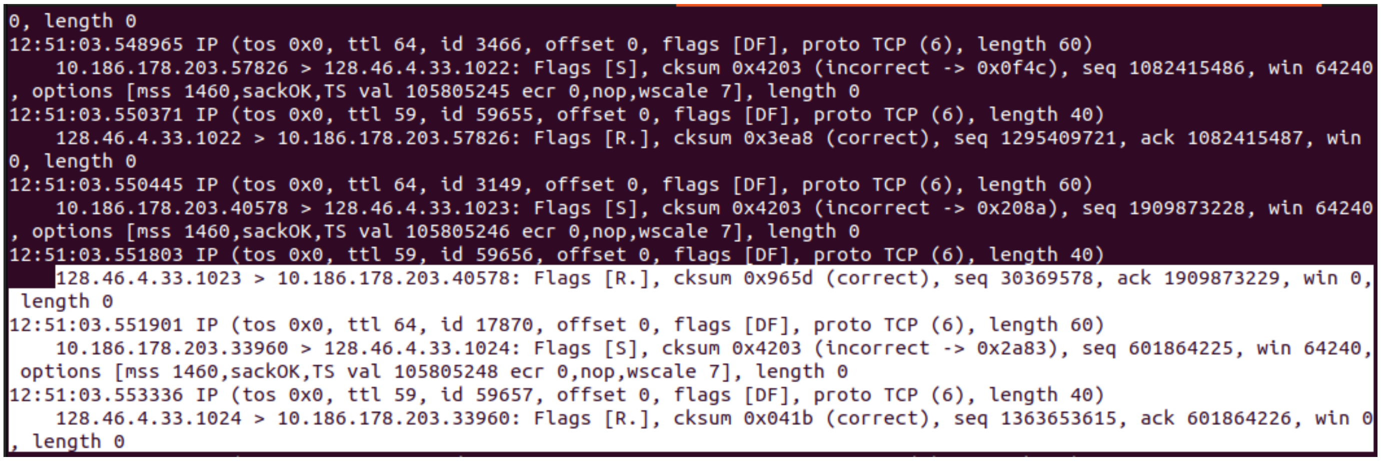
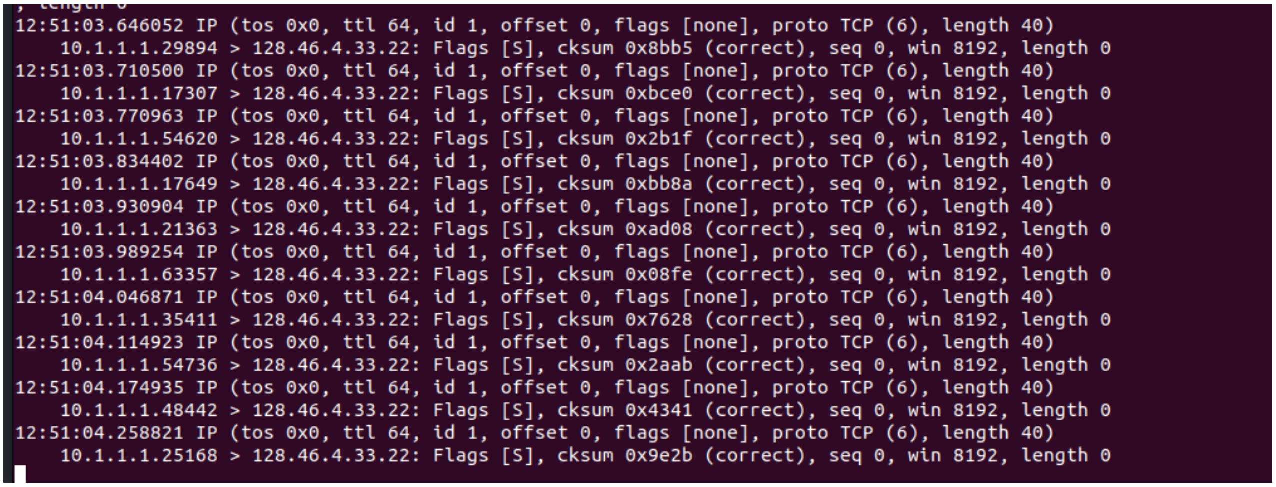
HW 8 ECE 404

Nimal Padmanabhan
March 21, 2023

For this homework, we were tasked to do port scanning as well attempt to perform a DoS attack on another IP address. The script runs through all possible ports from 1 to 1024. For this assignment, I used the **tcpdump** utility in Linux to obtain ports being scanned as well as any network traffic that is happening between the two IP address (target and spoof). The ones highlighted below show the port scanning, and the ports are getting incremented each time.



```
0, length 0
12:51:03.548965 IP (tos 0x0, ttl 64, id 3466, offset 0, flags [DF], proto TCP (6), length 60)
    10.186.178.203.57826 > 128.46.4.33.1022: Flags [S], cksum 0x4203 (incorrect -> 0x0f4c), seq 1082415486, win 64240
, options [mss 1460,sackOK,TS val 105805245 ecr 0,nop,wscale 7], length 0
12:51:03.550371 IP (tos 0x0, ttl 59, id 59655, offset 0, flags [DF], proto TCP (6), length 40)
    128.46.4.33.1022 > 10.186.178.203.57826: Flags [R.], cksum 0x3ea8 (correct), seq 1295409721, ack 1082415487, win
0, length 0
12:51:03.550445 IP (tos 0x0, ttl 64, id 3149, offset 0, flags [DF], proto TCP (6), length 60)
    10.186.178.203.40578 > 128.46.4.33.1023: Flags [S], cksum 0x4203 (incorrect -> 0x208a), seq 1909873228, win 64240
, options [mss 1460,sackOK,TS val 105805246 ecr 0,nop,wscale 7], length 0
12:51:03.551803 IP (tos 0x0, ttl 59, id 59656, offset 0, flags [DF], proto TCP (6), length 40)
    128.46.4.33.1023 > 10.186.178.203.40578: Flags [R.], cksum 0x965d (correct), seq 30369578, ack 1909873229, win 0,
 length 0
12:51:03.551901 IP (tos 0x0, ttl 64, id 17870, offset 0, flags [DF], proto TCP (6), length 60)
    10.186.178.203.33960 > 128.46.4.33.1024: Flags [S], cksum 0x4203 (incorrect -> 0x2a83), seq 601864225, win 64240,
 options [mss 1460,sackOK,TS val 105805248 ecr 0,nop,wscale 7], length 0
12:51:03.553336 IP (tos 0x0, ttl 59, id 59657, offset 0, flags [DF], proto TCP (6), length 40)
    128.46.4.33.1024 > 10.186.178.203.33960: Flags [R.], cksum 0x041b (correct), seq 1363653615, ack 601864226, win 0
, length 0
```



```
12:51:03.646052 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.29894 > 128.46.4.33.22: Flags [S], cksum 0x8bb5 (correct), seq 0, win 8192, length 0
12:51:03.710500 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.17307 > 128.46.4.33.22: Flags [S], cksum 0xbce0 (correct), seq 0, win 8192, length 0
12:51:03.770963 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.54620 > 128.46.4.33.22: Flags [S], cksum 0x2b1f (correct), seq 0, win 8192, length 0
12:51:03.834402 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.17649 > 128.46.4.33.22: Flags [S], cksum 0xbb8a (correct), seq 0, win 8192, length 0
12:51:03.930904 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.21363 > 128.46.4.33.22: Flags [S], cksum 0xad08 (correct), seq 0, win 8192, length 0
12:51:03.989254 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.63357 > 128.46.4.33.22: Flags [S], cksum 0x08fe (correct), seq 0, win 8192, length 0
12:51:04.046871 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.35411 > 128.46.4.33.22: Flags [S], cksum 0x7628 (correct), seq 0, win 8192, length 0
12:51:04.114923 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.54736 > 128.46.4.33.22: Flags [S], cksum 0x2aab (correct), seq 0, win 8192, length 0
12:51:04.174935 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.48442 > 128.46.4.33.22: Flags [S], cksum 0x4341 (correct), seq 0, win 8192, length 0
12:51:04.258821 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.1.1.1.25168 > 128.46.4.33.22: Flags [S], cksum 0x9e2b (correct), seq 0, win 8192, length 0
```

The figure above shows the attack done on a computer on the ececomp/eceprog network over 10 iterations. The left IP address is the spoof address followed by the spoof IP address.