NetHawk | Cybersecurity Portfolio

Project 1: Web Application Penetration Test

Client: E-commerce Startup (Remote)

Tools Used: Burp Suite, OWASP ZAP, Nmap, SQLMap

Performed a full black-box web application test. Discovered:

- SQL Injection on login endpoint
- Insecure Direct Object Reference (IDOR) on order history
- Missing security headers and weak session management

Delivered a detailed PDF report with CVSS scoring, proof-of-concept screenshots, and fix recommendations.

Project 2: SIEM Threat Hunting & Log Analysis

Client: Small FinTech Firm (Freelance)

Tools Used: Wazuh, Suricata, Kibana

Monitored live system logs for suspicious activity. Detected:

- Repeated SSH brute force attempts
- Unauthorized admin panel access after hours
- Outbound traffic to a malicious domain

Provided alerts and a detailed incident response workflow.

Project 3: TryHackMe Red Team Lab - "Hotel"

Environment: TryHackMe

Spoofed MAC address to bypass captive portal paywall and captured flag.

Steps:

- Cloned Alice's MAC address using `macchanger`
- Replayed ARP packets using Wireshark
- Monitored the network and successfully accessed the internal site

Flag: THM{mac_spoofing_success}

Project 4: Linux Server Hardening

Client: Crypto Blog Admin (Telegram)

Tools Used: SSH, UFW, fail2ban, chkrootkit

Secured a Linux VPS by:

- Disabling root SSH login and enabling key-based authentication
- Setting up firewall rules and intrusion detection tools
- Removing unnecessary packages and scanning for rootkits

Delivered config summary and hardening checklist.

Project 5: Social Engineering Simulation

Client: Red Team Training

Tools Used: Gophish, VirusTotal, WHOIS

Simulated phishing email campaign and tracked user interaction.

- 30% click-through rate on malicious link
- Logged IPs, timestamps, and browser info
- Created awareness training slides and mitigation strategy

Report submitted to internal security team.