37.130
Discovered open port 80/tcp on 192.168.37.130
Discovered open port 512/tcp on 192.168.37.130
Discovered open port 514/tcp on 192.168.37.130
Discovered open port 2121/tcp on 192.168.37.130
Discovered open port 37208/tcp on 192.168.37.130
Discovered open port 3632/tcp on 192.168.37.130
Discovered open port 8180/tcp on 192.168.37.130
```

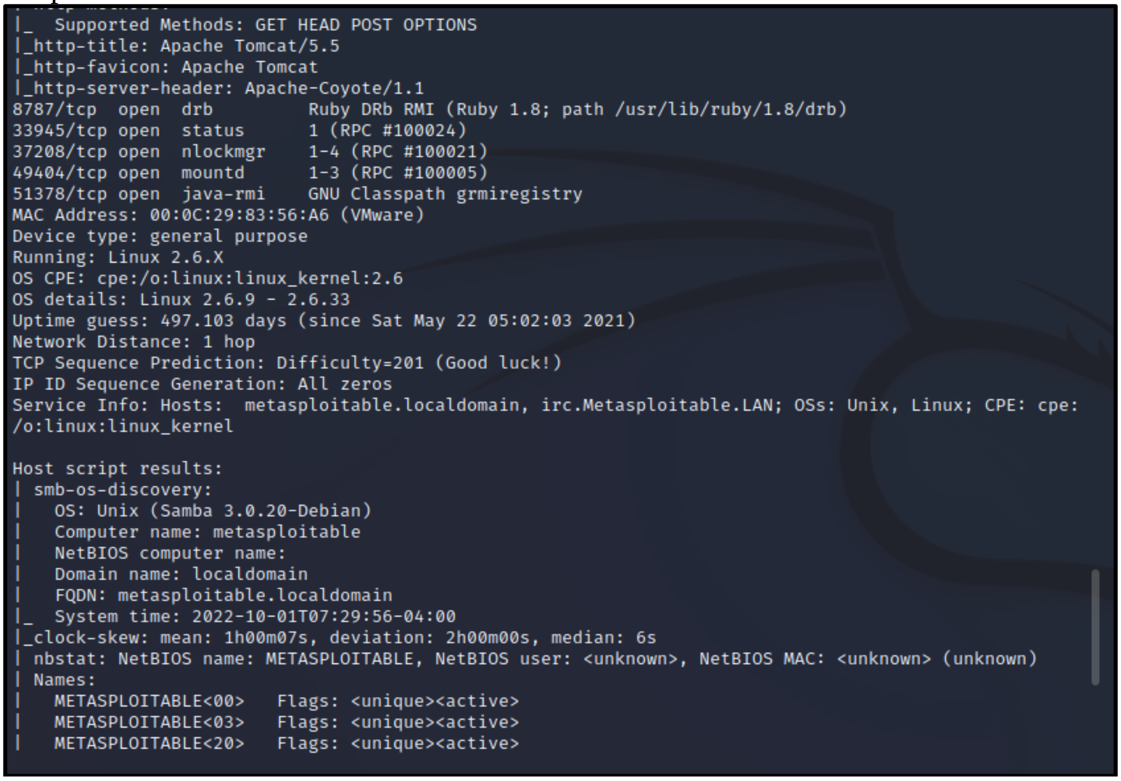


```
Discovered open port 1524/tcp on 192.168.37.130
Discovered open port 8009/tcp on 192.168.37.130
Discovered open port 513/tcp on 192.168.37.130
Discovered open port 33945/tcp on 192.168.37.130
Discovered open port 1099/tcp on 192.168.37.130
Completed SYN Stealth Scan at 07:27, 6.10s elapsed (65536 total ports)
Initiating Service scan at 07:27
Scanning 30 services on 192.168.37.130
Completed Service scan at 07:29, 126.31s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.37.130
NSE: Script scanning 192.168.37.130.
Initiating NSE at 07:29
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 07:29, 9.21s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.22s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Nmap scan report for 192.168.37.130
Host is up (0.00045s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.37.131
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```



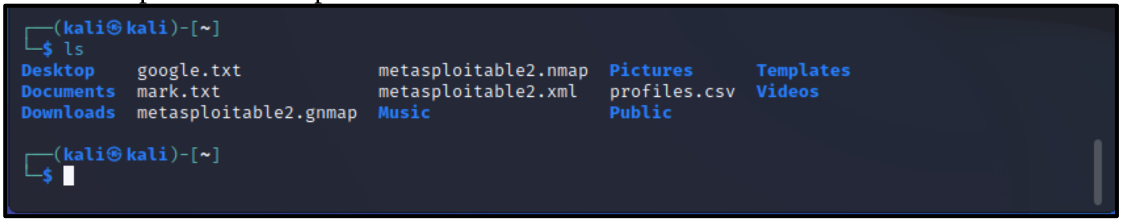
```
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-01T07:29:56-04:00
|_clock-skew: mean: 1h00m07s, deviation: 2h00m00s, median: 6s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.37.130

NSE: Script Post-scanning.
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Initiating NSE at 07:29
Completed NSE at 07:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 144.42 seconds
           Raw packets sent: 65556 (2.885MB) | Rcvd: 65552 (2.623MB)

┌──(kali㉿kali)-[~]
└─$ █
```

4. You will be able to identify the operating system and the target machine's open port details.



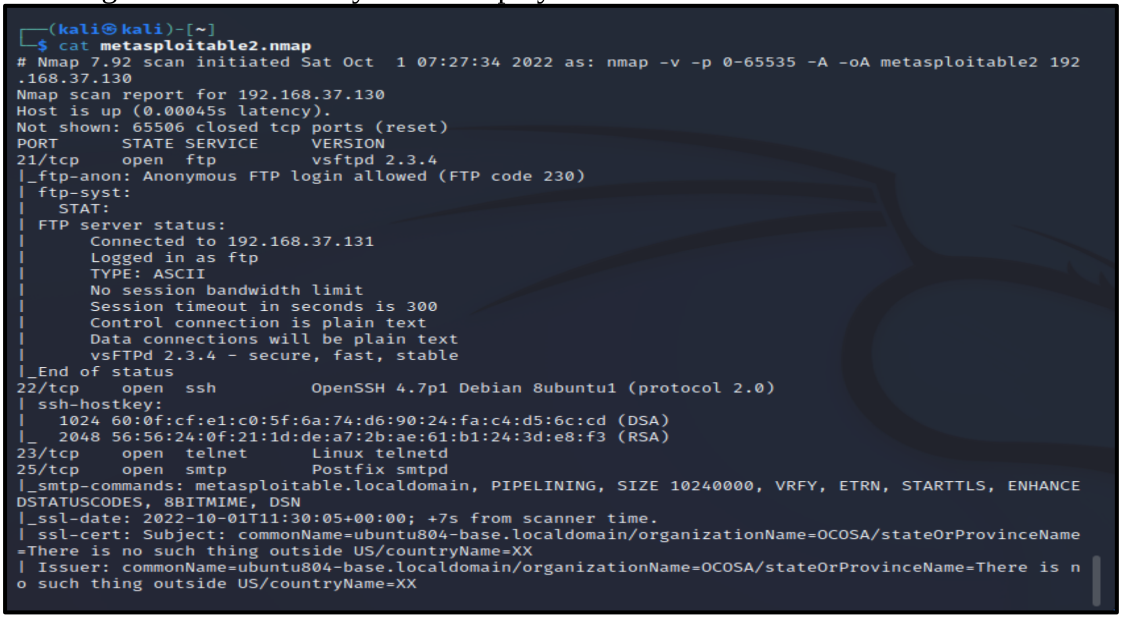
```
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33945/tcp open  status      1 (RPC #100024)
37208/tcp open  nlockmgr    1-4 (RPC #100021)
49404/tcp open  mountd      1-3 (RPC #100005)
51378/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 00:0C:29:83:56:A6 (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
Uptime guess: 497.103 days (since Sat May 22 05:02:03 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:
/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-01T07:29:56-04:00
|_clock-skew: mean: 1h00m07s, deviation: 2h00m00s, median: 6s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
```

5. View the output file created which stores all the scan results in "metasploitable.nmap".

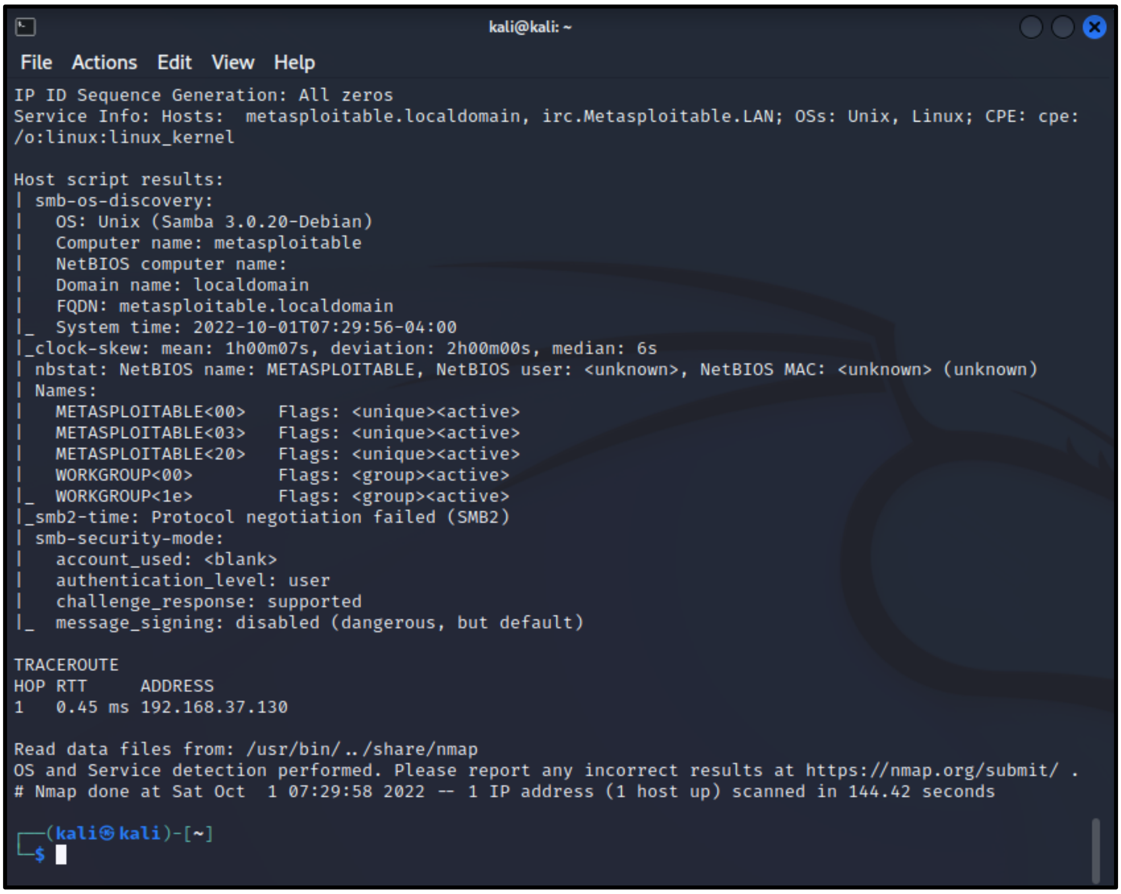


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    google.txt             metasploitable2.nmap  Pictures      Templates
Documents  mark.txt               metasploitable2.xml   profiles.csv  Videos
Downloads  metasploitable2.gnmap  Music                 Public

┌──(kali㉿kali)-[~]
└─$ 
```

6. Using the cat command you can display the contents of the file.



```
┌──(kali㉿kali)-[~]
└─$ cat metasploitable2.nmap
# Nmap 7.92 scan initiated Sat Oct  1 07:27:34 2022 as: nmap -v -p 0-65535 -A -oA metasploitable2 192
.168.37.130
Nmap scan report for 192.168.37.130
Host is up (0.00045s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.37.131
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2022-10-01T11:30:05+00:00; +7s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName
=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is n
o such thing outside US/countryName=XX
```

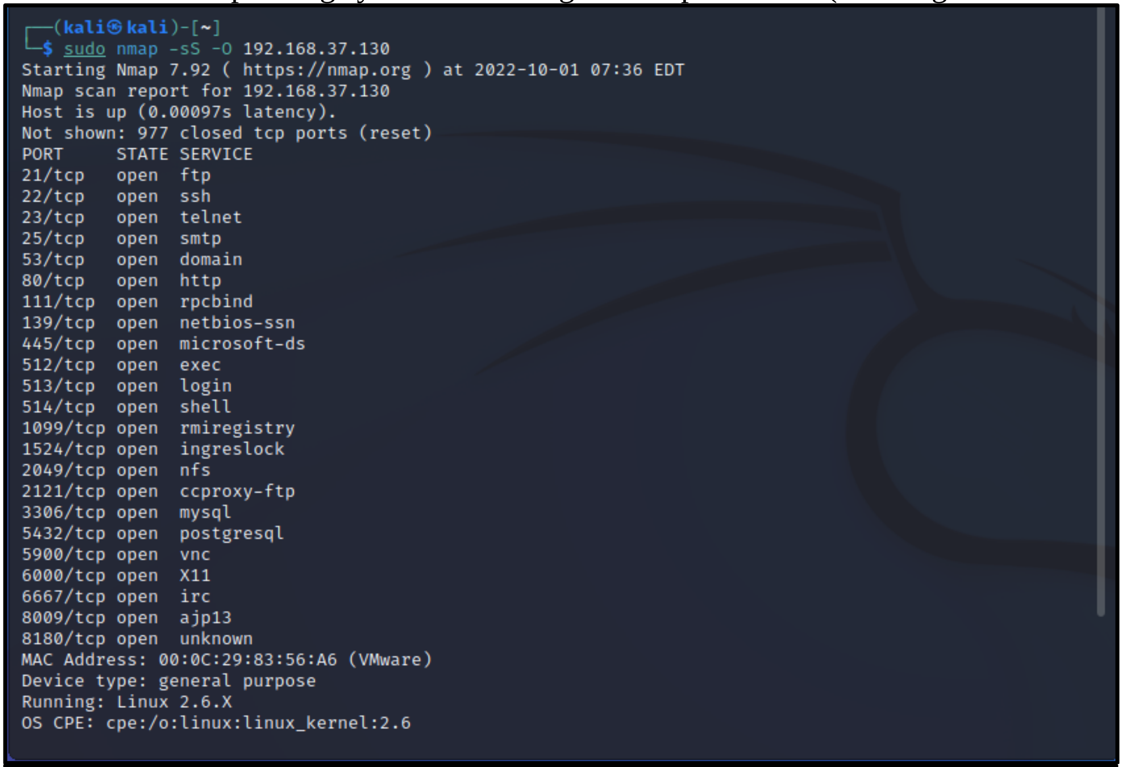


```
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:
/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-10-01T07:29:56-04:00
|_clock-skew: mean: 1h00m07s, deviation: 2h00m00s, median: 6s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.37.130

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct  1 07:29:58 2022 -- 1 IP address (1 host up) scanned in 144.42 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

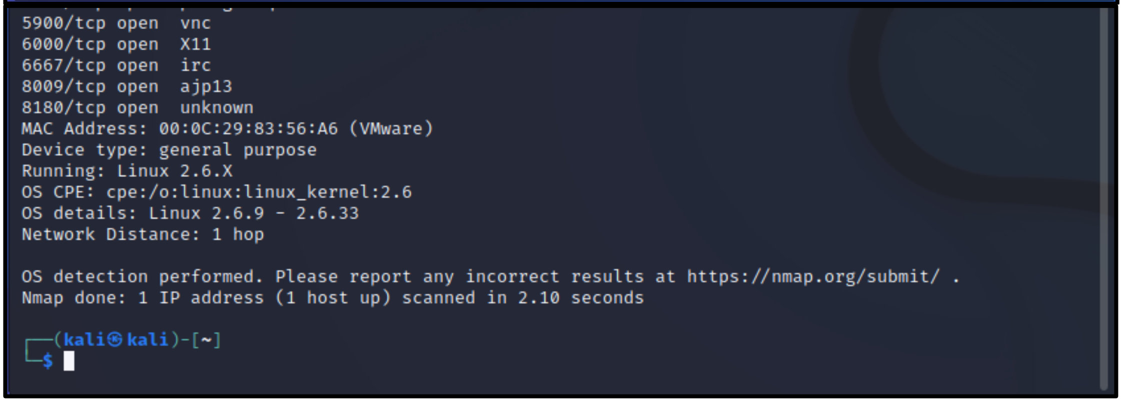
Enumerating Hosts:

- Enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system.
- Enumeration is used to gather the following:
  - Usernames, group names
  - Hostnames
  - Network shares and services
  - IP tables and routing tables
  - Service settings and audit configurations
  - Application and banners
  - SNMP and DNS details

1. Find out the operating system of the target metasploitable2. (Running: Linux 2.6.X)



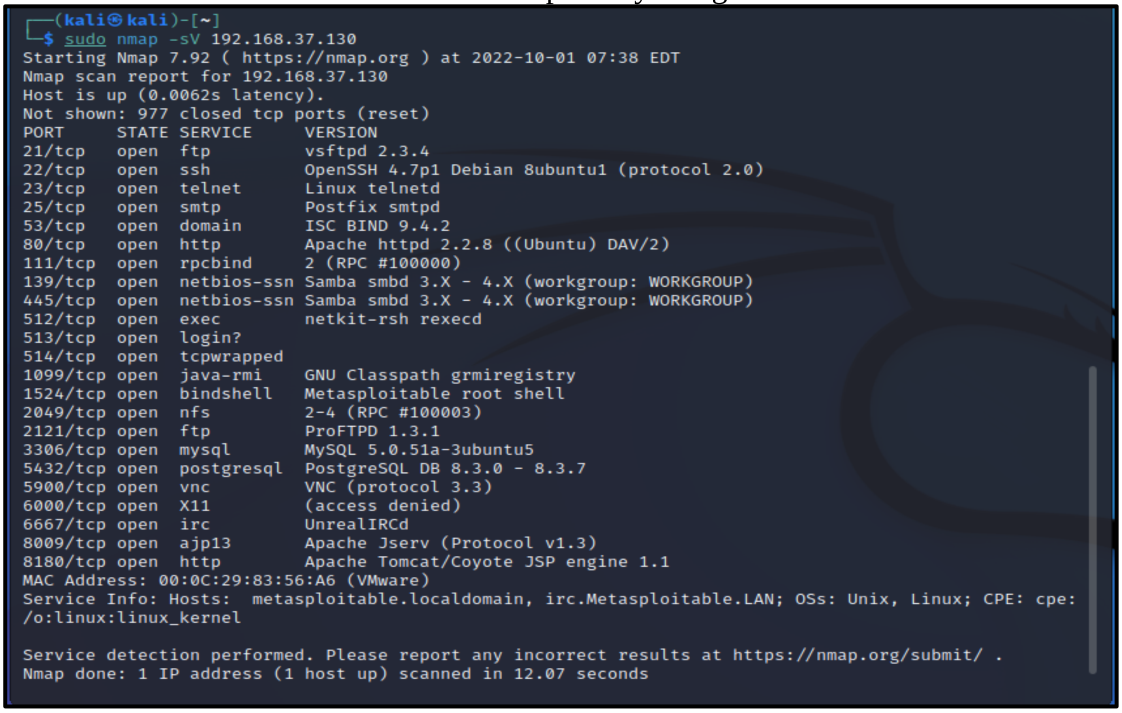
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:36 EDT
Nmap scan report for 192.168.37.130
Host is up (0.00097s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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:29:83:56:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```



```
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:83:56:A6 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

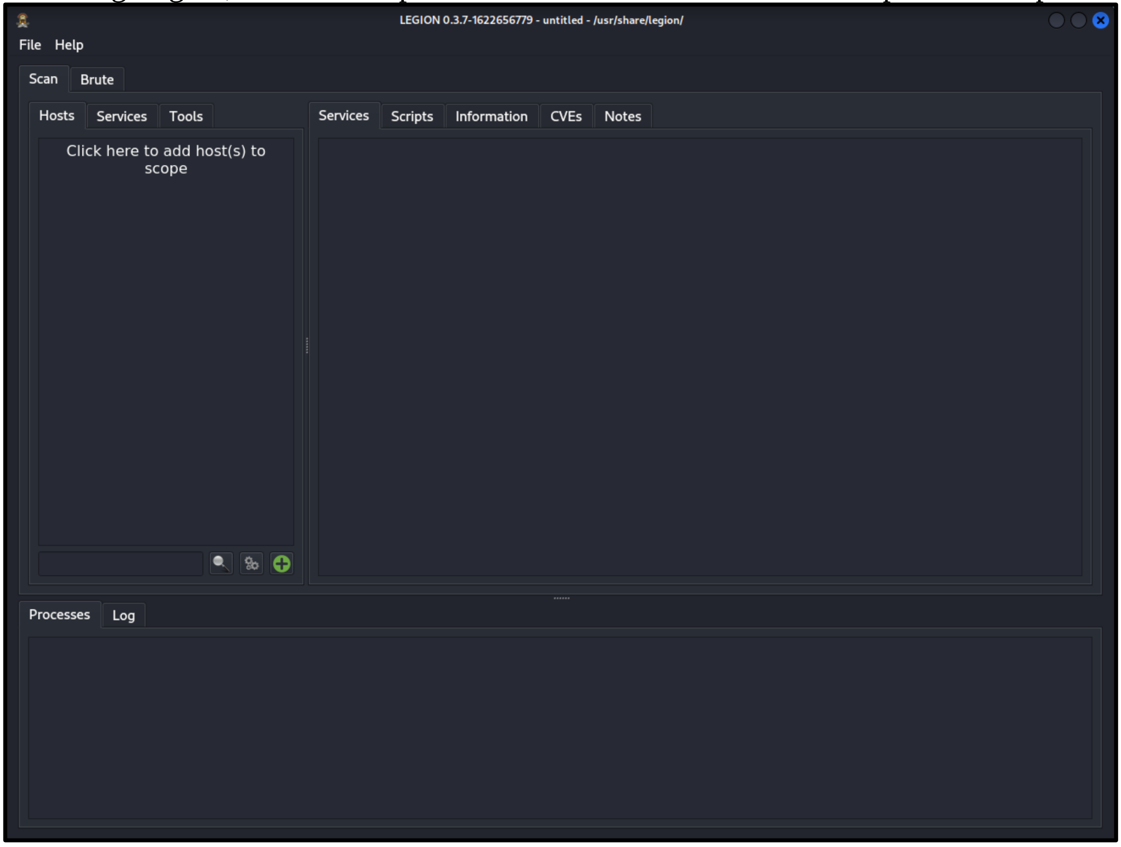
```
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.10 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

2. Find out all the host services and their ports by using –sV.

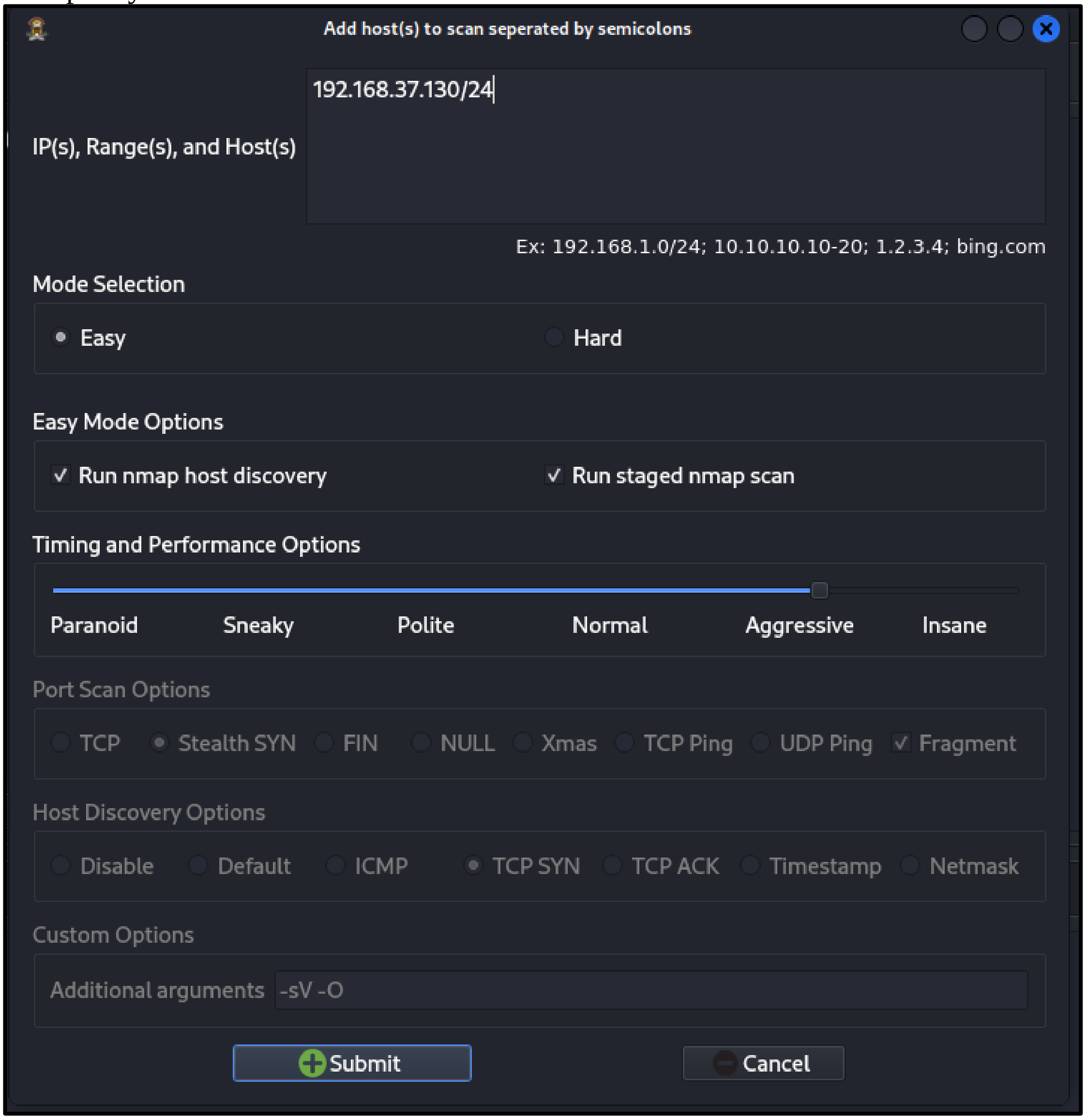


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.37.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-01 07:38 EDT
Nmap scan report for 192.168.37.130
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:83:56:A6 (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 12.07 seconds
```

3. Using Legion, we can also perform enumeration and search for open service ports.


LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File
Help
Scan
Brute
Hosts
Services
Tools
Click here to add host(s) to scope
Services
Scripts
Information
CVEs
Notes
Processes
Log

4. Specify the IP Subnet and Bits as shown and click on submit.



Add host(s) to scan seperated by semicolons

IP(s), Range(s), and Host(s): 192.168.37.130/24

Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com

Mode Selection

● Easy ○ Hard

Easy Mode Options

☑ Run nmap host discovery ☑ Run staged nmap scan

Timing and Performance Options

Paranoid Sneaky Polite Normal Aggressive Insane

Port Scan Options

○ TCP ● Stealth SYN ○ FIN ○ NULL ○ Xmas ○ TCP Ping ○ UDP Ping ☑ Fragment

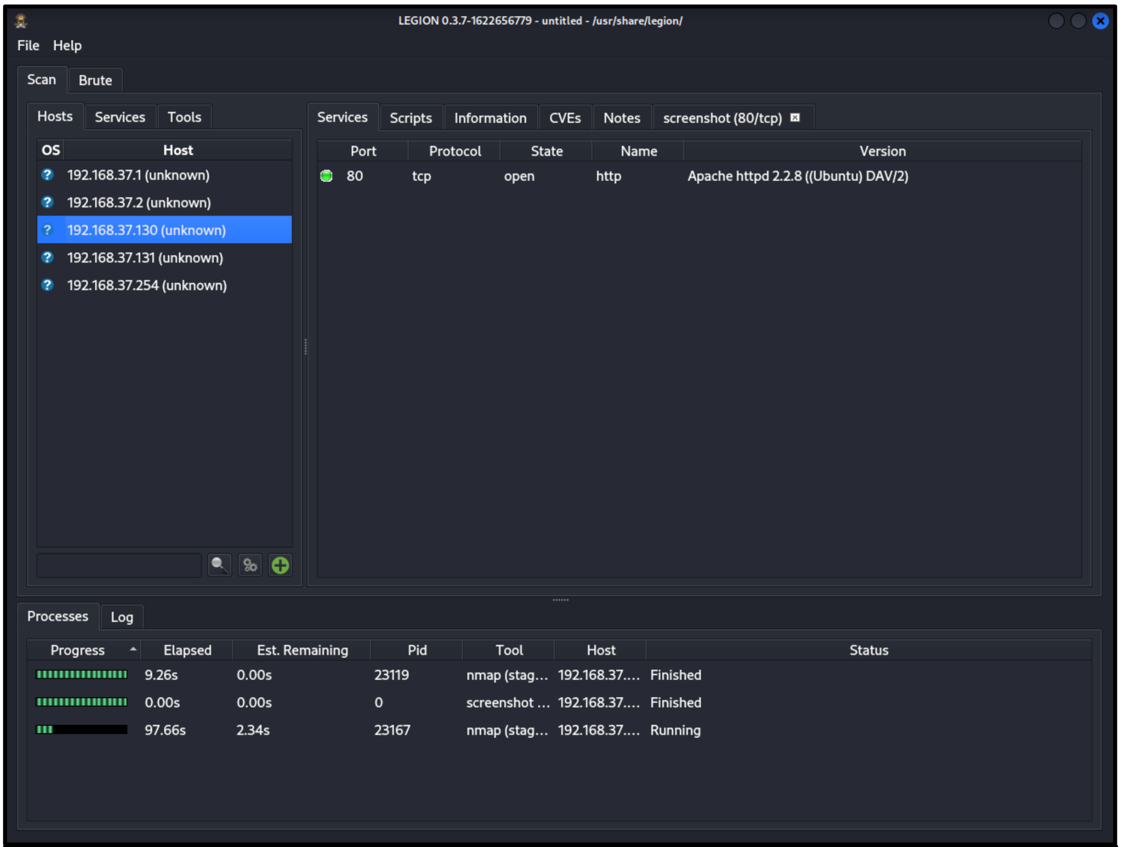
Host Discovery Options

○ Disable ○ Default ○ ICMP ● TCP SYN ○ TCP ACK ○ Timestamp ○ Netmask

Custom Options

Additional arguments: -sV -O

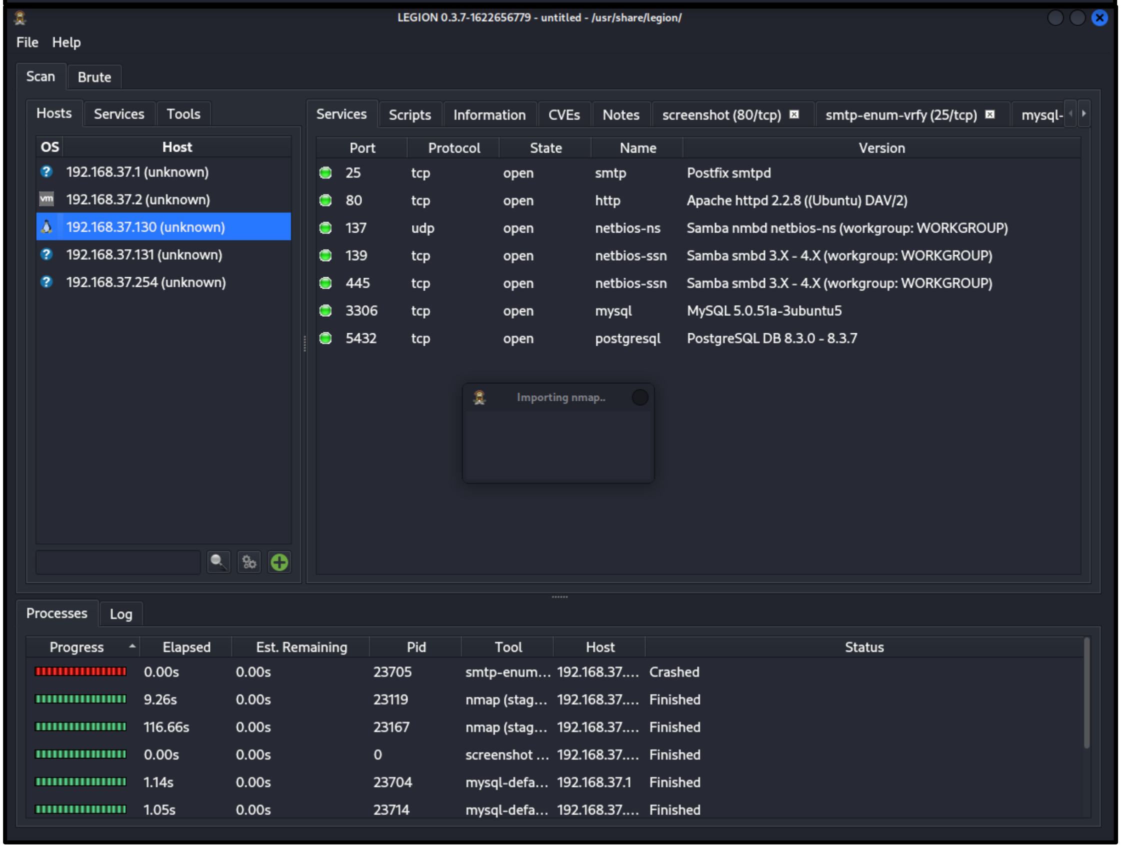
5. After submitting it will start scanning all the available hosts in that subnet and you will see the Windows XP and Metasploitable2 Operating systems also displayed in the scan.



OS	Host
?	192.168.37.1 (unknown)
?	192.168.37.2 (unknown)
?	192.168.37.130 (unknown)
?	192.168.37.131 (unknown)
?	192.168.37.254 (unknown)

	Port	Protocol	State	Name	Version
●	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	9.26s	0.00s	23119	nmap (stag…	192.168.37.…	Finished
	0.00s	0.00s	0	screenshot …	192.168.37.…	Finished
	97.66s	2.34s	23167	nmap (stag…	192.168.37.…	Running



OS	Host
?	192.168.37.1 (unknown)
vm	192.168.37.2 (unknown)
	192.168.37.130 (unknown)
?	192.168.37.131 (unknown)
?	192.168.37.254 (unknown)

	Port	Protocol	State	Name	Version
●	25	tcp	open	smtp	Postfix smtpd
●	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
●	137	udp	open	netbios-ns	Samba nmbd netbios-ns (workgroup: WORKGROUP)
●	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)
●	3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
●	5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7

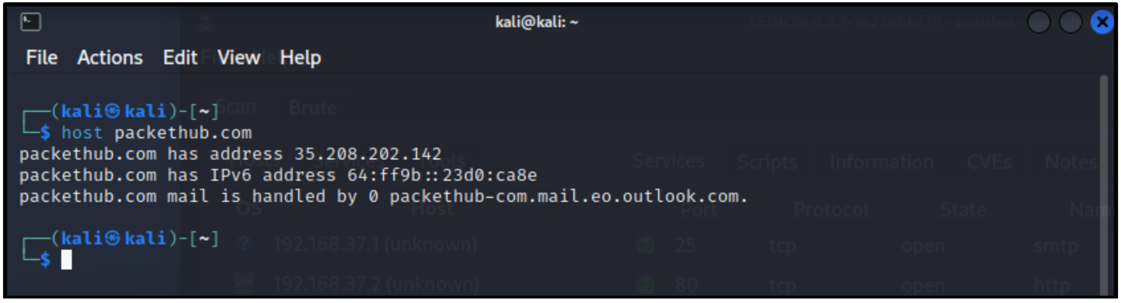
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	0.00s	0.00s	23705	smtp-enum…	192.168.37.…	Crashed
	9.26s	0.00s	23119	nmap (stag…	192.168.37.…	Finished
	116.66s	0.00s	23167	nmap (stag…	192.168.37.…	Finished
	0.00s	0.00s	0	screenshot …	192.168.37.…	Finished
	1.14s	0.00s	23704	mysql-defa…	192.168.37.1	Finished
	1.05s	0.00s	23714	mysql-defa…	192.168.37.…	Finished

DNS Enumeration:

- The process which locates all DNS servers and records of an organization is DNS enumeration.
- Domain Name System can be utilized as a source of information by an attacker to exploit and gain access to internal resources and systems of a specific organization.
- DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

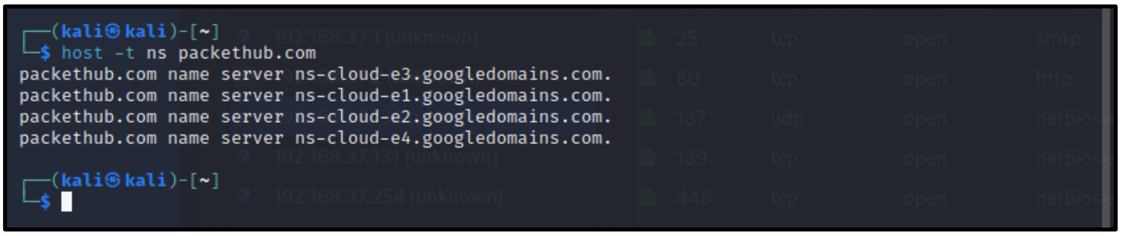
Note: DNS Enumeration needs to be performed while Legion runs in the background.

1. To find out the host IP Address, IPv6 address and Mail Servers

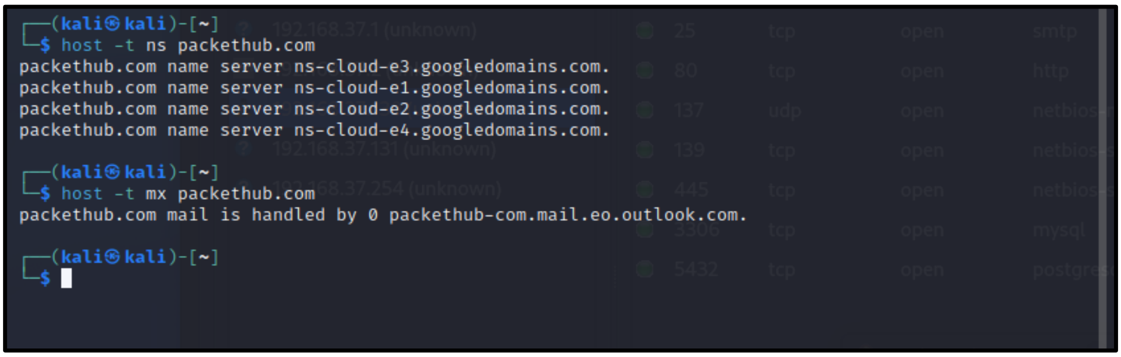


```
┌──(kali㉿kali)-[~]
└─$ host packethub.com
packethub.com has address 35.208.202.142
packethub.com has IPv6 address 64:ff9b::23d0:ca8e
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ 
```

2. To find out the host name servers and mail servers

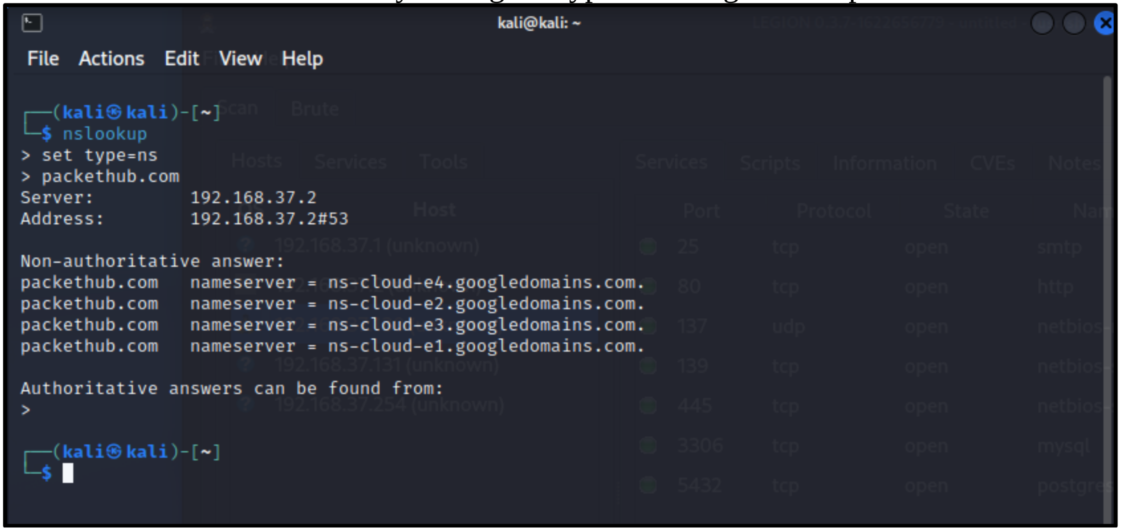


```
┌──(kali㉿kali)-[~]
└─$ host -t ns packethub.com
packethub.com name server ns-cloud-e3.googledomains.com.
packethub.com name server ns-cloud-e1.googledomains.com.
packethub.com name server ns-cloud-e2.googledomains.com.
packethub.com name server ns-cloud-e4.googledomains.com.

┌──(kali㉿kali)-[~]
└─$ 
```



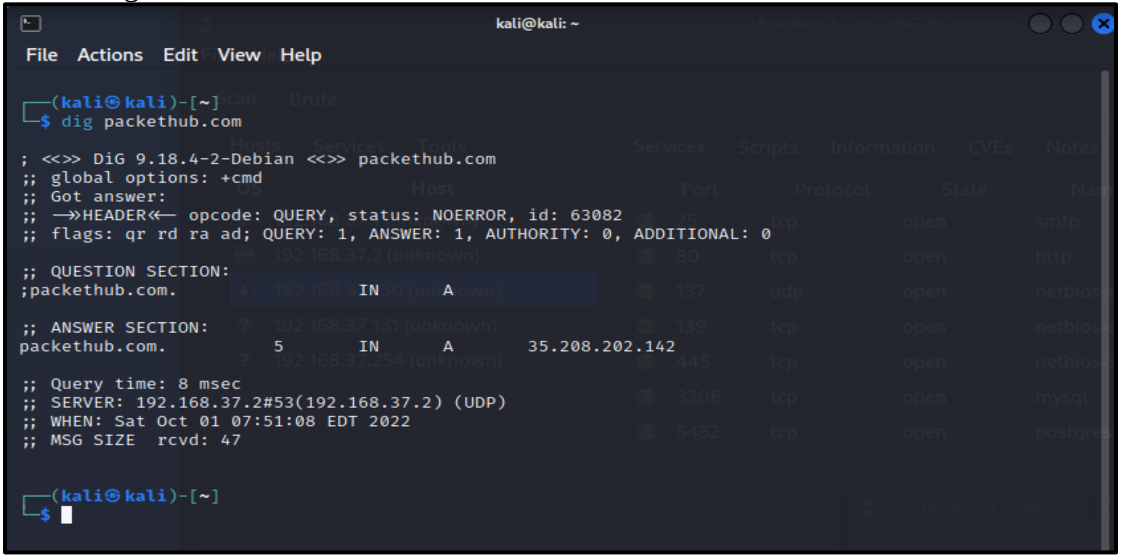
```
┌──(kali㉿kali)-[~]
└─$ host -t ns packethub.com
packethub.com name server ns-cloud-e3.googledomains.com.
packethub.com name server ns-cloud-e1.googledomains.com.
packethub.com name server ns-cloud-e2.googledomains.com.
packethub.com name server ns-cloud-e4.googledomains.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx packethub.com
packethub.com mail is handled by 0 packethub-com.mail.eo.outlook.com.

┌──(kali㉿kali)-[~]
└─$ 
```

3. To find the Name Servers by setting the type=ns using nslookup



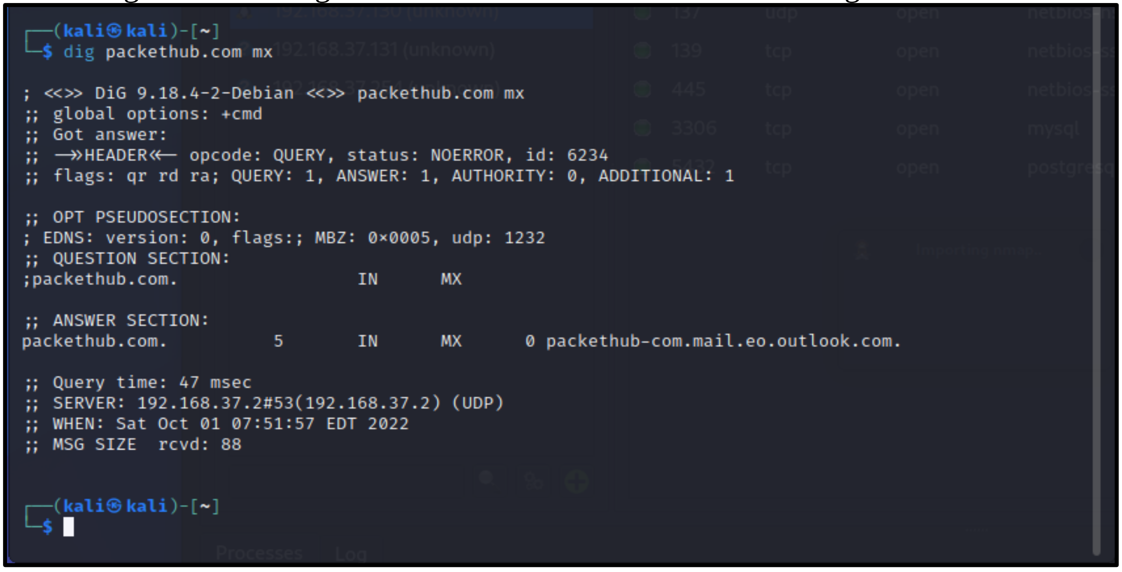
```
┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=ns
> packethub.com
Server:         192.168.37.2
Address:        192.168.37.2#53

Non-authoritative answer:
packethub.com   nameserver = ns-cloud-e4.googledomains.com.
packethub.com   nameserver = ns-cloud-e2.googledomains.com.
packethub.com   nameserver = ns-cloud-e3.googledomains.com.
packethub.com   nameserver = ns-cloud-e1.googledomains.com.

Authoritative answers can be found from:
>

┌──(kali㉿kali)-[~]
└─$ 
```

4. The dig command can be used for advanced dns enumeration.



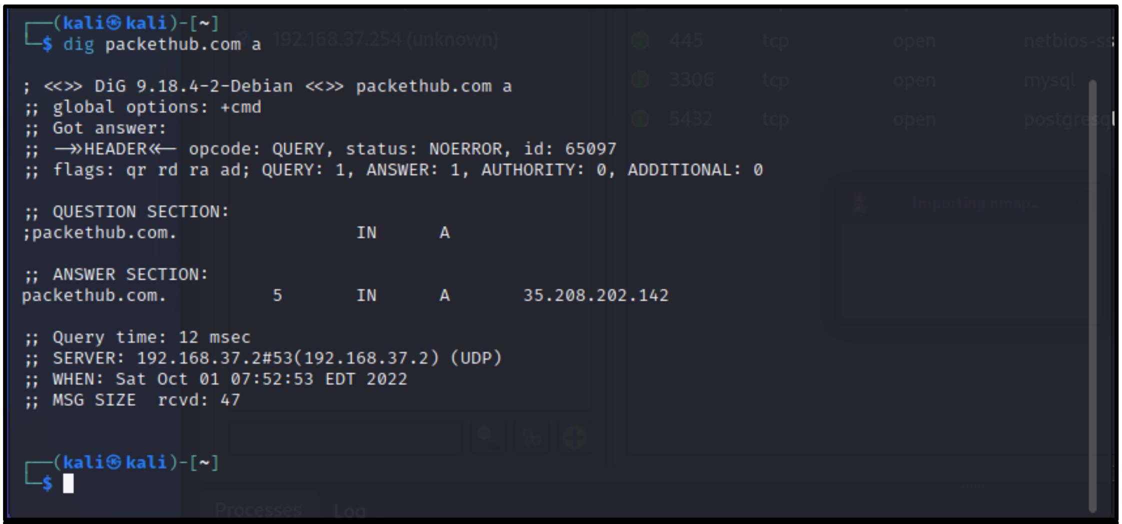
```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com

; <<>> DiG 9.18.4-2-Debian <<>> packethub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63082
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          5       IN      A       35.208.202.142

;; Query time: 8 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:51:08 EDT 2022
;; MSG SIZE  rcvd: 47


┌──(kali㉿kali)-[~]
└─$ 
```

5. Use dig command to get detailed info of mail servers of the target

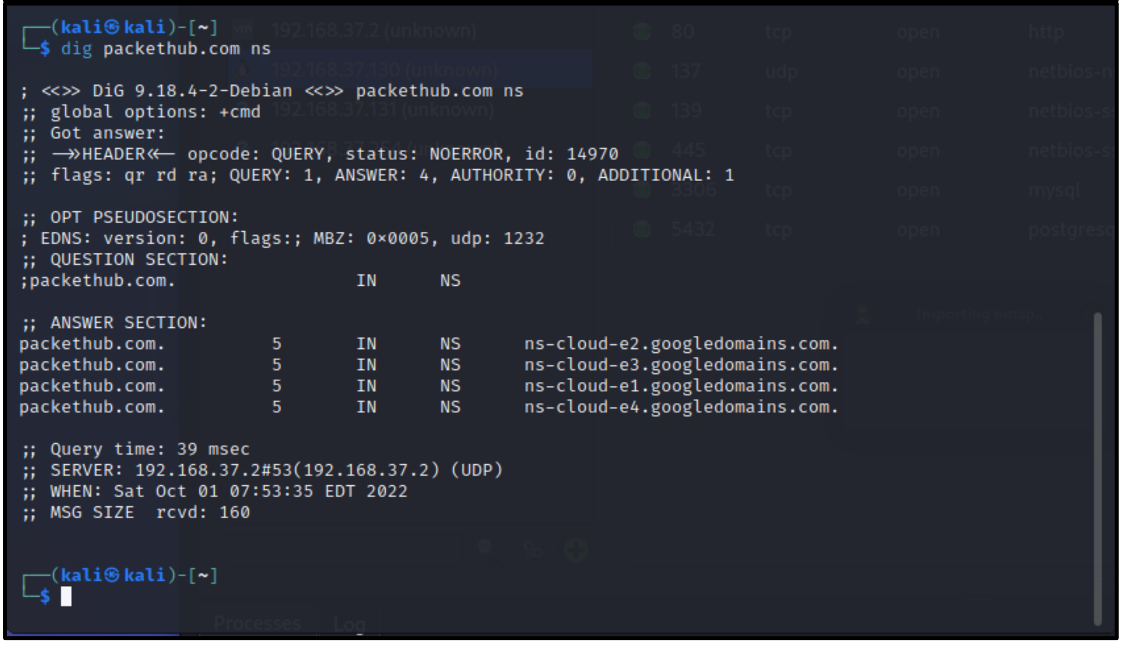


```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com mx

; <<>> DiG 9.18.4-2-Debian <<>> packethub.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6234
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 1232
;; QUESTION SECTION:
;packethub.com.                 IN      MX

;; ANSWER SECTION:
packethub.com.          5       IN      MX      0 packethub-com.mail.eo.outlook.com.

;; Query time: 47 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:51:57 EDT 2022
;; MSG SIZE  rcvd: 88


┌──(kali㉿kali)-[~]
└─$ 
```

6. Enter the keywords “dig packtpub.com <record>” to get the details about the target host

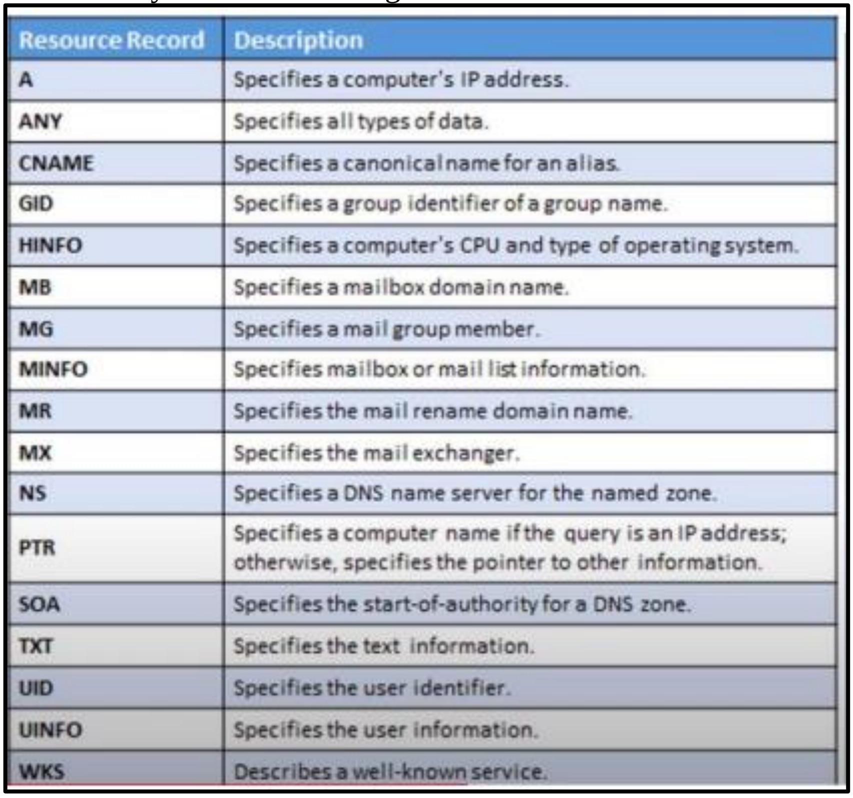


```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com a

; <<>> DiG 9.18.4-2-Debian <<>> packethub.com a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65097
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;packethub.com.                 IN      A

;; ANSWER SECTION:
packethub.com.          5       IN      A       35.208.202.142

;; Query time: 12 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:52:53 EDT 2022
;; MSG SIZE  rcvd: 47


┌──(kali㉿kali)-[~]
└─$ █
```



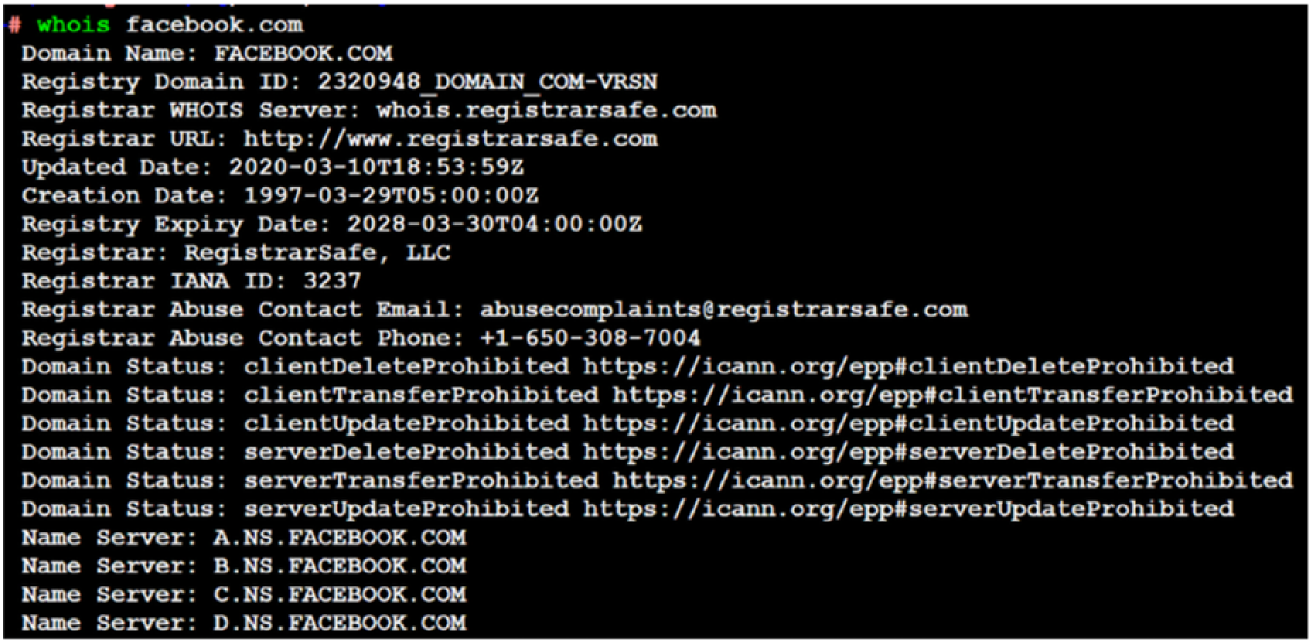
```
┌──(kali㉿kali)-[~]
└─$ dig packethub.com ns

; <<>> DiG 9.18.4-2-Debian <<>> packethub.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14970
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 1232
;; QUESTION SECTION:
;packethub.com.                 IN      NS

;; ANSWER SECTION:
packethub.com.          5       IN      NS      ns-cloud-e2.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e3.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e1.googledomains.com.
packethub.com.          5       IN      NS      ns-cloud-e4.googledomains.com.

;; Query time: 39 msec
;; SERVER: 192.168.37.2#53(192.168.37.2) (UDP)
;; WHEN: Sat Oct 01 07:53:35 EDT 2022
;; MSG SIZE  rcvd: 160


┌──(kali㉿kali)-[~]
└─$ █
```

Various functional keywords for the “dig” command:



Resource Record	Description
A	Specifies a computer's IP address.
ANY	Specifies all types of data.
CNAME	Specifies a canonical name for an alias.
GID	Specifies a group identifier of a group name.
HINFO	Specifies a computer's CPU and type of operating system.
MB	Specifies a mailbox domain name.
MG	Specifies a mail group member.
MINFO	Specifies mailbox or mail list information.
MR	Specifies the mail rename domain name.
MX	Specifies the mail exchanger.
NS	Specifies a DNS name server for the named zone.
PTR	Specifies a computer name if the query is an IP address; otherwise, specifies the pointer to other information.
SOA	Specifies the start-of-authority for a DNS zone.
TXT	Specifies the text information.
UID	Specifies the user identifier.
UINFO	Specifies the user information.
WKS	Describes a well-known service.

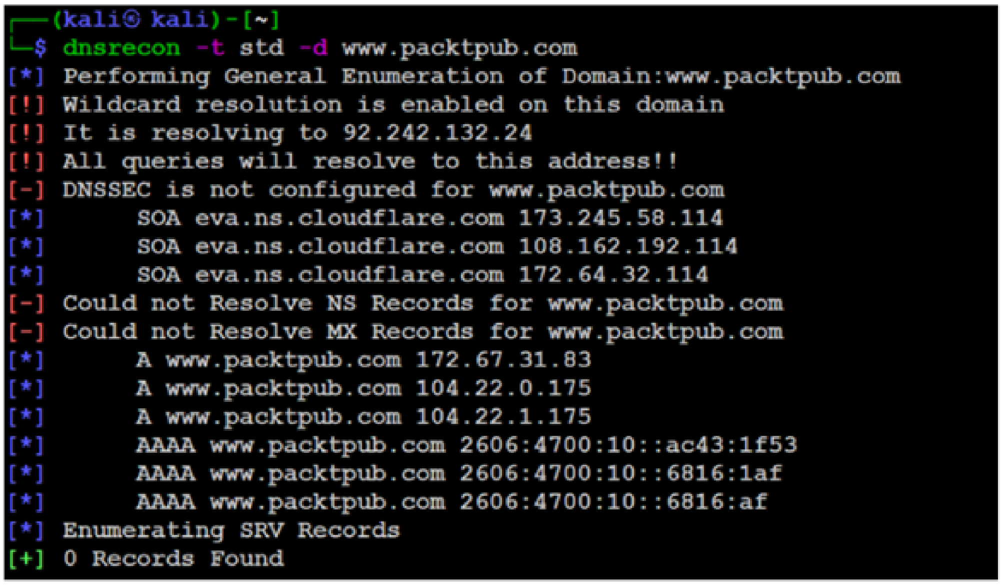
Using whois to enumeratate domain details



```
# whois facebook.com
 Domain Name: FACEBOOK.COM
 Registry Domain ID: 2320948_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.registrarsafe.com
 Registrar URL: http://www.registrarsafe.com
 Updated Date: 2020-03-10T18:53:59Z
 Creation Date: 1997-03-29T05:00:00Z
 Registry Expiry Date: 2028-03-30T04:00:00Z
 Registrar: RegistrarSafe, LLC
 Registrar IANA ID: 3237
 Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
 Registrar Abuse Contact Phone: +1-650-308-7004
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
 Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
 Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
 Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
 Name Server: A.NS.FACEBOOK.COM
 Name Server: B.NS.FACEBOOK.COM
 Name Server: C.NS.FACEBOOK.COM
 Name Server: D.NS.FACEBOOK.COM
```

Figure 3.6: whois details on the facebook.com domain that includes Name Server details

In *Figure 3.10*, `dnsrecon` has been used to generate a standard DNS record search, and a search that is specific for SRV records. An excerpt of the results is shown for each case:

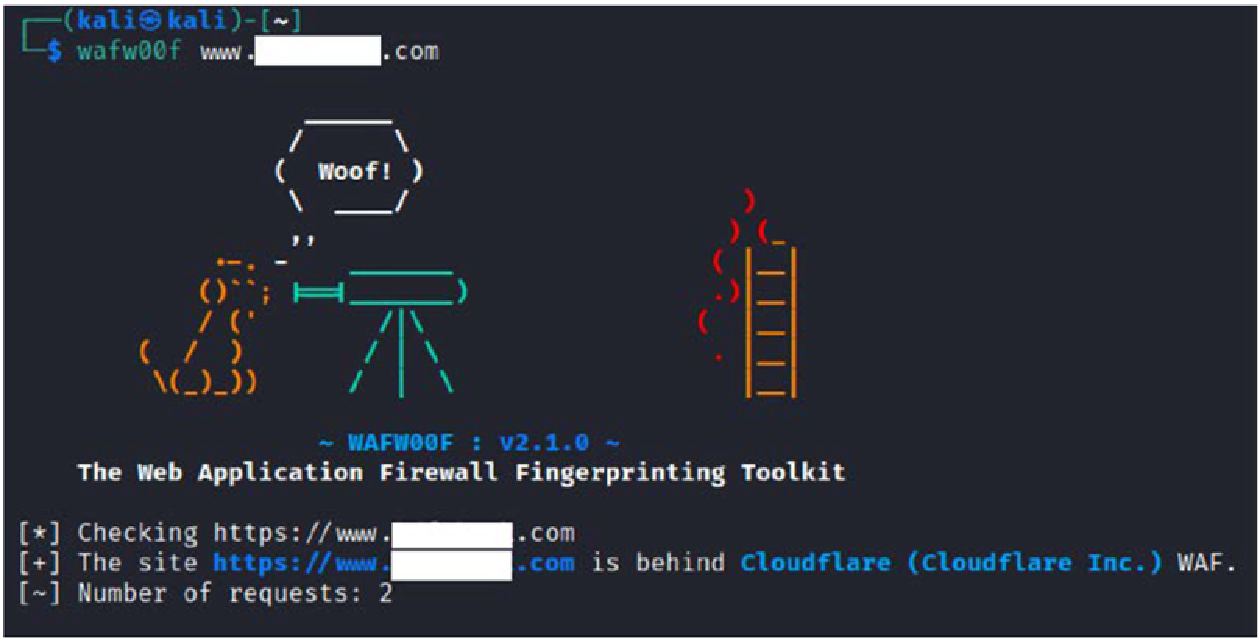


```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t std -d www.packtpub.com
[*] Performing General Enumeration of Domain:www.packtpub.com
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 92.242.132.24
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for www.packtpub.com
[*]      SOA eva.ns.cloudflare.com 173.245.58.114
[*]      SOA eva.ns.cloudflare.com 108.162.192.114
[*]      SOA eva.ns.cloudflare.com 172.64.32.114
[-] Could not Resolve NS Records for www.packtpub.com
[-] Could not Resolve MX Records for www.packtpub.com
[*]      A www.packtpub.com 172.67.31.83
[*]      A www.packtpub.com 104.22.0.175
[*]      A www.packtpub.com 104.22.1.175
[*]      AAAA www.packtpub.com 2606:4700:10::ac43:1f53
[*]      AAAA www.packtpub.com 2606:4700:10::6816:1af
[*]      AAAA www.packtpub.com 2606:4700:10::6816:af
[*] Enumerating SRV Records
[+] 0 Records Found
```

Figure 3.10: Running the dnsrecon tool on www.packtpub.com

`dnsrecon` allows the penetration tester to obtain the SOA record, **Name Servers** (**NS**), **mail exchanger** (**MX**) hosts, servers sending emails using **Sender Policy Framework** (**SPF**), and the IP address ranges in use.

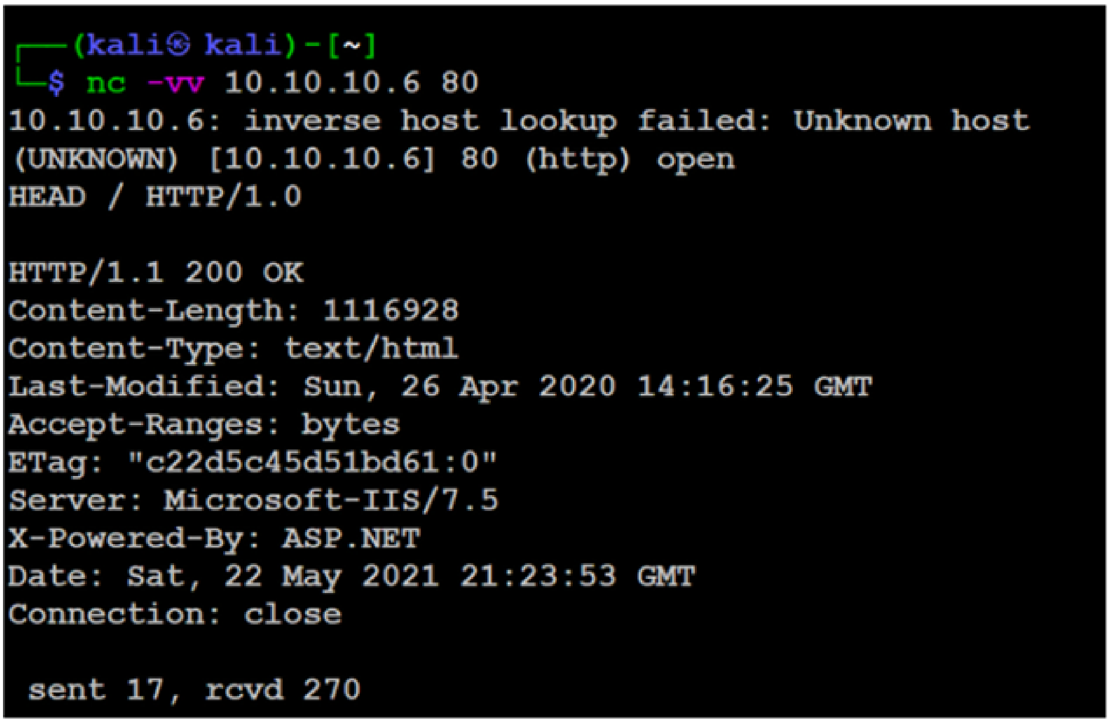
Another tool that attackers utilize during active reconnaissance is WAFW00F; this tool is preinstalled in the latest version of Kali Linux. It is used to identify and fingerprint the WAF products. It also provides a list of well-known WAFs. The version of the WAF in use can be extracted by adding the -l switch to the command (for example, `wafw00f -l`). *Figure 3.18* shows the exact WAF running behind a web application:



```
┌──(kali㉿kali)-[~]
└─$ wafw00f www.[redacted].com

                ~ WAFW00F : v2.1.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.[redacted].com
[+] The site https://www.[redacted].com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

Figure 3.18: Running wafw00f to fingerprint a web application firewall

```
nc -vv www.target.com port number and then enter HEAD / HTTP/1.0
```



```
┌──(kali㉿kali)-[~]
└─$ nc -vv 10.10.10.6 80
10.10.10.6: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.6] 80 (http) open
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Content-Length: 1116928
Content-Type: text/html
Last-Modified: Sun, 26 Apr 2020 14:16:25 GMT
Accept-Ranges: bytes
ETag: "c22d5c45d51bd61:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sat, 22 May 2021 21:23:53 GMT
Connection: close

 sent 17, rcvd 270
```

Figure 3.21: Using netcat to grab the banner of a target