

Anish Laddha
Professor Avinash Kak
ECE404
February 19 2024

Homework 8

tcpdump command indicating port scanning:

```
sudo tcpdump -vvv -nn 'host 128.46.144.123 and tcp[tcpflags] & tcp-syn != 0'
```

This will dump only the packets containing the host '128.46.144.123' (moonshine) where the tcp-syn flag is on.

tcpdump output indicating port scanning:

```
192.168.4.23.65475 > 128.46.144.123.3990: Flags [S], cksum 0xc89d (correct), seq 444441609, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 2921143543 ecr 0,sackOK,eol], length 0
01:29:51.360210 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65476 > 128.46.144.123.3991: Flags [S], cksum 0x5e4f (correct), seq 599301153, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1128788166 ecr 0,sackOK,eol], length 0
01:29:51.367893 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65477 > 128.46.144.123.3992: Flags [S], cksum 0x329f (correct), seq 3763061181, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1047936790 ecr 0,sackOK,eol], length 0
01:29:51.374407 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65478 > 128.46.144.123.3993: Flags [S], cksum 0x918a (correct), seq 2784100941, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 846718449 ecr 0,sackOK,eol], length 0
01:29:51.380723 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65479 > 128.46.144.123.3994: Flags [S], cksum 0x3732 (correct), seq 1069813972, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 3209104159 ecr 0,sackOK,eol], length 0
01:29:51.388126 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65480 > 128.46.144.123.3995: Flags [S], cksum 0x9441 (correct), seq 2513823212, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 4059648049 ecr 0,sackOK,eol], length 0
01:29:51.395317 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65481 > 128.46.144.123.3996: Flags [S], cksum 0x12b6 (correct), seq 1282191463, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 2415964834 ecr 0,sackOK,eol], length 0
01:29:51.402431 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65482 > 128.46.144.123.3997: Flags [S], cksum 0x9afd (correct), seq 1929028046, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 2938565437 ecr 0,sackOK,eol], length 0
01:29:51.409524 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65483 > 128.46.144.123.3998: Flags [S], cksum 0x424b (correct), seq 3933303604, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 4241732963 ecr 0,sackOK,eol], length 0
01:29:51.416968 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65484 > 128.46.144.123.3999: Flags [S], cksum 0x4e01 (correct), seq 1197261132, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 1992656055 ecr 0,sackOK,eol], length 0
01:29:51.424020 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 64)
192.168.4.23.65485 > 128.46.144.123.4000: Flags [S], cksum 0xc599 (correct), seq 1556588167, win 65535, options [mss 1460,nop,wscale 6,nop,nop,TS val 125206982 ecr 0,sackOK,eol], length 0
```

In the first red box, we see that my IP is sending out numerous requests to the moonshine IP.

In the second column of red boxes, we see that the port number that we are sending these packets to is incrementing by 1 every packet, from 1000 -> 4000.

Finally, we see that we are sending a Syn packet. In scanning the port, we are initializing a socket connection for a very small amount of time, and the first step of establishing a socket is sending a syn packet.

ALL PACKETS IN IMAGE WERE SENT BY ME

(continued on next page)

tcpdump command indicating SYN flood attack on port 1716:

```
sudo tcpdump -vvv -nn 'host 10.10.10.10 and host 128.46.144.123 and tcp[tcpflags] & tcp-syn != 0'
```

This will dump only the packets between the host ‘128.46.144.123’ (moonshine) and host 10.10.10.10 (spoofed IP) where the tcp-syn flag is on.

tcpdump output indicating SYN flood attack on port 1716:

```
00:43:21.388480 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.44705 > 128.46.144.123.1716: Flags [S], cksum 0xb5cf (correct), seq 0, win 8192, length 0
00:43:21.391941 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.64179 > 128.46.144.123.1716: Flags [S], cksum 0x69bd (correct), seq 0, win 8192, length 0
00:43:21.395659 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.48585 > 128.46.144.123.1716: Flags [S], cksum 0xa6a7 (correct), seq 0, win 8192, length 0
00:43:21.399274 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.59125 > 128.46.144.123.1716: Flags [S], cksum 0x7d7b (correct), seq 0, win 8192, length 0
00:43:21.402859 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.24619 > 128.46.144.123.1716: Flags [S], cksum 0x0446 (correct), seq 0, win 8192, length 0
00:43:21.406364 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.55285 > 128.46.144.123.1716: Flags [S], cksum 0x8c7b (correct), seq 0, win 8192, length 0
00:43:21.410811 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.10962 > 128.46.144.123.1716: Flags [S], cksum 0x399f (correct), seq 0, win 8192, length 0
00:43:21.414470 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.55418 > 128.46.144.123.1716: Flags [S], cksum 0x8bf6 (correct), seq 0, win 8192, length 0
00:43:21.418305 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.61903 > 128.46.144.123.1716: Flags [S], cksum 0x72a1 (correct), seq 0, win 8192, length 0
00:43:21.422188 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.21713 > 128.46.144.123.1716: Flags [S], cksum 0x0fa0 (correct), seq 0, win 8192, length 0
00:43:21.425663 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.57285 > 128.46.144.123.1716: Flags [S], cksum 0x84ab (correct), seq 0, win 8192, length 0
00:43:21.429366 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.4070 > 128.46.144.123.1716: Flags [S], cksum 0x548b (correct), seq 0, win 8192, length 0
00:43:21.432967 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.37303 > 128.46.144.123.1716: Flags [S], cksum 0xd2b9 (correct), seq 0, win 8192, length 0
00:43:21.436545 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.20559 > 128.46.144.123.1716: Flags [S], cksum 0x1422 (correct), seq 0, win 8192, length 0
00:43:21.440077 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.20163 > 128.46.144.123.1716: Flags [S], cksum 0x15ae (correct), seq 0, win 8192, length 0
00:43:21.443702 IP (tos 0x0, ttl 64, id 1, offset 0, flags [none], proto TCP (6), length 40)
    10.10.10.10.13996 > 128.46.144.123.1716: Flags [S], cksum 0x2dc5 (correct), seq 0, win 8192, length 0
```

The red box in the first column shows that the packets we create are being sent with a spoofed source IP of 10.10.10.10

The red boxes in the second column show that the port we are spamming these packets to is 1716

The red box in the third column indicates that these are syn packets, and that I’m engaged in syn Flooding.

ALL PACKETS IN IMAGE WERE SENT BY ME