Network Attack Simulation (Suricata + Kali)

Executive Summary

This project covers network-based threat detection using Suricata IDS. Conducted recon, brute-force attacks, and payload-based simulations.

Architecture

Suricata sensor, Kali attacker, eve.json log analysis, and Kibana dashboards for network events.

Attack Simulation

Performed Nmap scans, SSH brute-force attacks, and malicious HTTP payloads to trigger Suricata alerts.

Detection Engineering

Tuned signatures, added threshold-based rules, and refined alert quality while reducing noise.

MITRE ATT&CK; Mapping

Mapped detections to T1046, T1110, T1190.

Outcome

Produced actionable IOCs, improved rule fidelity, and documented investigation steps.