CSDS-325 Computer Networks, proj4.extraCredit

Nicolas Slavonia, njs140

November 2022

Here are some of the interesting things I found.

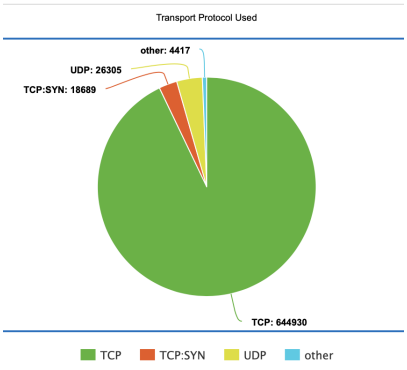
Using -s, all 694,341 packets were IPv4 packets and the trace spans over 23 hours.

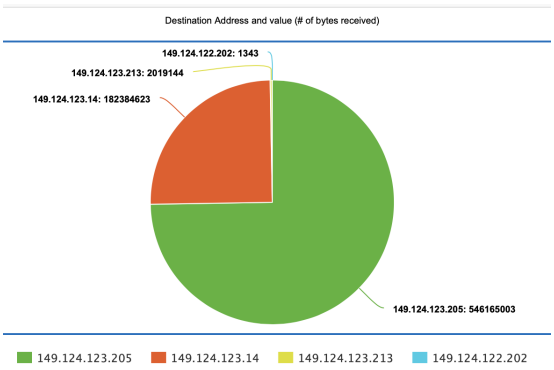
Using -l can tell us the average delay between each packet was 0.1189 seconds. We also know there are 663,619 TCP packets, 26,305 UDP packets and 4,417 unknown protocol packets.

Using -p, we get 18,689 (2.8%) of TCP packets are setting up a connection (SYN = 1). This means each connection is using lots of packets to transfer the data. We can also see the majority of sent packets use port number 80 (http) and 22 (ssh), while receiving packets use port numbers ranging from 49,000 to 52,000 (and others).

Lastly, -m tells us 99.9998% of the traffic is sent to a class C server with IP address "149.124.123.XXX". The total number of bytes sent to this server is 730,570,112 bytes. There were 14 destination addresses with "149.124.122.XXX", and 32 with "149.124.123.XXX" which is where just about all of the traffic went to. However, most addressees received no data. These addresses only respond with ACK packets. There were also over 1,000 different IP addresses setting up connections to this server.

Conclusion. This traces spans 23 hours, mainly uses TCP and sends lots of data to a server, that does not send any data back, and uses the internet and ssh. My guess is that this server is a cold storage unit for old data that isn't used very often. Clients send their data to this storage via a website or a virtual machine (or some other use of ssh) and no one has accessed their data during this trace. The fact that the class C server uses a broad range of ports and IP addresses means it plans on accepting lots of connections. (pie charts below)


Transport Protocol Used
other: 4417
UDP: 26305
TCP:SYN: 18689
TCP: 644930
TCP
TCP:SYN
UDP
other


Destination Address and value (# of bytes received)
149.124.122.202: 1343
149.124.123.213: 2019144
149.124.123.14: 182384623
149.124.123.205: 546165003
149.124.123.205
149.124.123.14
149.124.123.213
149.124.122.202