3.0 Incident Response and Management

3.1 Explain concepts related to attack methodology frameworks.

- **Cyber kill chains**
- **Diamond Model of Intrusion Analysis**
- **MITRE ATT&CK**
- **Open Source Security Testing Methodology Manual (OSS TMM)**
- **OWASP Testing Guide**

3.2 Given a scenario, perform incident response activities.

- **Detection and analysis**
  - IoC
  - Evidence acquisitions
    - Chain of custody
    - Validating data integrity
    - Preservation
    - Legal hold
  - Data and log analysis
- **Containment, eradication, and recovery**
  - Scope
  - Impact
  - Isolation
  - Remediation
  - Re-imaging
  - Compensating controls

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

- **Preparation**
  - Incident response plan
  - Tools
  - Playbooks
  - Tabletop
  - Training
  - Business continuity (BC)/ disaster recovery (DR)
- **Post-incident activity**
  - Forensic analysis
  - Root cause analysis
  - Lessons learned