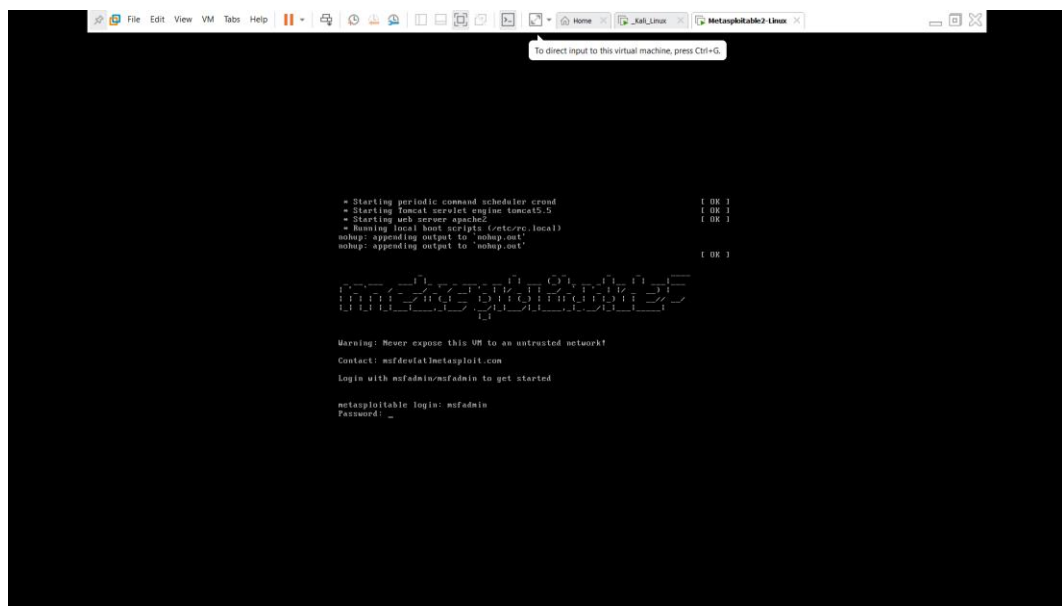


Minor Project-1

A) Take a target (metasploitable 2) and scan using NMAP

Collect all open port information, then get version details of all open ports

Step1:- Open Metasploitable2 machine and login using default username and password.



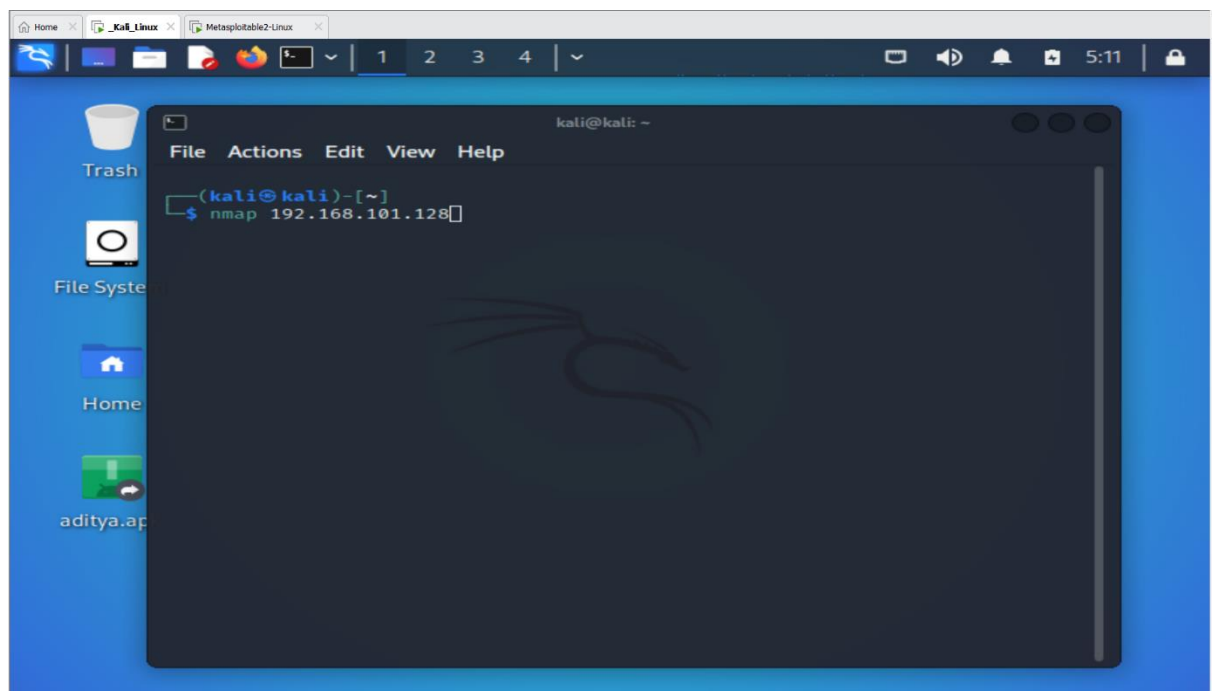
Step2:- Type ifconfig and press Enter
(To know the Ip Address of metasploitable machine)

```
File Edit View VM Tabs Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fa:dd:2a
          inet addr:192.168.101.128  Bcast:192.168.101.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fefa:dd2a/64 Scope:link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5374 (5.2 KB)  TX bytes:7342 (7.1 KB)
          Interrupt:17 Base address:0x2000

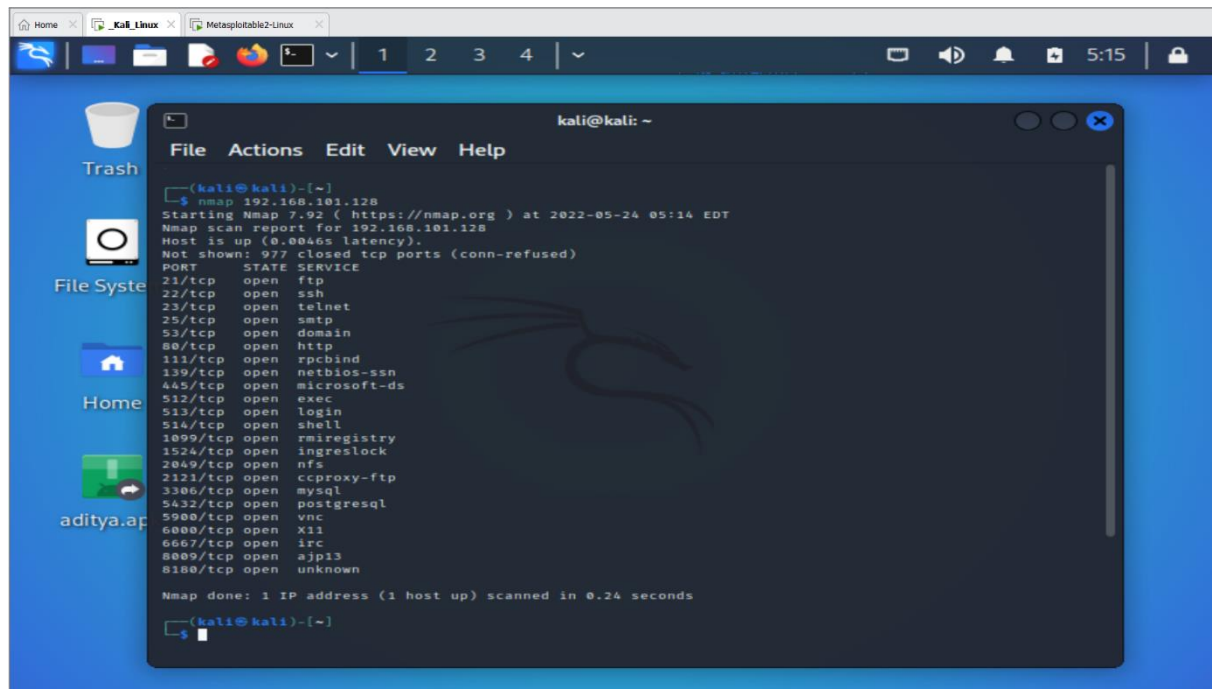
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)

msfadmin@metasploitable:~$ _
```

Step3:- Open terminal in your kali machine and type nmap <ip address of your metasploitable machine> and then press Enter.



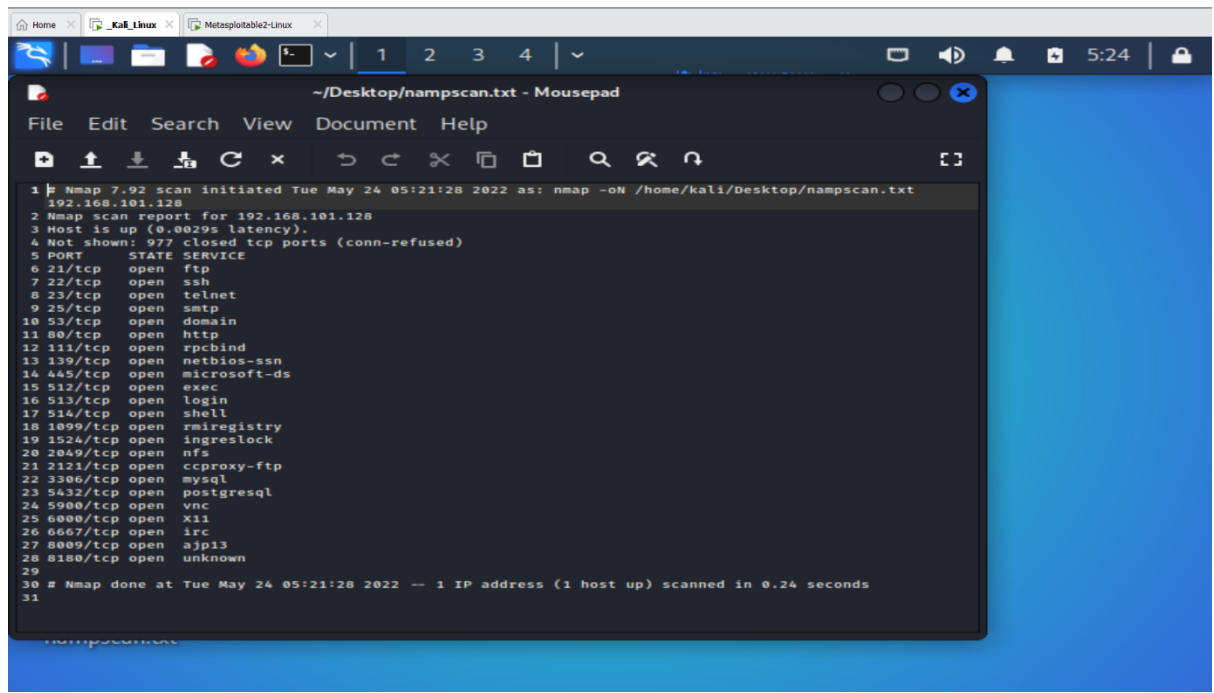
Step4:- you Got all the port with state and service.

A screenshot of a Kali Linux desktop environment. The desktop background is blue. On the left side, there are icons for 'Trash', 'File System', 'Home', and 'aditya.ap'. A terminal window is open in the center, displaying the output of an nmap scan. The terminal title is 'kali@kali: ~'. The output shows the scan of 192.168.101.128, listing open ports and their corresponding services. The scan was completed in 0.24 seconds.

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
$ nmap 192.168.101.128  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 05:14 EDT  
Nmap scan report for 192.168.101.128  
Host is up (0.0046s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds  
  
(kali@kali)-[~]  
$
```

Step5:- save it to the folder on the specified location where you want..

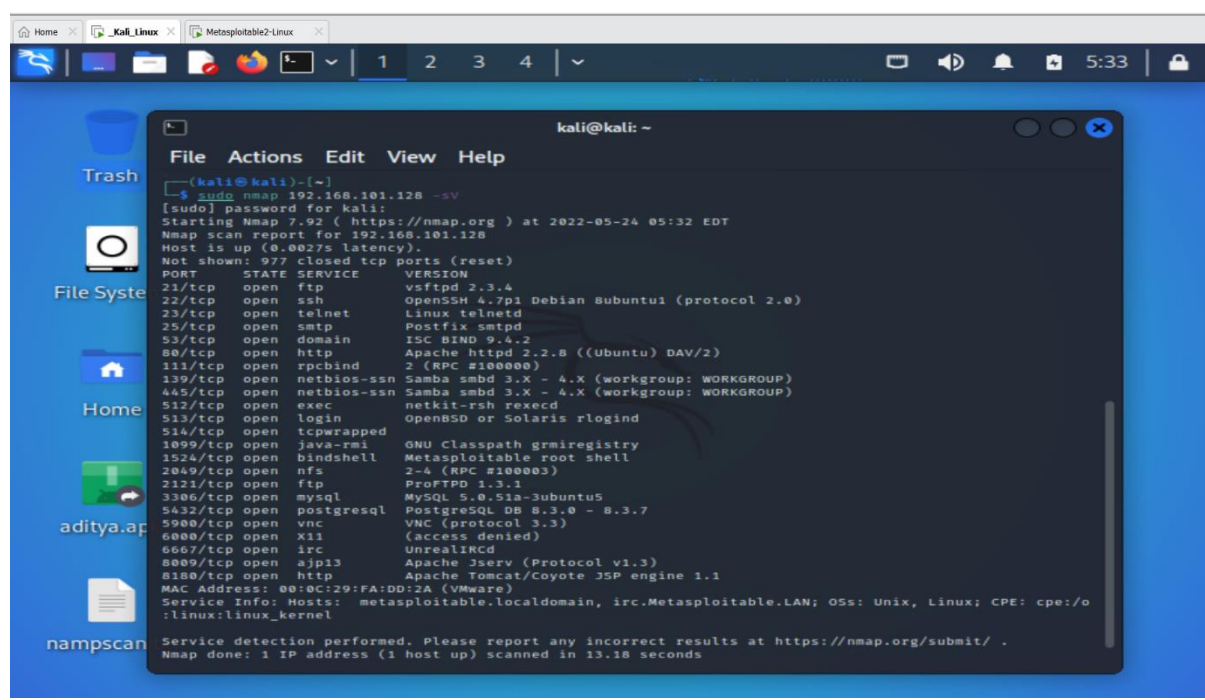
Using the command nmap <ip address> -oN <path>/<filename>

A screenshot of a Kali Linux desktop environment. The top panel shows the system menu, taskbar with various application icons, and the system clock displaying 5:24. A terminal window titled '~/.Desktop/nampscan.txt - Mousepad' is open, showing the output of an Nmap scan. The scan was initiated on Tue May 24 05:21:28 2022 for the IP address 192.168.101.128. The report indicates that the host is up and lists 28 open ports with their corresponding services. The terminal output is as follows:

```
1 # Nmap 7.92 scan initiated Tue May 24 05:21:28 2022 as: nmap -oN /home/kali/Desktop/nampscan.txt
2 Nmap scan report for 192.168.101.128
3 Host is up (0.0029s latency).
4 Not shown: 977 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE
6 21/tcp    open  ftp
7 22/tcp    open  ssh
8 23/tcp    open  telnet
9 25/tcp    open  smtp
10 53/tcp    open  domain
11 80/tcp    open  http
12 111/tcp   open  rpcbind
13 139/tcp   open  netbios-ssn
14 445/tcp   open  microsoft-ds
15 512/tcp   open  exec
16 513/tcp   open  login
17 514/tcp   open  shell
18 1089/tcp  open  rmiregistry
19 1524/tcp  open  ingreslock
20 2049/tcp  open  nfs
21 2121/tcp  open  ccproxy-ftp
22 3306/tcp  open  mysql
23 5432/tcp  open  postgresql
24 5900/tcp  open  vnc
25 6000/tcp  open  X11
26 6667/tcp  open  irc
27 8009/tcp  open  ajp13
28 8180/tcp  open  unknown
29
30 # Nmap done at Tue May 24 05:21:28 2022 -- 1 IP address (1 host up) scanned in 0.24 seconds
31
```

Step6:-Detect the version of all port service using this command
sudo nmap <ip address> -sV

and enter the password of kali for root privilege then press enter



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying the output of an Nmap scan. The user has entered the password for kali to gain root access. The scan results show various open ports and services on the target IP address.

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap 192.168.101.128 -sV  
[sudo] password for kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 05:32 EDT  
Nmap scan report for 192.168.101.128  
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 Subuntu1 (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        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
1049/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:FA:DD: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 13.18 seconds
```

Step7:- Save it to the specifiad file path using command

sudo nmap <ip address> -sV -oN
<path>/<filename>

```
Home x_Kali_Linux x_Metasploitable2-Linux
kali@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

(kali@kali)-[~]
$ nmap 192.168.101.128 -oV -oN /home/kali/Desktop/nampscanversion.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 05:34 EDT
Nmap scan report for 192.168.101.128
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login          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
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  x11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o
:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.37 seconds

(kali@kali)-[~]
$
```

Step7:- Now your port information, services and version details collected into the specific file .