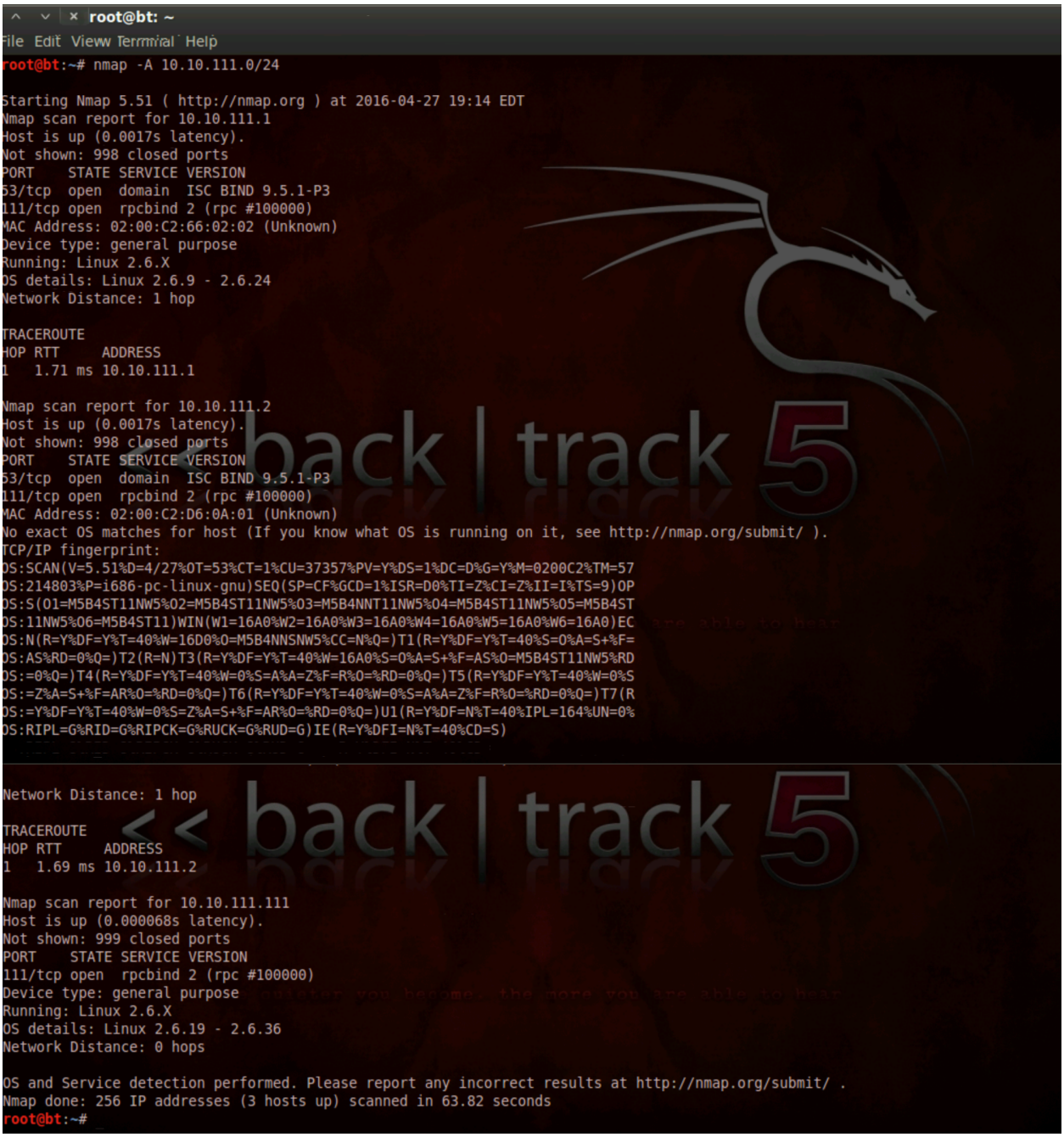
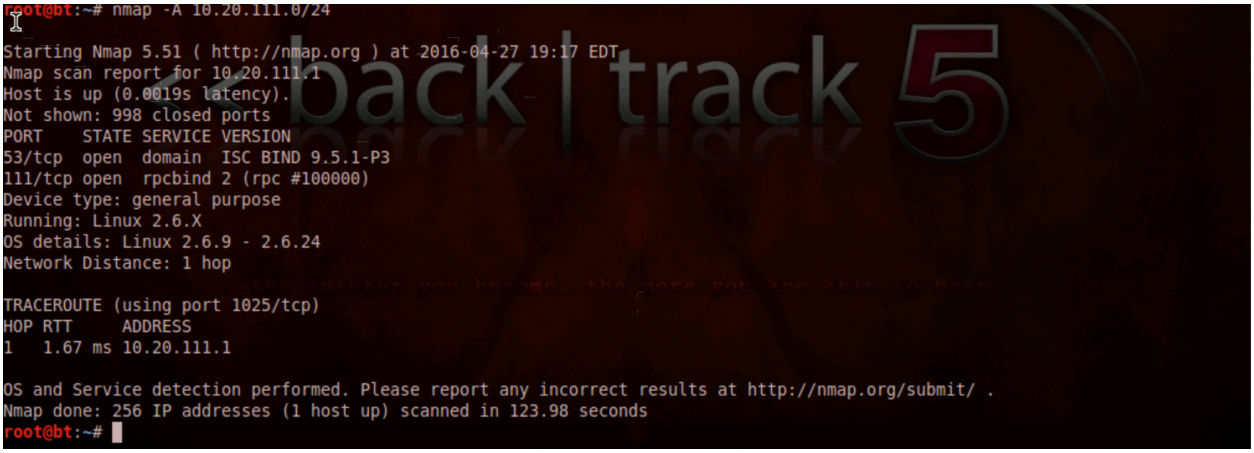
Masato Anzai
Lab #4: nmap/iptables
N12725403

# NMAP:

1. Ports open on 10.10.111.0/24: 63/tcp, 111/tcp
   OS Details: Linux 2.6.9 - 2.6.24
   Command Used: nmap -A 10.10.111.0/24

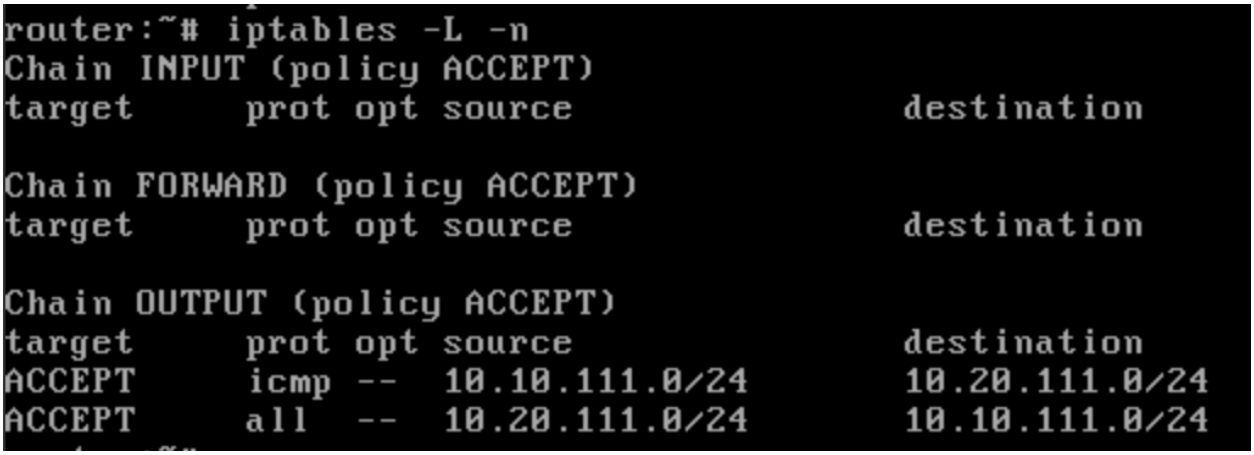


2. Ports Open on 10.20.111.0/24: 53/tcp, 111/tcp
   OS Details: Linux 2.6.9 - 2.6.24
   Command Used: nmap -A 10.20.111.0/24

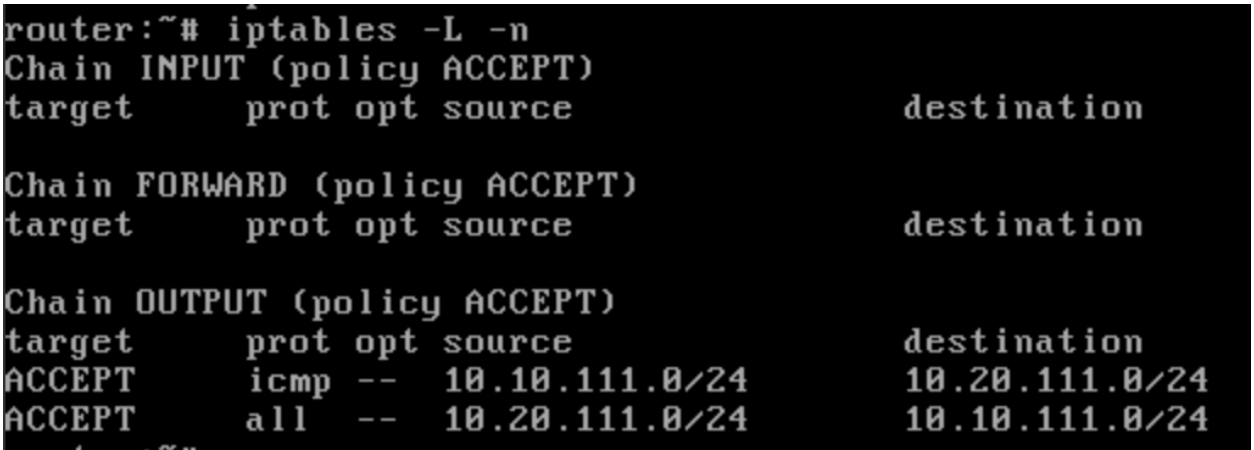



## IPTABLES:

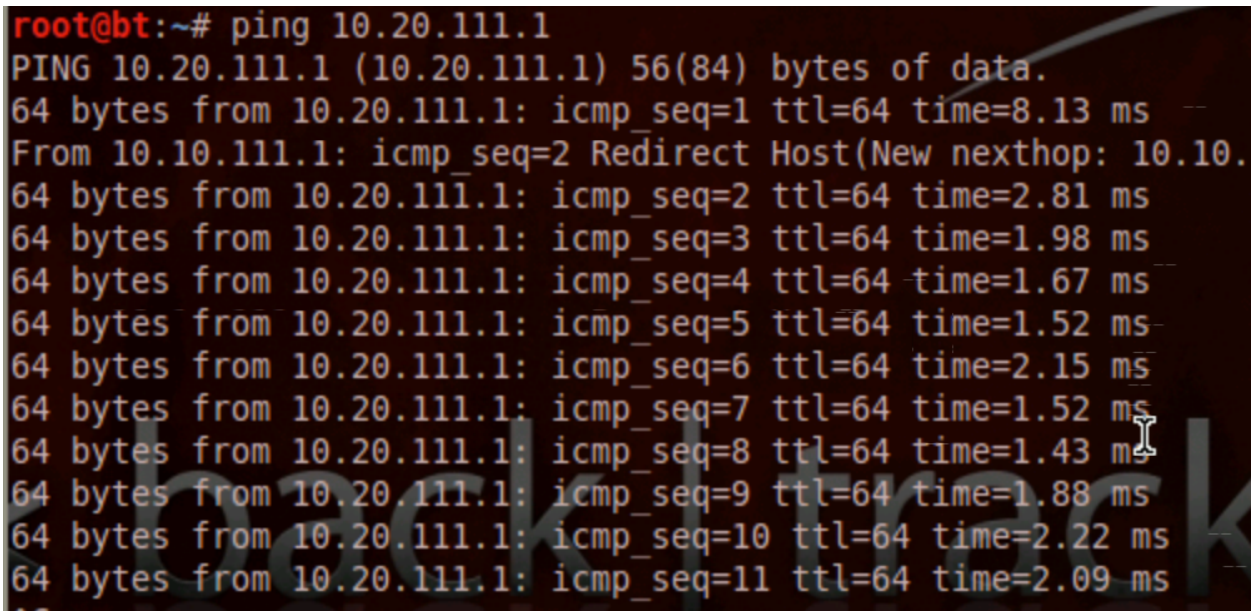
A)
Accepts all outgoing traffic at this point and can communicate with 10.10.111.0/24

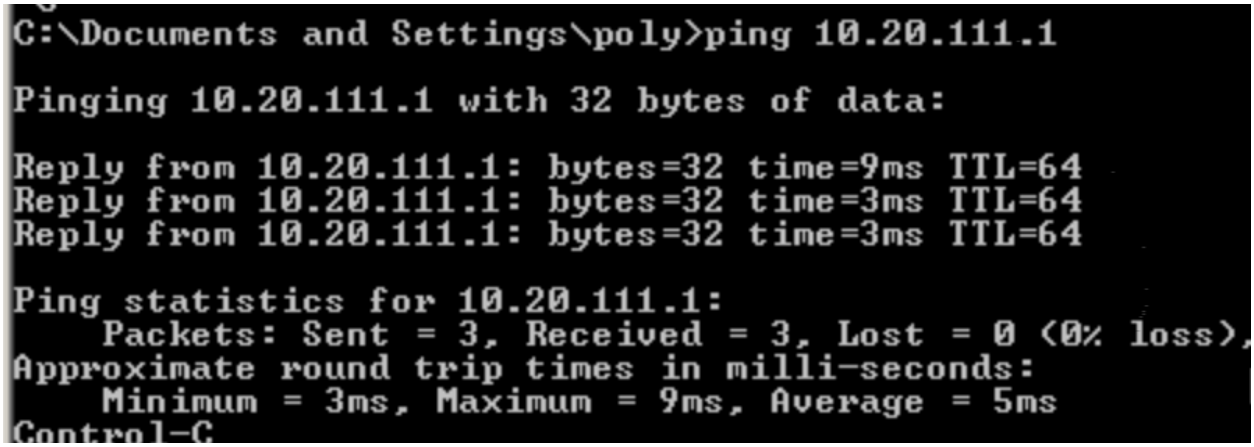



B)
1) Internal Machine responds to ping from 10.10.111.0/24



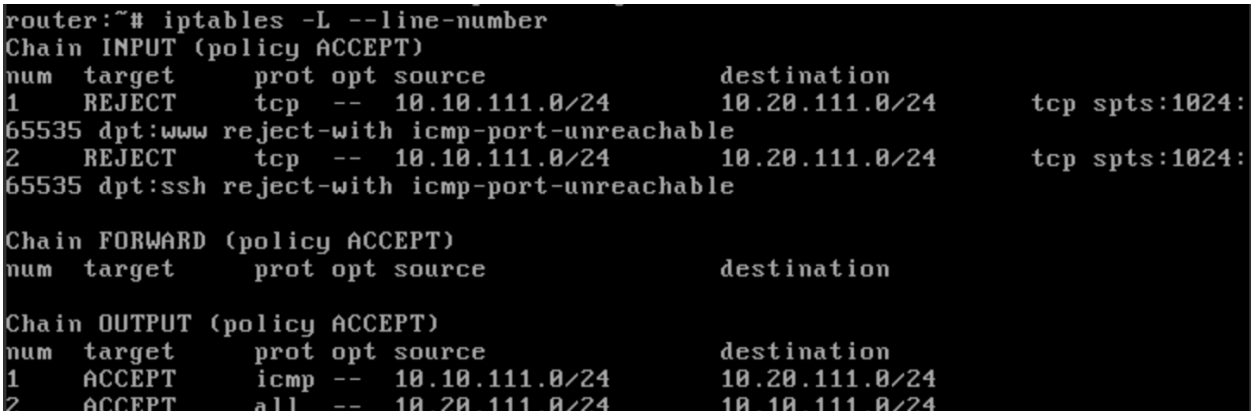
Example Pings:




2) Block incoming HTTP and SSH requests
Command: iptables -A INPUT -p tcp -s 10.10.111.0/24 —source-port 1024:65535 -d 10.20.111.0/24 —destination-port 80 -j REJECT

iptables -A INPUT -p tcp -s 10.10.111.0/24 —source-port 1024:65535 -d 10.20.111.0/24 —destination-port 80 -j REJECT



3) Internal machine accepts telnet connection:

Code:

```
router:~# iptables -A INPUT -m mac --mac-source 02:00:c2:4a:00:01 -p tcp -d 10.2
0.111.0/24 --destination-port 23 -j ACCEPT
```

IPTABLE:

```
router:~# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  10.10.111.0/24       10.20.111.0/24      tcp spts:1024
65535 dpt:www reject-with icmp-port-unreachable
2    REJECT     tcp  --  10.10.111.0/24       10.20.111.0/24      tcp spts:1024
65535 dpt:ssh reject-with icmp-port-unreachable
3    ACCEPT     tcp  --  anywhere             10.20.111.0/24      MAC 02:00:C2:4
A:00:01 tcp dpt:telnet

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     icmp --  10.10.111.0/24       10.20.111.0/24
2    ACCEPT     all  --  10.20.111.0/24       10.10.111.0/24
```

TELNET:

```
root@bt:~# telnet 10.20.111.0
Trying 10.20.111.0...
```