Enterprise Security Monitoring Homelab Report

(Pending updates: This is a rough draft)

Project Overview

This project involved engineering a **multi-OS virtualized enterprise environment** designed for **comprehensive attack simulation, defense validation, and security monitoring**. The primary goal was to establish a realistic, segmented network architecture and deploy an industry-standard **Security Information and Event Management (SIEM)** solution to centralize log analysis and threat detection. The environment serves as a practical, hands-on lab for validating security controls, practicing incident response, and executing security operations workflows.

I. Technical Architecture and Infrastructure

The homelab was built on **VMware Workstation Pro 17** and included the following key components:

- **Virtualization Platform: VMware Workstation Pro 17** was used as the hypervisor to manage the entire multi-OS infrastructure.
- **Operating Systems:**
    - **Servers:** Windows Server 2019 and Windows Server 2022 (Domain Controller and application server).
    - **Database:** Integrated SQL Server database instance on a Windows Server VM.
    - **Clients:** Windows 11 Enterprise and Ubuntu Linux VMs (simulating diverse client workstations).
    - **Offensive:** Kali Linux and Parrot OS VMs for penetration testing and reconnaissance.
- **Network Segmentation:**
    - A **pfSense firewall** was deployed as the central gateway and segmentation device.
    - The network was logically divided into distinct zones (e.g., Production/Application Zone and Database Zone).
    - **Access Control Lists (ACLs)** were configured on the pfSense firewall to strictly control and monitor traffic flow between the Production and Database segments, mirroring **Zero Trust** or **defense-in-depth** principles in a real-world enterprise setting.

II. Security Monitoring Deployment

A dedicated Security Operations platform was integrated to provide centralized visibility and threat detection.

- **Security Onion Deployment:**
    - **Security Onion** (a Linux distribution incorporating tools like Elastic Stack, Suricata, and Zeek) was deployed on a dedicated Virtual Machine (VM).
    - This VM functions as the **SIEM/IDS** (Security Information and Event Management/Intrusion Detection System) for the entire lab.
- **Log Integration and Centralization:**
    - Log forwarders (e.g., Winlogbeat, Syslog) were configured on all servers (Windows Server 2019/2022) and client machines (Windows 11/Ubuntu).
    - Logs from the **pfSense firewall** (e.g., connection attempts, blocked traffic) were ingested into Security Onion.
    - This process successfully established **centralized logging**, providing a single pane of glass for monitoring system events, application activity, and network traffic.

III. Validation and Threat Analysis

To validate the efficacy of the monitoring solution, a controlled offensive exercise was executed.

- **Attack Scenarios:**
    - **Offensive security and reconnaissance scenarios** were executed using the Kali Linux and Parrot OS VMs against the virtualized domain infrastructure.
    - Simulated attacks included, but were not limited to, port scanning, network enumeration, and credential brute-forcing attempts.
- **Results and Validation:**
    - The resulting **alerts and forensic data** generated by these activities were analyzed within the Security Onion dashboard (Kibana/Elasticsearch).
    - This validation confirmed:
        1. **Successful Log Ingestion:** All event data from disparate sources (OS, Firewall) was correctly being forwarded and processed.
        2. **Rule Efficacy:** The Intrusion Detection System (IDS) and SIEM correlation rules were successfully triggered by the simulated malicious activity, proving the platform's capability to detect threats.
        3. **Incident Response Readiness:** The exercise provided practical experience in pivoting between network alerts (e.g., Suricata) and host-level logs (e.g., Windows Event Logs) to conduct thorough **forensic analysis**.

Next Steps

- Implement a full **Endpoint Detection and Response (EDR)** solution (e.g., Elastic Agent or Microsoft Defender ATP) to supplement network-level monitoring.
- Develop custom detection rules and playbooks for automated response to high-priority alerts.