

## Part 1: Running a default Nmap scan on Metasploitable 2 to see which ports are open

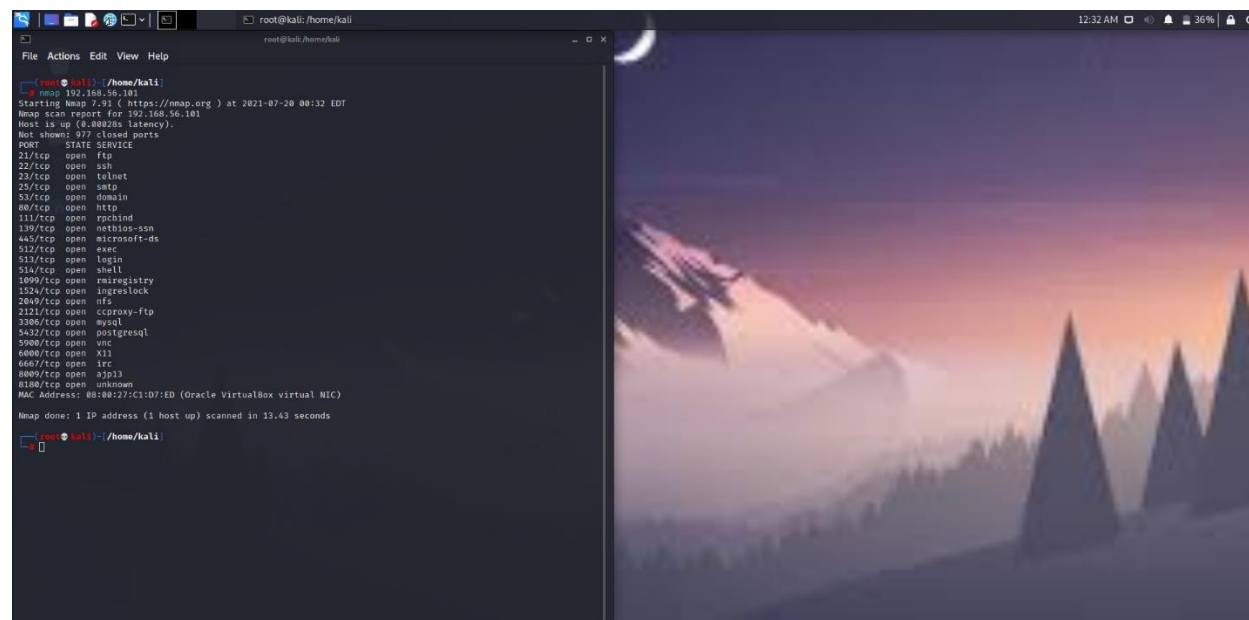
First, we ran an ifconfig on Metasploitable to see what its IP address was

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c1:d7:ed
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec1:d7ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66885 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66755 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4285505 (4.0 MB)  TX bytes:3613969 (3.4 MB)
          Base address:0xd020  Memory:f0200000-f0220000

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:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)

msfadmin@metasploitable:~$
```

Using the IP address given to us, we ran the Nmap scan in Kali Linux



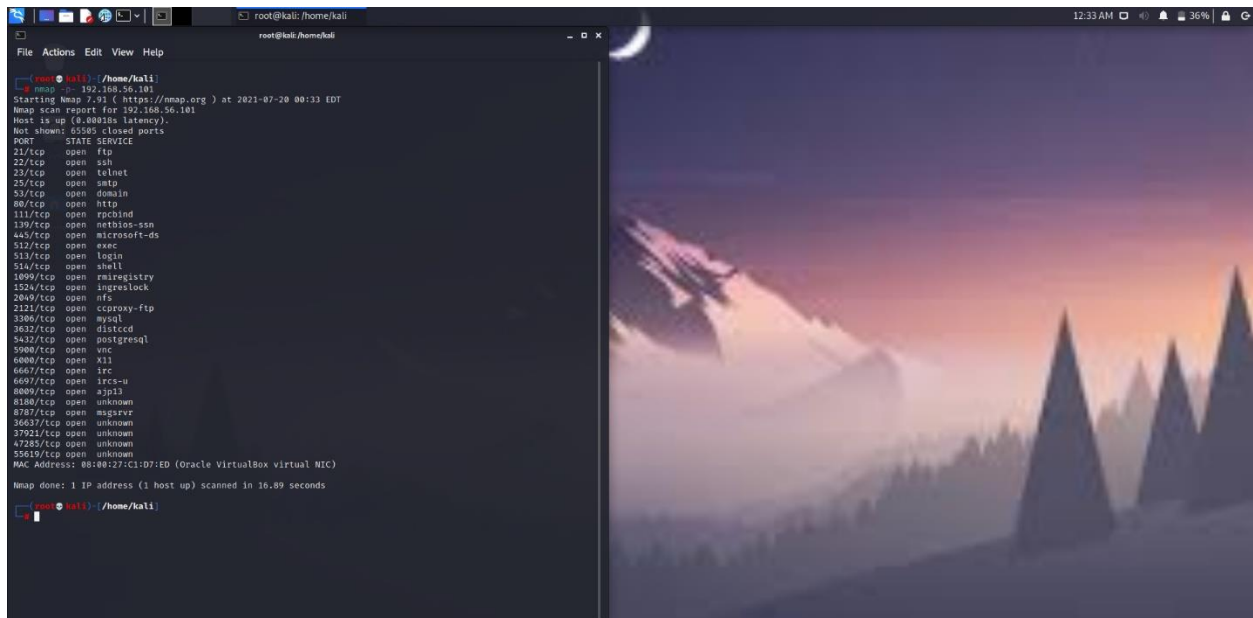
```
root@kali:~/home/kali# nmap 192.168.56.101
Starting Nmap 7.91 (https://nmap.org) at 2021-07-20 00:32 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00028s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    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
8080/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C1:D7:ED (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds

root@kali:~/home/kali#
```

Between ports 0 and 1000, these are all the ports open

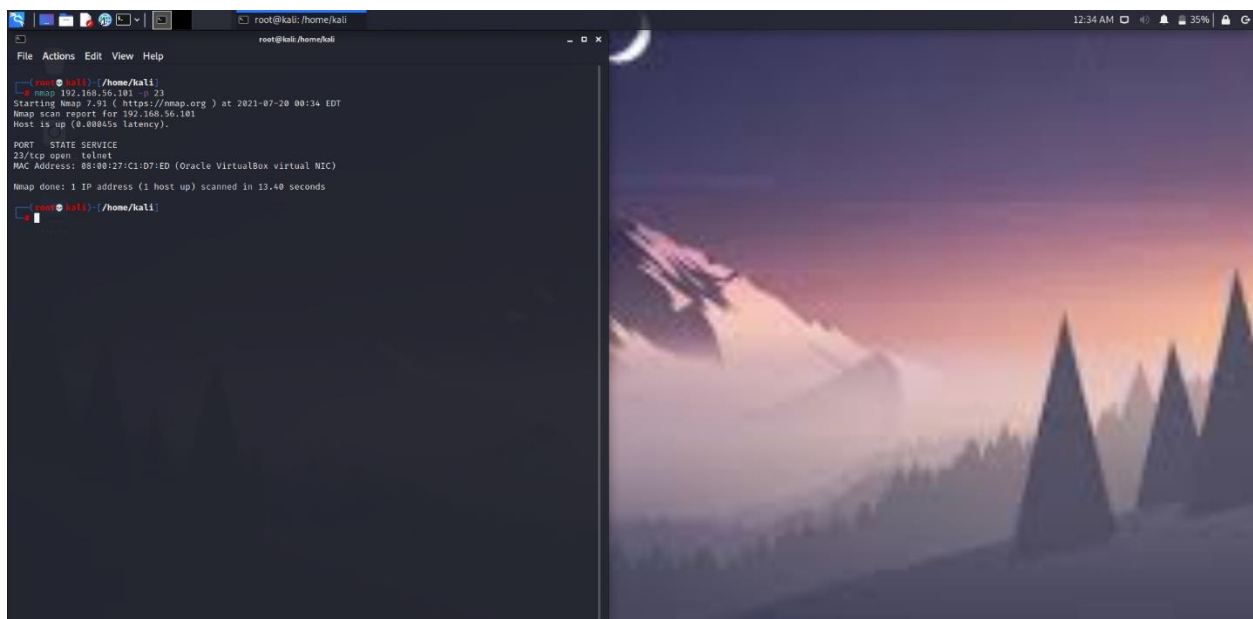
## Part 2: Running a Nmap scan for all ports



```
root@kali:~/home/kali# nmap -p- 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-20 00:33 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00010s latency).
Not shown: 65535 closed ports
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
1522/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3200/tcp  open  nsvl
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
6697/tcp  open  irc-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8187/tcp  open  msgrtr
36637/tcp open  unknown
37921/tcp open  unknown
47285/tcp open  unknown
55619/tcp open  unknown
MAC Address: 08:00:27:C1:D7:ED (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
root@kali:~/home/kali#
```

## Part 3: Exploiting a service

In this case we have decided to exploit telnet service.



```
root@kali:~/home/kali# nmap 192.168.56.101 -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-20 00:34 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00045s latency).
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 08:00:27:C1:D7:ED (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
root@kali:~/home/kali#
```

Using telnet, we managed to get access to Metasploitable's user credentials and were able to login with admin privileges.



Now switching over to Metasploitable where we see if this file has been made or not and what it contains

```
msfadmin@metasploitable:~$ ls
new  vulnerable
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ cd new
msfadmin@metasploitable:~/new$ ls
hi.txt
msfadmin@metasploitable:~/new$ _
```

```
msfadmin@metasploitable:~/new$ cat hi.txt
Hi. This VM has been hacked. Have a good day. Bye.
msfadmin@metasploitable:~/new$ _
```

With this we can say that the target has been successfully hacked using the telnet exploit.