CYBER SECURITY ASSESSMENT

1. Scenario Creation:

    - Design a realistic cybersecurity incident scenario (e.g., malware attack, phishing attempt).
    - Outline the scenario's context, objectives, and scope.

2. Incident Detection:

    - Assign interns roles within the incident response team.
    - Simulate incident detection through monitoring tools or provided logs.

3. Response Plan Execution:

    - Initiate the incident response plan according to predefined roles and procedures.
    - Contain and mitigate the simulated incident using appropriate strategies

4. Forensic Analysis:

    - Perform forensic analysis on affected systems or data to understand the incident's root cause.
    - Gather evidence and logs for post-incident analysis.

5. Post-Incident Assessment:

    - Review the effectiveness of the response plan and actions taken.
    - Identify areas for improvement and lessons learned from the simulation.

6. Documentation and Presentation:

    - Document the incident response process, actions taken, and outcomes.
    - Present findings and recommendations for enhancing incident response capabilities.

ASSESSMENT BASED ON RANSOMWARE ATTACK

1. **Scenario Creation:**
   - **Scenario:** Ransomware Attack on a Small Business
   - **Context:** A small accounting firm, ABC Accounting Services, is targeted by a ransomware attack. The firm holds sensitive financial data for numerous clients and operates on a networked system with interconnected devices.

   - **Objectives:** The attackers aim to encrypt critical data stored on the firm's servers and demand a ransom payment in exchange for decryption keys. The objective is to disrupt business operations, extort money, and potentially expose sensitive client information.

- **Scope:** The scenario encompasses all devices and systems connected to ABC Accounting Services' network, including servers, workstations, and any cloud storage services utilized by the firm.

2. **Incident Detection:**
    - **Interns Roles:**
        - Intern 1: Monitoring network traffic for any unusual patterns or glitches that may indicate a ransomware infection, using tools like intrusion detection systems (IDS) or network traffic analysis software.
        - Intern 2: Analyzing server and endpoint logs for any signs of unauthorized access, file modifications, or suspicious processes indicative of ransomware activity.
        - Intern 3: Monitoring email gateways for any phishing emails or malicious attachments that could serve as the initial vector for the ransomware attack.
    - **Incident Detection Simulation:**
        - **Intern 1:** detects a sudden increase in outbound network traffic to known malicious domains associated with ransomware payloads.
        - **Intern 2:** observes unauthorized access attempts and file encryption activities on the firm's servers, indicating a potential ransomware infection.
        - **Intern 3:** identifies phishing emails with malicious attachments containing ransomware payloads, which were blocked by the email gateway but could pose a threat if opened.

3. **Response Plan Execution:**

- Incident Response Plan:
    - Incident Response Team Lead: Senior IT Security Analyst
    - Incident Response Roles:
        - Communications Lead: Office Manager
        - Technical Lead: Lead System Administrator
        - Recovery Lead: Data Backup and Recovery Specialist
        - Legal Lead: External Legal Counsel

- **Response Execution:**
    - The incident response team is activated upon detection of the ransomware attack.
    - The Communications Lead notifies all employees about the incident and advises them to disconnect from the network to prevent further spread.
    - The Technical Lead isolates infected systems from the network and begins restoring data from backups to mitigate data loss.
    - The Recovery Lead oversees the restoration process, ensuring critical systems are prioritized for recovery.
    - The Legal Lead advises on legal obligations, potential regulatory implications, and communications with law enforcement if necessary.

4. **Forensic Analysis:**
    - The Forensics Lead and their team conduct a forensic analysis on affected systems and data to understand the root cause of the ransomware attack.
    - They gather evidence such as system logs, network traffic captures, and malware samples for post-incident analysis.
    - Forensic analysis involves examining file system metadata, registry entries, and memory dumps to identify the ransomware variant, its entry point, and any indicators of compromise.

5. **Post-Incident Assessment:**
    - The incident response team conducts a post-incident assessment to review the effectiveness of the response plan and actions taken.
    - They identify areas for improvement, such as enhancing employee training on phishing awareness and implementing more robust backup and recovery procedures.
    - Lessons learned from the simulation are documented for future incident response planning and training sessions.

6. **Documentation and Presentation:**
    - The incident response team documents the entire incident response process, including actions taken, evidence collected, and outcomes achieved.
    - Findings and recommendations for enhancing incident response capabilities are presented to relevant stakeholders, including management and IT teams, to improve readiness for future cyber threats.