Suricata IDS

Inventory list for rule implementation

Olof Magnusson

May 21, 2025

1 Introduction

To ensure a effective threat detection, it is essential to maintain a clear understanding of the network, applications, and services in operation. Suricata is designed to monitor and identify malicious patterns, but its effectiveness depends on accurate and up-to-date information about the infrastructure.

1.1 Identify network topologies

- IP address ranges.
- Network segmentation details (network map highly desirable).
- DNS-server configurations.
- Internal/external connections that is expected in the environment.

1.2 List application and services

- Web servers (e.g., Apache, Nginx, IIS).
- Databases (e.g., MySQL, PostgreSQL, MSSQL).
- Web Application Frameworks (e.g., PHP, Node.js, .NET, Django).
- Internal application/APIs that needs might need custom rule sets or logic.

1.3 Collect Service-Specific Details

- Protocols in use (e.g., HTTP, HTTPs, DNS, SMB, SSH).
- High risk protocols (e.g., RDP, SMB, Telnet)
- Application-layer fingerprinting (e.g, TLS certs, HTTP headers, versions)

Summary

To summarize, an effective network inventory for Suricata includes:

- **Network discovery**: A list of hosts, subnets, and devices.
- **Service enumeration**: A list of applications and protocols with services.
- **Traffic profiling**: To form a baseline of expected data and develop logic to detect anomalies.