Scapy 2

Note: The videos found here could help if you are stuck.

TCP Handshake

Write and execute the code that will perform a three-way TCP handshake to [packtpub.samsclass.info] with a destination port of 40001. Here is some code to get you started (it generates the 3 way handshake):

```python
#!/usr/bin/python
from scapy.all import *
conf.L3socket
conf.L3socket=L3RawSocket
i=IP()
i.dst = "cit.dixie.edu"

t = TCP()
t.dport = 80
r = sr1(i/t)
t.flags = "A"
t.seq = r.ack
t.ack = r.seq + 1
p = i/t
send(p)
```

You will probably have to disable RST packets by doing something like:

```bash
sudo iptables -A OUTPUT
sudo iptables -A OUTPUT -p tcp -s 144.38.199.108 --tcp-flags RST RST --j DROP
```

The ip address above is the ip address of the machine that we don’t want to drop RST packets for.

Send an 8 character code as raw data. (Probably not your last name). You should be able to see if you succeeded by visiting this site. No more than 8 characters.

Firewalking

Modify your previous code so to send to destination port of 40002 on 144.38.193.245. Your packet should arrive with a TTL of 1 to the destination. HINT: This is very easy and should only necessitate adding a single line of code to the previous one. You will probably also make use of the traceroute program. You should be able to see if you succeeded by visiting this site (you should see an entry for firewalk). You may need to double check that port 40002 is actually open if you are doing this on a non-cit farm computer. Write a short paragraph on what TCP firewalking is.

To Submit

❖ Tell me what code you submitted to the website. Also upload your code.
❖