Cybersecurity Lab Portfolio - Alen Guner

Lab 1: Brute Force Detection & Alerting in a SIEM (Wazuh + Linux)

Objective:

Simulate a brute-force attack on Linux SSH and configure Wazuh SIEM to detect and alert.

Outcome / What I Learned:

- Identified brute-force patterns and built detection rules.
- Improved log analysis and SIEM alert configuration.

Lab 2: Phishing Investigation with Splunk & VirusTotal

Objective:

Investigate a phishing email using Splunk, extract IOCs, and enrich findings with VirusTotal.

Outcome / What I Learned:

- Correlated phishing indicators, built alert logic, and wrote a triage workflow.

Lab 3: Cloud IAM Misconfiguration Detection & Remediation (AWS)

Objective:

Audit AWS IAM roles for risky permissions and simulate privilege escalation paths.

Outcome / What I Learned:

- Remediated misconfigured policies and documented least privilege principles.

Lab 4: Malware Analysis & IOC Extraction Using Any.Run + Wireshark

Objective:

Analyze malware in a sandbox and extract IOCs using Wireshark and VirusTotal.

Outcome / What I Learned:

- Captured network traffic and documented malware behavior and threat indicators.

Lab 5: SQL Injection Detection via Web Logs

Objective:

Use SQLMap on DVWA and detect attack patterns in Apache and Zeek logs.

Outcome / What I Learned:

- Created filters for injection signatures and built detection rules.

Cybersecurity Lab Portfolio - Alen Guner

Lab 6: Ransomware Simulation & Incident Response Report

Objective:

Simulate ransomware in a VM, observe system behavior, and write an IR report.

Outcome / What I Learned:

- Identified IOCs, created a timeline, and documented response recommendations.

Lab 7: Network Segmentation & Defense-in-Depth Design

Objective:

Segment a network into VLANs and restrict access using pfSense or Packet Tracer.

Outcome / What I Learned:

- Prevented lateral movement and verified isolation using firewall rules and traffic inspection.