INCIDENT REPORT: 11382-RK

Date: 1/25/2022

Executive summary:

I learned more about Wireshark, and how it is used to find more malicious code and malware attacks to websites. Wireshark is also used to see what devices are affected with said malicious code.

Methodology:

By running multiple scans on Wireshark, I am able to see where/what device(s) are attempting to connect to my server, or my devices. This helps to prevent any possible or future attacks.

Findings/solutions:

I will be able to further test and keep websites secure, and run Wireshark to “sniff” out the malicious traffic.