CIS 192 – Practice Test 2 – Spring 2010 Name _____

Each question worth 2 points:

Figure 1 – Active FTP data transfer

SIP	SP	DIP	DP	Protocol	Info	
172.30.4.83	42855	192.168.2.150	21	FTP	Request: PORT 172,30,4,83,166,75	1
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 200 PORT command successful. Consider using PAS	2
172.30.4.83	42855	192.168.2.150	21	FTP	Request: RETR legolas	3
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=	4
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MS	5
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=1 Ack=1 Win=5888 Len=0	6
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 150 Opening BINARY mode data connection for leg	7
192.168.2.150	20	172.30.4.83	42571	FTP-DATA	FTP Data: 18 bytes	8
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [FIN, ACK] Seq=19 Ack=1 Win=5888 Len=0	9
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [ACK] Seq=1 Ack=19 Win=5856 Len=0	10
172.30.4.83	42571	192.168.2.150	20	TCP	42571 > ftp-data [FIN, ACK] Seq=1 Ack=20 Win=5856 Len=0	11
192.168.2.150	20	172.30.4.83	42571	TCP	ftp-data > 42571 [ACK] Seq=20 Ack=2 Win=5888 Len=0	12
192.168.2.150	21	172.30.4.83	42855	FTP	Response: 226 File send OK.	13
172.30.4.83	42855	192.168.2.150	21	TCP	42855 > ftp [ACK] Seq=82 Ack=263 Win=5856 Len=0	14

1. Referring to figure 1 above and using the packet numbers on the right, which packet marks the point where the connection used for the data transfer is closed on the server?

   _____

2. Referring to figure 1 above, what socket is used for the FTP data transfer?
   (To answer, fill in the table below)

Client	Server
IP:	IP:
Port:	Port:

3. What command on Red Hat family systems would configure the DHCP service to startup automatically when powering up?

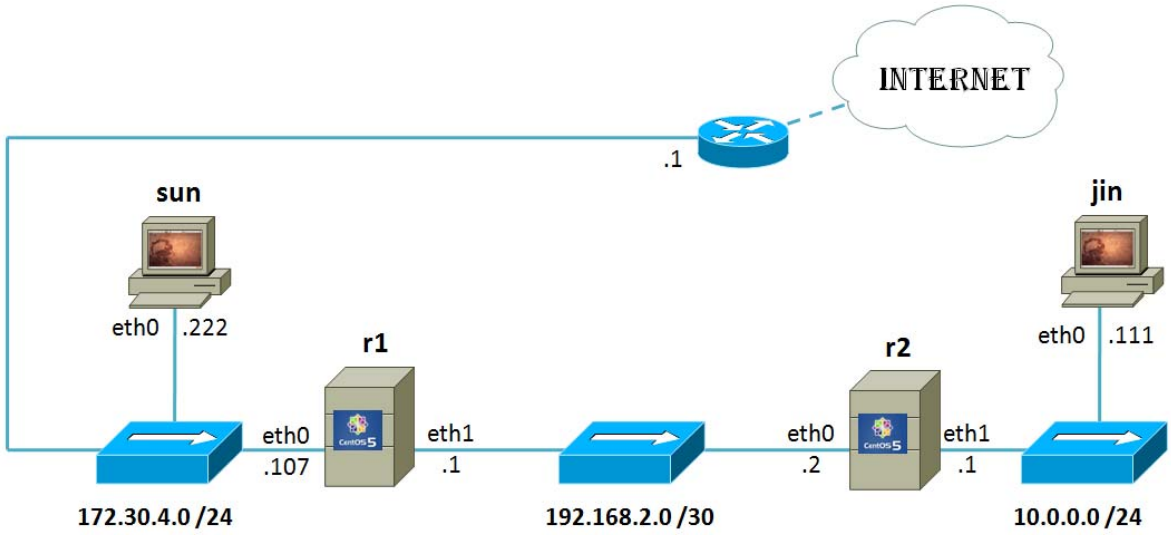
   _____

4. For firewall purposes when is a TCP stream considered to be *established* on the server side?

   _____

   _____

5. How would you permanently configure the Ubuntu system named **sun** below



with a static IP, default gateway, and all necessary routes to reach the other two private networks?

Configuration file to edit on Sun: _____

Fill in the blanks below for Sun's configuration file :

```
auto lo
iface lo inet loopback
auto _____
iface _____ inet _______
address _____________________________
netmask 255.255.255.0

_________  _____________________________
network _____________________________

_________  _____________________________
up _________ add _____ _____________________/___ gw _____________
up _________ add _____ _____________________/___ gw _____________
```

6. What are **two** different commands on Red Hat family systems that would cause the xinetd daemon to reread its configuration files?

1)_____

2)_____

7. How would you configure TCP wrappers to only allow incoming SSH connections from hosts in the 192.168.3.0/24 network? (Answer by writing the lines you would add to the two files below)

   /etc/hosts.allow: _____

   /etc/hosts.deny: _____

8. What port number is used by the Telnet service?

   _____

9. In the DOS world the first serial port is called COM 1, what Linux device is used to reference this same port?

   _____

10. A DHCP service is running on Elrond using the file below.

```
[root@elrond ~]# cat /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
option time-offset              -25200;  # Pacific Daylight Time (-7 HR)

#
#   R I V E N D E L L
#
subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers                  192.168.2.107; # Default GW
        option subnet-mask              255.255.255.0;
        option domain-name              "rivendell";
        option domain-name-servers      207.62.187.54;

        range dynamic-bootp             192.168.2.50 192.168.2.99;
        default-lease-time              21600; # 6 hours
        max-lease-time                  43200; # 12 hours

        # reservations
        host legolas {
                hardware ethernet       00:0C:29:7C:18:F5;
                fixed-address           192.168.2.150;
        }
}
```

   For Rivendell clients that get their IP address from Elrond how long will they wait before attempting to renew their leases? Assume they did not specify a lease time on their original request.

   _____

11. Regarding the command below:

```
pppd updetach crtscts defaultroute /dev/ttyS0 38400 connect \
"exec chat -v TIMEOUT 3 ogin:--ogin: ppp assword: secret"
```

a) What does this command do? _____

b) What are the arguments *assword:* and *secret* used for?

_____

_____

12. What **five** complete iptables commands would a) flush all the rules from the current filter chains, b) delete any custom chains and c) set the policy to ACCEPT on the INPUT, FORWARD and OUTPUT chains?

_____

_____

_____

_____

_____

13. Given the following default firewall on a CentOS (Red Hat) system:

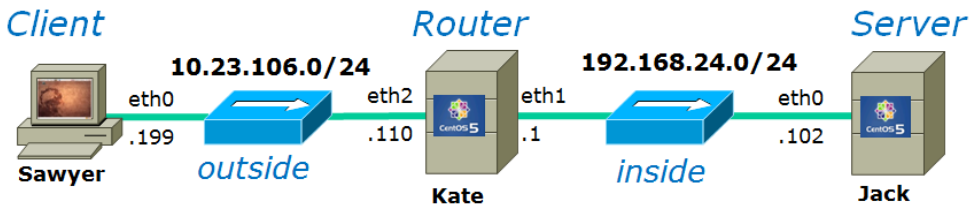
```
[root@arwen ~]# iptables -nL RH-Firewall-1-INPUT --line-numbers
Chain RH-Firewall-1-INPUT (2 references)
num  target     prot opt source         destination
1    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0
2    ACCEPT     icmp --  0.0.0.0/0      0.0.0.0/0      icmp type 255
3    ACCEPT     esp  --  0.0.0.0/0      0.0.0.0/0
4    ACCEPT     ah   --  0.0.0.0/0      0.0.0.0/0
5    ACCEPT     udp  --  0.0.0.0/0      224.0.0.251    udp dpt:5353
6    ACCEPT     udp  --  0.0.0.0/0      0.0.0.0/0      udp dpt:631
7    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0      tcp dpt:631
8    ACCEPT     all  --  0.0.0.0/0      0.0.0.0/0      state RELATED,ESTABLISHED
9    ACCEPT     tcp  --  0.0.0.0/0      0.0.0.0/0      state NEW tcp dpt:22
10   REJECT     all  --  0.0.0.0/0      0.0.0.0/0      reject-with icmp-host-
prohibited
[root@arwen ~]#
```

What complete iptables command would **insert** a rule to enable *new* incoming Telnet connections?

_____

_____

14. Refer to the diagram below. Kate's firewall allows incoming new and established SSH connections from the outside. All other new connection attempts from the outside are blocked. A Telnet server is running on Jack that can be accessed from all "inside" systems including Kate.



a) What command would set up SSH port forwarding so that Sawyer could use its own port 9000 to access the Telnet server on Jack? **and** b) once the port forwarding had been set up what second command on Sawyer would be used to make the actual connection to the Telnet server?

a)_____

b)_____

15. A Linux system named Rascal has the following firewall configured:

```
[root@rascal ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@rascal ~]#
```

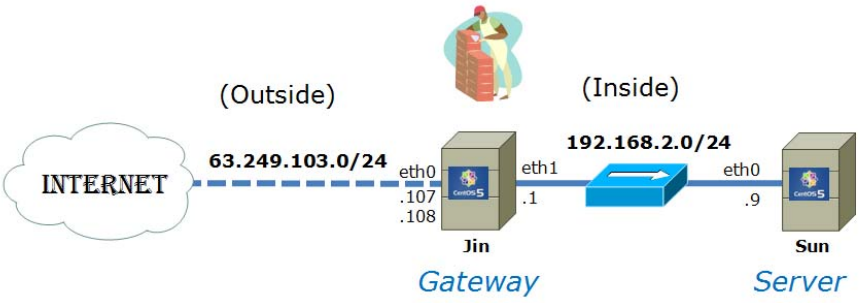
Rascal is getting bombarded with malicious login attempts from a host with an IP address of 63.45.78.22. What single iptables command would drop (without any error feedback) all packets coming from this malicious system yet allow in everything else?

_____

16. Extra Credit
(2 point)

A translation service is set up on Jin for hosts on the private inside network, including Sun, using:

```
iptables -t nat -A PREROUTING -i eth0 -d 63.249.103.108 -j DNAT --to-destination 192.168.2.9
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.9 -j SNAT --to-source 63.249.103.108
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to-source 63.249.103.107
```



Imagine that Sun has made an ssh connection to a system, opus.cabrillo.edu, on the Internet. If you were to sniff the packets that Opus **receives** from Sun, what would the source and destination IP addresses be?

SIP: _____

DIP:_____

17. Extra Credit
(2 points)

Elrond has been configured to provide DHCP services.

```
[root@elrond ~]# cat /var/lib/dhcpd/dhcpd.leases
# All times in this file are in UTC (GMT), not your local timezone.   This is
# not a bug, so please don't ask about it.   There is no portable way to
# store leases in the local timezone, so please don't request this as a
# feature.   If this is inconvenient or confusing to you, we sincerely
# apologize.   Seriously, though - don't ask.
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.0.5-RedHat

lease 172.30.4.83 {
  starts 5 2009/03/20 18:24:00;
  ends 5 2009/03/20 18:33:55;
  tstp 5 2009/03/20 18:33:55;
  binding state free;
  hardware ethernet 00:0c:29:6f:53:d9;
}
lease 172.30.4.83 {
  starts 5 2009/03/20 18:34:02;
  ends 6 2009/03/21 00:34:02;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:6f:53:d9;
```

```
  client-hostname "frodo";
}
lease 192.168.2.99 {
  starts 5 2009/03/20 18:20:55;
  ends 5 2009/03/20 18:34:10;
  tstp 5 2009/03/20 18:34:10;
  binding state free;
  hardware ethernet 00:0c:29:d4:38:ad;
  uid "\001\000\014)\3248\255";
}
lease 192.168.2.99 {
  starts 5 2009/03/20 18:34:16;
  ends 6 2009/03/21 00:34:16;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:d4:38:ad;
  uid "\001\000\014)\3248\255";
  client-hostname "william";
}
lease 192.168.2.99 {
  starts 5 2009/03/20 18:34:17;
  ends 6 2009/03/21 00:34:17;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:d4:38:ad;
  uid "\001\000\014)\3248\255";
  client-hostname "william";
}
lease 192.168.3.99 {
  starts 5 2009/03/20 18:17:34;
  ends 5 2009/03/20 18:34:58;
  tstp 5 2009/03/20 18:34:58;
  binding state free;
  hardware ethernet 00:0c:29:4c:9a:97;
}
lease 192.168.3.99 {
  starts 5 2009/03/20 18:35:04;
  ends 6 2009/03/21 00:35:04;
  binding state active;
  next binding state free;
  hardware ethernet 00:0c:29:4c:9a:97;
  client-hostname "sauron";
}
[root@elrond ~]#


[root@elrond ~]# cat /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
option time-offset              -25200;  # Pacific Daylight Time (-7 HR)

#
#   S H I R E
#
subnet 172.30.4.0 netmask 255.255.255.0 {
        option routers                  172.30.4.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "shire";
        option domain-name-servers      207.62.187.54;

        range dynamic-bootp             172.30.4.80 172.30.4.84;
        default-lease-time              21600;
        max-lease-time                  43200;
```

```
}
[root@elrond ~]#
```

Using the information above, what IP address, netmask and default gateway were leased to Frodo?

IP: _____

Netmask: _____

Default gw:_____