Network Traffic Analysis & Detection (Current)

My team and I will build and evaluate a network traffic monitoring and intrusion detection laboratory, using synthetic or publicly available attack traffic datasets to validate detection rules and logic. Measuring accuracy of malicious traffic, False positive/negative rates, Detection Time, Precision (amount of attacks detected), Using repeatable/tangible attacks that are reliable in order to differentiate which attacks were detected and alerted by the customly altered rules utilizing 3rd party tools.

Our research and project demonstrates how detection rules can be utilized to improve overall security and minimise gaps across security frameworks into one solution.

Responsibilities

As project manager my roles include combing individual reports, creating network diagrams, assisting with work and questions, and creating presentations. Literature Review of IPS/IDS technology and gaps. Submit proposals and ensure everyone is performing tasks in a timely manner.

Furthermore I will be cross performing in red and blue team tasks such as generating traffic generation,reconnaissance and performing IPS and IDS evaluation to tabulate results of accuracy and severity of results.

Tools Required for Project

Red Team tools 🔴

iperf3 , wireshark , nmap and hydra

Blue Team tools 🔵

Wazuh manager & agent, Zeek, Suricata and wireshark

Network Infrastructure