Final Project Instructions: Interactive Cybersecurity Case Study

---

Project Overview

In this comprehensive final project, you will apply the cybersecurity concepts learned throughout the semester to analyze, mitigate, and resolve a simulated real-world cybersecurity incident. This case study will challenge you with ethical dilemmas, technical problems, and data security concerns, mirroring the complexities faced by cybersecurity professionals. Your work will demonstrate your understanding of key cybersecurity principles and your ability to apply them in practical scenarios.

Scenario

You are a member of the cybersecurity task force at **CyberProtect Inc.**, a fictional company specializing in cybersecurity solutions. Recently, CyberProtect Inc. experienced a **data breach** that has exposed sensitive information, including:

- **Employee Records:** Personal data, salaries, and performance evaluations.
- **Customer Personal Data:** Names, contact information, and purchase histories.
- **Confidential Company Documents:** Proprietary technologies, strategic plans, and internal communications.

As part of the task force, your responsibilities are to:

1. **Investigate the breach**
2. **Assess its impact**
3. **Develop mitigation strategies**
4. **Address the ethical implications of the incident**

You have access to various narrative scenarios, including phishing attempts, internal communications, system and network logs, incident reports, and company documents, which will aid in your investigation.

Project Components

Your project consists of the following components:

---

1. Initial Analysis

Objective: Identify how the breach occurred and assess the extent of the damage.

Tasks:

1. **Review Provided Materials:**
    - **Narratives Included:** Phishing Attempt, Suspicious Internal Communication, External Contact from Unknown Source, Unauthorized Access Attempts in System Logs, Data Export Detected in System Logs, Unusual Network Traffic Patterns, Initial Breach Detection Incident Report, Follow-Up Investigation Incident Report.
    - **Action:** Carefully examine these narratives and corresponding snippets to gather information about the breach.
2. **Identify the Breach Method:**
    - **Possible Methods:** Phishing attack, exploitation of a software vulnerability, insider threat, etc.

- **Action:** Determine the exact method used by the attackers based on the provided narratives and snippets.
- **Deliverable:** Provide detailed evidence (e.g., specific log entries, email content) supporting your conclusion.

3. **Assess the Damage:**

   - **Data Compromised:** List all types of data that were exposed.
   - **Affected Systems and Networks:** Identify which systems and networks were impacted.
   - **Impact Evaluation:** Discuss the potential consequences for the company and its stakeholders (e.g., financial loss, reputational damage, legal implications).

Guidelines:

- Use diagrams or charts to illustrate the breach timeline or affected systems.
- Reference specific parts of the provided narratives and snippets to support your analysis.

---

2. Designing Solutions

Objective: Develop a comprehensive action plan to mitigate the damage and prevent future breaches.

Tasks:

1. **Technical Measures:**

   - **Propose at Least Three Solutions:** Examples include implementing advanced firewalls, encryption protocols, multi-factor authentication (MFA), intrusion detection systems (IDS), etc.
   - **Explanation:** For each solution, explain how it addresses the vulnerabilities identified in the breach.
   - **Deliverable:** Detailed descriptions of each technical solution and its implementation.

2. **Non-Technical Measures:**

   - **Propose at Least Two Solutions:** Examples include employee cybersecurity training programs, updating company policies and procedures, conducting regular security audits, etc.
   - **Explanation:** Detail how these measures will enhance the company's security posture.
   - **Deliverable:** Comprehensive plan for non-technical solutions with justifications.

Guidelines:

- Ensure that your solutions are realistic and feasible for a company like CyberProtect Inc.
- Reference course materials or real-world examples to support your proposals.

---

3. Ethical Dilemmas

Objective: Analyze the ethical considerations surrounding the breach.

Tasks:

1. **Disclosure Decision:**
    - **Debate:** Should CyberProtect Inc. disclose the breach to the public?
    - **Argument:** Provide a well-reasoned argument supporting your position.
    - **Considerations:** Reference ethical principles (e.g., honesty, transparency), legal obligations (e.g., data protection laws), and potential consequences (e.g., loss of customer trust).
2. **Stakeholder Analysis:**
    - **Identify Stakeholders:** At least two key stakeholders (e.g., customers, employees, shareholders).
    - **Conflict of Interests:** Discuss potential conflicts between their interests.
    - **Influence on Decision-Making:** Explain how these conflicts influence the company's decisions regarding the breach.

Guidelines:

- Use ethical frameworks (e.g., utilitarianism, deontology) to structure your arguments.
- Provide examples to illustrate stakeholder conflicts and their impact.

---

4. Technical Implementation

Objective: Apply technical concepts from the course to practical scenarios.

Tasks:

1. **Encryption/Decryption Exercise:**
    - **Activity:** Use the provided plaintext and encryption keys to perform encryption and subsequent decryption.
    - **Demonstration:** Show your understanding of encryption algorithms and key management.
    - **Deliverable:** Document the steps taken and results obtained.
2. **Network Traffic Analysis:**
    - **Activity:** Examine the provided network traffic patterns.
    - **Action:** Identify and explain any suspicious activities or anomalies.
    - **Deliverable:** Report detailing your findings with supporting evidence from the narratives and snippets.
3. **Password Policy Development:**
    - **Propose:** Develop a comprehensive password policy for CyberProtect Inc.
    - **Testing:** Use provided tools to test the strength of sample passwords according to your policy.
    - **Deliverable:** Detailed password policy document and results of password strength tests.

Guidelines:

- Clearly explain each technical step you perform.
- Use screenshots or diagrams where applicable to illustrate your work.

---

5. Presentation

Objective: Summarize your findings and recommendations in a clear and professional manner.

Tasks:

1. **Report Preparation:**
    - **Content:** Include all components above in a detailed written report.
    - **Organization:** Ensure the report is well-organized, free of grammatical errors, and includes necessary visuals (e.g., risk matrices, network diagrams).
    - **Structure:**
        - **Title Page:** Project title, your name, course name, date.
        - **Table of Contents:** List of sections with page numbers.
        - **Introduction:** Brief overview of the case study.
        - **Main Content:** Detailed analysis and findings as per the project components.
        - **Conclusion:** Summarize your key points and recommendations.
        - **References:** Cite any external sources used, following appropriate citation guidelines.
        - **Appendices (if necessary):** Additional materials, charts, or code snippets.
2. **In-Class Presentation:**
    - **Duration:** 10 minutes.
    - **Content:** Highlight the main points from your report, including:
        - The root cause of the breach.
        - Your proposed mitigation and prevention measures.
        - The ethical decisions made and your justifications.
    - **Visual Aids:** Use slides created with PowerPoint, Google Slides, or similar software.
    - **Delivery:** Be prepared to answer questions from the instructor and classmates.

Guidelines:

- Practice your presentation to stay within the time limit.
- Use engaging visuals to enhance understanding and retention.
- Ensure clarity and professionalism in both your report and presentation.

Explicit Instructions

1. **Resources Provided**
    - **Narrative Scenarios and Snippets:**
        - Phishing Attempt (Email 1)
        - Suspicious Internal Communication (Email 2)
        - External Contact from Unknown Source (Email 3)
        - Unauthorized Access Attempts in System Logs (System Log 1 & 2)
        - Data Export Detected in System Logs (System Log 3)

        - Unusual Network Traffic Patterns (Network Traffic Snapshot 1 & 2)
        - Initial Breach Detection Incident Report
        - Follow-Up Investigation Incident Report
        - Confidential Company Document Excerpt (Document 1)
        - Employee Handbook Security Policies Excerpt (Document 2)
        - Security Policy Violation Report (Document 3)
        - Sample Encryption/Decryption Scenario
        - Password Strength Testing Scenario
        - Network Diagram Scenario
        - Risk Matrix Application
        - Incident Timeline Narrative
        - Reference Materials and Cybersecurity Frameworks
    - **Tools:**
        - Encryption and decryption software.
        - Password strength testing tools.
        - Access to network analysis applications.
    - **Reference Materials:**
        - Course slides, notes, and previous case studies.
        - Access to recommended readings and cybersecurity frameworks.

2. **Timeline**

   This project spans **two weeks**. Please manage your time effectively to meet all deadlines.

3. **Submission Requirements**

    - **Written Report:**
        - **Format:** Typed, double-spaced, 12-point Times New Roman font, standard margins.
        - **Length:** Approximately 6-8 pages total.
            - **Breach Analysis:** 1-2 pages.
            - **Proposed Solutions:** 2-3 pages.
            - **Ethical Discussion:** 1 page.
            - **Technical Implementation:** 1-2 pages.
        - **Sections to Include:**
            - **Title Page**
                - Project title, your name, course name, date.
                    - **Table of Contents**
                - List of sections with page numbers.
                    - **Introduction**
                - Brief overview of the case study.
                    - **Main Content**
                - Detailed analysis and findings as per the project components.
                    - **Conclusion**
                - Summarize your key points and recommendations.
                    - **References**

        - Cite any external sources used, following appropriate citation guidelines.
            - **Appendices (if necessary)**
        - Additional materials, charts, or code snippets.

- **In-Class Presentation:**
    - **Duration:** 10 minutes.
    - **Visual Aids:** Slides created using PowerPoint, Google Slides, or similar software.
    - **Content:** Highlight the main points from your report.
    - **Delivery:** Be prepared to answer questions from the instructor and classmates.
- **Submission Deadlines:**
    - **Written Report:** Due at the beginning of class on Day 14.
    - **Presentation Slides:** Submit electronically by **8:00 PM on Day 13**.

4. **Evaluation Criteria**

   Your project will be evaluated based on the following criteria. Please refer to the detailed rubric provided to understand how points are allocated for each component.

    - **1. Initial Analysis (20 points)**
        - **Identifying the Breach Method (10 points):**
            - Accuracy and depth in identifying how the breach occurred.
        - **Assessing the Damage (10 points):**
            - Completeness in listing compromised data and systems.
    - **2. Designing Solutions (25 points)**
        - **Technical Measures (15 points):**
            - Relevance and effectiveness of proposed technical solutions.
        - **Non-Technical Measures (10 points):**
            - Practicality and potential impact of suggested non-technical solutions.
    - **3. Ethical Dilemmas (15 points)**
        - **Discussion of Disclosure (7 points):**
            - Quality of argumentation regarding breach disclosure.
        - **Evaluation of Stakeholder Interests (8 points):**
            - Insightfulness in analyzing stakeholder conflicts.
    - **4. Technical Implementation (25 points)**
        - **Encryption/Decryption Example (5 points):**
            - Correctness in performing encryption and decryption tasks.
        - **Network Traffic Analysis (15 points):**

        - Thoroughness in identifying and explaining suspicious activities.
    - **Password Policy and Strength Testing (5 points):**
        - Soundness of the proposed password policy and effectiveness of strength testing.

- **5. Presentation and Report (15 points)**
    - **Report Quality (10 points):**
        - Clarity, organization, grammar, and inclusion of all required sections.
    - **Presentation Delivery and Visuals (5 points):**
        - Engagement, professionalism, and quality of visual aids.

5. **Additional Guidelines**
    - **Original Work:**
        - Your submission must be entirely your own work. Plagiarism will result in severe penalties, including a score of zero for affected sections.
    - **Collaboration Policy:**
        - You may discuss ideas and concepts with classmates, but all analysis, writing, and presentations must be done individually.
    - **Formatting and Professionalism:**
        - Ensure that your report is professionally presented, with attention to detail in formatting and language.
    - **Questions and Clarifications:**
        - If you have any questions or need clarification on any aspect of the project, please contact the instructor well before the deadlines.

Success Tips

- **Start Early:** Begin reviewing the narratives and snippets as soon as possible to give yourself ample time for analysis.
- **Stay Organized:** Keep track of your findings and sources as you progress through each component.
- **Be Detailed:** Provide thorough explanations and justifications for your decisions and recommendations.
- **Practice Your Presentation:** Rehearse to ensure you can confidently deliver your findings within the time limit.
- **Review the Rubric:** Use the provided rubric as a checklist to ensure you meet all the requirements for maximum points.

We look forward to your insightful analyses and innovative solutions. This project is not only a test of your knowledge but also an opportunity to experience the challenges and rewards of working in the field of cybersecurity.

Good luck!