Network Attack Simulation (Suricata + Kali)

Executive Summary

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

Screenshot Placeholder

Architecture

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

Screenshot Placeholder

Attack Simulation

Executed Nmap scans, SSH brute-force, and crafted payloads; captured Suricata alerts including scans and anomalies.

Screenshot Placeholder

Detection Engineering

Tuned signatures, added thresholding rules, enriched alerts and reduced noise.

Screenshot Placeholder

MITRE ATT&CK; Mapping

Mapped detections to T1046, T1110, T1190.

Screenshot Placeholder

Outcome

Generated IOCs, improved alert fidelity, documented investigation and containment steps.

Screenshot Placeholder