Sam Mishra
N12140743

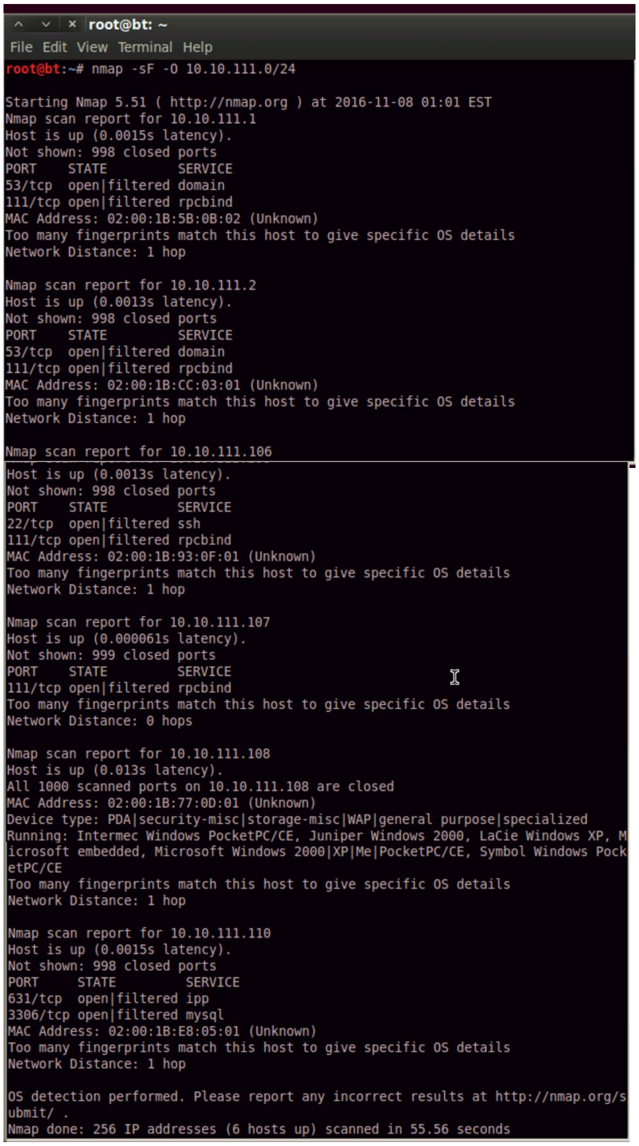
# Lab 3

## PART 1:

1) The screenshots to the right show the nmap scan of the range of addresses 10.10.111.0/24 given in CIDR notation. The options used in this scan in -sF and -O. -sF specifies a TCP FIN scan and -O specifies to try and OS fingerprint the scanned hosts. The scan of this network found 6 hosts. It found a few open|filtered ports which nmap defines as:

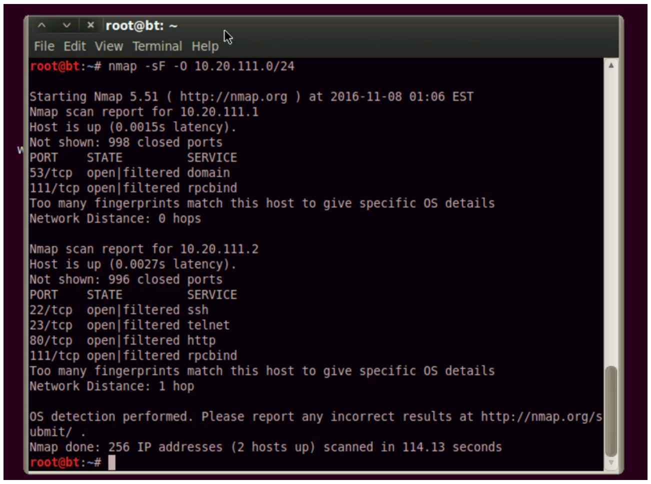
   > "Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered."

   The OS scan was unsuccessful for all but the IP address 10.10.111.108. 10.10.111.108 was not able to narrow it down much but it most likely is Windows, possibly 2000 or XP.



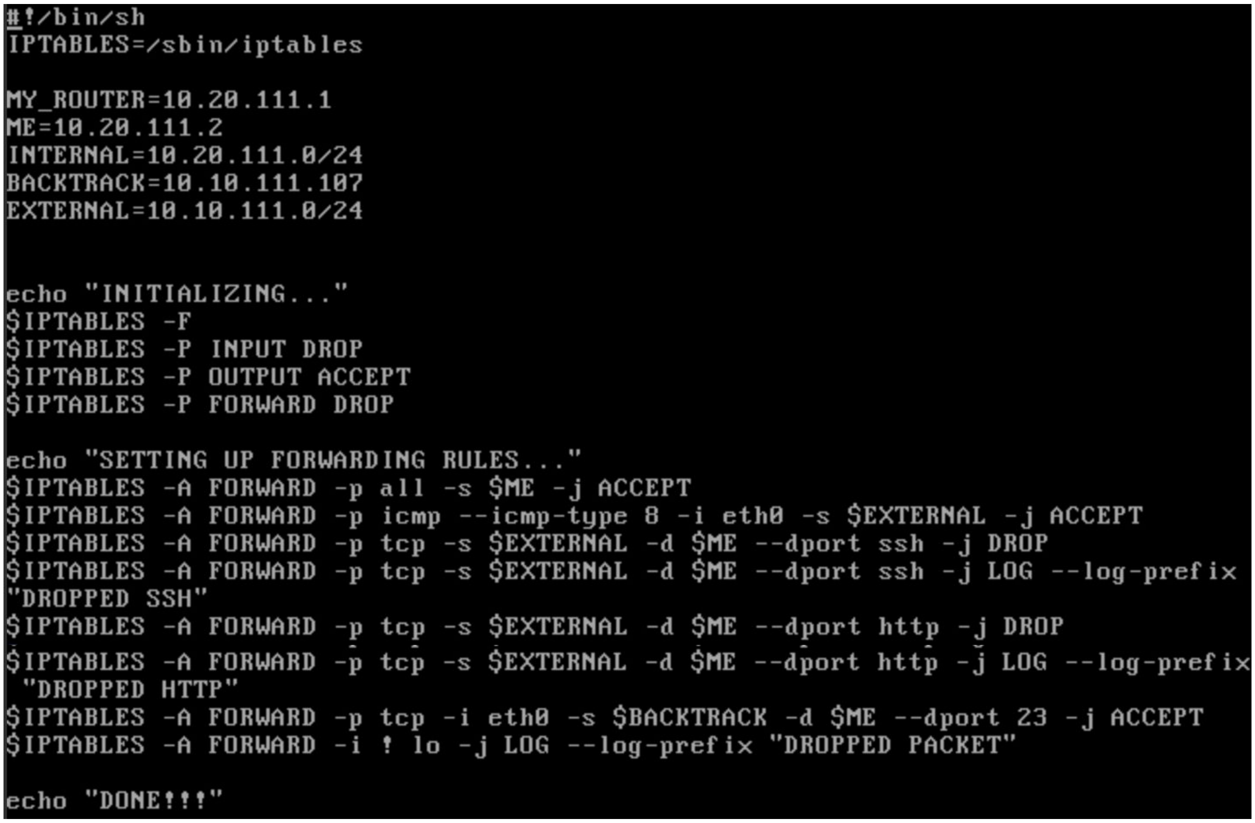
```
root@bt:~# nmap -sF -O 10.10.111.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 01:01 EST
Nmap scan report for 10.10.111.1
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
53/tcp  open|filtered domain
111/tcp open|filtered rpcbind
MAC Address: 02:00:1B:5B:0B:02 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.10.111.2
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
53/tcp  open|filtered domain
111/tcp open|filtered rpcbind
MAC Address: 02:00:1B:CC:03:01 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.10.111.106
Host is up (0.0013s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
111/tcp open|filtered rpcbind
MAC Address: 02:00:1B:93:0F:01 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.10.111.107
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
111/tcp open|filtered rpcbind
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Nmap scan report for 10.10.111.108
Host is up (0.013s latency).
All 1000 scanned ports on 10.10.111.108 are closed
MAC Address: 02:00:1B:77:0D:01 (Unknown)
Device type: PDA|security-misc|storage-misc|WAP|general purpose|specialized
Running: Intermec Windows PocketPC/CE, Juniper Windows 2000, LaCie Windows XP, M
icrosoft embedded, Microsoft Windows 2000|XP|Me|PocketPC/CE, Symbol Windows Pock
etPC/CE
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.10.111.110
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT     STATE         SERVICE
631/tcp  open|filtered ipp
3306/tcp open|filtered mysql
MAC Address: 02:00:1B:E8:05:01 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 55.56 seconds
```

2) This next screenshot shows the scan of the 10.20.111.0/24 range. Again a FIN scan was used and OS fingerprinting was requested. Again OS failed and only open|filtered ports were found.



```
root@bt:~# nmap -sF -O 10.20.111.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 01:06 EST
Nmap scan report for 10.20.111.1
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT    STATE         SERVICE
53/tcp  open|filtered domain
111/tcp open|filtered rpcbind
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

Nmap scan report for 10.20.111.2
Host is up (0.0027s latency).
Not shown: 996 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
23/tcp  open|filtered telnet
80/tcp  open|filtered http
111/tcp open|filtered rpcbind
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 114.13 seconds
root@bt:~#
```

**PART 2:**



```
#!/bin/sh
IPTABLES=/sbin/iptables

MY_ROUTER=10.20.111.1
ME=10.20.111.2
INTERNAL=10.20.111.0/24
BACKTRACK=10.10.111.107
EXTERNAL=10.10.111.0/24


echo "INITIALIZING..."
$IPTABLES -F
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -P FORWARD DROP

echo "SETTING UP FORWARDING RULES..."
$IPTABLES -A FORWARD -p all -s $ME -j ACCEPT
$IPTABLES -A FORWARD -p icmp --icmp-type 8 -i eth0 -s $EXTERNAL -j ACCEPT
$IPTABLES -A FORWARD -p tcp -s $EXTERNAL -d $ME --dport ssh -j DROP
$IPTABLES -A FORWARD -p tcp -s $EXTERNAL -d $ME --dport ssh -j LOG --log-prefix
"DROPPED SSH"
$IPTABLES -A FORWARD -p tcp -s $EXTERNAL -d $ME --dport http -j DROP
$IPTABLES -A FORWARD -p tcp -s $EXTERNAL -d $ME --dport http -j LOG --log-prefix
 "DROPPED HTTP"
$IPTABLES -A FORWARD -p tcp -i eth0 -s $BACKTRACK -d $ME --dport 23 -j ACCEPT
$IPTABLES -A FORWARD -i ! lo -j LOG --log-prefix "DROPPED PACKET"

echo "DONE!!!"
```

-P sets the default target.  So all INPUT is DROPPED.  All OUTPUT is ACCEPTED and FORWARDED traffic is DROPPED.

-A adds a new rule to the end of the specified chain (chains being the rules you follow when either INPUT, OUTPUT, or FORWARD traffic is encountered by our firewall.)

-p specifies the protocol the rule is targeting.

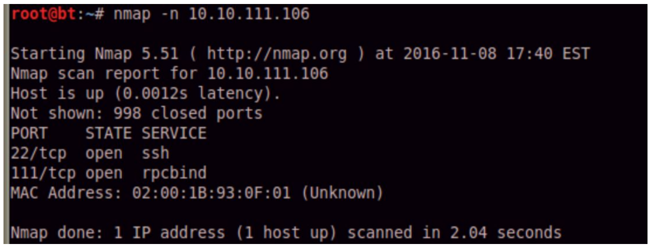
-s is the source address, so traffic with this source address is a candidate for our rule.

-d is the destination address, so traffic with this destination address is a candidate for our rule.

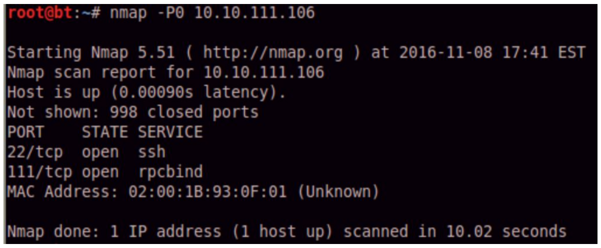
-j specifies what action you take when a packet matches the specifics of your rule.

## PART 3:

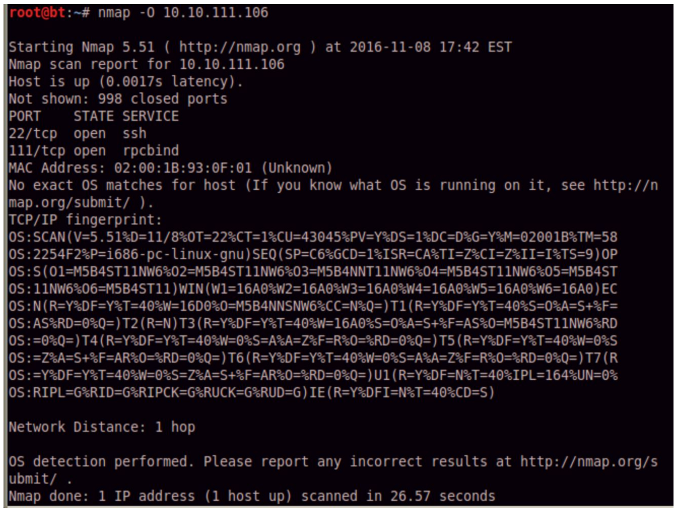
### (1)



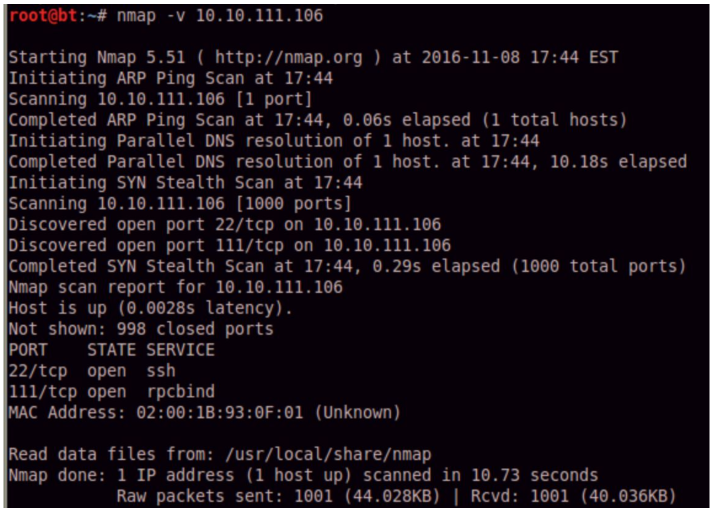
```
root@bt:~# nmap -n 10.10.111.106

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 17:40 EST
Nmap scan report for 10.10.111.106
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 02:00:1B:93:0F:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```



```
root@bt:~# nmap -P0 10.10.111.106

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 17:41 EST
Nmap scan report for 10.10.111.106
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 02:00:1B:93:0F:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds
```



```
root@bt:~# nmap -O 10.10.111.106

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 17:42 EST
Nmap scan report for 10.10.111.106
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 02:00:1B:93:0F:01 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see http://n
map.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.51%D=11/8%OT=22%CT=1%CU=43045%PV=Y%DS=1%DC=D%G=Y%M=02001B%TM=58
OS:2254F2%P=i686-pc-linux-gnu)SEQ(SP=C6%GCD=1%ISR=CA%TI=Z%CI=Z%II=I%TS=9)OP
OS:S(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST
OS:11NW6%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC
OS:N(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW6%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.57 seconds
```



```
root@bt:~# nmap -v 10.10.111.106

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-08 17:44 EST
Initiating ARP Ping Scan at 17:44
Scanning 10.10.111.106 [1 port]
Completed ARP Ping Scan at 17:44, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:44
Completed Parallel DNS resolution of 1 host. at 17:44, 10.18s elapsed
Initiating SYN Stealth Scan at 17:44
Scanning 10.10.111.106 [1000 ports]
Discovered open port 22/tcp on 10.10.111.106
Discovered open port 111/tcp on 10.10.111.106
Completed SYN Stealth Scan at 17:44, 0.29s elapsed (1000 total ports)
Nmap scan report for 10.10.111.106
Host is up (0.0028s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: 02:00:1B:93:0F:01 (Unknown)

Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.73 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.036KB)
```

-n

FROM nmap.org:

> “Tells Nmap to never do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.”

-P0 (-Pn in new nmap version)

FROM nmap.org:

> “This option skips the Nmap discovery stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host discovery with -Pn causes Nmap to attempt the requested scanning functions against every target IP address specified.”

-O

Enables OS detection

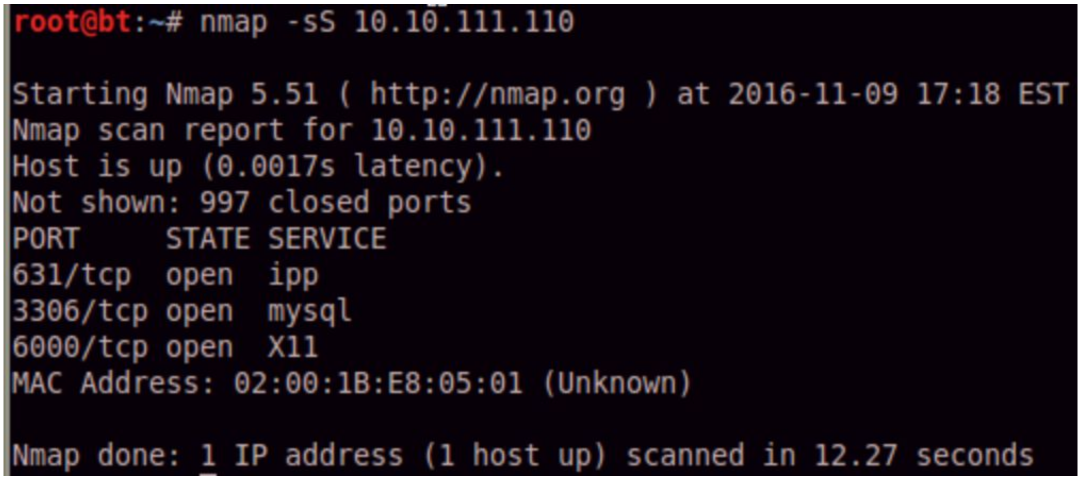
-v

Increase verbosity level

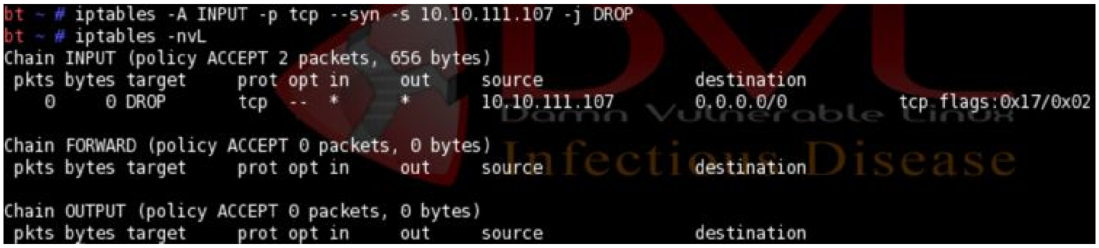
-oN

Output scan in Normal format

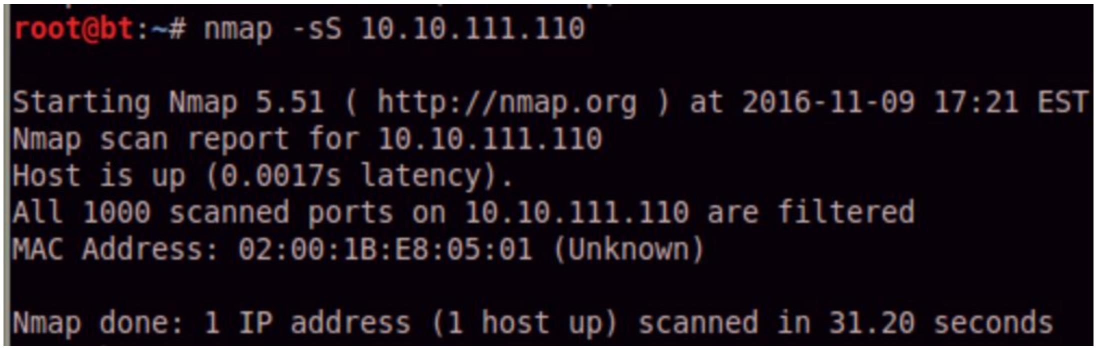
**(3)**



```
root@bt:~# nmap -sS 10.10.111.110

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-09 17:18 EST
Nmap scan report for 10.10.111.110
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
631/tcp  open  ipp
3306/tcp open  mysql
6000/tcp open  X11
MAC Address: 02:00:1B:E8:05:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 12.27 seconds
```



```
bt ~ # iptables -A INPUT -p tcp --syn -s 10.10.111.107 -j DROP
bt ~ # iptables -nvL
Chain INPUT (policy ACCEPT 2 packets, 656 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       10.10.111.107        0.0.0.0/0           tcp flags:0x17/0x02

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```



```
root@bt:~# nmap -sS 10.10.111.110

Starting Nmap 5.51 ( http://nmap.org ) at 2016-11-09 17:21 EST
Nmap scan report for 10.10.111.110
Host is up (0.0017s latency).
All 1000 scanned ports on 10.10.111.110 are filtered
MAC Address: 02:00:1B:E8:05:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 31.20 seconds
```

Blocking all TCP SYN packets means that no machine can initiate a TCP connection with you.  This limits or excludes certain applications from functioning but protects you from SYN scans and other malicious actions that use SYN packets.