

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
```

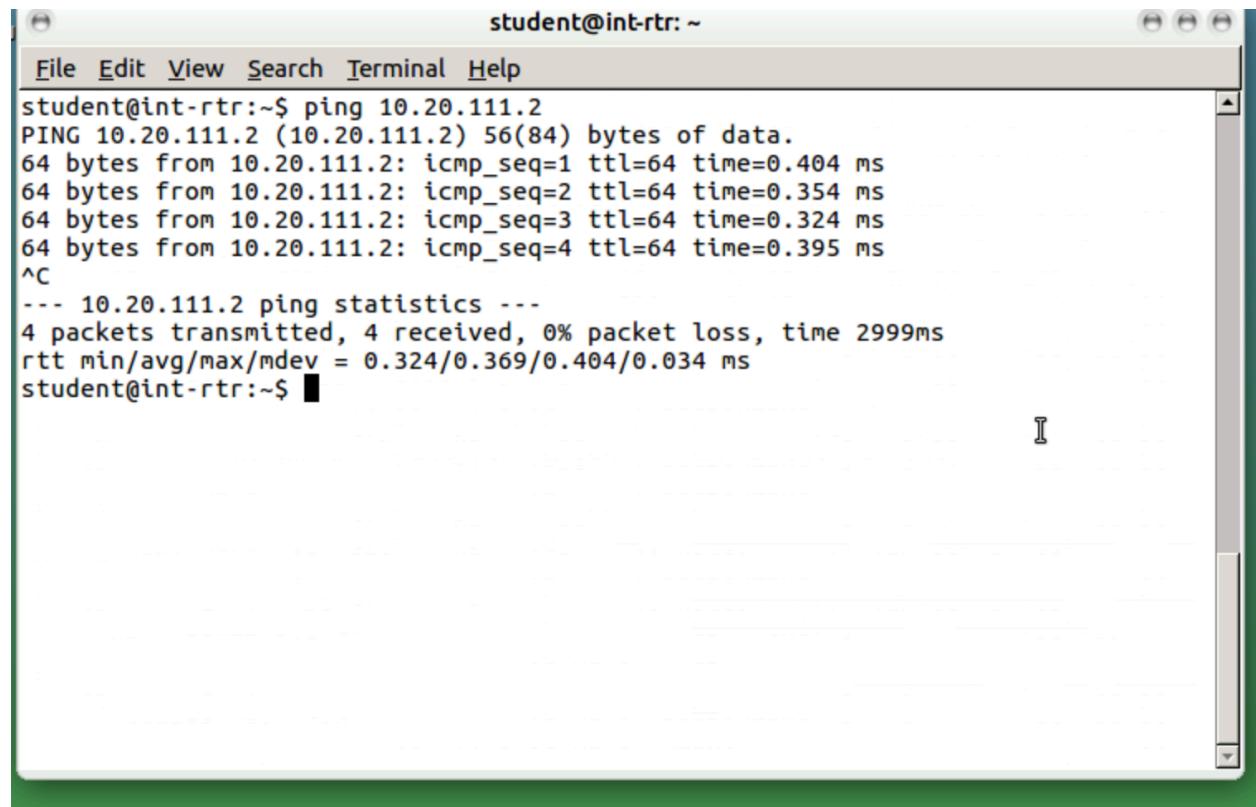
```
sudo iptables -A OUTPUT -s 10.20.111.0/24 -d 10.10.111.0/24 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
student@int-rtr:~$ sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT    icmp --  10.10.111.100        0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT    all   --  10.20.111.2        10.10.111.0/24      state NEW,RELATED,ESTABLISHED
ACCEPT    icmp --  10.10.111.0/24       10.20.111.2
ACCEPT    tcp   --  10.10.111.0/24       10.20.111.2      state NEW,RELATED,ESTABLISHED tcp dpt:80
ACCEPT    tcp   --  10.10.111.0/24       10.20.111.2      state NEW,RELATED,ESTABLISHED tcp dpt:25
ACCEPT    tcp   --  10.10.111.0/24       10.20.111.2      state NEW,RELATED,ESTABLISHED tcp dpt:25
ACCEPT    tcp   --  10.10.111.0/24       10.12.1.10       state NEW,RELATED,ESTABLISHED tcp dpt:80

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT    all   --  10.20.111.2        10.10.111.0/24      state NEW,RELATED,ESTABLISHED
student@int-rtr:~$
```

- 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



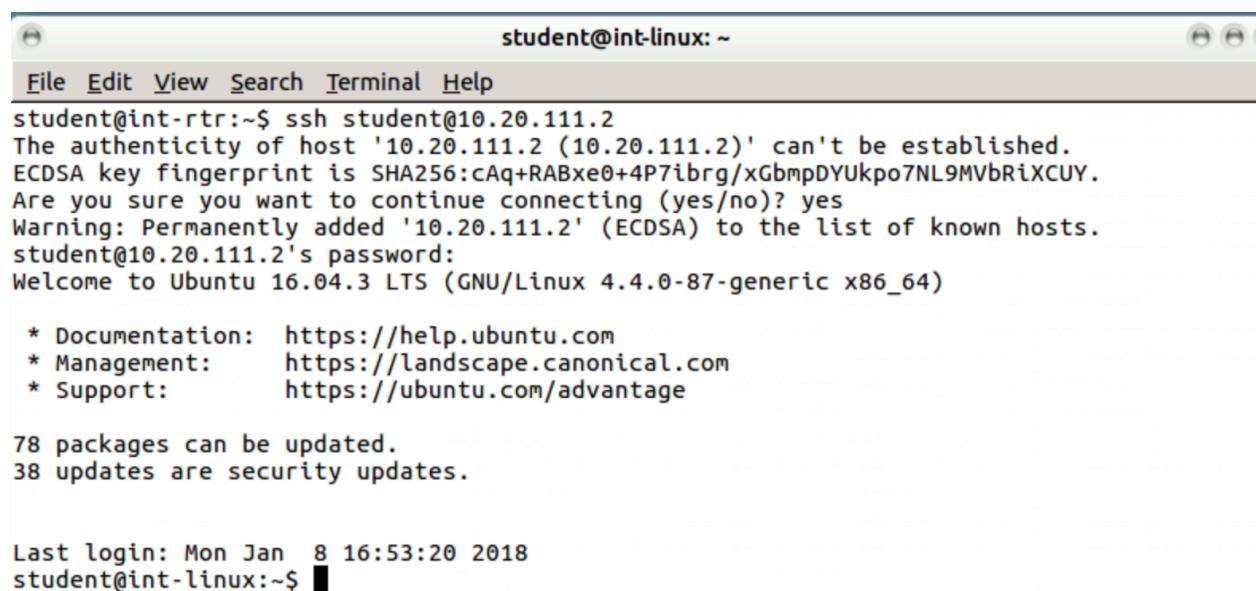
A screenshot of a terminal window titled "student@int-rtr: ~". The window contains the following text:

```
student@int-rtr:~$ ping 10.20.111.2
PING 10.20.111.2 (10.20.111.2) 56(84) bytes of data.
64 bytes from 10.20.111.2: icmp_seq=1 ttl=64 time=0.404 ms
64 bytes from 10.20.111.2: icmp_seq=2 ttl=64 time=0.354 ms
64 bytes from 10.20.111.2: icmp_seq=3 ttl=64 time=0.324 ms
64 bytes from 10.20.111.2: icmp_seq=4 ttl=64 time=0.395 ms
^C
--- 10.20.111.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.324/0.369/0.404/0.034 ms
student@int-rtr:~$
```

- 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
```



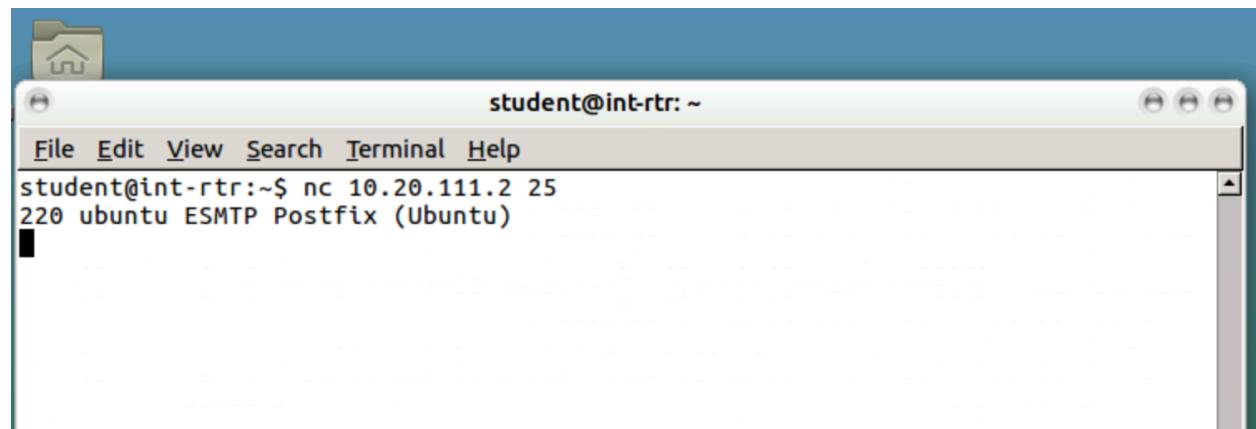
A screenshot of a terminal window titled "student@int-linux: ~". The window has a standard window title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main terminal area shows the following text:

```
student@int-rtr:~$ ssh student@10.20.111.2
The authenticity of host '10.20.111.2 (10.20.111.2)' can't be established.
ECDSA key fingerprint is SHA256:cAq+RABxe0+4P7ibrg/xGbmpDYUkpo7NL9MVbRiXCUY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.111.2' (ECDSA) to the list of known hosts.
student@10.20.111.2's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

78 packages can be updated.
38 updates are security updates.

Last login: Mon Jan  8 16:53:20 2018
student@int-linux:~$ █
```



A screenshot of a terminal window titled "student@int-rtr: ~". The window has a standard window title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main terminal area shows the following text:

```
student@int-rtr:~$ nc 10.20.111.2 25
220 ubuntu ESMTP Postfix (Ubuntu)
█
```

- 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

```
student@int-linux:~$ nslookup fakebook.vlab.local
Server:      10.10.111.1
Address:     10.10.111.1#53
Name:   fakebook.vlab.local
Address: 10.13.1.10

student@int-linux:~$
```

- 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

```
root@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=0.505 ms
64 bytes from 10.10.111.2: icmp_seq=2 ttl=64 time=0.444 ms
64 bytes from 10.10.111.2: icmp_seq=3 ttl=64 time=0.451 ms
64 bytes from 10.10.111.2: icmp_seq=4 ttl=64 time=0.485 ms
64 bytes from 10.10.111.2: icmp_seq=5 ttl=64 time=0.493 ms
^C
--- 10.10.111.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.444/0.475/0.505/0.033 ms
root@kali:~#
root@kali:~# ping 10.20.111.2
PING 10.20.111.2 (10.20.111.2) 56(84) bytes of data.
64 bytes from 10.20.111.2: icmp_seq=1 ttl=62 time=1.07 ms
64 bytes from 10.20.111.2: icmp_seq=2 ttl=62 time=1.35 ms
64 bytes from 10.20.111.2: icmp_seq=3 ttl=62 time=1.24 ms
64 bytes from 10.20.111.2: icmp_seq=4 ttl=62 time=1.10 ms
64 bytes from 10.20.111.2: icmp_seq=5 ttl=62 time=1.71 ms
64 bytes from 10.20.111.2: icmp_seq=6 ttl=62 time=1.04 ms
^C
--- 10.20.111.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.044/1.256/1.711/0.232 ms
root@kali:~#
```

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

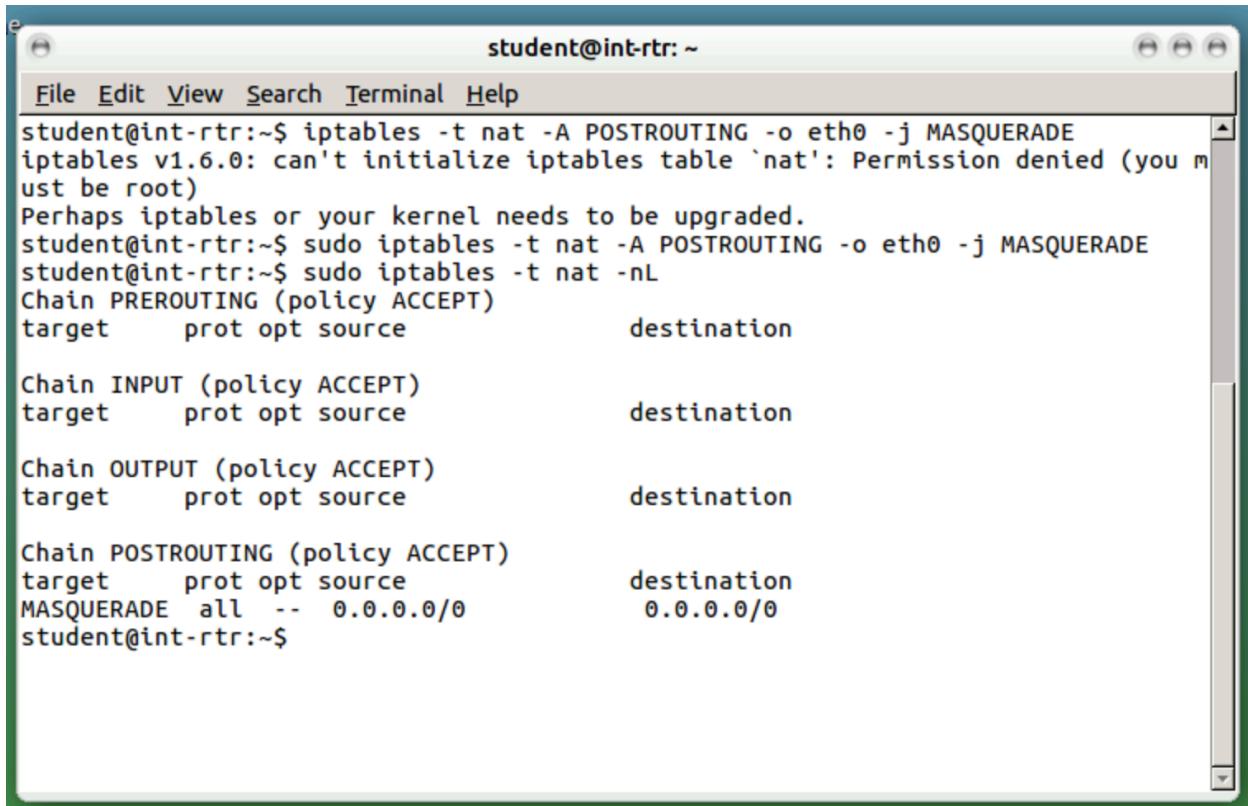
```
student@int-rtr:~$ ping 10.10.111.100
PING 10.10.111.100 (10.10.111.100) 56(84) bytes of data.
64 bytes from 10.10.111.100: icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from 10.10.111.100: icmp_seq=2 ttl=64 time=0.393 ms
64 bytes from 10.10.111.100: icmp_seq=3 ttl=64 time=0.376 ms
64 bytes from 10.10.111.100: 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



A terminal window titled "student@int-rtr: ~" showing the output of the command "sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE". The output indicates that the operation failed because the user is not root. It then shows the successful execution of the command with sudo, followed by the current state of the iptables table.

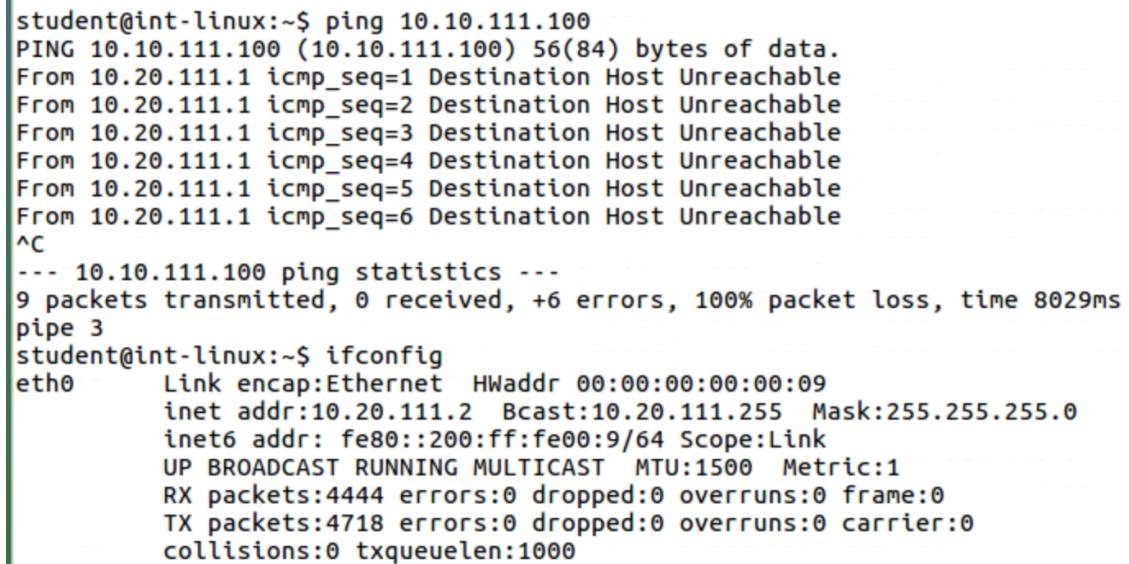
```
student@int-rtr:~$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables v1.6.0: can't initialize iptables table `nat': Permission denied (you must be root)
Perhaps iptables or your kernel needs to be upgraded.
student@int-rtr:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
student@int-rtr:~$ sudo iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination

Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source          destination
MASQUERADE  all  --  0.0.0.0/0      0.0.0.0/0
student@int-rtr:~$
```

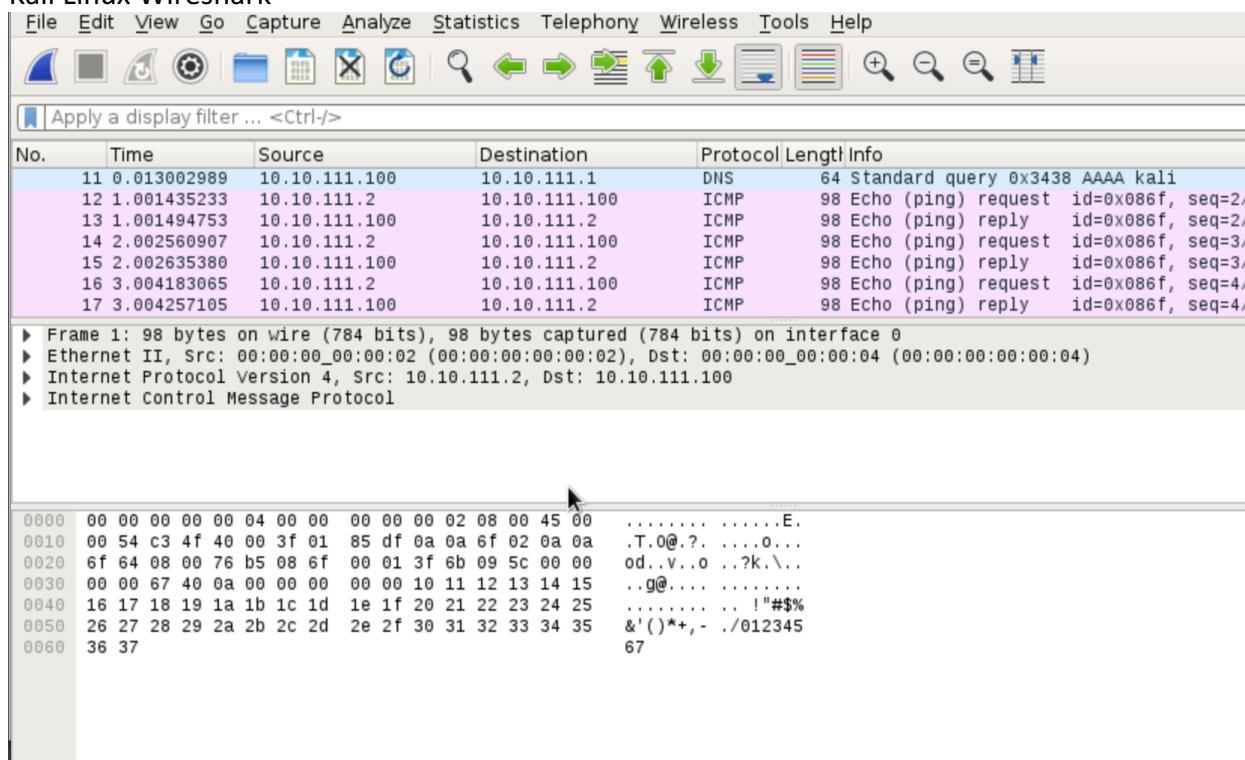
PINGING KALI LINUX MACHINE:



A terminal window titled "student@int-linux: ~" showing the output of the "ping" command to 10.10.111.100 and the "ifconfig" command. The ping command shows 9 packets transmitted, 0 received, and 6 errors. The ifconfig command shows the interface eth0 with an IP address of 10.20.111.2 and a MAC address of 00:00:00:00:00:09.

```
student@int-linux:~$ ping 10.10.111.100
PING 10.10.111.100 (10.10.111.100) 56(84) bytes of data.
From 10.20.111.1 icmp_seq=1 Destination Host Unreachable
From 10.20.111.1 icmp_seq=2 Destination Host Unreachable
From 10.20.111.1 icmp_seq=3 Destination Host Unreachable
From 10.20.111.1 icmp_seq=4 Destination Host Unreachable
From 10.20.111.1 icmp_seq=5 Destination Host Unreachable
From 10.20.111.1 icmp_seq=6 Destination Host Unreachable
^C
--- 10.10.111.100 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 8029ms
pipe 3
student@int-linux:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:00:00:00:00:09
          inet addr:10.20.111.2 Bcast:10.20.111.255 Mask:255.255.255.0
                  inet6 addr: fe80::200:ff:fe00:9/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:4444 errors:0 dropped:0 overruns:0 frame:0
                      TX packets:4718 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
```

Kali Linux Wireshark



Shows IP as 10.10.111.1 when IP is 10.20.111.1

Ssh

The screenshot shows a terminal window titled "student@kali: ~". The user has run the command "ssh student@10.10.111.100" and is prompted for the password. The terminal also displays the standard Kali Linux license information and a note about warranty.

```
student@kali: ~$ ssh student@10.10.111.100  
student@10.10.111.100's password:  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
student@kali: ~$
```

```
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
      Active: active (running) since Thu 2018-12-06 07:49:50 EST; 5min ago
        Main PID: 1724 (sshd)
          CGroup: /system.slice/ssh.service
                  └─1724 /usr/sbin/sshd -D

Dec  06 07:50:57 kali sshd[1733]: Failed password for root from 10.10.111.2 ...
Dec  06 07:51:01 kali sshd[1733]: Failed password for root from 10.10.111.2 ...
Dec  06 07:51:01 kali sshd[1733]: Connection closed by 10.10.111.2 [preauth]
Dec  06 07:51:01 kali sshd[1733]: PAM 2 more authentication failures; lognam...
Dec  06 07:53:14 kali sshd[1736]: pam_unix(sshd:auth): authentication failur...
Dec  06 07:53:16 kali sshd[1736]: Failed password for root from 10.10.111.2 ...
Dec  06 07:53:22 kali sshd[1736]: Failed password for root from 10.10.111.2 ...
Dec  06 07:53:27 kali sshd[1736]: Failed password for root from 10.10.111.2 ...
Dec  06 07:53:27 kali sshd[1736]: Connection closed by 10.10.111.2 [preauth]
Dec  06 07:53:27 kali sshd[1736]: PAM 2 more authentication failures; lognam...
Hint: Some lines were ellipsized, use -l to show in full.
student@kali:~$ sudo netstat -tnpa | grep "ESTABLISHED.*sshd"
sudo: unable to open /var/lib/sudo/ts/student: Read-only file system
[sudo] password for student:
tcp      0      0 10.10.111.100:22          10.10.111.2:49152      ESTABLISHED
2216/sshd: student
student@kali:~$ xXXXXXXXX
```

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.