# ECE 404 Homework 8

Ranjan Behl (rbehl)

March 30, 2021

## 1. Coding HW

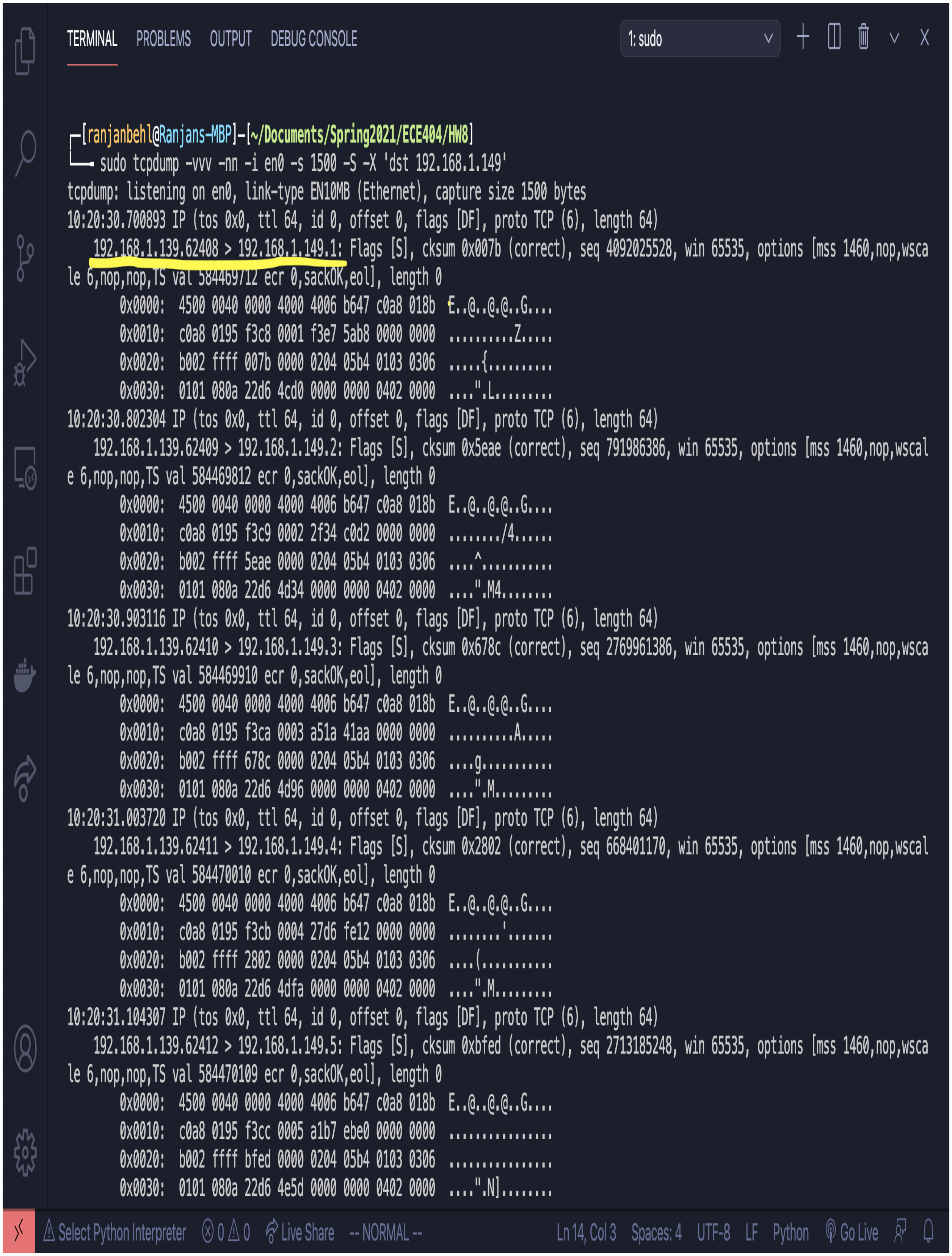
HW 8 - TcpAttack

## 2. Explanation of the Code

The testscript I used is below

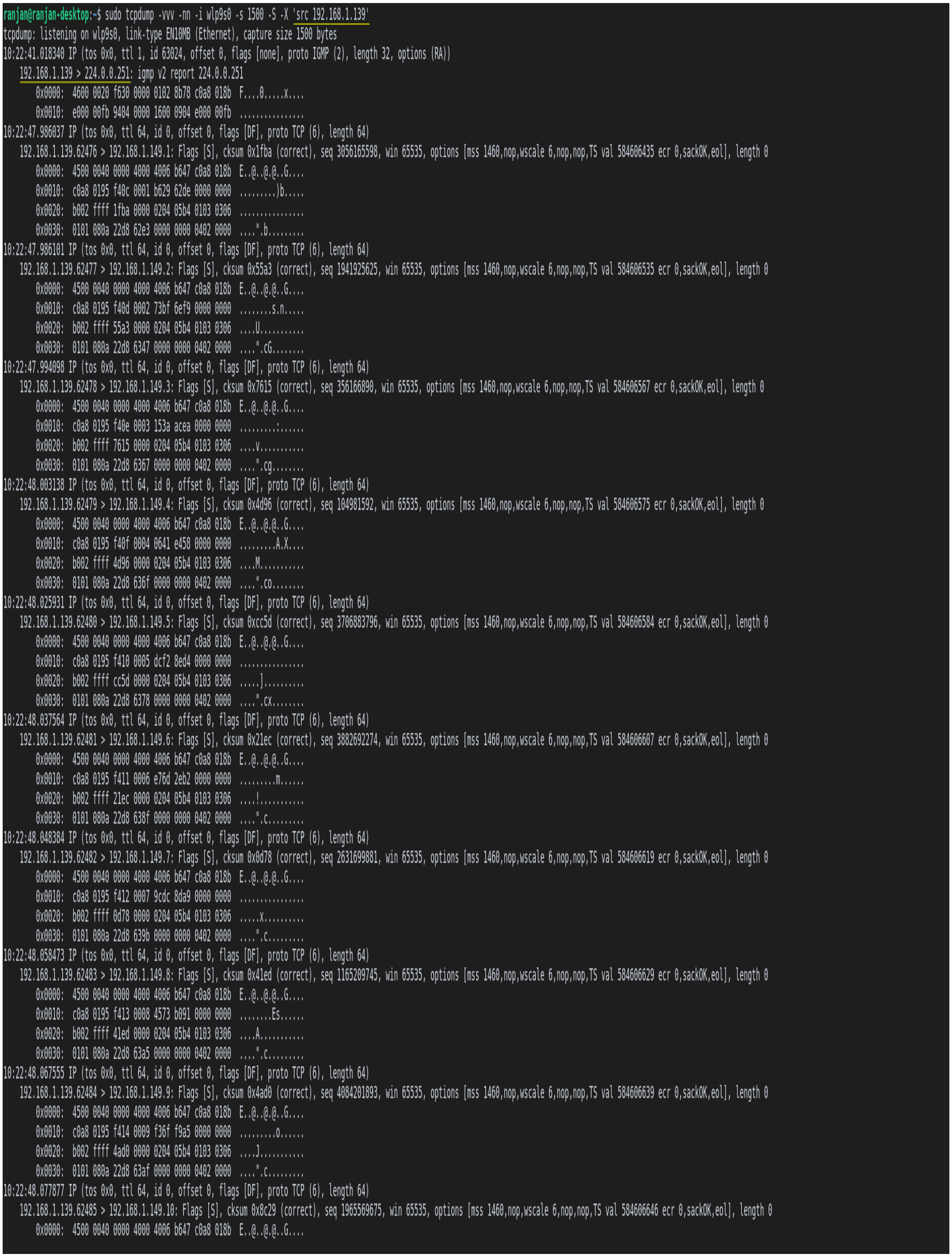
```
from TcpAttack import *
spoofIP = '192.168.1.137' # real ip is 192.168.1.139
targetIP = '192.168.1.149'
rangeStart = 1
rangeEnd = 60
port = 53
Tcp = TcpAttack(spoofIP,targetIP)
Tcp.scanTarget(rangeStart,rangeEnd)
if Tcp.attackTarget(port,1000):
    print("Port was open to attack")
else:
     print("Port is closed")
```

## 3. Port Scanning



```
┌─[ranjanbehl@Ranjans-MBP]─[~/Documents/Spring2021/ECE404/HW8]
└──╼ sudo tcpdump -vvv -nn -i en0 -s 1500 -S -X 'dst 192.168.1.149'
tcpdump: listening on en0, link-type EN10MB (Ethernet), capture size 1500 bytes
10:20:30.700893 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62408 > 192.168.1.149.1: Flags [S], cksum 0x007b (correct), seq 4092025528, win 65535, options [mss 1460,nop,wsca
le 6,nop,nop,TS val 584469712 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f3c8 0001 f3e7 5ab8 0000 0000  ..........Z.....
        0x0020:  b002 ffff 007b 0000 0204 05b4 0103 0306  .....{..........
        0x0030:  0101 080a 22d6 4cd0 0000 0000 0402 0000  ....".L.........
10:20:30.802304 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62409 > 192.168.1.149.2: Flags [S], cksum 0x5eae (correct), seq 791986386, win 65535, options [mss 1460,nop,wscal
e 6,nop,nop,TS val 584469812 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f3c9 0002 2f34 c0d2 0000 0000  ......../4......
        0x0020:  b002 ffff 5eae 0000 0204 05b4 0103 0306  ....^...........
        0x0030:  0101 080a 22d6 4d34 0000 0000 0402 0000  ....".M4........
10:20:30.903116 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62410 > 192.168.1.149.3: Flags [S], cksum 0x678c (correct), seq 2769961386, win 65535, options [mss 1460,nop,wsca
le 6,nop,nop,TS val 584469910 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f3ca 0003 a51a 41aa 0000 0000  ..........A.....
        0x0020:  b002 ffff 678c 0000 0204 05b4 0103 0306  ....g...........
        0x0030:  0101 080a 22d6 4d96 0000 0000 0402 0000  ....".M.........
10:20:31.003720 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62411 > 192.168.1.149.4: Flags [S], cksum 0x2802 (correct), seq 668401170, win 65535, options [mss 1460,nop,wscal
e 6,nop,nop,TS val 584470010 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f3cb 0004 27d6 fe12 0000 0000  ........'.......
        0x0020:  b002 ffff 2802 0000 0204 05b4 0103 0306  ....(...........
        0x0030:  0101 080a 22d6 4dfa 0000 0000 0402 0000  ....".M.........
10:20:31.104307 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62412 > 192.168.1.149.5: Flags [S], cksum 0xbfed (correct), seq 2713185248, win 65535, options [mss 1460,nop,wsca
le 6,nop,nop,TS val 584470109 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f3cc 0005 a1b7 ebe0 0000 0000  ................
        0x0020:  b002 ffff bfed 0000 0204 05b4 0103 0306  ................
        0x0030:  0101 080a 22d6 4e5d 0000 0000 0402 0000  ....".N]........
```

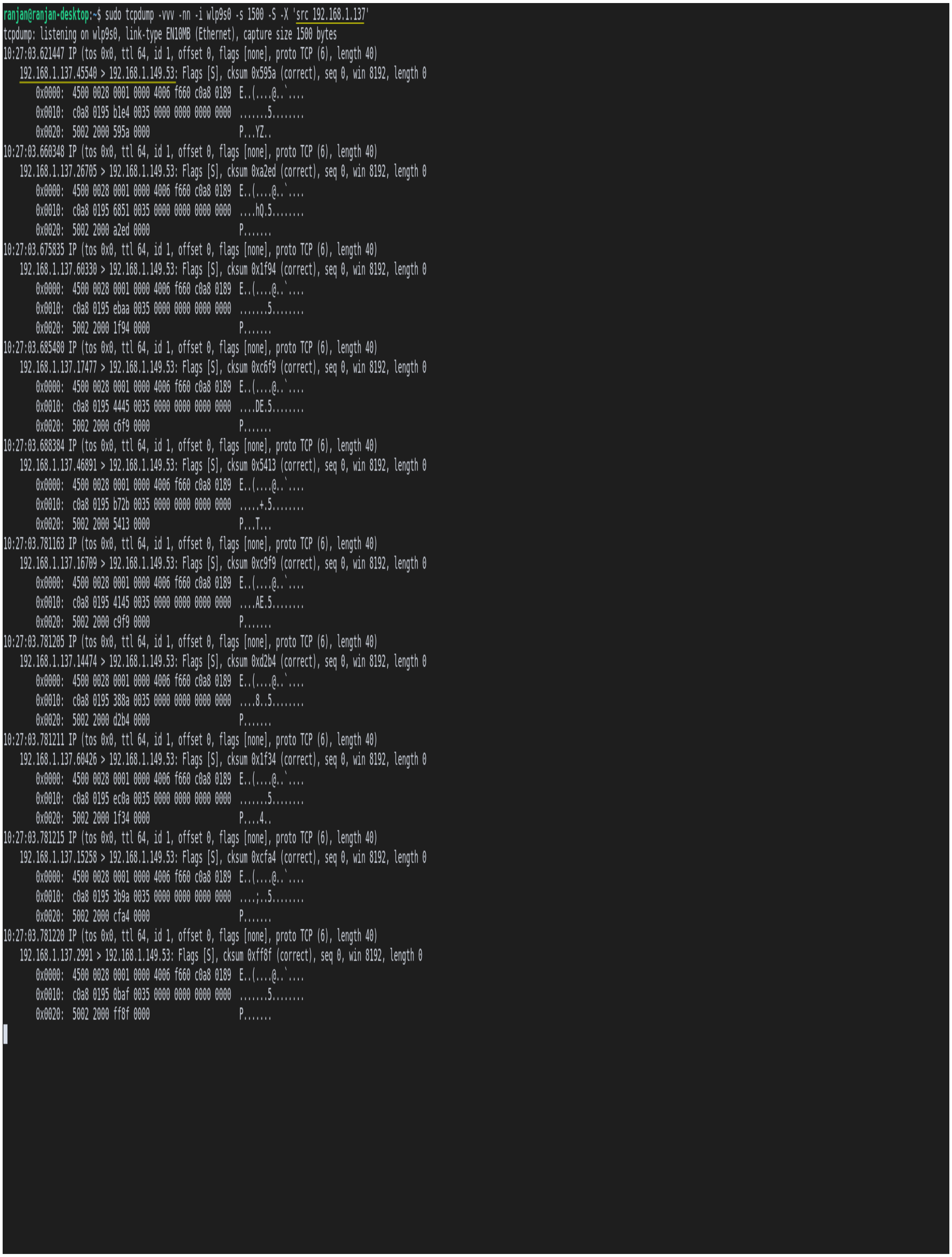
Figure 1: Port Scan tcpdump output from original machine



```
ranjan@ranjan-desktop:~$ sudo tcpdump -vvv -nn -i wlp9s0 -s 1500 -S -X 'src 192.168.1.139'
tcpdump: listening on wlp9s0, link-type EN10MB (Ethernet), capture size 1500 bytes
10:22:41.018340 IP (tos 0x0, ttl 1, id 63024, offset 0, flags [none], proto IGMP (2), length 32, options (RA))
    192.168.1.139 > 224.0.0.251: igmp v2 report 224.0.0.251
        0x0000:  4600 0020 f630 0000 0102 8b78 c0a8 018b  F....0.....x....
        0x0010:  e000 00fb 9404 0000 1600 0904 e000 00fb  ................
10:22:47.986037 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62476 > 192.168.1.149.1: Flags [S], cksum 0x1fba (correct), seq 3056165598, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606435 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f40c 0001 b629 62de 0000 0000  .........)b.....
        0x0020:  b002 ffff 1fba 0000 0204 05b4 0103 0306  ................
        0x0030:  0101 080a 22d8 62e3 0000 0000 0402 0000  ....".b.........
10:22:47.986101 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62477 > 192.168.1.149.2: Flags [S], cksum 0x55a3 (correct), seq 1941925625, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606535 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f40d 0002 73bf 6ef9 0000 0000  ........s.n.....
        0x0020:  b002 ffff 55a3 0000 0204 05b4 0103 0306  ....U...........
        0x0030:  0101 080a 22d8 6347 0000 0000 0402 0000  ....".cG........
10:22:47.994098 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62478 > 192.168.1.149.3: Flags [S], cksum 0x7615 (correct), seq 356166890, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606567 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f40e 0003 153a acea 0000 0000  .........:......
        0x0020:  b002 ffff 7615 0000 0204 05b4 0103 0306  ....v...........
        0x0030:  0101 080a 22d8 6367 0000 0000 0402 0000  ....".cg........
10:22:48.003138 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62479 > 192.168.1.149.4: Flags [S], cksum 0x4d96 (correct), seq 104981592, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606575 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f40f 0004 0641 e458 0000 0000  .........A.X....
        0x0020:  b002 ffff 4d96 0000 0204 05b4 0103 0306  ....M...........
        0x0030:  0101 080a 22d8 636f 0000 0000 0402 0000  ....".co........
10:22:48.025931 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62480 > 192.168.1.149.5: Flags [S], cksum 0xcc5d (correct), seq 3706883796, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606584 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f410 0005 dcf2 8ed4 0000 0000  ................
        0x0020:  b002 ffff cc5d 0000 0204 05b4 0103 0306  .....]..........
        0x0030:  0101 080a 22d8 6378 0000 0000 0402 0000  ....".cx........
10:22:48.037564 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62481 > 192.168.1.149.6: Flags [S], cksum 0x21ec (correct), seq 3882692274, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606607 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f411 0006 e76d 2eb2 0000 0000  .........m......
        0x0020:  b002 ffff 21ec 0000 0204 05b4 0103 0306  ....!...........
        0x0030:  0101 080a 22d8 638f 0000 0000 0402 0000  ....".c.........
10:22:48.048384 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62482 > 192.168.1.149.7: Flags [S], cksum 0x0d78 (correct), seq 2631699881, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606619 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f412 0007 9cdc 8da9 0000 0000  ................
        0x0020:  b002 ffff 0d78 0000 0204 05b4 0103 0306  .....x..........
        0x0030:  0101 080a 22d8 639b 0000 0000 0402 0000  ....".c.........
10:22:48.058473 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62483 > 192.168.1.149.8: Flags [S], cksum 0x41ed (correct), seq 1165209745, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606629 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f413 0008 4573 b091 0000 0000  ........Es......
        0x0020:  b002 ffff 41ed 0000 0204 05b4 0103 0306  ....A...........
        0x0030:  0101 080a 22d8 63a5 0000 0000 0402 0000  ....".c.........
10:22:48.067555 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62484 > 192.168.1.149.9: Flags [S], cksum 0x4ad0 (correct), seq 4084201893, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606639 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
        0x0010:  c0a8 0195 f414 0009 f36f f9a5 0000 0000  .........o......
        0x0020:  b002 ffff 4ad0 0000 0204 05b4 0103 0306  ....J...........
        0x0030:  0101 080a 22d8 63af 0000 0000 0402 0000  ....".c.........
10:22:48.077877 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
    192.168.1.139.62485 > 192.168.1.149.10: Flags [S], cksum 0x8c29 (correct), seq 1965569675, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 584606646 ecr 0,sackOK,eol], length 0
        0x0000:  4500 0040 0000 4000 4006 b647 c0a8 018b  E..@..@.@..G....
```

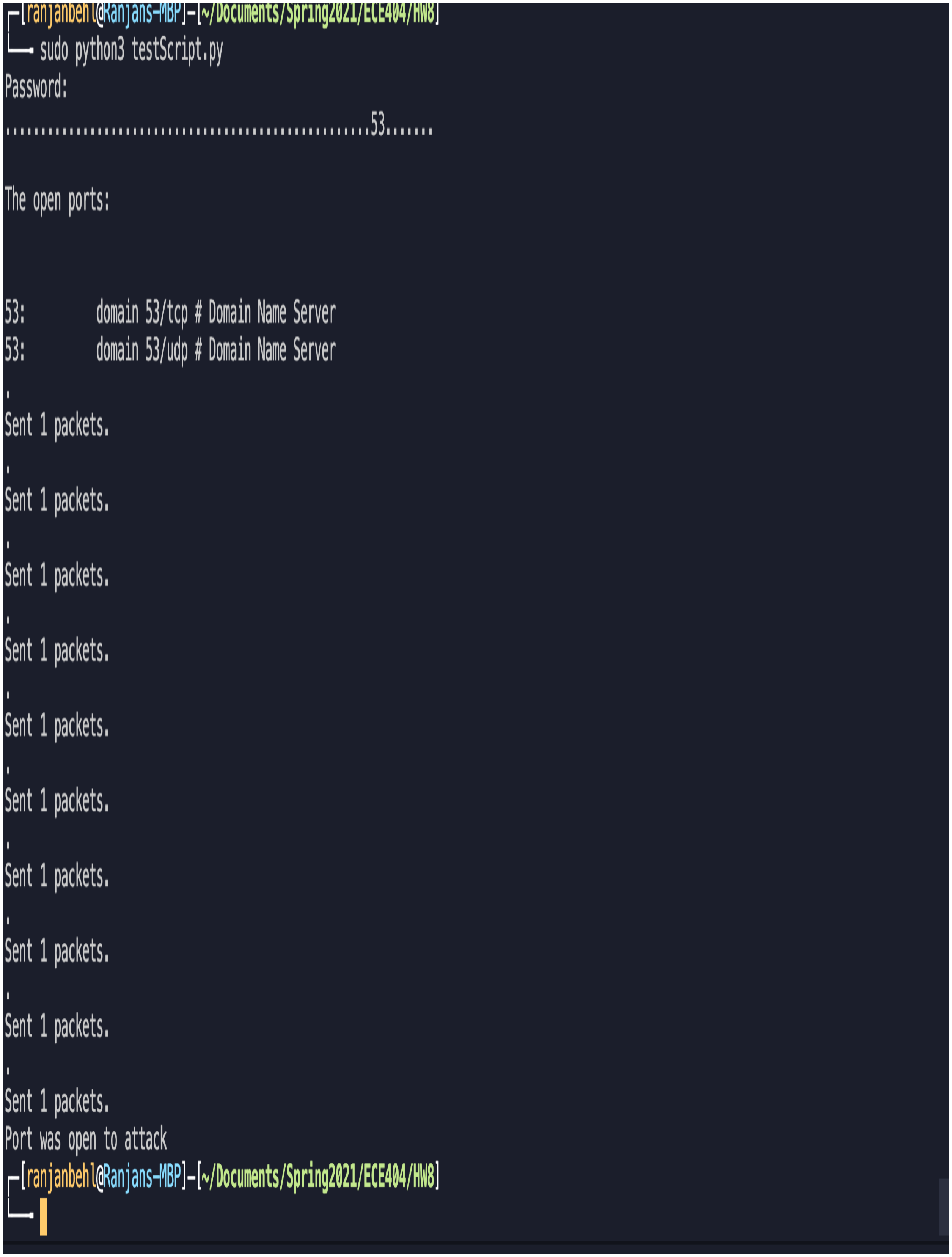
Figure 2: Ports being scanned on target machine

## 4. TcpAttack



```
ranjan@ranjan-desktop:~$ sudo tcpdump -vvv -nn -i wlp9s0 -s 1500 -S -X 'src 192.168.1.137'
tcpdump: listening on wlp9s0, link-type EN10MB (Ethernet), capture size 1500 bytes
10:27:03.621447 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.45540 > 192.168.1.149.53: Flags [S], cksum 0x595a (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 b1e4 0035 0000 0000 0000 0000  .......5........
        0x0020:  5002 2000 595a 0000                      P...YZ..
10:27:03.660348 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.26705 > 192.168.1.149.53: Flags [S], cksum 0xa2ed (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 6851 0035 0000 0000 0000 0000  ....hQ.5........
        0x0020:  5002 2000 a2ed 0000                      P.......
10:27:03.675835 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.60330 > 192.168.1.149.53: Flags [S], cksum 0x1f94 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 ebaa 0035 0000 0000 0000 0000  .......5........
        0x0020:  5002 2000 1f94 0000                      P.......
10:27:03.685480 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.17477 > 192.168.1.149.53: Flags [S], cksum 0xc6f9 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 4445 0035 0000 0000 0000 0000  ....DE.5........
        0x0020:  5002 2000 c6f9 0000                      P.......
10:27:03.688384 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.46891 > 192.168.1.149.53: Flags [S], cksum 0x5413 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 b72b 0035 0000 0000 0000 0000  .....+.5........
        0x0020:  5002 2000 5413 0000                      P...T...
10:27:03.781163 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.16709 > 192.168.1.149.53: Flags [S], cksum 0xc9f9 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 4145 0035 0000 0000 0000 0000  ....AE.5........
        0x0020:  5002 2000 c9f9 0000                      P.......
10:27:03.781205 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.14474 > 192.168.1.149.53: Flags [S], cksum 0xd2b4 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 388a 0035 0000 0000 0000 0000  ....8..5........
        0x0020:  5002 2000 d2b4 0000                      P.......
10:27:03.781211 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.60426 > 192.168.1.149.53: Flags [S], cksum 0x1f34 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 ec0a 0035 0000 0000 0000 0000  .......5........
        0x0020:  5002 2000 1f34 0000                      P....4..
10:27:03.781215 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.15258 > 192.168.1.149.53: Flags [S], cksum 0xcfa4 (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 3b9a 0035 0000 0000 0000 0000  ....;..5........
        0x0020:  5002 2000 cfa4 0000                      P.......
10:27:03.781220 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    192.168.1.137.2991 > 192.168.1.149.53: Flags [S], cksum 0xff8f (correct), seq 0, win 8192, length 0
        0x0000:  4500 0028 0001 0000 4006 f660 c0a8 0189  E..(....@..`....
        0x0010:  c0a8 0195 0baf 0035 0000 0000 0000 0000  .......5........
        0x0020:  5002 2000 ff8f 0000                      P.......
```

Figure 3: TCP attack tcpdump on target machine



```
┌─[ranjanbehl@Ranjans-MBP]─[~/Documents/Spring2021/ECE404/HW8]
└──╼ sudo python3 testScript.py
Password:
..................................................53.......

The open ports:



53:        domain 53/tcp # Domain Name Server
53:        domain 53/udp # Domain Name Server
.
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
┌─[ranjanbehl@Ranjans-MBP]─[~/Documents/Spring2021/ECE404/HW8]
└──╼
```

Figure 4: Output of testScript.py