Stephen Hogeman

Professor Mark Allman

CSDS 325

November 13, 2023

Project 4: 425 Extension (Extra Credit)

For the 425 trace, I decided to analyze the common application layer protocols in the source and destination of the IP header. To do this, I created -w, which works as the other modes of project 4 do (it has no arguments and is run with -r being the input file). I analyzed a few common ports within 0-1023, with all ports not covered being set as UNKNOWN IN for being unknown inside the common bounds. The protocols I focused on were HTTP, HTTPS, SSH, SMTP, DNS, POP3, and IMAP for both source and destination ports. Any ports outside of the given range were printed as UNKNOWN OUT, to signify they were unknown ports outside of the given range. One interesting thing I found was that there were no packets using IMAP and POP3 protocol on the source port, but there were a few destination ports being set to IMAP and POP3. Largely, protocols for the source and destination ports were HTTP (80), SSH (22), and HTTPS (443) in that order of frequency. Around 33.8% of source ports were outside of common bounds, and 43.9% of destination ports were outside of common bounds.