Capstone Project & Incident Response — Web Application Pentest Report

Objective

Produce a capstone-level deliverable that demonstrates proficiency in web application penetration testing, vulnerability assessment of a test network, building a mini SIEM with the ELK stack, conducting a phishing simulation for security awareness, and performing incident detection & response. All active testing must be done in authorized, isolated labs.

Capstone Project Selection (Choose one)

Options:
- Web Application Pentest on DVWA or bWAPP (recommended for web security fundamentals).
- Vulnerability Assessment of a controlled test network (hosts, services, and small AD-like environment).
- Build a Mini SIEM using ELK Stack to collect, parse, and visualize logs from simulated hosts.
- Create a Security Awareness Phishing Simulation with training and metrics.

Choose the option that best matches learning goals and available lab resources; combining two complementary options (e.g., DVWA pentest + ELK SIEM for detection) makes a strong capstone.

1. Project Planning

Define Objectives, Scope, Tools, Timeline

Objectives: State measurable goals (e.g., identify OWASP Top 10 vulnerabilities in DVWA, demonstrate detection of simulated SQLi via SIEM dashboards, and create a phishing awareness campaign with <10% click-through target after training).

Scope: List in-scope hosts (e.g., DVWA VM IP), out-of-scope assets, allowed test types (passive, active, social-engineering only if authorized), time windows, and contact points.

Tools (examples): Recon & scanning tools, web proxies, vulnerability scanners, log shippers (Filebeat), Elasticsearch, Logstash, Kibana, dashboard templates, phishing simulation platform or controlled mail server, and documentation tools.

Timeline: Use a Gantt-like plan with milestones: planning (1 week), lab setup (1 week), reconnaissance/scanning (1 week), exploitation & validation (1 week), SIEM build & integration (2 weeks), phishing campaign & training (1 week), reporting & presentation (1 week).

Create ER Diagram or Network Diagram

Include at least one diagram showing the lab architecture. Example elements for a network diagram:

- Attacker VM (Kali) in isolated network
- Target VMs: DVWA/bWAPP web server, database server
- SIEM host: ELK stack (Filebeat on targets -> Logstash -> Elasticsearch -> Kibana)
- Simulated email server for phishing (internal test domain)

ER Diagram: If the project involves an application backend, include entities (Users, Sessions, Posts, Comments) and relationships. Provide a legend and note any sensitive fields.

2. Implementation

Conduct Recon, Scanning, Exploitation (controlled). Document Findings with Evidence. Suggest Mitigation Strategies.

Reconnaissance & Scanning

Perform passive recon and authorized scanning to enumerate hosts, services, and application endpoints. Document tool configurations, scan windows, and any rate-limiting considerations.

Record findings: discovered endpoints, versions, authenticated vs unauthenticated scan results, and potential false positives with reasoning.

Controlled Exploitation & Validation

In an isolated lab, validate vulnerabilities using non-destructive techniques or safe proof-of-concept methods. Avoid destructive payloads and never run attacks against production systems without explicit authorization.

For each confirmed issue, document: vulnerability title, affected component, CVE or reference (if applicable), proof evidence (screenshots, response snippets), impact summary, and exploitability likelihood.

Mitigation Strategies

Provide prioritized remediation: immediate configuration changes, patching, authentication hardening, input validation, output encoding, session management improvements, and web application firewall (WAF) recommendations.

3. Build a Mini SIEM (ELK Stack) — High-level Guide

Purpose: Collect logs from test hosts (web server, DB server, attacker VM), parse them, and create dashboards/alerts to detect simulated attacks.

High-level components and steps:

- Provision an ELK host (sized for lab use).

- Install Elasticsearch, Logstash, and Kibana; secure the stack with basic auth and network restrictions.

- Install Filebeat on target VMs to forward webserver logs and system logs to Logstash/Elasticsearch.

- Configure Logstash pipelines to parse webserver logs (access, error), application logs, and database logs. Add fields for source host, event type, and timestamp.

- Create Kibana index patterns and build dashboards for HTTP error spikes, repeated 4xx/5xx, unusual user-agent strings, and authentication failures.

- Create simple detection rules (e.g., threshold alert for 500 errors, repeated failed logins within a short timeframe).

- Document the ingestion pipeline, sample queries, and alerting logic.

Testing the SIEM: Replay sample logs or generate simulated attack traffic from attacker VM to validate that dashboards and alerts trigger correctly. Capture screenshots of dashboards as evidence.

4. Create Security Awareness Phishing Simulation

Design a low-risk phishing simulation aimed at measuring user susceptibility and teaching detection. Use a dedicated testing domain and only test consenting organizational users.

Key components:

- Design mock email templates that emphasize learning (no credential harvesting).

- Use a simulation platform that anonymizes results and provides training follow-ups.

- Segment recipients (pilot group, broader group) and define success metrics (click rate, credential submission rate, report rate).

- Provide immediate in-browser or email-based training to users who click, explaining red flags and next steps.

- Measure campaign results, prepare anonymized metrics, and recommend targeted training sessions based on findings.

5. Incident Detection & Response (Capstone Implementation)

Detect attack in logs. Contain & eradicate the simulated threat. Write Post-Incident Report.

Detection

Use SIEM dashboards and alerts to detect suspicious activity (e.g., abnormal SQL error rates, repeated failed logins, spikes in POST requests to login endpoints). Document the alert timeline and raw events (redact sensitive data).

Containment & Eradication

Containment steps (safe and reversible): isolate affected VM(s) from network, revoke or rotate credentials used in the simulation, block attacker IP(s) at the firewall, and apply temporary mitigations (e.g., disable vulnerable endpoints).

Eradication: apply patches or configuration changes, remove malicious artifacts from hosts, and verify via scans and log analysis that indicators are no longer present.

Post-Incident Reporting

A post-incident report should include: incident summary, timeline of detection/response activities with timestamps, indicators of compromise (IOCs), root cause analysis, scope of impact, remediation actions taken, lessons learned, and recommended follow-up actions including monitoring and user training.

Documentation & Evidence

Collect and store evidence securely in an encrypted archive. Include hashes (SHA-256) of log exports and screenshots. Maintain a chain-of-custody record for any artifacts used in the report. Redact sensitive data when sharing broadly.

Deliverables

- Project plan and RoE document.

- Network/ER diagram and lab topology.

- Scan and test logs (redacted) with summary of findings.

- SIEM configuration notes, pipelines, and dashboards (screenshots).

- Phishing campaign design, anonymized metrics, and training materials.

- Final capstone report (executive summary, technical findings, appendices).

- Post-incident report and remediation roadmap.

Ethics, Safety & Legal Considerations

All activities must be authorized in writing. Do not perform social engineering against non-consenting users. Never run malware or attack tools on production or third-party systems. Use isolated lab environments and follow data handling and privacy rules.