Entwurf und Realisierung einer Netzwerküberwachungslösung für das CyberLab

Studiengang: BSc in Informatik
Vertiefung: IT Security
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. Igor Metz (Glue Software Engineering AG)

Moderne Netzwerke erfordern zuverlässige und zentral auswertbare Sicherheitslösungen zur Erkennung und Abwehr von Angriffen. In dieser Arbeit wird gezeigt, wie im Rahmen des CyberLabs der Berner Fachhochschule ein modulares Überwachungssystem mit dem IDS/IPS Suricata und der Open-Source-SIEM-Plattform Wazuh realisiert werden kann. Die IDS/IPS-Sensoren wurden mit Ansible automatisiert eingerichtet, die Logübertragung erfolgt TLS-verschlüsselt.

Einleitung / Problemstellung

Die zunehmende Komplexität heutiger Netzwerke und die Vielfalt potenzieller Angriffsvektoren erfordern maßgeschneiderte, flexible Überwachungslösungen. In Ausbildungs- und Testumgebungen wie dem CyberLab der BFH ist es besonders wichtig, eine effektive Erkennung und Analyse von Bedrohungen sicherzustellen, um Netzwerkeverkehr nach zu verfolgen und gleichzeitig Logs zentral auswerten zu können – idealerweise ohne die Abhängigkeit von kommerzieller Software.

Zieldefinition

Das Ziel dieser Bachelorarbeit war es, ein Open-Source-basiertes Netzwerküberwachungssystem zu entwerfen und umzusetzen, welches die folgenden Hauptanforderungen erfüllt:

- Überwachung mehrerer Netzwerksegmente mithilfe von IDS/IPS (Intrusion Detection System/Intrusion Prevention System).
- Integration des IDS/IPS-Systems Suricata in das bereits bestehende SIEM-System Wazuh, um die Logs und Sicherheitsereignisse von Suricata zu sammeln und zu analysieren.
- Einbindung von Flow-Daten (wie NetFlow oder IPFIX) zur umfassenden Analyse des Netzwerkverkehrs.
- Implementierung einer flexiblen Lösung unter Verwendung von Open-Source-Software, die Kosten minimiert und eine hohe Anpassungsfähigkeit bietet.

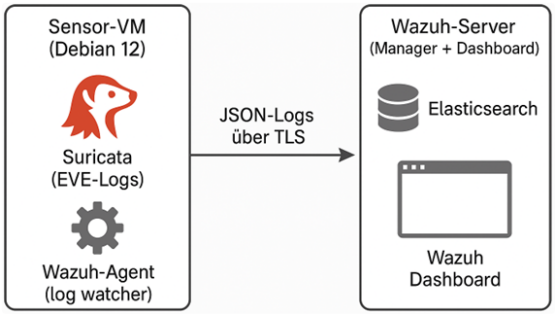
Umsetzung

Zur Umsetzung des Systems wurden das IDS/IPS Suricata, die SIEM-Plattform Wazuh sowie TLS-verschlüsselte Logweiterleitung eingesetzt. Die Installation und Konfiguration der Suricata-Sensoren wurde vollständig mit Ansible automatisiert, was eine schnelle und fehlerfreie Bereitstellung auf mehreren Systemen ermöglichte. Der Wazuh-Agent wurde auf den Sensoren installiert, um die erzeugten Suricata-Logs zu überwachen und sicher an den zentralen Wazuh-Manager zu übermitteln. Verschiedene Testszenarien, wie SQL-Injections, Brute-Force-Angriffe und unerwünschte Verbindungen, wurden durchgeführt, um die Funktionsfähigkeit und Skalierbarkeit des Systems zu validieren.

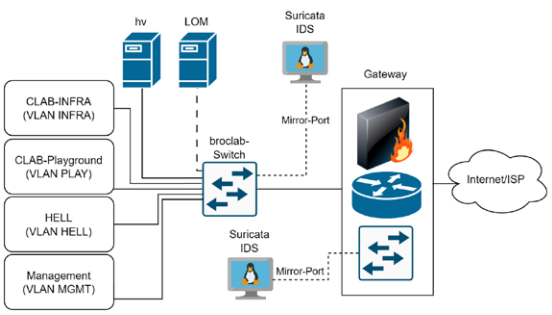
Ergebnis

Das entwickelte System zeigte sich robust, flexibel und leicht erweiterbar. Alle Komponenten arbeiteten erfolgreich zusammen und lieferten verwertbare, sicherheitsrelevante Informationen. Die Lösung bietet eine solide Grundlage für den Einsatz in Lern- und Laborszenarien und kann als Ausgangspunkt für weiterführende Sicherheitsarchitekturen dienen.
In Zukunft könnten ergänzende Komponenten wie die Integration der Monitoring-Plattform Malcolm oder zusätzliche Logquellen das bestehende System weiter ausbauen und die Analysefähigkeiten gezielt erweitern.

Michael Thossy



TLS-verschlüsselte Logverarbeitung von Suricata zu Wazuh



Vereinfachte Darstellung der Netzwerkstruktur des CyberLabs