Capstone Project & Incident Response Report

Executive Summary

This project served as the Capstone for the Cybersecurity & Ethical Hacking Internship, applying all knowledge gained from Task 1 through Task 4.

- **Project Chosen:** [**Select one: Web Application Pentest Report (on DVWA/bWAPP) / Vulnerability Assessment of Test Network / Build a Mini SIEM with ELK Stack / Create Security Awareness Phishing Simulation**]
- **Key Findings:** Briefly list 2-3 most critical findings (e.g., "Critical SQL Injection vulnerability identified," "Unpatched services exposing the target network," or "Successfully detected simulated attack using SIEM rules").
- **Impact:** Summarize the potential business impact of the findings.
- **Final Recommendation:** State the most crucial step for the target environment's security.

I. Capstone Project Documentation

1. Project Planning & Methodology

- **Objective:** The primary goal of this project was to [State your objective, e.g., perform a comprehensive security review of a web application].
- **Scope:** The scope included the following target systems/applications: [List VMs, IPs, or application endpoints].
- **Tools Used:** [List primary tools used, e.g., Nmap, Burp Suite, Metasploit, OpenVAS, ELK Stack].
- **Diagrams:** Refer to the **Network Diagram** / **ER Diagram** included in the evidence/ folder.

2. Findings (Vulnerabilities & Analysis)

Document your findings here, following a professional reporting format. Use the CVSS or a High/Medium/Low scale for severity.

ID	Finding/Vulnerability	Severity	Technical Details/Evidence	Mitigation Strategy
F-01	Example: Broken Authentication (Weak Password Hash)	High	Explain where and how the vulnerability was found (e.g., hash cracked using John the Ripper). Include screenshot reference: [evidence/F01_hashdump.png]	Implement stronger hashing algorithms (e.g., bcrypt) and multi-factor authentication.
F-02	Example: Exposed Network Service	Medium	Describe the service/port and	Disable unused services and

ID	Finding/Vulnerability	Severity	Technical Details/Evidence	Mitigation Strategy
			the risk (e.g., FTP running with anonymous login enabled).	implement firewall rules to restrict access.
...	...	...	...	...

II. Incident Response Simulation

This section details the simulated cyber incident and the corresponding response, following the standard IR lifecycle (Detection, Containment, Eradication).

- **Simulated Threat Scenario:** A brief description of the attack you simulated (e.g., a reverse shell was established on a low-privilege system via an unauthenticated web vulnerability).
- **Detection:**
  - **Method:** How the incident was initially detected (e.g., SIEM alert, high CPU load, or manual log review).
  - **Evidence:** Reference the relevant log snippet or alert screenshot: [evidence/IR_detection_log.png].
- **Containment:**
  - **Actions Taken:** Steps to isolate the affected system (e.g., isolated the host VM using a Host-Only adapter, blocked attacker IP via iptables).
- **Eradication:**
  - **Actions Taken:** Steps to remove the threat (e.g., terminated the rogue process, patched the exploited service, removed the backdoor/shell file).
- **Recovery:**
  - **Actions Taken:** Steps to bring the system back to production (e.g., verified system integrity, re-enabled network access, monitored logs).