Suricata IDS Home Lab Report

This project sets up a Suricata IDS in a home lab.

Custom rules were created to detect SSH brute force and HTTP scans.

Logs and alerts were verified with tcpdump and Suricata logs.

Impact: Improved detection capabilities in a simulated SOC environment.