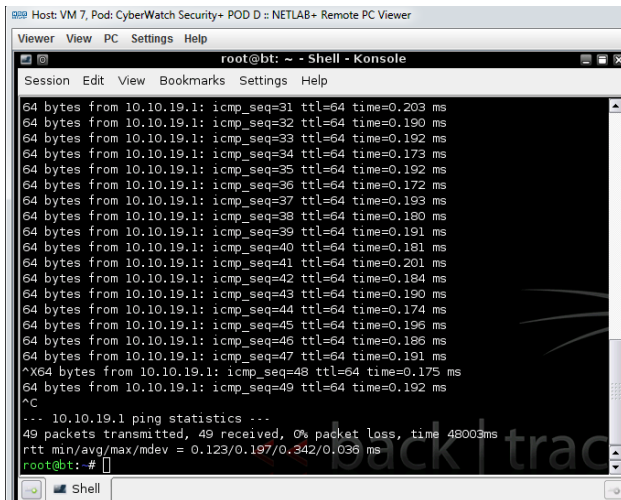


Lab 8 - CompTIA Lab 7 (pfSense Firewall)

- This is an individual assignment, and is worth 10 points.
- The due date is Thursday, November 17th (before the class).
- Follow the usual naming convention.
- The screenshot should look like the one on the lab file.

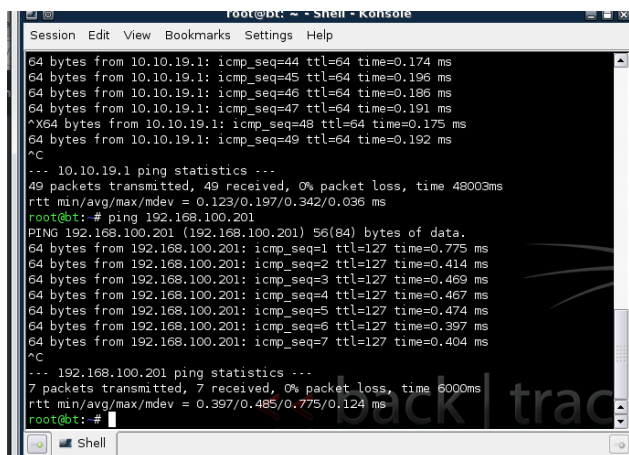
Tasks

1. (3 points) Take a screenshot (Figure 28) after completing step 22 on page 17.



```
Host: VM 7, Pod: CyberWatch Security - POD D :: NETLAB+ Remote PC Viewer
Viewer View PC Settings Help
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
64 bytes from 10.10.19.1: icmp_seq=31 ttl=64 time=0.203 ms
64 bytes from 10.10.19.1: icmp_seq=32 ttl=64 time=0.190 ms
64 bytes from 10.10.19.1: icmp_seq=33 ttl=64 time=0.192 ms
64 bytes from 10.10.19.1: icmp_seq=34 ttl=64 time=0.173 ms
64 bytes from 10.10.19.1: icmp_seq=35 ttl=64 time=0.192 ms
64 bytes from 10.10.19.1: icmp_seq=36 ttl=64 time=0.172 ms
64 bytes from 10.10.19.1: icmp_seq=37 ttl=64 time=0.193 ms
64 bytes from 10.10.19.1: icmp_seq=38 ttl=64 time=0.180 ms
64 bytes from 10.10.19.1: icmp_seq=39 ttl=64 time=0.191 ms
64 bytes from 10.10.19.1: icmp_seq=40 ttl=64 time=0.181 ms
64 bytes from 10.10.19.1: icmp_seq=41 ttl=64 time=0.201 ms
64 bytes from 10.10.19.1: icmp_seq=42 ttl=64 time=0.184 ms
64 bytes from 10.10.19.1: icmp_seq=43 ttl=64 time=0.190 ms
64 bytes from 10.10.19.1: icmp_seq=44 ttl=64 time=0.174 ms
64 bytes from 10.10.19.1: icmp_seq=45 ttl=64 time=0.196 ms
64 bytes from 10.10.19.1: icmp_seq=46 ttl=64 time=0.186 ms
64 bytes from 10.10.19.1: icmp_seq=47 ttl=64 time=0.191 ms
^X64 bytes from 10.10.19.1: icmp_seq=48 ttl=64 time=0.175 ms
64 bytes from 10.10.19.1: icmp_seq=49 ttl=64 time=0.192 ms
^C
... 10.10.19.1 ping statistics ...
49 packets transmitted, 49 received, 0% packet loss, time 48003ms
rtt min/avg/max/mdev = 0.123/0.197/0.342/0.036 ms
root@bt: #
```

2. (3 points) After task 1 above, attempt to ping Windows 2k3 Internal Server Victim from the BackTrack 4 External Attack machine. Report the result by providing a screenshot.



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
64 bytes from 10.10.19.1: icmp_seq=44 ttl=64 time=0.174 ms
64 bytes from 10.10.19.1: icmp_seq=45 ttl=64 time=0.196 ms
64 bytes from 10.10.19.1: icmp_seq=46 ttl=64 time=0.186 ms
64 bytes from 10.10.19.1: icmp_seq=47 ttl=64 time=0.191 ms
^X64 bytes from 10.10.19.1: icmp_seq=48 ttl=64 time=0.175 ms
64 bytes from 10.10.19.1: icmp_seq=49 ttl=64 time=0.192 ms
^C
... 10.10.19.1 ping statistics ...
49 packets transmitted, 49 received, 0% packet loss, time 48003ms
rtt min/avg/max/mdev = 0.123/0.197/0.342/0.036 ms
root@bt: # ping 192.168.100.201
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data.
64 bytes from 192.168.100.201: icmp_seq=1 ttl=127 time=0.775 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=127 time=0.414 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=127 time=0.469 ms
64 bytes from 192.168.100.201: icmp_seq=4 ttl=127 time=0.467 ms
64 bytes from 192.168.100.201: icmp_seq=5 ttl=127 time=0.474 ms
64 bytes from 192.168.100.201: icmp_seq=6 ttl=127 time=0.397 ms
64 bytes from 192.168.100.201: icmp_seq=7 ttl=127 time=0.404 ms
^C
... 192.168.100.201 ping statistics ...
7 packets transmitted, 7 received, 0% packet loss, time 6000ms
rtt min/avg/max/mdev = 0.397/0.485/0.775/0.124 ms
root@bt: #
```

3. (3 points) Explain what happened before and after the firewall setting changes.
Change in firewall setting allowed for ICMP requests to go through which in turn allowed us to run some of the other commands.

4. (3 points) Take a screenshot (Figure 37) after completing step 10 on page 21.

```
Host: VM 1, Pod: CyberWatch Security+ POD D :: NETLAB+ Remote PC Viewer
Viewer View PC Settings Help
File Edit View Terminal Help
root@bt:~# nmap 192.168.100.1

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2016-11-17 14:16 EST
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00028s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:99:F5:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.79 seconds
root@bt:~# nmap 192.168.100.1

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2016-11-17 14:43 EST
Nmap scan report for pfSense.localdomain (192.168.100.1)
Host is up (0.00029s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
MAC Address: 00:50:56:99:F5:6C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.43 seconds
root@bt:~#
```

5. (3 points) Explain the configuration changes you made on the firewall to allow port and re-directing responses.

Settings were changed to connect a port on the internal server. All requests for a specific port were accepted and redirected to the same port on the internal network server. In this case, requests for SSH port were sent to SSH port on the internal network.

6. (3 points) Take a screenshot (Figure 73) after completing step 32 on page 38.

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1

PPP adapter XYZ:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 169.254.83.228
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 169.254.83.228

C:\>
```

7. (2 points) Explain the changes you made for the VPN setup.

Port forwarding was set up for PPTP and an exception was created in the system firewall to allow the traffic to go through. VPN was then set up on the internal server with customer properties which allowed for a static IP address. Admin was given access to dial in to the vpn with remote access permissions. Connection wizard was run on the external server to connect as a VPN via port forwarding technique.