Scapy 2

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):

```
    #!/usr/bin/python

    from scapy.all import *

    conf.L3socket
    conf.L3socket=L3RawSocket

    i=IP()
    i.dst = "computing.utahtech.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:

```
    sudo bash
    iptables -F; iptables -A OUTPUT -p tcp --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 site. No more than 8 characters.

Land Attack

Read what this type of attack is here. This attack could still be relevant due to IoT. Simulate the attack by sending a single packet to your windows machine. You should send it to port 445. If your windows machine isn't listening on 445, you could create a folder on the desktop and share it. Verify port 445 is open with nmap. Capture 1 packet with tcpdump as indicated on this page. You will run your scapy code in one terminal, then run tcpdump in another terminal on the same machine. Take a screenshot that you have entered the winners page. The correct link to the winners page is here

To Submit

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