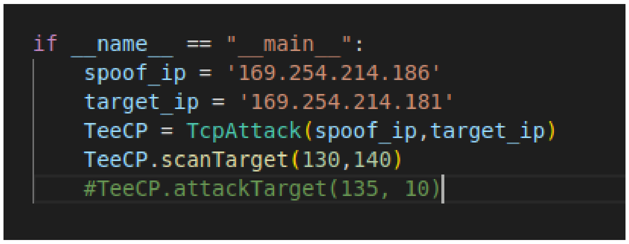
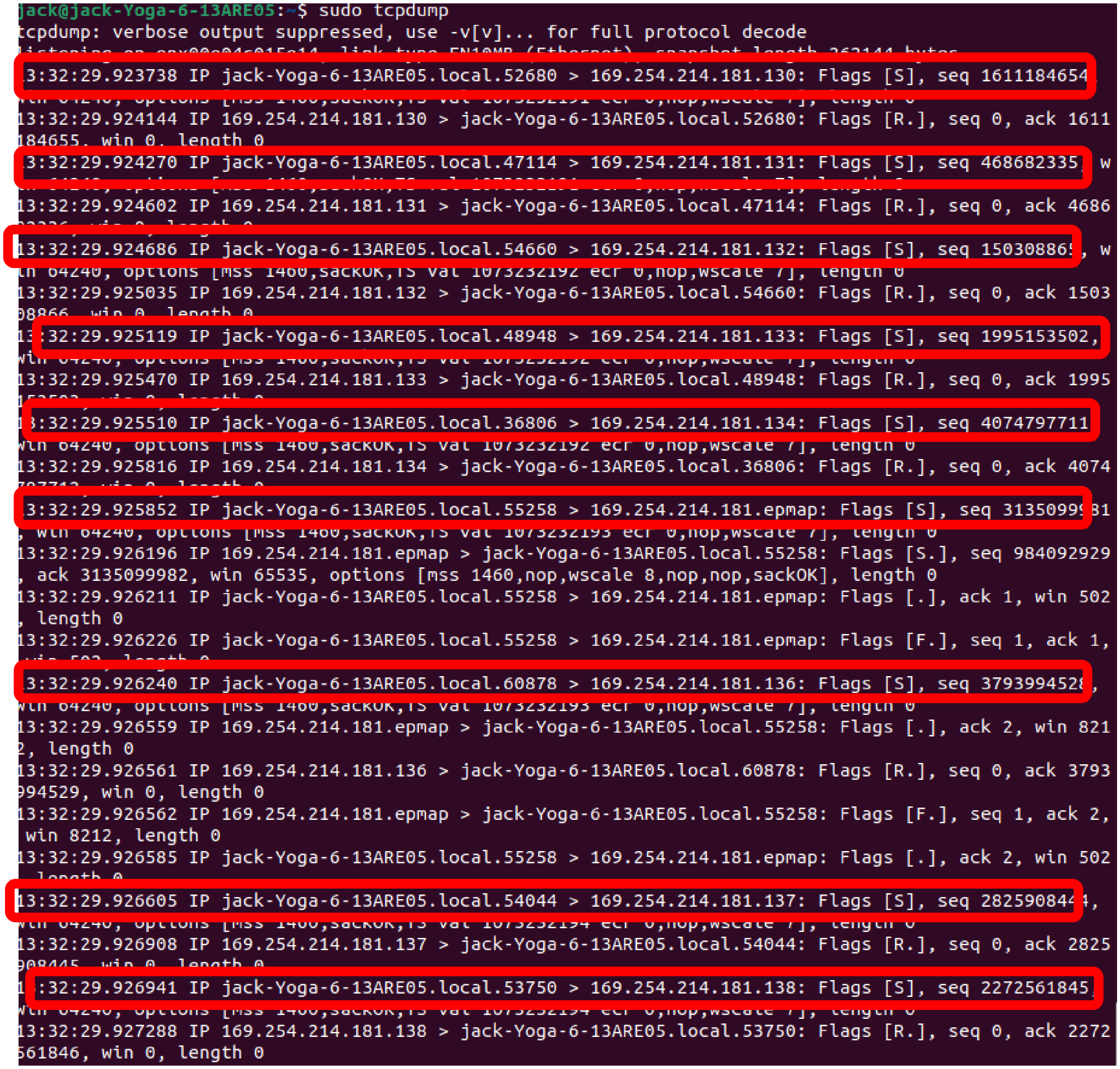
HW08: TCP Vulnerabilities, DOS Attacks
Name: Jack Gardner
ECN Login: gardne97
Due Date: 3/21/23



```
if __name__ == "__main__":
    spoof_ip = '169.254.214.186'
    target_ip = '169.254.214.181'
    TeeCP = TcpAttack(spoof_ip,target_ip)
    TeeCP.scanTarget(130,140)
    #TeeCP.attackTarget(135, 10)
```



```
jack@jack-Yoga-6-13ARE05:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enx00e04c015e14, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:32:29.923738 IP jack-Yoga-6-13ARE05.local.52680 > 169.254.214.181.130: Flags [S], seq 1611184654
win 64240, options [mss 1460,sackOK,TS val 1073232191 ecr 0,nop,wscale 7], length 0
13:32:29.924144 IP 169.254.214.181.130 > jack-Yoga-6-13ARE05.local.52680: Flags [R.], seq 0, ack 1611
184655, win 0, length 0
13:32:29.924270 IP jack-Yoga-6-13ARE05.local.47114 > 169.254.214.181.131: Flags [S], seq 468682335, w
in 64240, options [mss 1460,sackOK,TS val 1073232191 ecr 0,nop,wscale 7], length 0
13:32:29.924602 IP 169.254.214.181.131 > jack-Yoga-6-13ARE05.local.47114: Flags [R.], seq 0, ack 4686
82336, win 0, length 0
13:32:29.924686 IP jack-Yoga-6-13ARE05.local.54660 > 169.254.214.181.132: Flags [S], seq 1503088865, w
in 64240, options [mss 1460,sackOK,TS val 1073232192 ecr 0,nop,wscale 7], length 0
13:32:29.925035 IP 169.254.214.181.132 > jack-Yoga-6-13ARE05.local.54660: Flags [R.], seq 0, ack 1503
088866, win 0, length 0
13:32:29.925119 IP jack-Yoga-6-13ARE05.local.48948 > 169.254.214.181.133: Flags [S], seq 1995153502,
win 64240, options [mss 1460,sackOK,TS val 1073232192 ecr 0,nop,wscale 7], length 0
13:32:29.925470 IP 169.254.214.181.133 > jack-Yoga-6-13ARE05.local.48948: Flags [R.], seq 0, ack 1995
153503, win 0, length 0
13:32:29.925510 IP jack-Yoga-6-13ARE05.local.36806 > 169.254.214.181.134: Flags [S], seq 4074797711
win 64240, options [mss 1460,sackOK,TS val 1073232192 ecr 0,nop,wscale 7], length 0
13:32:29.925816 IP 169.254.214.181.134 > jack-Yoga-6-13ARE05.local.36806: Flags [R.], seq 0, ack 4074
797712, win 0, length 0
13:32:29.925852 IP jack-Yoga-6-13ARE05.local.55258 > 169.254.214.181.epmap: Flags [S], seq 3135099981
, win 64240, options [mss 1460,sackOK,TS val 1073232193 ecr 0,nop,wscale 7], length 0
13:32:29.926196 IP 169.254.214.181.epmap > jack-Yoga-6-13ARE05.local.55258: Flags [S.], seq 984092929
, ack 3135099982, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
13:32:29.926211 IP jack-Yoga-6-13ARE05.local.55258 > 169.254.214.181.epmap: Flags [.], ack 1, win 502
, length 0
13:32:29.926226 IP jack-Yoga-6-13ARE05.local.55258 > 169.254.214.181.epmap: Flags [F.], seq 1, ack 1,
win 502, length 0
13:32:29.926240 IP jack-Yoga-6-13ARE05.local.60878 > 169.254.214.181.136: Flags [S], seq 3793994528,
win 64240, options [mss 1460,sackOK,TS val 1073232193 ecr 0,nop,wscale 7], length 0
13:32:29.926559 IP 169.254.214.181.epmap > jack-Yoga-6-13ARE05.local.55258: Flags [.], ack 2, win 821
2, length 0
13:32:29.926561 IP 169.254.214.181.136 > jack-Yoga-6-13ARE05.local.60878: Flags [R.], seq 0, ack 3793
994529, win 0, length 0
13:32:29.926562 IP 169.254.214.181.epmap > jack-Yoga-6-13ARE05.local.55258: Flags [F.], seq 1, ack 2,
 win 8212, length 0
13:32:29.926585 IP jack-Yoga-6-13ARE05.local.55258 > 169.254.214.181.epmap: Flags [.], ack 2, win 502
, length 0
13:32:29.926605 IP jack-Yoga-6-13ARE05.local.54044 > 169.254.214.181.137: Flags [S], seq 2825908444,
win 64240, options [mss 1460,sackOK,TS val 1073232194 ecr 0,nop,wscale 7], length 0
13:32:29.926908 IP 169.254.214.181.137 > jack-Yoga-6-13ARE05.local.54044: Flags [R.], seq 0, ack 2825
908445, win 0, length 0
13:32:29.926941 IP jack-Yoga-6-13ARE05.local.53750 > 169.254.214.181.138: Flags [S], seq 2272561845,
win 64240, options [mss 1460,sackOK,TS val 1073232194 ecr 0,nop,wscale 7], length 0
13:32:29.927288 IP 169.254.214.181.138 > jack-Yoga-6-13ARE05.local.53750: Flags [R.], seq 0, ack 2272
561846, win 0, length 0
```

As seen in the image, the TCP dump shows 8 of the 10 packets being sent from the spoof IP address to the target IP address with the “S” flag set, with each packet having a different port number to determine if that port is open. Since port 135 is open, the port sends a reply back to the spoof ip.