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](http://packtpub.samsclass.info) with a destination port of [40001](http://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
r.ack = r.seq + 1
p = i/t
reply = sr(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
```

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](http://this) site. No more than 8 characters.

Firewalking

Modify your previous code so to send to destination port of [40002](http://40002) on the previous server. 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](http://this) site. Write a short paragraph on what TCP firewalking is.

To Submit

- Tell me what code you submitted to the website. Also upload your code.
- [ ]