Executive Summary — WCDN CyberGuard Network Lab

The CyberGuard Network Lab simulates an enterprise-grade defensive security environment using pfSense as the firewall gateway and Snort as the primary IDS/IPS platform. This project demonstrates key blue-team capabilities including network segmentation, intrusion detection, exploit monitoring, alert analysis, and foundational SOC-style incident response.

The environment was built using three virtual machines: a pfSense firewall serving as the perimeter device, a Metasploitable2 server representing a vulnerable target, and a Kali Linux machine used to simulate reconnaissance and exploitation attempts. pfSense provided stable routing, NAT, packet filtering, and logging, while Snort was deployed on the LAN interface to monitor internal activity and detect malicious patterns.

Across multiple tests, Snort successfully detected high-value threat categories such as Nmap port scans, service enumeration, Nikto web scanning, exploit probing, and brute-force attempts. The Emerging Threats (ET) ruleset and community rules triggered appropriately, generating alerts with meaningful metadata including signature IDs, priority levels, timestamps, and source/destination IP addresses.

IPS mode was enabled to evaluate real blocking behavior. Snort prevented certain exploit attempts and displayed blocked traffic in pfSense system logs. Although effective, these tests reinforced the importance of rule action configuration and signature tuning to balance detection accuracy with false positive reduction.

Blue-team analysis confirmed strong alert correlation, accurate timestamp alignment, and clear visibility into attack progression. However, the assessment identified opportunities for improvement such as reducing alert noise, introducing SIEM integration, enabling more granular firewall segmentation, and expanding IPS-enabled rule sets.

Overall, the CyberGuard Network Lab successfully validated the analyst’s ability to deploy defensive network controls, analyze threat behavior, evaluate detection accuracy, and simulate SOC-style monitoring and investigation workflows. This project demonstrates essential foundational skills for entry-level SOC and network security analyst roles.