COMP3028 Computer Security Coursework 3 (Group Coursework)

Deadline: 28 April 2025, 4pm

Group Size: 4 students

Scenario:
As part of a cybersecurity team at a tech company, you've been tasked with reviewing and improving the security of user authentication. The company needs to implement secure password storage and evaluate their current password management practices. You will also assess how vulnerable common passwords are in an attack scenario.

Task 1: Implement Secure Password Storage (Hashing and Salting)

Instructions:

- Choose a hashing algorithm and write a small Python script that accepts a user's password, hashes it, and stores it in a secure format.
- Include a salt in the process and explain its importance for security.
- Validate the stored password by comparing the hashed version to the user's input during login attempts.

Deliverable: Python script demonstrating password hashing and a brief explanation of your design choices and the importance of salting.

Marking Scheme for Task 1 (Total: 10 Marks):

- **Implementation of Hashing** (4 marks)
- **Salting** (3 marks)
- **Verification Function** (2 marks)
- **Explanation** (1 mark)

Task 2: Simple Multi-Factor Authentication (MFA) Design

Instructions:

- Design a simple MFA system that uses two factors: something the user knows (password) and something the user has (e.g., one-time password (OTP)).
- Implement a short Python script that simulates the MFA process.
- Briefly explain how MFA improves security compared to a single password and what threats it mitigates.

Deliverable: Python script implementing MFA and a short explanation of its security benefits.

Marking Scheme for Task 2 (Total: 10 Marks):

- **Implementation of MFA** (6 marks)
- **Explanation** (3 marks)
- **Code Quality** (1 mark)

Task 3: Password Cracking Simulation

Instructions:

- Use a password cracking tool to attempt cracking a sample hashed password (use the password you created in Task 1).
- Report on how long it would take to crack the password using common attacks and evaluate the strength of the password based on this.
- Suggest ways to improve password strength.

Deliverable: A short report on your cracking results, how long it would take to crack your password, and recommendations for improving password policies.

Marking Scheme for Task 3 (Total: 10 Marks):

- **Use of Cracking Tool** (5 marks)
- **Analysis of Results** (3 marks)
- **Explanation of Password Policies** (2 marks)

Overall Marking Scheme:

- **Task 1: Implement Secure Password Storage**: 10 marks
- **Task 2: Simple Multi-Factor Authentication Design**: 10 marks
- **Task 3: Password Cracking Simulation**: 10 marks
- **Team Reflections Report (350-500 words)**: 10 marks

Total: 40 marks