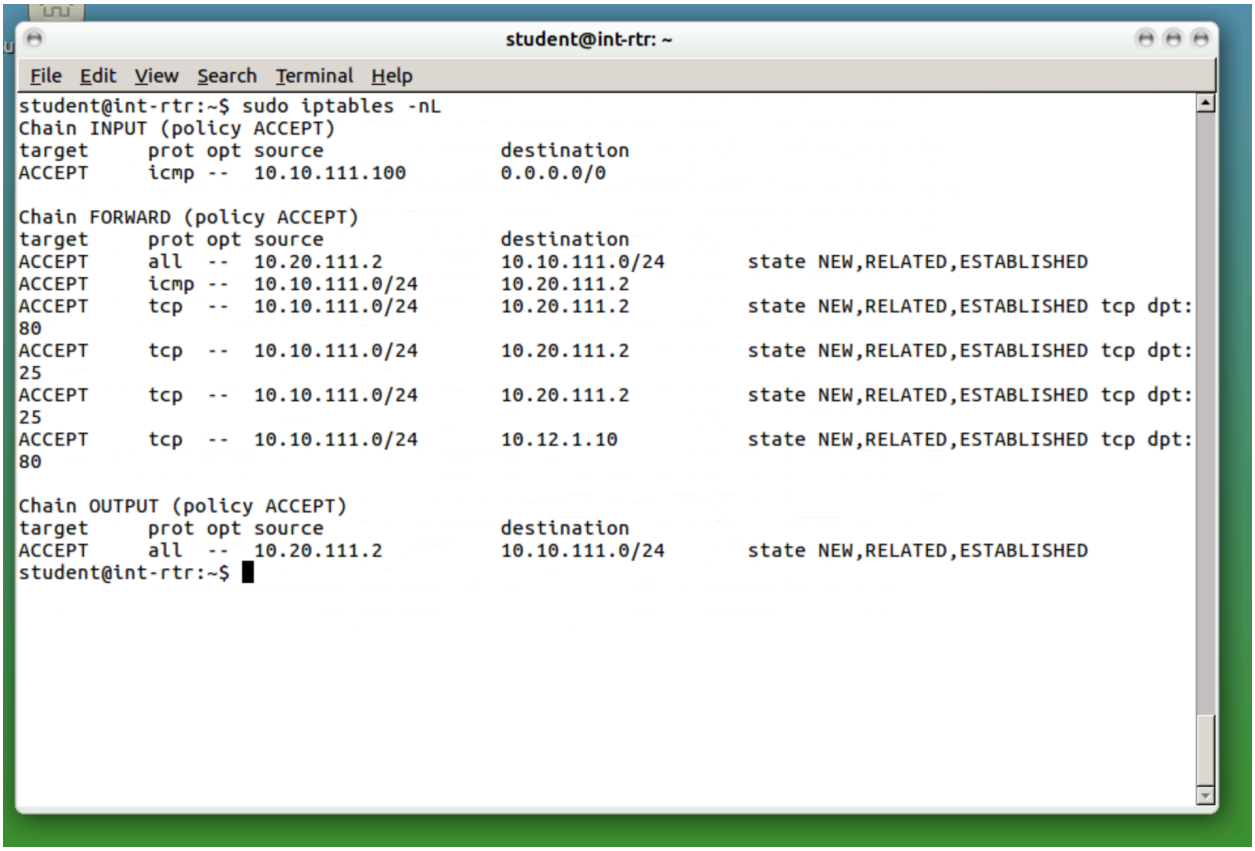
Lab 5: IPTables

Part A:

For outgoing traffic (from 10.20.111.0/24 to 10.10.111.0/24) - your internal machine should be able to communicate with the external network and the external machines without restrictions. For incoming traffic (from the 10.10.111.0/24 to the 10.20.111.0/24) - all incoming connection requests should be rejected with the following exceptions:

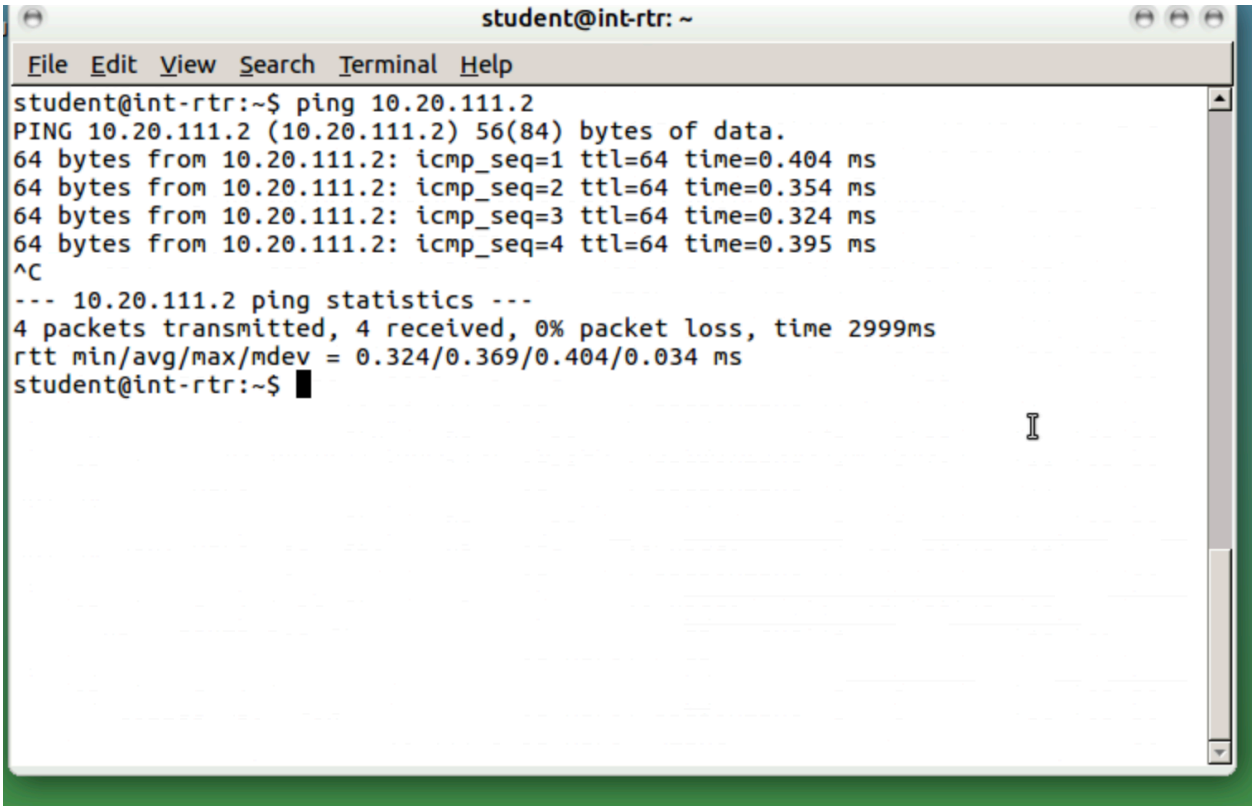
sudo iptables -A FORWARD -s 10.20.111.2 -d 10.10.111.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

sudo iptables -A OUTPUT -s 10.20.111.0/24 -d 10.10.111.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT



1) The internal machine should respond to a ping from 10.10.111.0/24

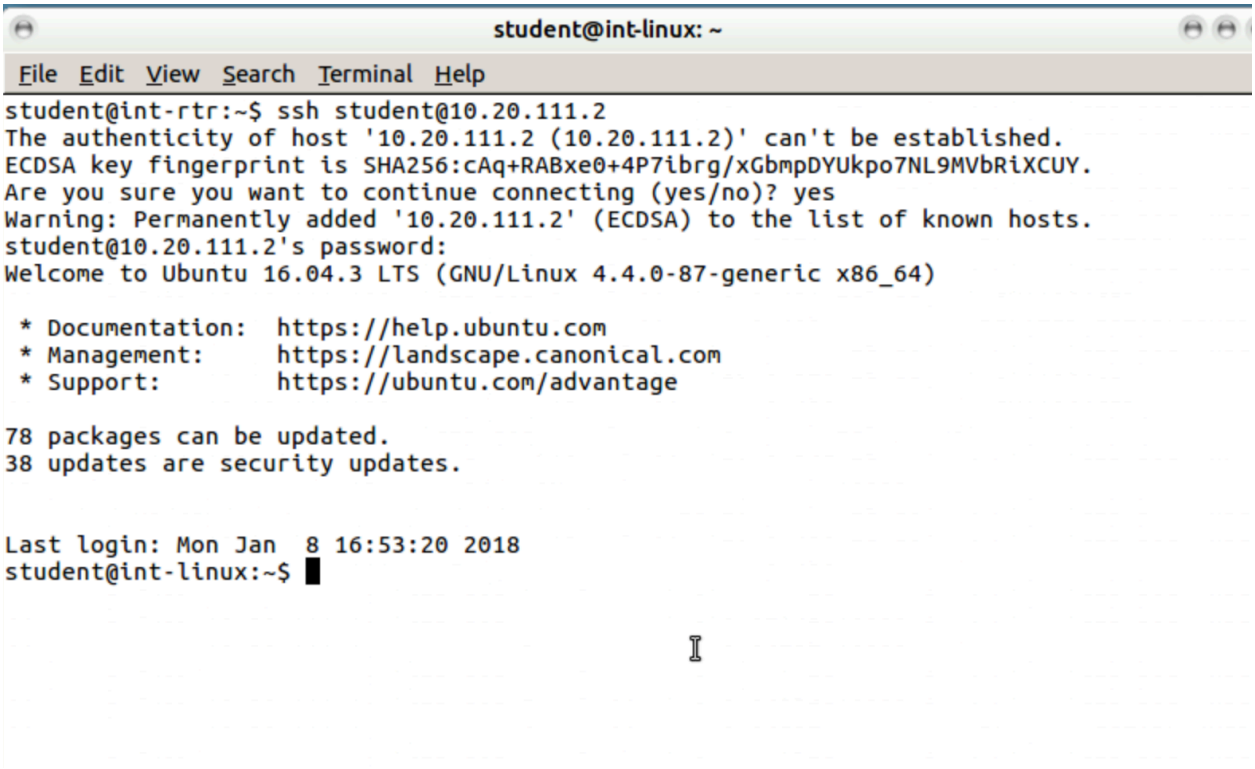
sudo iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -p icmp -j ACCEPT

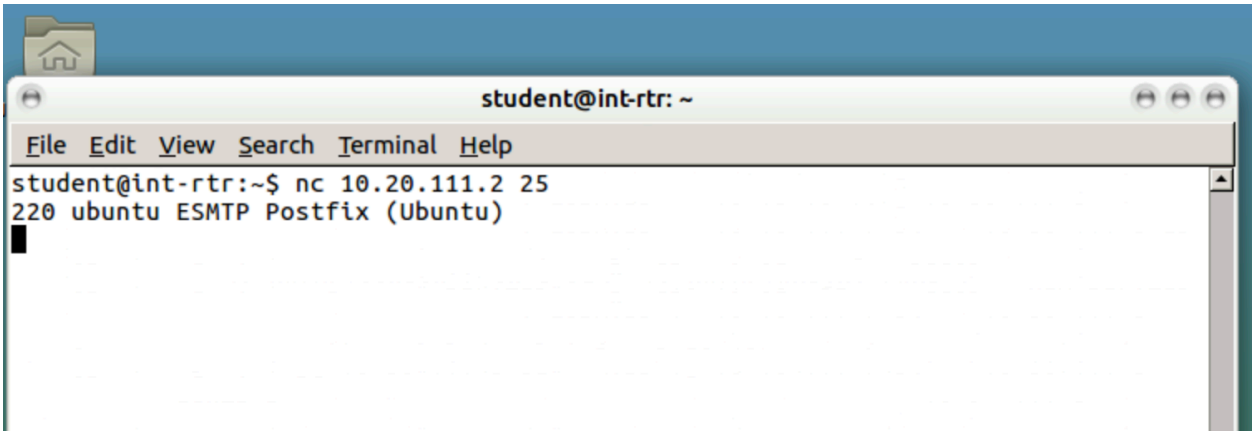


2) The internal machine (10.20.111.2) should accept all incoming SSH and SMTP (TCP 25) requests from 10.10.111.0/24. Hint: You can test SMTP by using the following netcat command: “nc [IP] 25” then type “HELO”.

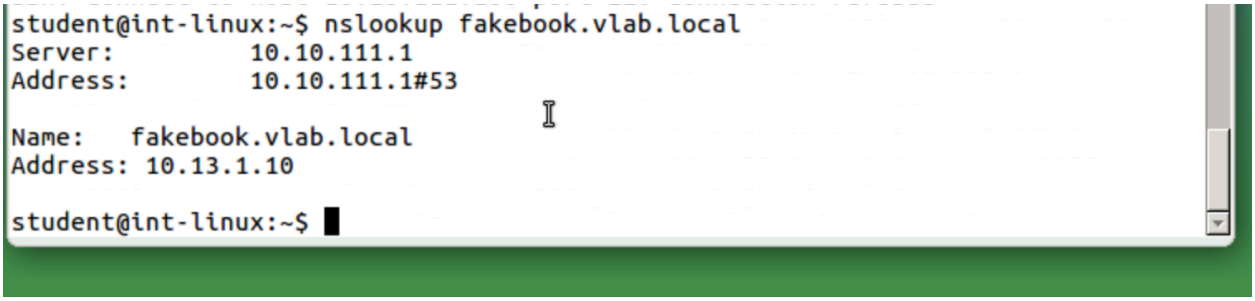
sudo iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -m state --state NEW,ESTABLISHED,RELATED -p tcp --dport 80 -j ACCEPT

sudo iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -m state --state NEW,ESTABLISHED,RELATED -p tcp --dport 25 -j ACCEPT

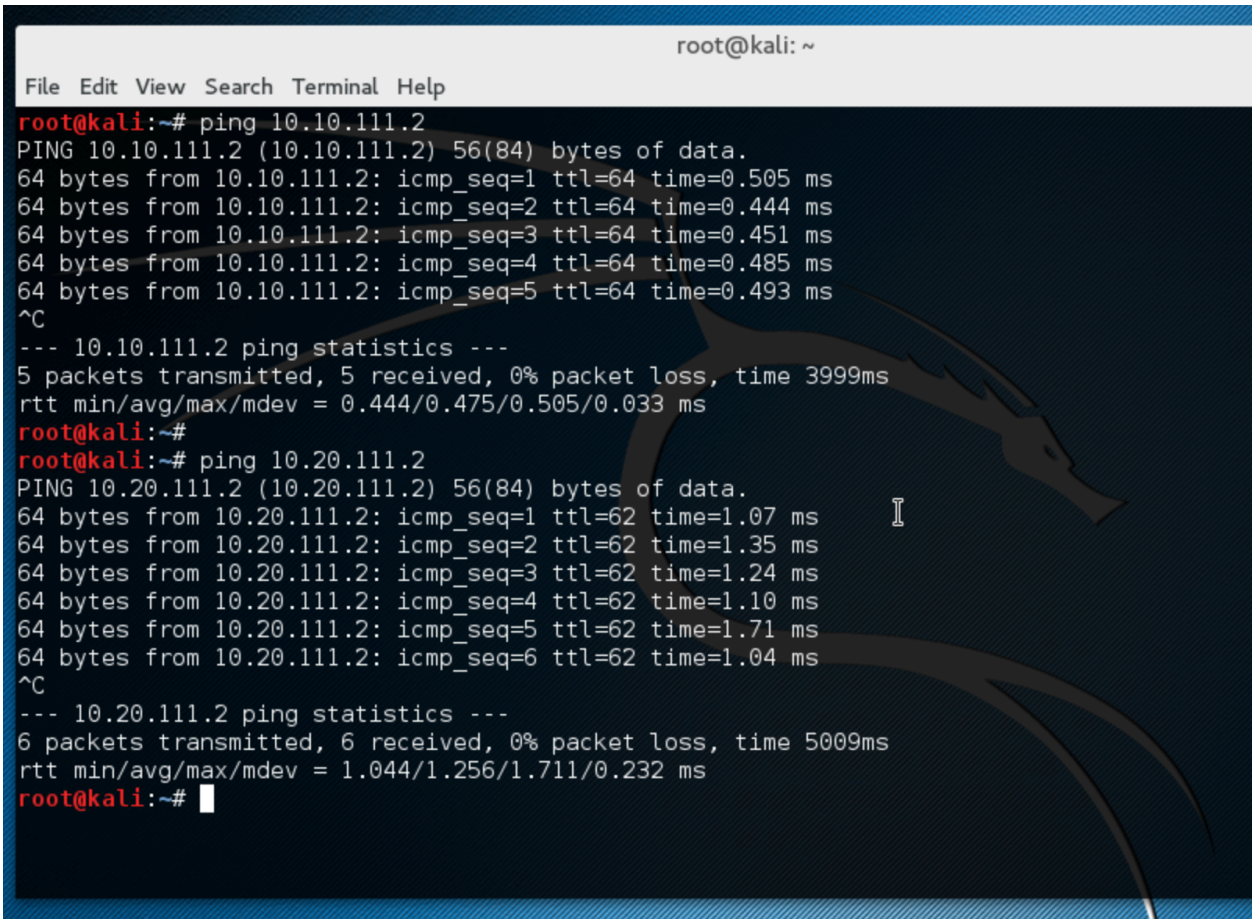




3) The internal machine should be able to perform a nslookup of fakebook.vlab.local
sudo iptables -A FORWARD -s 10.20.111.0/24 -d 10.12.1.10 -m state --state NEW,ESTABLISHED,RELATED -p tcp --dport 80 -j ACCEPT



4) The internal router should accept pings from the Kali machine only
sudo iptables -A INPUT -s 10.10.111.100 -p icmp -j ACCEPT



5) Proof for each attached in each question. More attached below

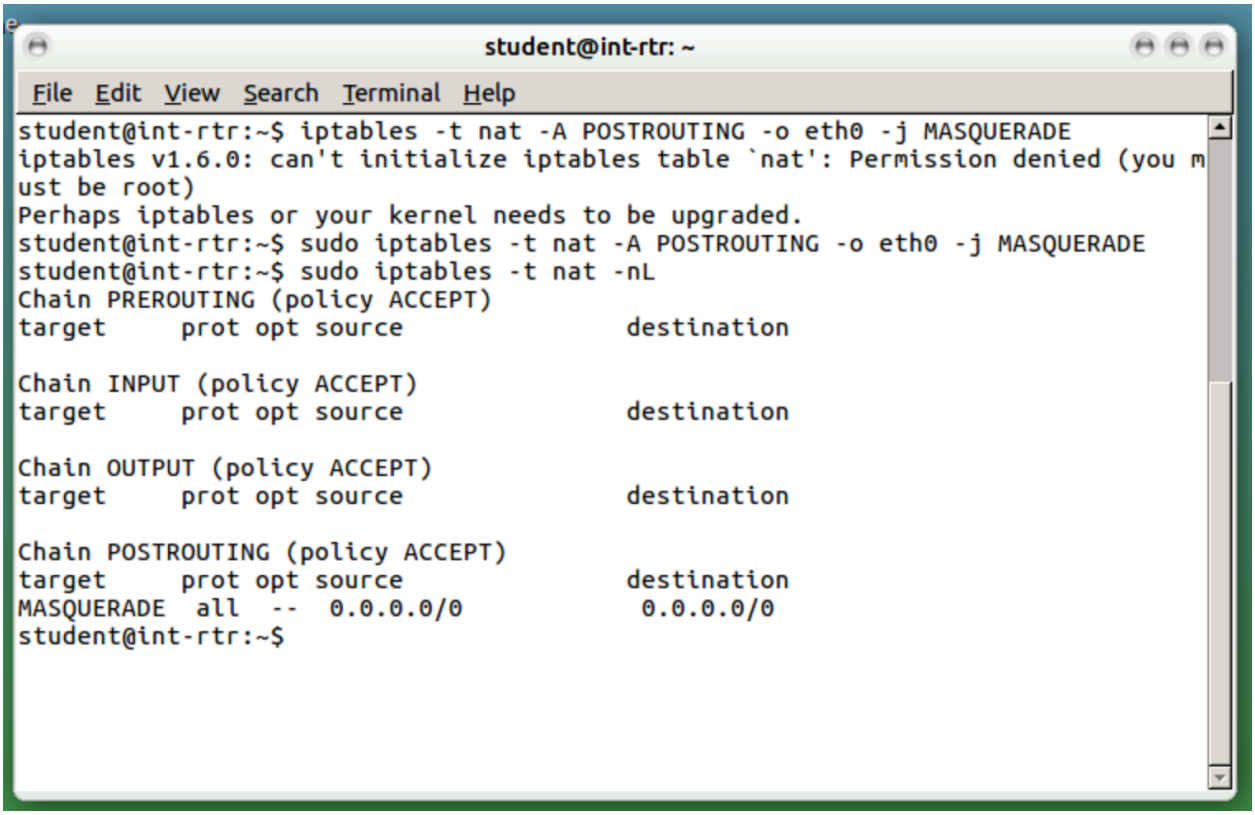
```
student@int-rtr:~$ ping 10.10.111.100
PING 10.10.111.100 (10.10.111.100) 56(84) bytes of data.
64 bytes from 10.10.111.100: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 10.10.111.100: icmp_seq=2 ttl=64 time=0.393 ms
64 bytes from 10.10.111.100: icmp_seq=3 ttl=64 time=0.376 ms
64 bytes from 10.10.111.100: icmp_seq=4 ttl=64 time=0.417 ms
64 bytes from 10.10.111.100: icmp_seq=5 ttl=64 time=0.383 ms
64 bytes from 10.10.111.100: icmp_seq=6 ttl=64 time=0.371 ms
64 bytes from 10.10.111.100: icmp_seq=7 ttl=64 time=0.430 ms
64 bytes from 10.10.111.100: icmp_seq=8 ttl=64 time=0.421 ms
64 bytes from 10.10.111.100: icmp_seq=9 ttl=64 time=0.409 ms
64 bytes from 10.10.111.100: icmp_seq=10 ttl=64 time=0.365 ms
64 bytes from 10.10.111.100: icmp_seq=11 ttl=64 time=0.379 ms
64 bytes from 10.10.111.100: icmp_seq=12 ttl=64 time=0.420 ms
^C
--- 10.10.111.100 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 10999ms
rtt min/avg/max/mdev = 0.365/0.421/0.696/0.088 ms
student@int-rtr:~$
```

File Edit View Search Terminal Help

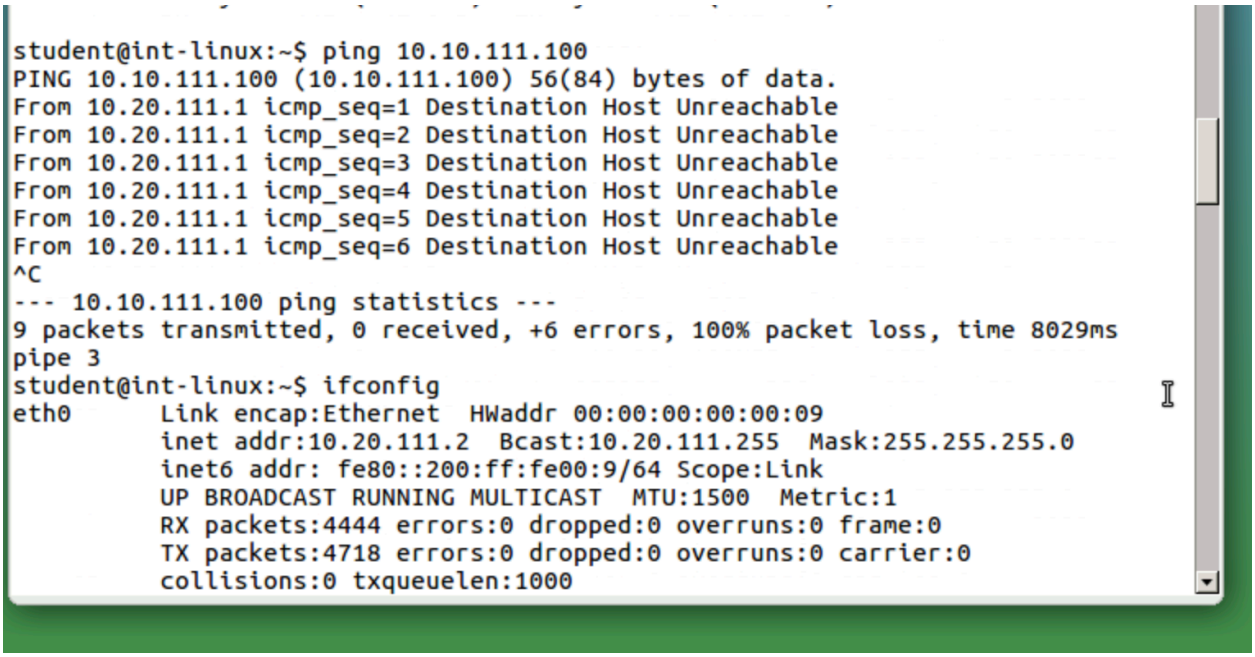
```
student@int-linux:~$ ping 10.10.111.100
PING 10.10.111.100 (10.10.111.100) 56(84) bytes of data.
64 bytes from 10.10.111.100: icmp_seq=1 ttl=63 time=0.693 ms
64 bytes from 10.10.111.100: icmp_seq=2 ttl=63 time=0.763 ms
64 bytes from 10.10.111.100: icmp_seq=3 ttl=63 time=0.685 ms
64 bytes from 10.10.111.100: icmp_seq=4 ttl=63 time=0.644 ms
64 bytes from 10.10.111.100: icmp_seq=5 ttl=63 time=0.715 ms
^C
--- 10.10.111.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.644/0.700/0.763/0.039 ms
student@int-linux:~$
```

PART B:

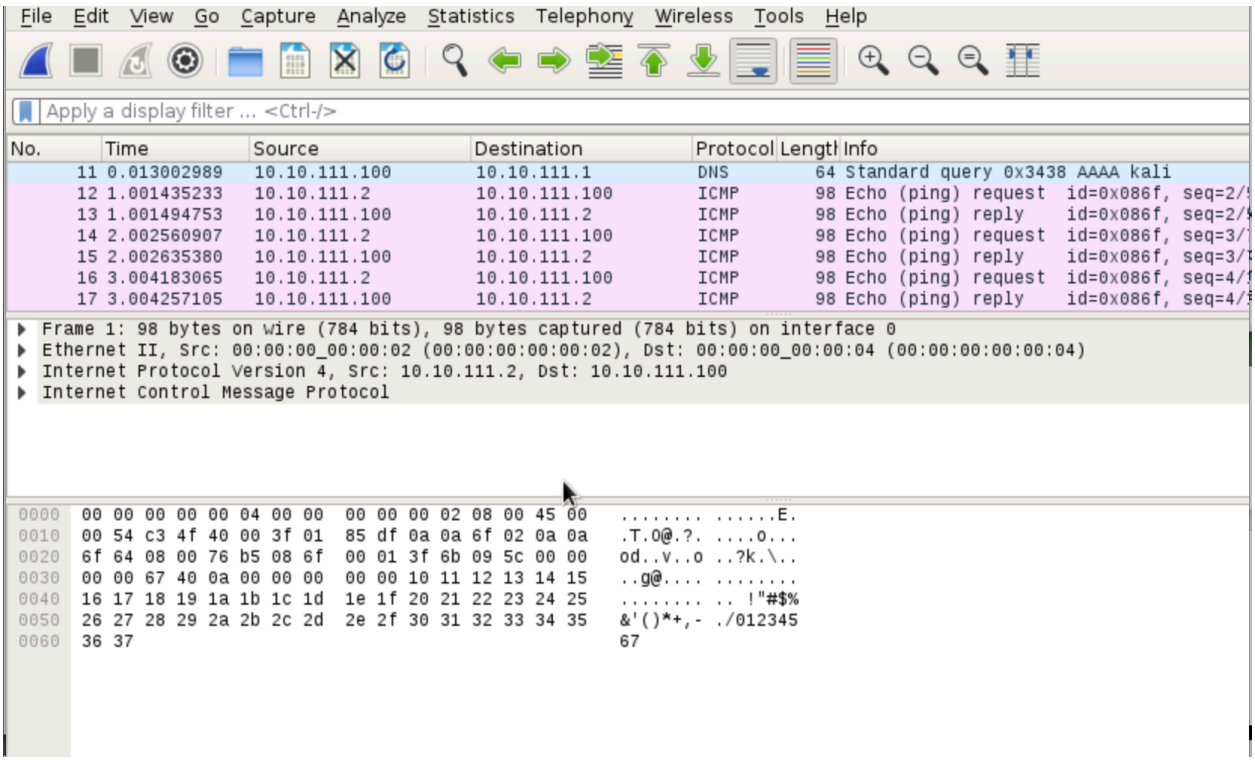
Sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE



PINGING KALI LINUX MACHINE:

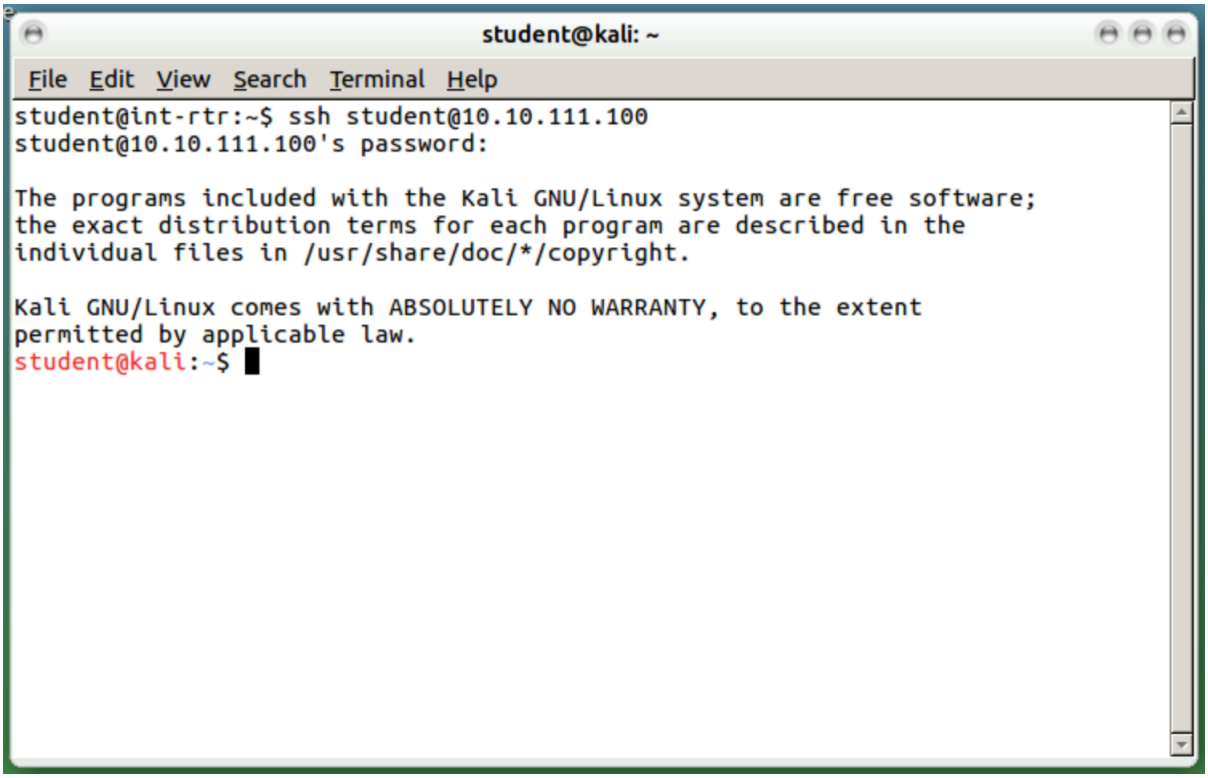


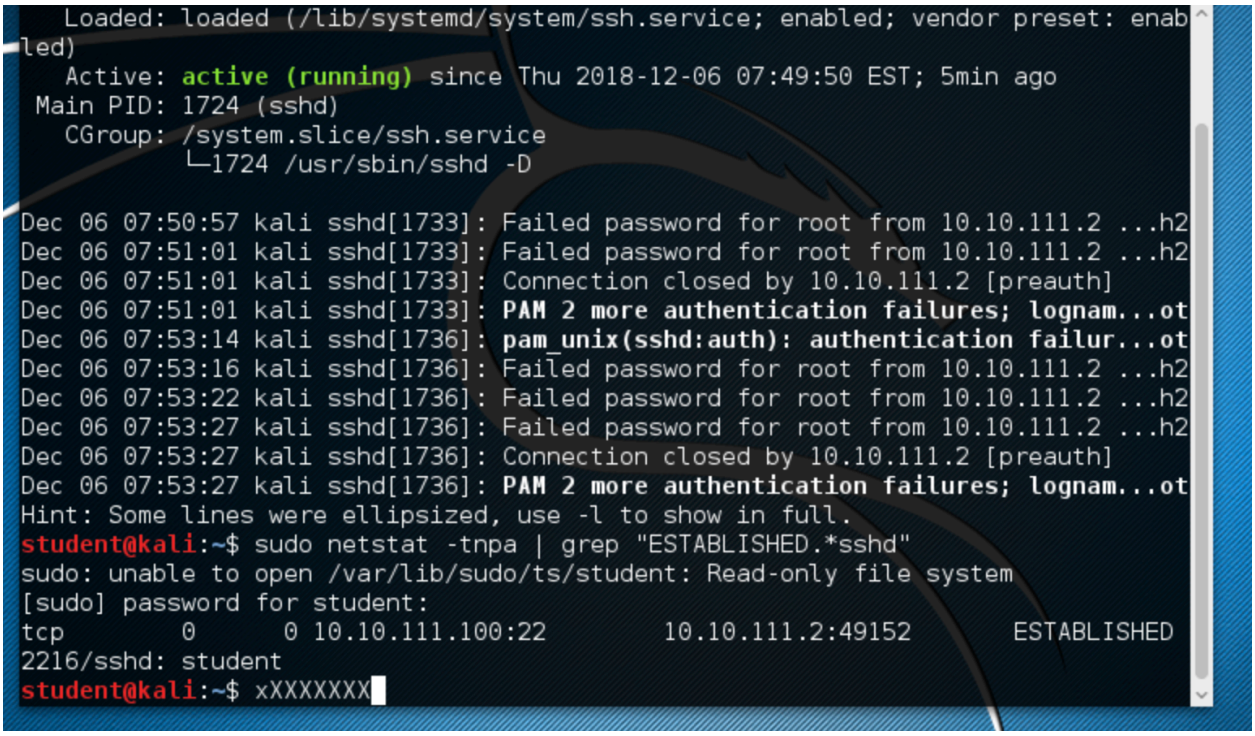
Kali Linux Wireshark



Shows IP as 10.10.111.1 when IP is 10.20.111.1

Ssh





PART C:
What is the difference between input, output, and forward chains?

All three, input, output, and forward chains, are a set of rules that the firewall uses to determine whether network traffic should be accepted or dropped. The difference in these chains is the source and destination of the packets. The input chain is the set of rules that is used when incoming packets have a destination of the actual computer or firewall; packets that are meant to be received by the actual computer. The output chain is used when the source address is the actual computer or firewall; packets that are created by the computer and are being sent out. Finally, the forward chain is when neither the source or destination is the computer; packets that are just passing through.

What is the difference between reject and drop?

Both reject and drop deny the request and packet. However, in a reject, the packet is not let through and a ICMP reject is sent back. In a drop, the packet is not let through and nothing is returned.