Lab #1: Packet Crafting Lab
CSE 3801 : Introduction to Cyber Operations
Team: Tyler Dionne

Challenge 1:
To earn the flag, submit a pcap containing an ICMP Echo Request, with a source IP of 10.10.10.10 and destination IP of 10.10.10.20
Solution:

```
$ sudo tcpdump -w capture.pcap
(while this listening, in another window do)
$ sudo scapy
>>> pkt = IP(src=”10.10.10.10”, dst=”10.10.10.20”)/ICMP (type=8)
>>> send(pkt)
```

Challenge 2:
To earn the flag, submit a pcap containing a TCP Packet with a IP source address of 10.10.10.100 and IP destination address of 10.10.10.200 the SYN, FIN, and RESET flags set
Solution:

```
$ sudo tcpdump -w capture.pcap
(while this listening, in another window do)
$ sudo scapy
>>> pkt = IP(src=”10.10.10.100”, dst=”10.10.10.200”)/TCP(sport=12345,
dport=80, flags=”SFR”)
>>> send(pkt)
```

Challenge 3:
To earn the flag, submit a pcap containing a DNS Request for www.fit.edu with an IP source address of 10.20.30.40 and IP destination address of 10.20.30.50
Solution:

```
$ sudo tcpdump -w capture.pcap
(while this listening, in another window do)
$ sudo scapy
>>> pkt = IP(src=”10.20.30.40”, dst=”10.20.30.50”)/UDP(sport=12345,
dport=53)/DNS(rd=1, qd=DNSQR(qname=”www.fit.edu”))
>>> send(pkt)
```

Challenge 4:
To earn the flag, submit a pcap containing a sequence of TCP Packets with a IP source address of 10.13.37.1 and IP destination address of 10.3.13.7, where the message SENDFLAG is encoded into the destination port

Solution:

```
$ sudo tcpdump -w capture.pcap
(while this listening, in another window do)
$ sudo scapy
>>> message = “SENDFLAG”
>>> for char in message:
…: port=ord(char)
…: pkt=IP(src=”10.13.37.1”, dst=”10.3.13.7”)/TCP(sport=12345,
dport=port)
…: send(pkt)
```