Practical 3

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

NOTE: Tool that we are going to use for enumerating host, port and for service scanning is nmap.

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.

Our Target Machine will be metasploitable2 and target live hosts will be packtpub.com and cyberhia.com

Port Scanning

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
 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**

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:70:18:72
          inet addr:192.168.101.130  Bcast:192.168.101.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe70:1872/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4526 (4.4 KB)  TX bytes:7294 (7.1 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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$ _
```

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

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

┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -p 0-65535 -A 192.168.101.130 -oA metasploitable2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 14:57 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating NSE at 14:57
Completed NSE at 14:57, 0.00s elapsed
Initiating ARP Ping Scan at 14:57
Scanning 192.168.101.130 [1 port]
Completed ARP Ping Scan at 14:57, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:57
Completed Parallel DNS resolution of 1 host. at 14:57, 2.17s elapsed
Initiating SYN Stealth Scan at 14:57
Scanning 192.168.101.130 [65536 ports]
Discovered open port 5900/tcp on 192.168.101.130
Discovered open port 22/tcp on 192.168.101.130
Discovered open port 21/tcp on 192.168.101.130
Discovered open port 80/tcp on 192.168.101.130
Discovered open port 25/tcp on 192.168.101.130
Discovered open port 23/tcp on 192.168.101.130
Discovered open port 3306/tcp on 192.168.101.130
Discovered open port 445/tcp on 192.168.101.130
Discovered open port 111/tcp on 192.168.101.130
Discovered open port 139/tcp on 192.168.101.130
Discovered open port 35591/tcp on 192.168.101.130
Discovered open port 52739/tcp on 192.168.101.130
Discovered open port 6667/tcp on 192.168.101.130
Discovered open port 6000/tcp on 192.168.101.130
Discovered open port 2049/tcp on 192.168.101.130
Discovered open port 1524/tcp on 192.168.101.130
Discovered open port 3632/tcp on 192.168.101.130
Discovered open port 38821/tcp on 192.168.101.130
Discovered open port 1099/tcp on 192.168.101.130
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35231/tcp open  mountd      1-3 (RPC #100005)
35591/tcp open  status      1 (RPC #100024)
38821/tcp open  nlockmgr    1-4 (RPC #100021)
52739/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 00:0C:29:70:18:72 (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: 497.102 days (since Fri May 21 12:33:33 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=193 (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: 2022-09-30T14:59:50-04:00
| 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>
```

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

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

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

┌──(kali㉿kali)-[~]
└─$
```

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

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

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

┌──(kali㉿kali)-[~]
└─$ cat metasploitable2.nmap
# Nmap 7.92 scan initiated Fri Sep 30 14:57:31 2022 as: nmap -v -p 0-65535 -A -oA metasploitable2 192.168.101.130
Nmap scan report for 192.168.101.130
Host is up (0.00039s latency).
Not shown: 65507 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 192.168.101.132
|      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
```

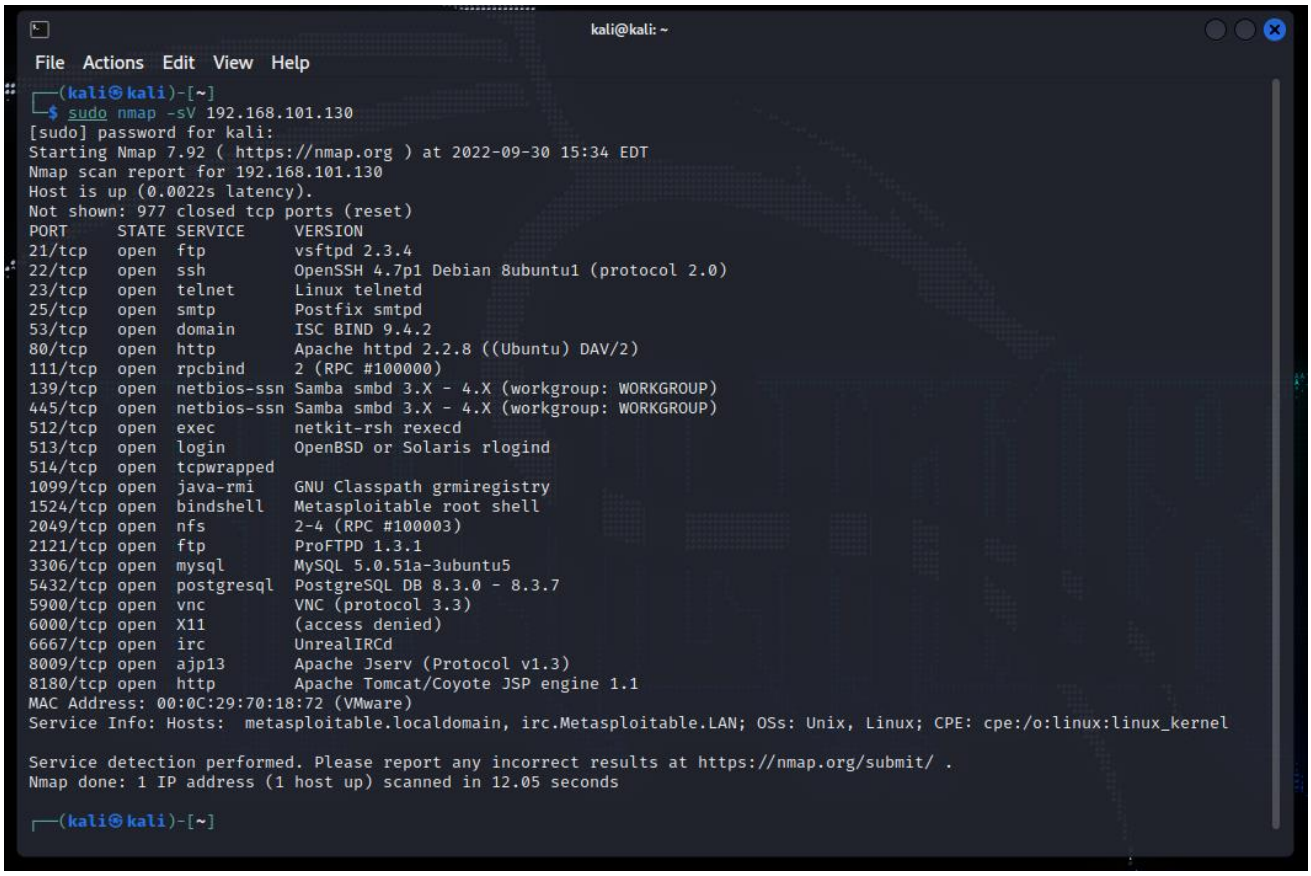
Enumeration of Hosts

1. Find out the operating system of the target metasploitable2

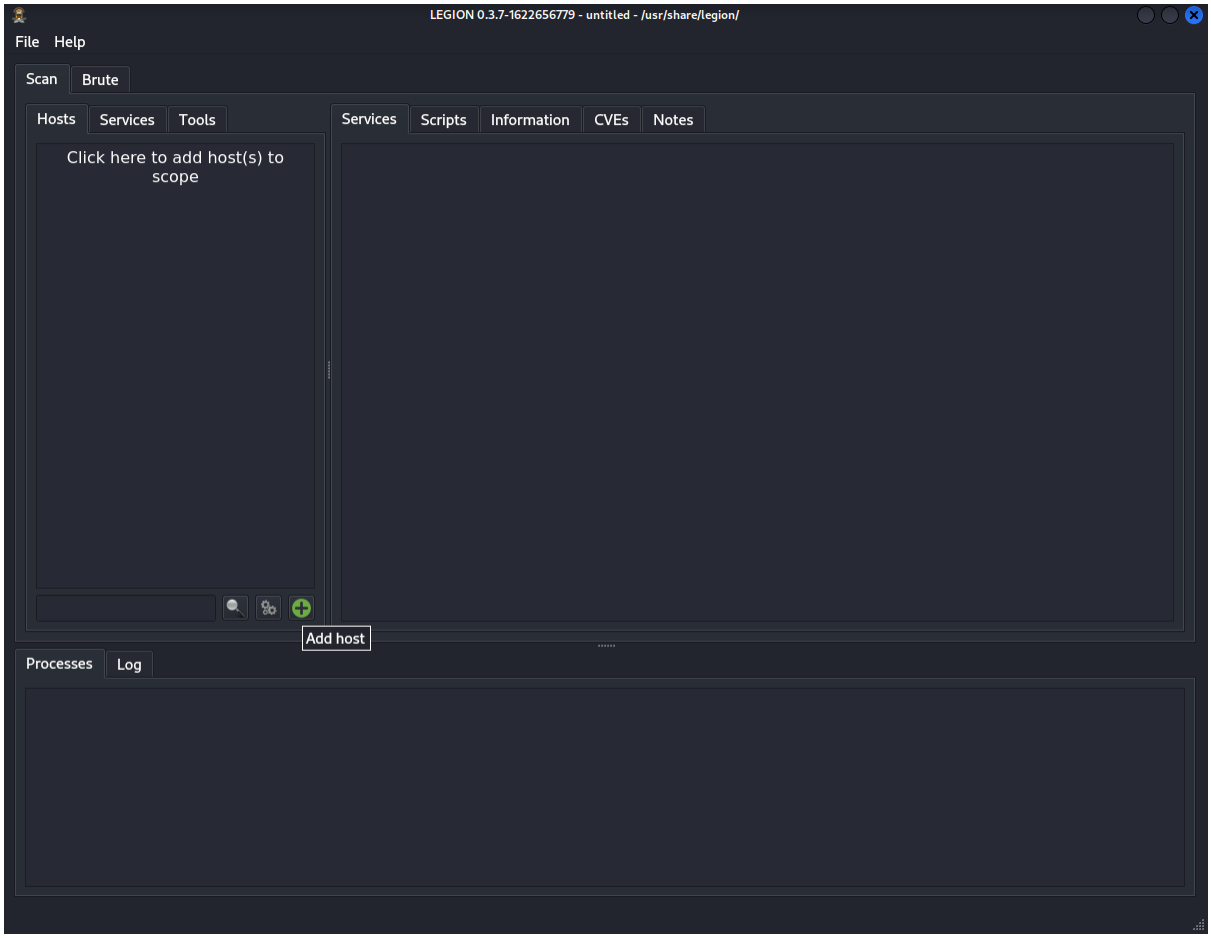
```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -O 192.168.101.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-30 15:30 EDT
Nmap scan report for 192.168.101.130
Host is up (0.00062s 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:29:70:18:72 (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
```

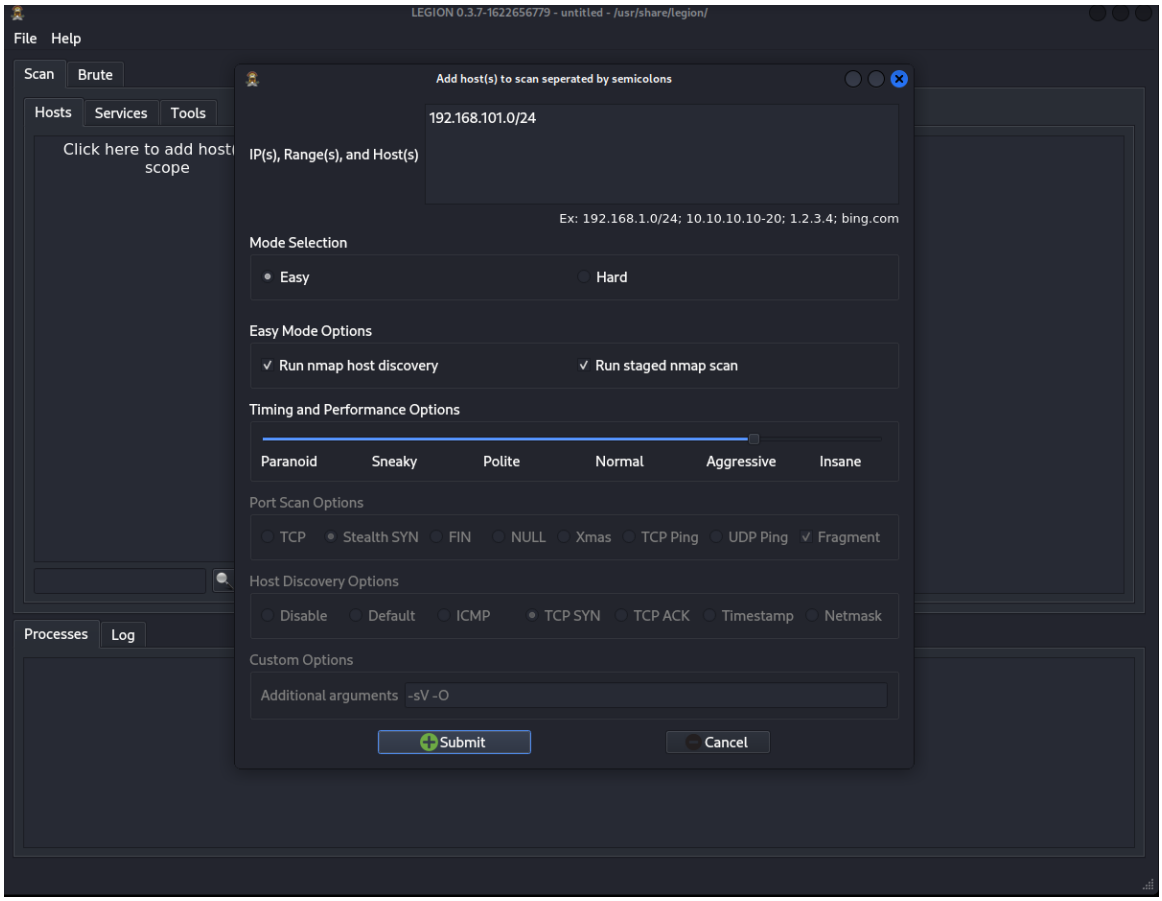
2. Find out all the host services and their ports by using –sV



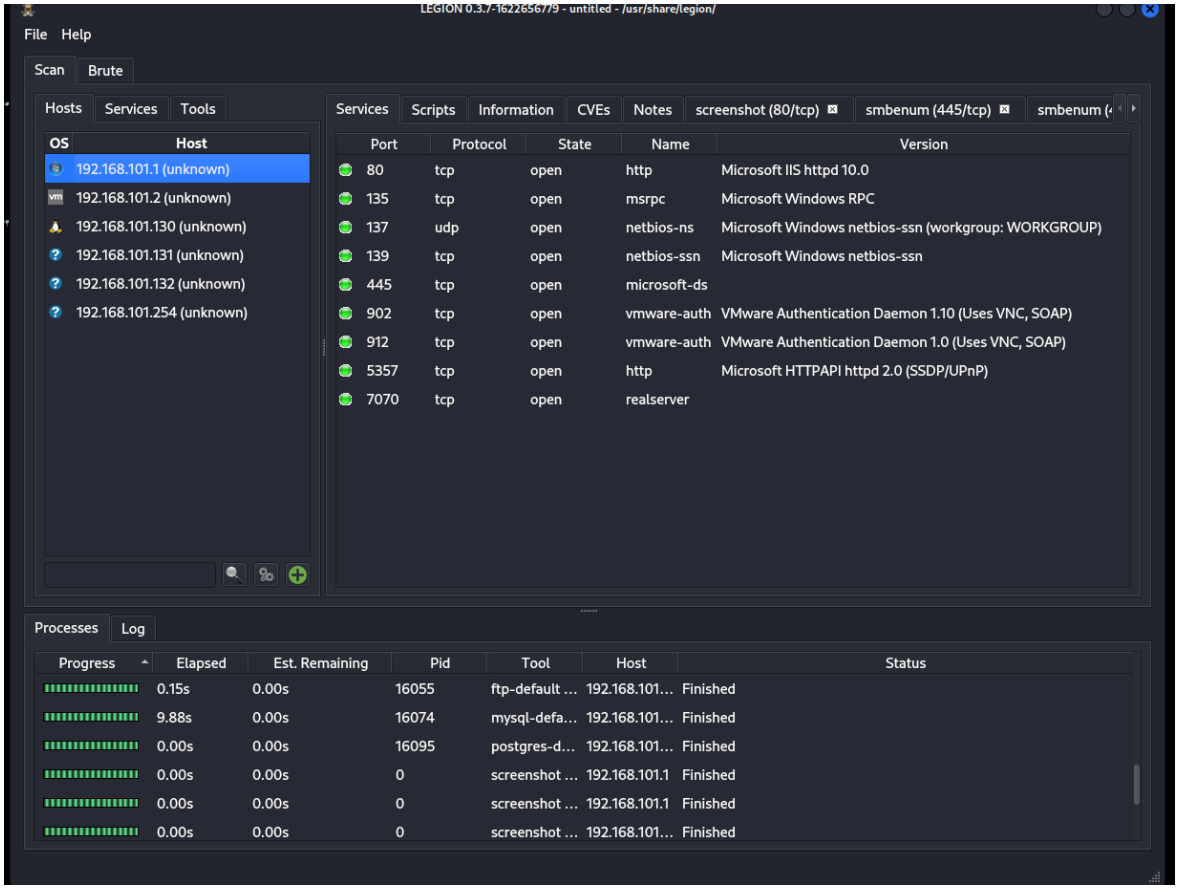
3. Using Legion we can also perform enumeration and search for open service ports



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



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.



DNS Enumeration

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

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

┌──(kali㉿kali)-[~]
└─$ host packtpub.com
packtpub.com has address 172.67.31.83
packtpub.com has address 104.22.0.175
packtpub.com has address 104.22.1.175
packtpub.com has IPv6 address 2606:4700:10::6816:1af
packtpub.com has IPv6 address 2606:4700:10::ac43:1f53
packtpub.com has IPv6 address 2606:4700:10::6816:af
packtpub.com mail is handled by 10 eu-smtp-inbound-1.mimecast.com.
packtpub.com mail is handled by 10 eu-smtp-inbound-2.mimecast.com.
packtpub.com mail is handled by 15 packtpub-com.mail.protection.outlook.com.

┌──(kali㉿kali)-[~]
└─$
```

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

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

┌──(kali㉿kali)-[~]
└─$ host -t ns packtpub.com
packtpub.com name server eva.ns.cloudflare.com.
packtpub.com name server max.ns.cloudflare.com.

┌──(kali㉿kali)-[~]
└─$ host -t mx packtpub.com
packtpub.com mail is handled by 10 eu-smtp-inbound-1.mimecast.com.
packtpub.com mail is handled by 10 eu-smtp-inbound-2.mimecast.com.
packtpub.com mail is handled by 15 packtpub-com.mail.protection.outlook.com.

┌──(kali㉿kali)-[~]
└─$
```

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

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

┌──(kali㉿kali)-[~]
└─$ nslookup
> set type=ns
> packtpub.com
Server:         192.168.101.2
Address:        192.168.101.2#53

Non-authoritative answer:
packtpub.com    nameserver = eva.ns.cloudflare.com.
packtpub.com    nameserver = max.ns.cloudflare.com.

Authoritative answers can be found from:
>
>

┌──(kali㉿kali)-[~]
└─$
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ dig packtpub.com

; <<>> DiG 9.18.4-2-Debian <<>> packtpub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33723
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packtpub.com.                  IN      A

;; ANSWER SECTION:
packtpub.com.           5       IN      A       104.22.1.175
packtpub.com.           5       IN      A       172.67.31.83
packtpub.com.           5       IN      A       104.22.0.175

;; Query time: 8 msec
;; SERVER: 192.168.101.2#53(192.168.101.2) (UDP)
;; WHEN: Fri Sep 30 16:11:17 EDT 2022
;; MSG SIZE  rcvd: 89


┌──(kali㉿kali)-[~]
└─$
```

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

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ dig packtpub.com mx

; <<>> DiG 9.18.4-2-Debian <<>> packtpub.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3291
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;packtpub.com.                  IN      MX

;; ANSWER SECTION:
packtpub.com.           5       IN      MX      10 eu-smtp-inbound-1.mimecast.com.
packtpub.com.           5       IN      MX      10 eu-smtp-inbound-2.mimecast.com.
packtpub.com.           5       IN      MX      15 packtpub-com.mail.protection.outlook.com.

;; Query time: 7 msec
;; SERVER: 192.168.101.2#53(192.168.101.2) (UDP)
;; WHEN: Fri Sep 30 16:13:07 EDT 2022
;; MSG SIZE  rcvd: 171
```

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

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.