**1. Alert Priority Levels**

**1.1 Core Concepts Learned**

**Priority Definitions:**

**Critical** = Ransomware encryption, major data breach, full service outage.

**High** = Unauthorized admin access, privilege escalation.

**Medium** = Lateral movement attempts, brute-force attacks with limited success.

**Low** = Reconnaissance activity (e.g., port scans).

**Assignment Criteria:**

**Asset criticality:** Production database > Test VM.

**Exploit likelihood:** Public exploit available = higher priority.

**Business impact:** Financial loss or compliance violation raises priority.

**Scoring Systems:**

Learned CVSS v3.1 metrics (Base, Temporal, Environmental).

Studied risk scoring in SOC tools (Splunk, Elastic SIEM).

**1.2 References Used**

FIRST CVSS v3.1 Guide

NIST SP 800-61 Rev. 2 (Incident Handling Guide)

CISA Log4Shell Alert (AA21-356A)

**1.3 Case Study Example**

**Vulnerability:** Log4Shell (CVE-2021-44228)

**CVSS Score:** 10.0 (Critical)

**Impact:** Remote Code Execution, widespread exploitation.

**Priority Level Assigned:** Critical

**1.4 Skills Developed**

Ability to map vulnerabilities and alerts to priority levels.

Capability to apply CVSS scoring in SOC workflows.

**2. Incident Classification**

**2.1 Core Concepts Learned**

**Incident Categories:**

Malware → Host-based infection.

Phishing → Email-based credential theft.

DDoS → Service disruption.

Insider Threat → Unauthorized data export.

Data Exfiltration → Unauthorized transfer of sensitive data.

**Taxonomies Studied:**

MITRE ATT&CK (techniques & tactics).

ENISA Incident Taxonomy.

VERIS Framework.

**Contextual Metadata:**

Timestamps, source/destination IPs.

Indicators of Compromise (file hashes, domains).

Affected system roles (server, workstation, network device).

**2.2 References Used**

MITRE ATT&CK Navigator

ENISA Incident Classification Taxonomy

VERIS Community Database (VCDB)

**2.3 Case Study Example**

**Incident Type**: Phishing Campaign

**MITRE ATT&CK Mapping:** T1566.001 (Phishing: Spearphishing Attachment)

**Metadata Collected:**

**IOC:** SHA256 hash of attachment

**Source IP:** 192.168.204.131

**Affected User:** 20hotdogg00@gmail.com

**2.4 Skills Developed**

Ability to standardize incident classification.

Capability to enrich alerts with metadata for investigations.

**3. Basic Incident Response**

**3.1 Core Concepts Learned**

**Incident Lifecycle (NIST SP 800-61):**

Preparation → Playbooks, IR tools.

Identification → Alert triage in SIEM.

Containment → Isolate infected host.

Eradication → Remove malware, revoke access.

Recovery → Restore from backups, monitor.

Lessons Learned → Post-mortem review.

**Procedures Practiced:**

System isolation using firewall rules.

Evidence preservation (hashing artifacts, memory dump).

Communication protocol (escalation matrix).

SOAR workflow basics (Splunk Phantom/Elastic SOAR).

**3.2 References Used**

NIST SP 800-61

SANS Incident Handler’s Handbook

Let’s Defend Labs

**3.3 Case Study Example**

Incident: Malware infection detected on a test VM.

Containment: Quarantined host from network using iptables.

Eradication: Removed malicious binary.

Recovery: Restored system from snapshot.

Lessons Learned: Improve email filtering to block attachment type.

**3.4 Skills Developed**

Mastery of incident response lifecycle.

Familiarity with evidence handling and system isolation.

Exposure to SOAR-based response automation.

**4. Overall Reflection**

Stronger grasp on alert prioritization frameworks.

Improved ability to classify incidents using MITRE ATT&CK.

Hands-on practice with incident lifecycle management.

Next Steps: Explore advanced threat hunting with Sigma rules and automation with SOAR platforms.