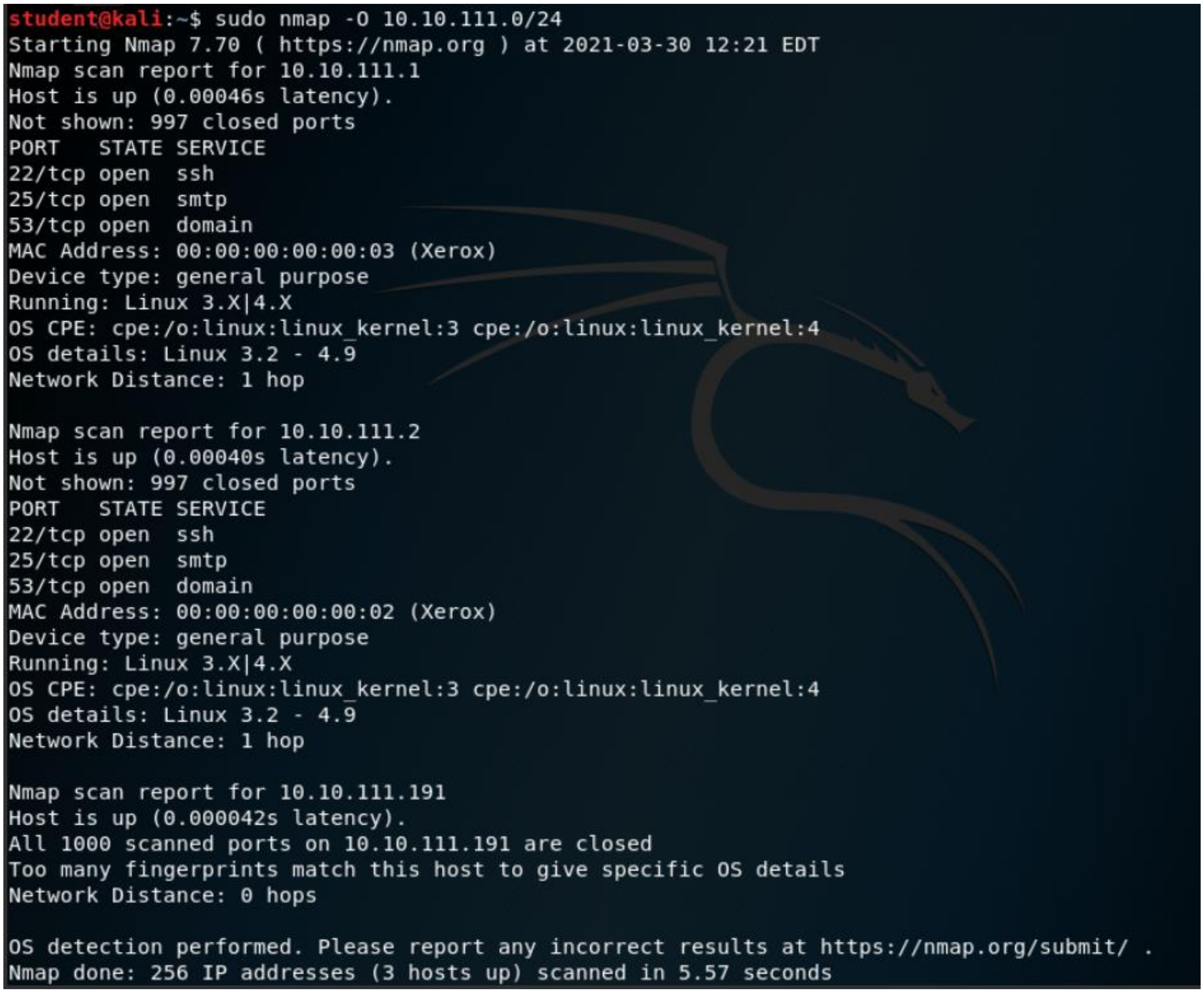
Brian Chan
March 31st, 2021

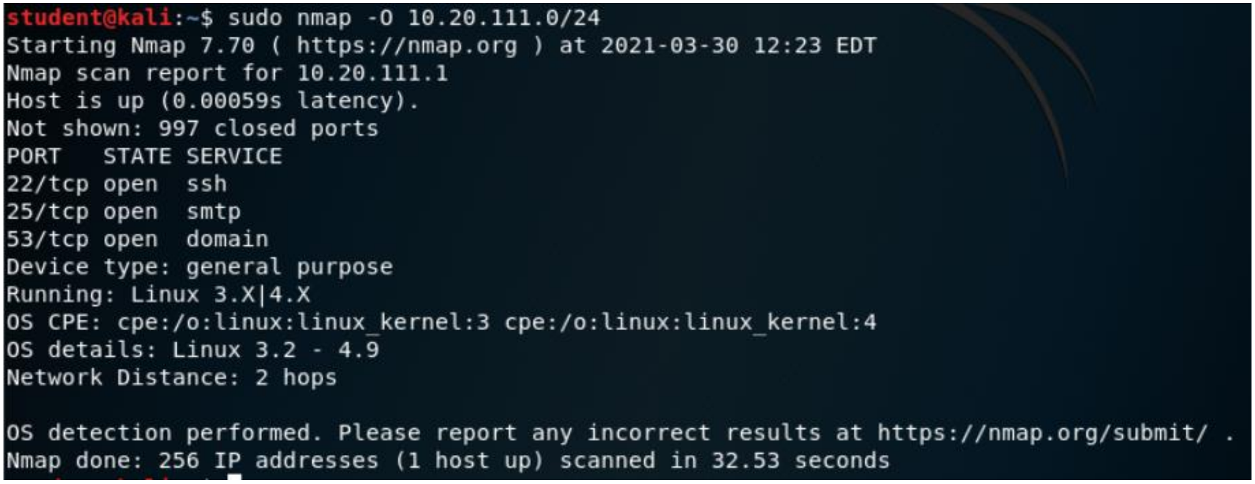
CS-UY 3933 Network Security
Lab 3

Part 1



```
student@kali:~$ sudo nmap -O 10.10.111.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 12:21 EDT
Nmap scan report for 10.10.111.1
Host is up (0.00046s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain
MAC Address: 00:00:00:00:00:03 (Xerox)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 10.10.111.2
Host is up (0.00040s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain
MAC Address: 00:00:00:00:00:02 (Xerox)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

Nmap scan report for 10.10.111.191
Host is up (0.000042s latency).
All 1000 scanned ports on 10.10.111.191 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.57 seconds
```

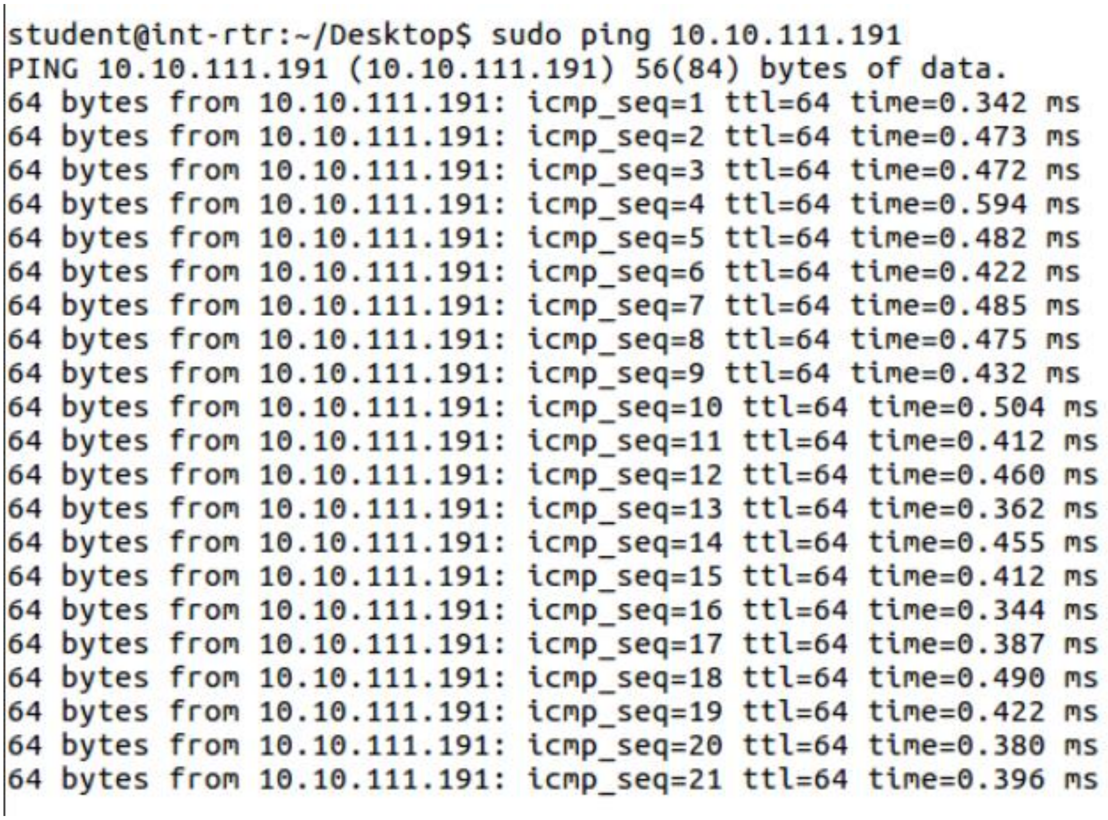
A. Command used: sudo nmap -O 10.10.111.0/24



```
student@kali:~$ sudo nmap -O 10.20.111.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2021-03-30 12:23 EDT
Nmap scan report for 10.20.111.1
Host is up (0.00059s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 32.53 seconds
```

B. Command used: sudo nmap -O 10.20.111.0/24

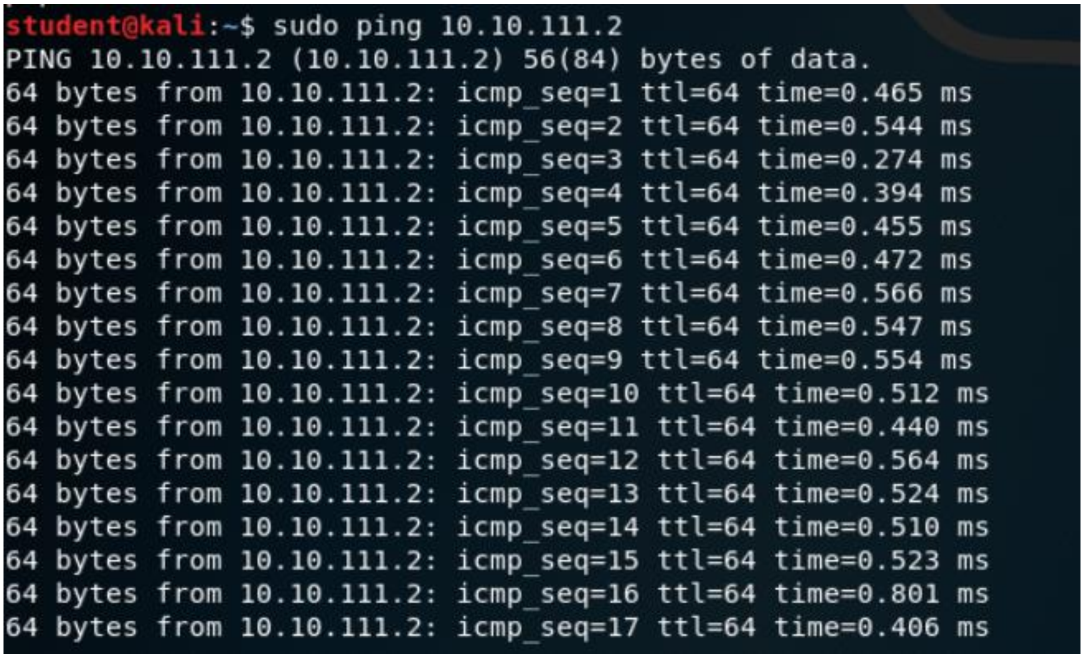
Part 2



```
student@int-rtr:~/Desktop$ sudo ping 10.10.111.191
PING 10.10.111.191 (10.10.111.191) 56(84) bytes of data.
64 bytes from 10.10.111.191: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 10.10.111.191: icmp_seq=2 ttl=64 time=0.473 ms
64 bytes from 10.10.111.191: icmp_seq=3 ttl=64 time=0.472 ms
64 bytes from 10.10.111.191: icmp_seq=4 ttl=64 time=0.594 ms
64 bytes from 10.10.111.191: icmp_seq=5 ttl=64 time=0.482 ms
64 bytes from 10.10.111.191: icmp_seq=6 ttl=64 time=0.422 ms
64 bytes from 10.10.111.191: icmp_seq=7 ttl=64 time=0.485 ms
64 bytes from 10.10.111.191: icmp_seq=8 ttl=64 time=0.475 ms
64 bytes from 10.10.111.191: icmp_seq=9 ttl=64 time=0.432 ms
64 bytes from 10.10.111.191: icmp_seq=10 ttl=64 time=0.504 ms
64 bytes from 10.10.111.191: icmp_seq=11 ttl=64 time=0.412 ms
64 bytes from 10.10.111.191: icmp_seq=12 ttl=64 time=0.460 ms
64 bytes from 10.10.111.191: icmp_seq=13 ttl=64 time=0.362 ms
64 bytes from 10.10.111.191: icmp_seq=14 ttl=64 time=0.455 ms
64 bytes from 10.10.111.191: icmp_seq=15 ttl=64 time=0.412 ms
64 bytes from 10.10.111.191: icmp_seq=16 ttl=64 time=0.344 ms
64 bytes from 10.10.111.191: icmp_seq=17 ttl=64 time=0.387 ms
64 bytes from 10.10.111.191: icmp_seq=18 ttl=64 time=0.490 ms
64 bytes from 10.10.111.191: icmp_seq=19 ttl=64 time=0.422 ms
64 bytes from 10.10.111.191: icmp_seq=20 ttl=64 time=0.380 ms
64 bytes from 10.10.111.191: icmp_seq=21 ttl=64 time=0.396 ms
```

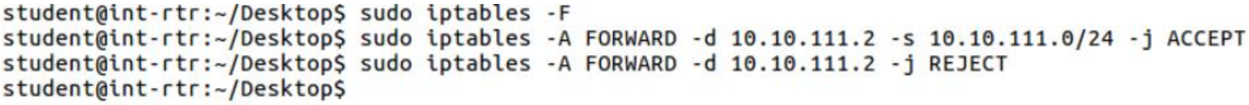
Pings show that the internal router can communicate with the external router and machines.

Command: sudo ping 10.10.111.2



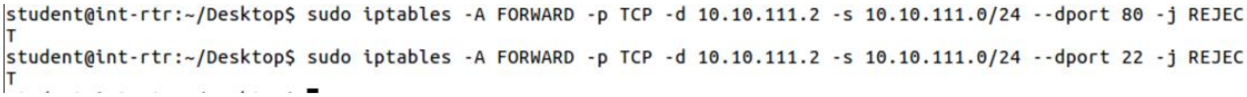
```
student@kali:~$ sudo ping 10.10.111.2
PING 10.10.111.2 (10.10.111.2) 56(84) bytes of data.
64 bytes from 10.10.111.2: icmp_seq=1 ttl=64 time=0.465 ms
64 bytes from 10.10.111.2: icmp_seq=2 ttl=64 time=0.544 ms
64 bytes from 10.10.111.2: icmp_seq=3 ttl=64 time=0.274 ms
64 bytes from 10.10.111.2: icmp_seq=4 ttl=64 time=0.394 ms
64 bytes from 10.10.111.2: icmp_seq=5 ttl=64 time=0.455 ms
64 bytes from 10.10.111.2: icmp_seq=6 ttl=64 time=0.472 ms
64 bytes from 10.10.111.2: icmp_seq=7 ttl=64 time=0.566 ms
64 bytes from 10.10.111.2: icmp_seq=8 ttl=64 time=0.547 ms
64 bytes from 10.10.111.2: icmp_seq=9 ttl=64 time=0.554 ms
64 bytes from 10.10.111.2: icmp_seq=10 ttl=64 time=0.512 ms
64 bytes from 10.10.111.2: icmp_seq=11 ttl=64 time=0.440 ms
64 bytes from 10.10.111.2: icmp_seq=12 ttl=64 time=0.564 ms
64 bytes from 10.10.111.2: icmp_seq=13 ttl=64 time=0.524 ms
64 bytes from 10.10.111.2: icmp_seq=14 ttl=64 time=0.510 ms
64 bytes from 10.10.111.2: icmp_seq=15 ttl=64 time=0.523 ms
64 bytes from 10.10.111.2: icmp_seq=16 ttl=64 time=0.801 ms
64 bytes from 10.10.111.2: icmp_seq=17 ttl=64 time=0.406 ms
```

Responding to the pings from the internal router



```
student@int-rtr:~/Desktop$ sudo iptables -F
student@int-rtr:~/Desktop$ sudo iptables -A FORWARD -d 10.10.111.2 -s 10.10.111.0/24 -j ACCEPT
student@int-rtr:~/Desktop$ sudo iptables -A FORWARD -d 10.10.111.2 -j REJECT
student@int-rtr:~/Desktop$
```

Commands used to accept communication with the external network, and to reject incoming communication requests.

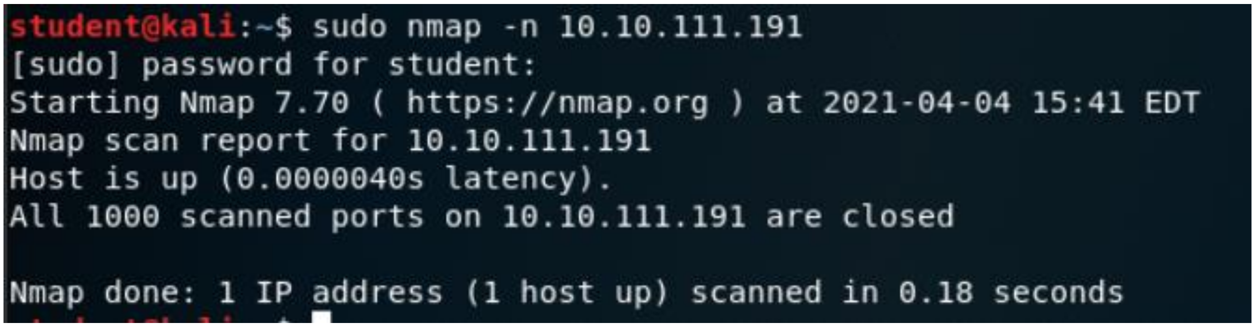


```
student@int-rtr:~/Desktop$ sudo iptables -A FORWARD -p TCP -d 10.10.111.2 -s 10.10.111.0/24 --dport 80 -j REJEC
T
student@int-rtr:~/Desktop$ sudo iptables -A FORWARD -p TCP -d 10.10.111.2 -s 10.10.111.0/24 --dport 22 -j REJEC
T
```

Commands used to block outgoing SSH and HTTP requests.

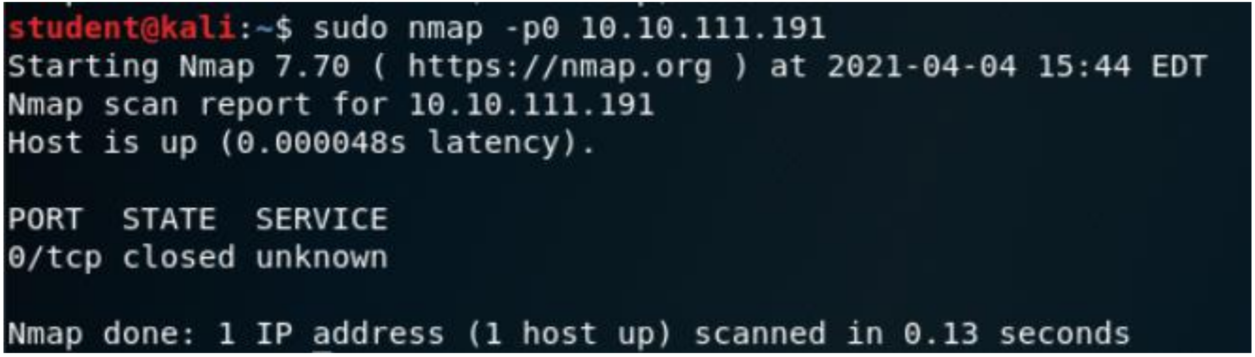
Part 3

1.
    a. -n: Command that disables reverse DNS resolutions



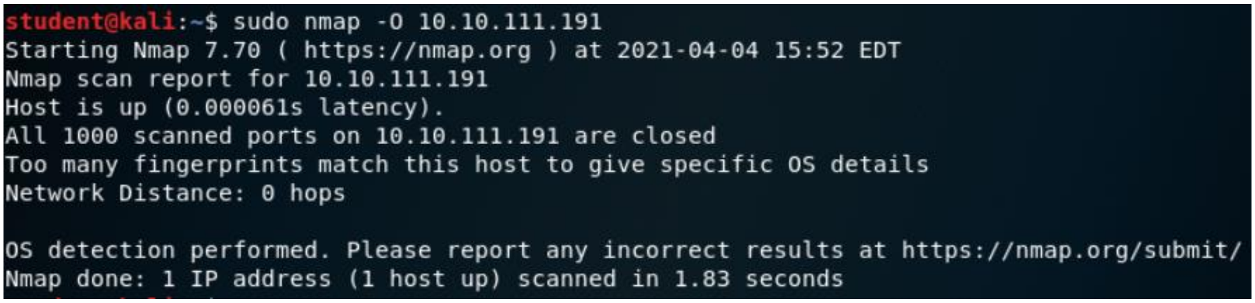
```
student@kali:~$ sudo nmap -n 10.10.111.191
[sudo] password for student:
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 15:41 EDT
Nmap scan report for 10.10.111.191
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.10.111.191 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
```

    b. -P0: Command that does the IP protocol ping



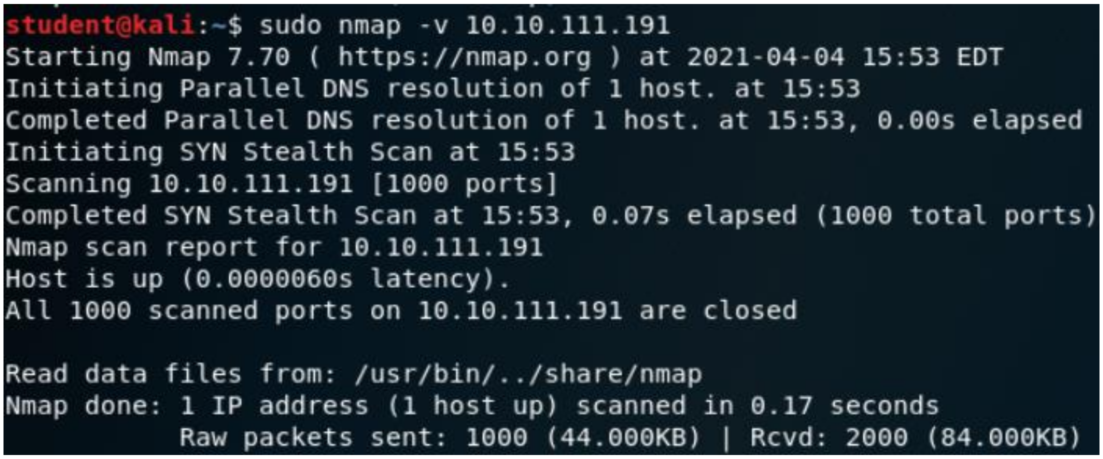
```
student@kali:~$ sudo nmap -p0 10.10.111.191
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 15:44 EDT
Nmap scan report for 10.10.111.191
Host is up (0.000048s latency).

PORT  STATE  SERVICE
0/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

    c. -O: Command that detects Operating System



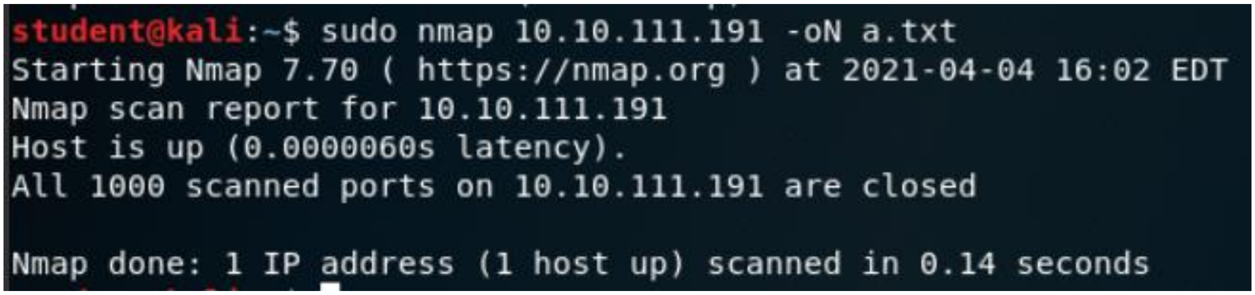
```
student@kali:~$ sudo nmap -O 10.10.111.191
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 15:52 EDT
Nmap scan report for 10.10.111.191
Host is up (0.000061s latency).
All 1000 scanned ports on 10.10.111.191 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1.83 seconds
```

    d. -v: Command that provides more verbose output



```
student@kali:~$ sudo nmap -v 10.10.111.191
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 15:53 EDT
Initiating Parallel DNS resolution of 1 host. at 15:53
Completed Parallel DNS resolution of 1 host. at 15:53, 0.00s elapsed
Initiating SYN Stealth Scan at 15:53
Scanning 10.10.111.191 [1000 ports]
Completed SYN Stealth Scan at 15:53, 0.07s elapsed (1000 total ports)
Nmap scan report for 10.10.111.191
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.10.111.191 are closed

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2000 (84.000KB)
```

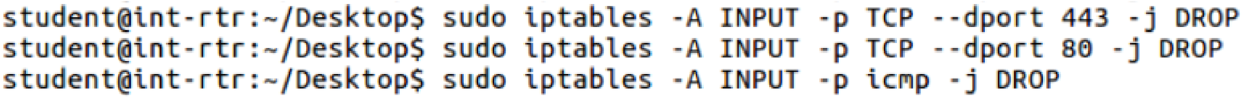
e. -oN: Command that provides the normal output to inputted text file



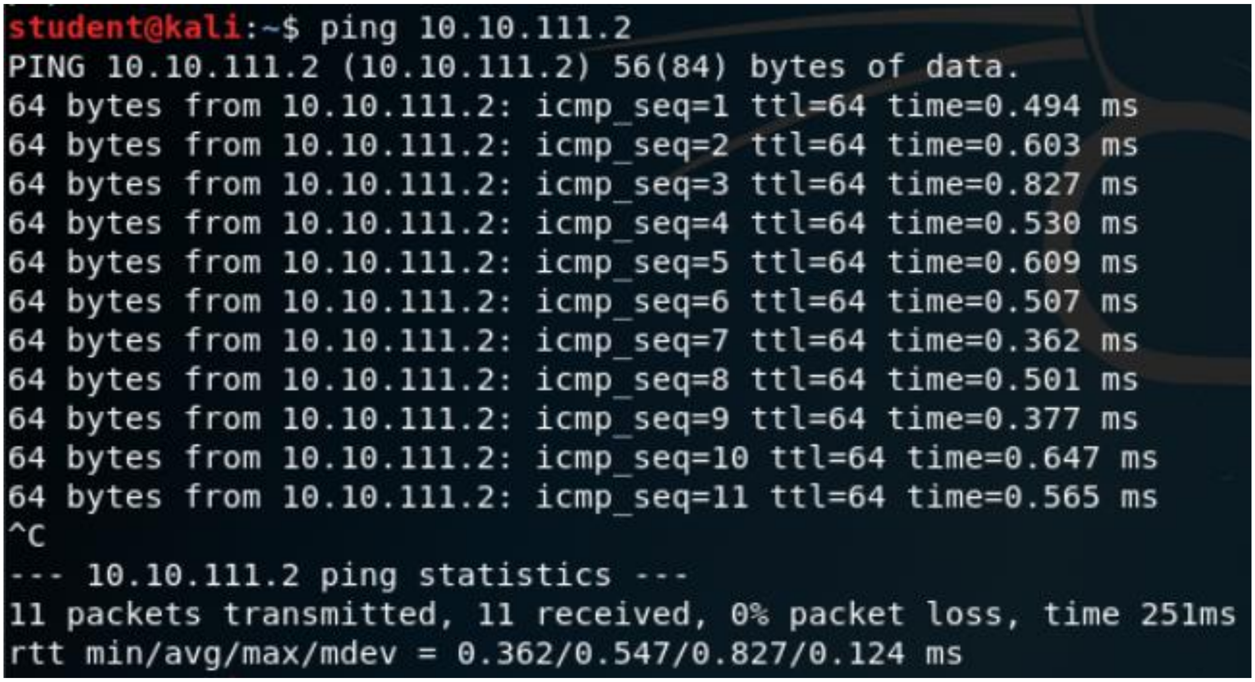
```
student@kali:~$ sudo nmap 10.10.111.191 -oN a.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 16:02 EDT
Nmap scan report for 10.10.111.191
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.10.111.191 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

2.

a. Commands:

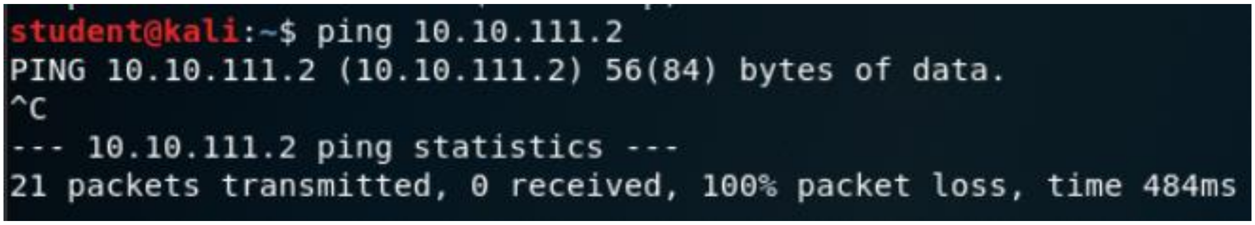


```
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p TCP --dport 443 -j DROP
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p TCP --dport 80 -j DROP
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p icmp -j DROP
```



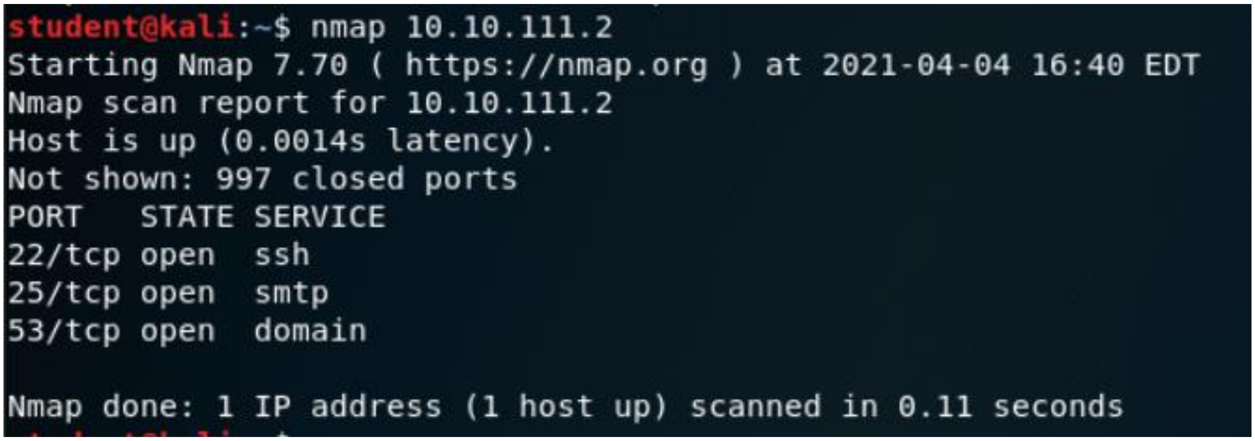
```
student@kali:~$ ping 10.10.111.2
PING 10.10.111.2 (10.10.111.2) 56(84) bytes of data.
64 bytes from 10.10.111.2: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 10.10.111.2: icmp_seq=2 ttl=64 time=0.603 ms
64 bytes from 10.10.111.2: icmp_seq=3 ttl=64 time=0.827 ms
64 bytes from 10.10.111.2: icmp_seq=4 ttl=64 time=0.530 ms
64 bytes from 10.10.111.2: icmp_seq=5 ttl=64 time=0.609 ms
64 bytes from 10.10.111.2: icmp_seq=6 ttl=64 time=0.507 ms
64 bytes from 10.10.111.2: icmp_seq=7 ttl=64 time=0.362 ms
64 bytes from 10.10.111.2: icmp_seq=8 ttl=64 time=0.501 ms
64 bytes from 10.10.111.2: icmp_seq=9 ttl=64 time=0.377 ms
64 bytes from 10.10.111.2: icmp_seq=10 ttl=64 time=0.647 ms
64 bytes from 10.10.111.2: icmp_seq=11 ttl=64 time=0.565 ms
^C
--- 10.10.111.2 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 251ms
rtt min/avg/max/mdev = 0.362/0.547/0.827/0.124 ms
```

Pinging internal router before writing firewall rules to stop probing.



```
student@kali:~$ ping 10.10.111.2
PING 10.10.111.2 (10.10.111.2) 56(84) bytes of data.
^C
--- 10.10.111.2 ping statistics ---
21 packets transmitted, 0 received, 100% packet loss, time 484ms
```

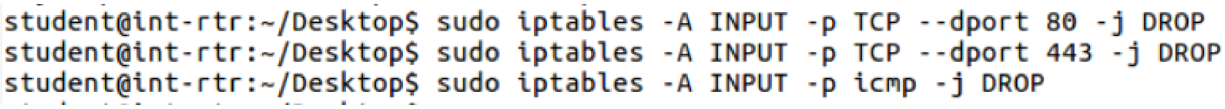
Probing has been blocked.



```
student@kali:~$ nmap 10.10.111.2
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 16:40 EDT
Nmap scan report for 10.10.111.2
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

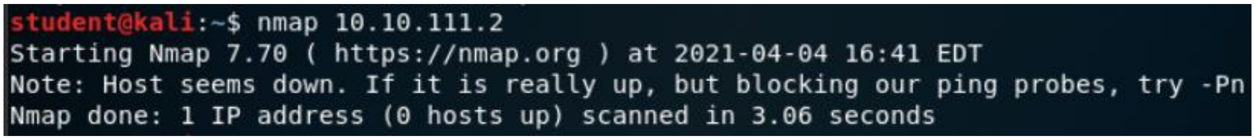
nmap scan before rules are written.

b.



```
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p TCP --dport 80 -j DROP
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p TCP --dport 443 -j DROP
student@int-rtr:~/Desktop$ sudo iptables -A INPUT -p icmp -j DROP
```

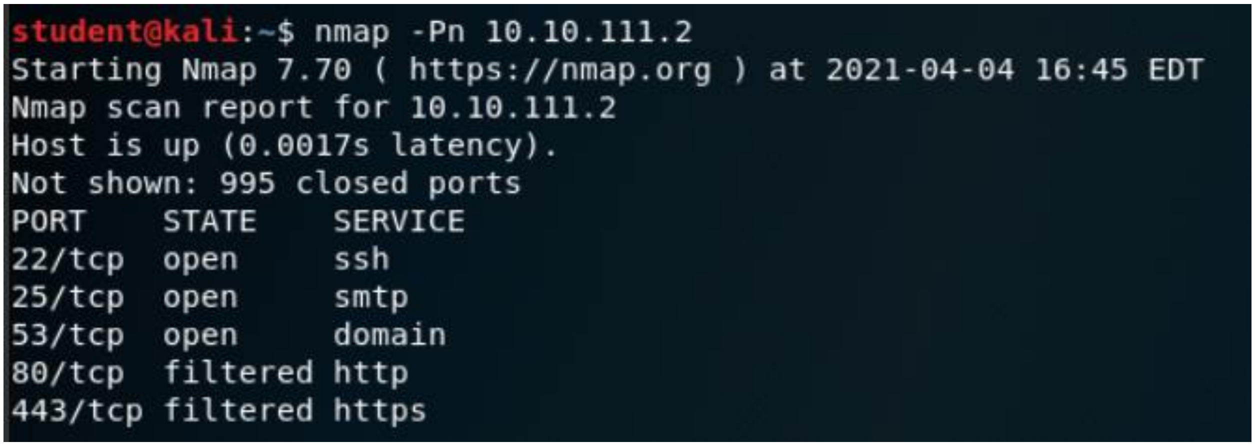
rules inputted, blocks icmp, ssh, and http.



```
student@kali:~$ nmap 10.10.111.2
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 16:41 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.06 seconds
```

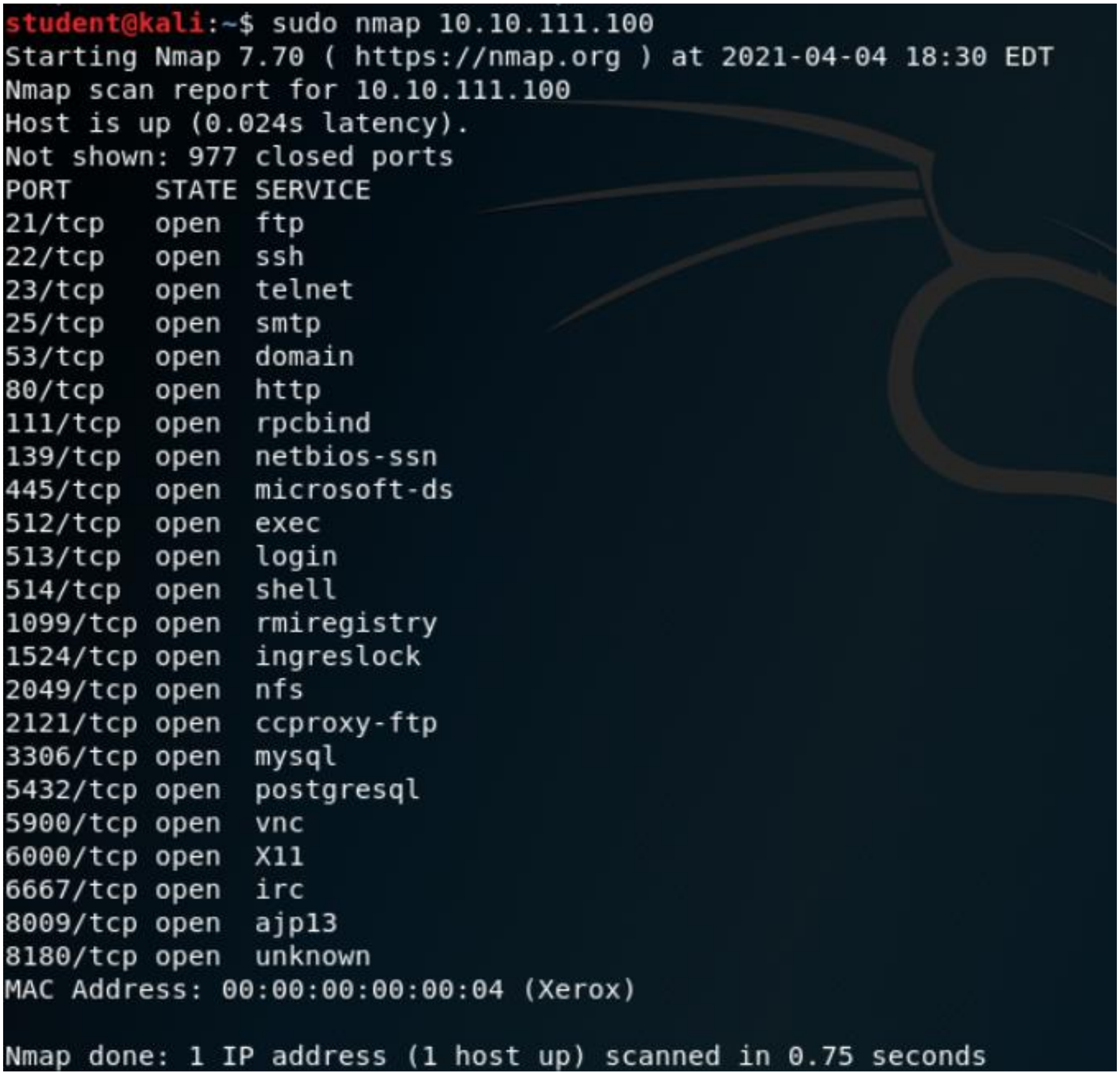
nmap scan after rules are written, the probing has been blocked.

c. Command: nmap -Pn 10.10.111.2 (sudo nmap 10.10.111.2 also works)



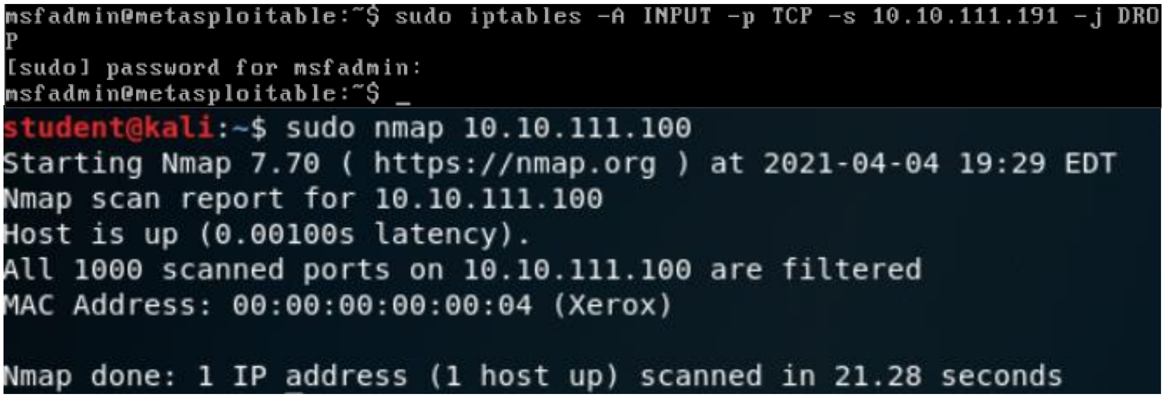
```
student@kali:~$ nmap -Pn 10.10.111.2
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 16:45 EDT
Nmap scan report for 10.10.111.2
Host is up (0.0017s latency).
Not shown: 995 closed ports
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  open     smtp
53/tcp  open     domain
80/tcp  filtered http
443/tcp filtered https
```

3.



```
student@kali:~$ sudo nmap 10.10.111.100
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 18:30 EDT
Nmap scan report for 10.10.111.100
Host is up (0.024s 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
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:00:00:00:00:04 (Xerox)

Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
```

Nmap scan of metaexploitable vm



```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p TCP -s 10.10.111.191 -j DRO
P
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ _
```

```
student@kali:~$ sudo nmap 10.10.111.100
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-04 19:29 EDT
Nmap scan report for 10.10.111.100
Host is up (0.00100s latency).
All 1000 scanned ports on 10.10.111.100 are filtered
MAC Address: 00:00:00:00:00:04 (Xerox)

Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds
```

Nmap scan of metaexploitable vm after command was inputted.

Blocking all the TCP SYN packets from an IP address could lead to an innocent user being blocked off. This could happen when the DHCP server leases the blocked IP to another user trying to connect to the network. Blocking the TCP SYN packets from one particular IP also seems like pooling resources to stop something that could easily be bypassed through spoofing a different IP address.