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 PHISHING ATTACK

1. **Scenario Creation:**
    - **Scenario:** Phishing Attempt Leading to Credential Theft
    - **Context**: A multinational corporation, XYZ Inc., operates in various sectors including finance, healthcare, and technology. It has a large workforce distributed across different locations globally. Recently, there has been a surge in targeted phishing attempts within the organization. Attackers are sending sophisticated phishing emails impersonating HR department officials, claiming to update employee benefits information.
    - **Objectives:** The attackers aim to deceive employees into disclosing their login credentials, potentially compromising sensitive company data and systems.
    - **Scope:** The scope of this scenario encompasses all employees of XYZ Inc. who may receive the phishing email, including those with access to critical systems and data.
2. **Incident Detection:**
    - **Interns Roles:**

- **Intern 1:** Monitoring the organization's email gateway for incoming emails and identifying suspicious patterns or anomalies.
- **Intern 2**: Analyzing network traffic logs for any unusual connections or activities indicative of a phishing campaign.
- **Intern 3:** Monitoring the organization's endpoint security solutions for any signs of malicious activity or attempts to ex-filtrate data.

- **Incident Detection Simulation:**
  - **Intern 1:** notices a sudden influx of emails with similar subject lines purporting to be from the HR department asking employees to update their benefits / personal information.
  - **Intern 2:** observes an increase in outbound network connections to suspicious domains known for hosting phishing landing pages.
  - **Intern 3:** detects abnormal file access patterns and login attempts on certain endpoints, indicating potential credential theft activities.

3. **Response Plan Execution:**
   - **Incident Response Plan:**
     - Designated Incident Response Team Lead: Senior Security Analyst
     - Incident Response Roles:
       - Communications Lead: PR and Communications Manager
       - Forensics Lead: Senior Forensics Analyst
       - Technical Lead: Lead Security Engineer
       - Legal Lead: General Counsel
   - **Response Execution:**
     - The incident response team is convened promptly upon detection of the phishing attempt.

- The Communications Lead drafts a notification to all employees warning them of the phishing campaign and advising them not to click on any suspicious links.
- The Technical Lead coordinates with the network and endpoint security teams to block access to the malicious domains and reset compromised credentials.
- The Forensics Lead conducts a detailed analysis of the incident to determine the extent of the breach and identify any further actions needed to remediate it.
- The Legal Lead assesses any legal obligations or implications arising from the incident, including potential regulatory reporting requirements.
- The incident response team works together to contain and mitigate the incident, while also implementing measures to prevent similar attacks in the future.

4. **Forensic Analysis:**
    - The Forensics Lead and their team will conduct a thorough forensic analysis on the affected systems and data to understand the root cause of the incident. This analysis involves:
        - Imaging and analyzing affected endpoints to identify any malware artifacts or suspicious files.
        - Reviewing system logs, including event logs and authentication logs, to trace the attacker's activities and identify any unauthorized access.
        - Examining network traffic logs to determine the communication patterns between compromised systems and external servers.

- Recovering any deleted files or artifacts left by the attacker for further analysis.
- Using digital forensic tools and techniques to extract and analyze relevant evidence, such as email headers, browser history, and system artifacts.

5. **Post-Incident Assessment:**
   - The incident response team, including all designated roles and interns, will convene for a post-incident assessment to review the effectiveness of the response plan and actions taken. This assessment involves:
     - Analyzing the timeline of events from initial detection to containment and remediation.
     - Evaluating the communication and coordination among team members during the incident response process.
     - Identifying any gaps or weaknesses in the response plan and procedures.
     - Reviewing the outcomes of the forensic analysis to understand the root cause of the incident and any lessons learned.
     - Documenting key findings, including successes and areas for improvement, for future incident response planning and training.

6. **Documentation and Presentation:**
    - The incident response team will document the entire incident response process, including actions taken, evidence collected, and outcomes achieved. This documentation includes:
        - A detailed incident report outlining the incident's timeline, root cause analysis, mitigation efforts, and post-incident assessment.
        - Recommendations for enhancing incident response capabilities, such as updating response procedures, improving employee awareness training, or enhancing security controls.
        - A presentation summarizing the incident, response efforts, and recommendations for stakeholders, including executive management, IT teams, and relevant departments.
        - Training materials or guidelines based on lessons learned from the simulation to educate employees and improve overall cybersecurity awareness and readiness.