Anish Laddha
Professor Avinash Kak
ECE404
February 19 2024

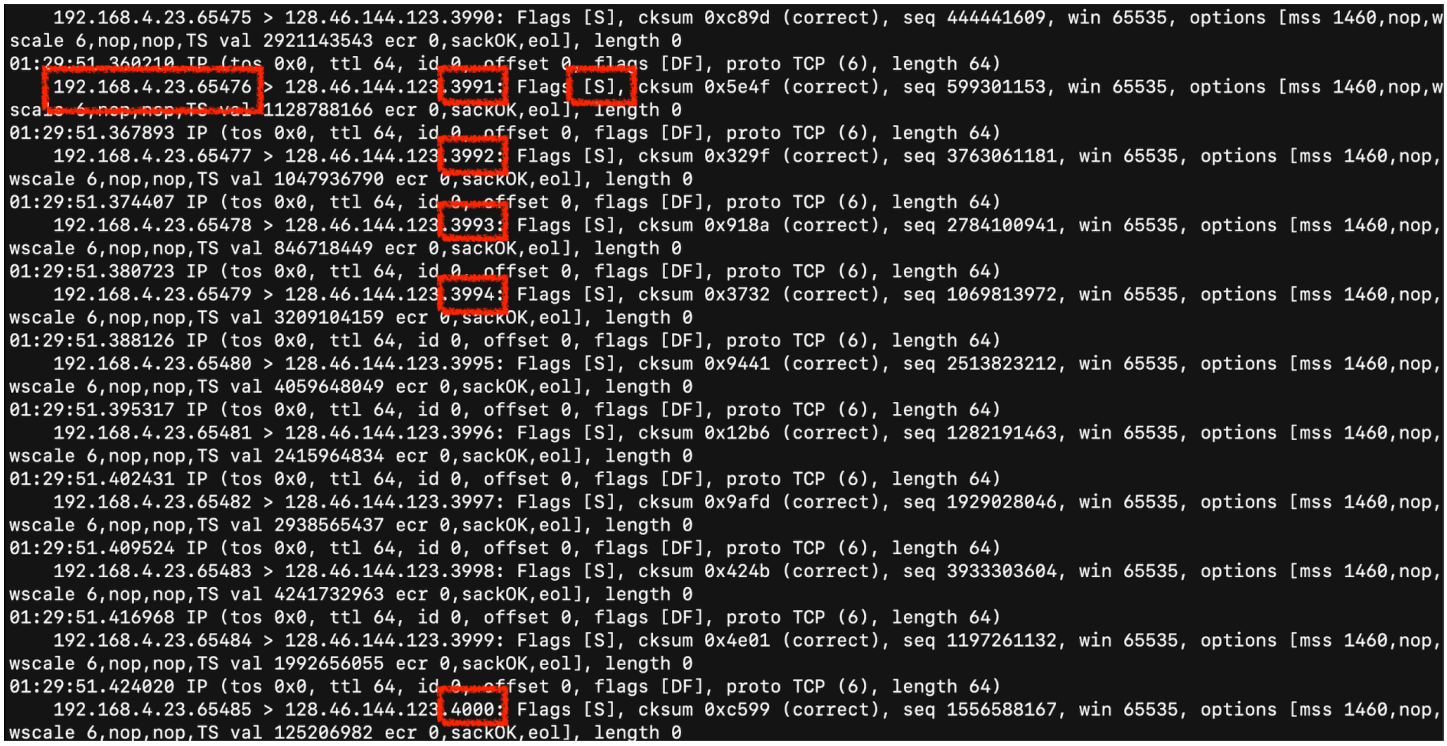
Homework 8

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:



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

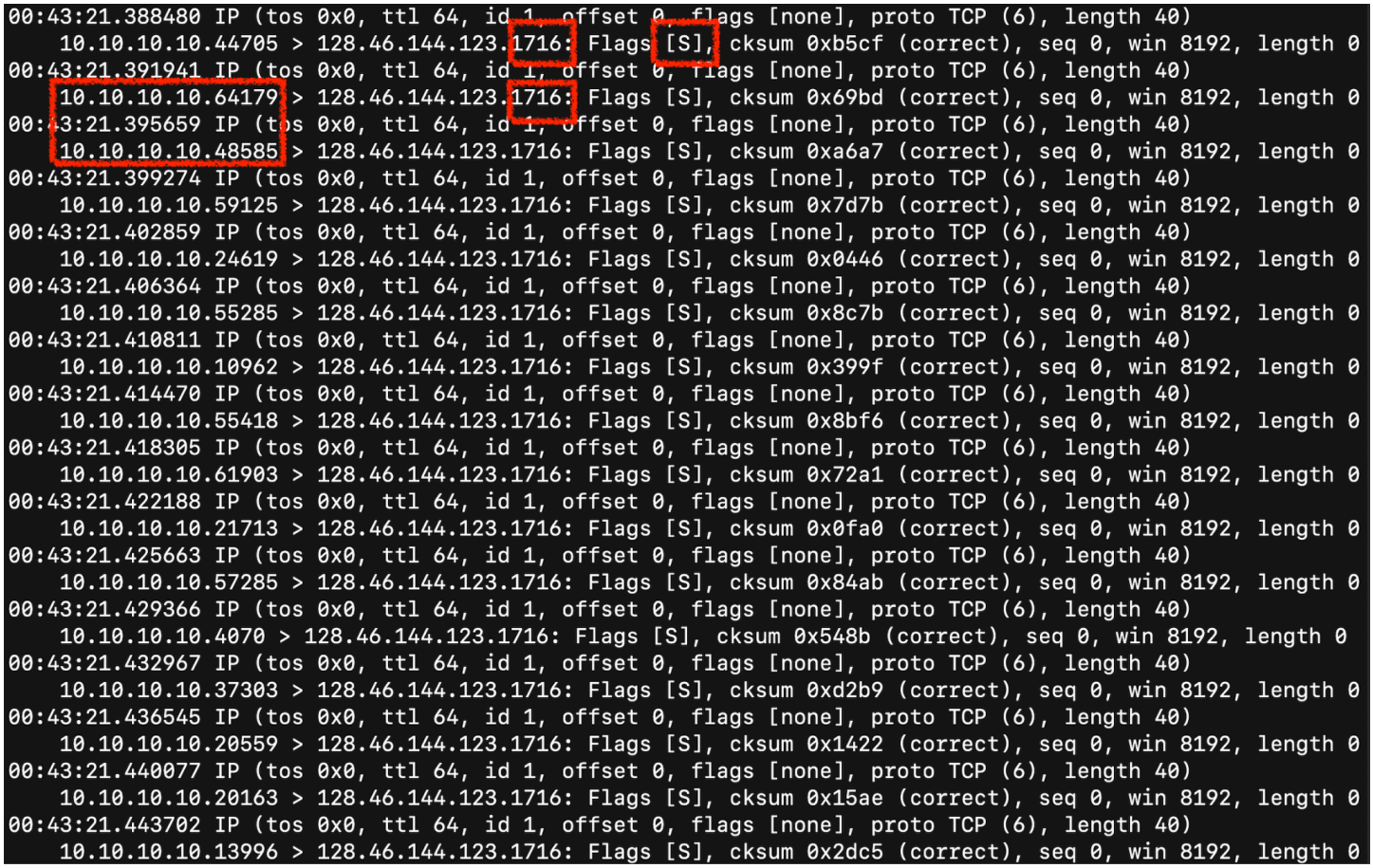
(continued on next page)

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:



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