Task 4: Password Security & Authentication Analysis – Detailed Explanation

Introduction

This document explains password security concepts and authentication mechanisms. The objective is to understand how passwords are protected, how attackers target weak passwords, and how strong authentication mechanisms improve security.

Hashing vs Encryption

Hashing is a one-way process used to store passwords securely, whereas encryption is reversible. Passwords are hashed so that original values cannot be retrieved even if databases are compromised.

Common Hash Types

Older hash algorithms such as MD5 and SHA-1 are considered weak. Modern systems use algorithms like bcrypt which are computationally expensive and resistant to brute-force attacks.

Password Attacks

Dictionary attacks use common passwords, while brute-force attacks attempt all combinations. Weak passwords are vulnerable due to predictability and short length.

Multi-Factor Authentication

MFA adds additional verification layers beyond passwords, significantly reducing the risk of account compromise even if passwords are exposed.

Recommendations

Strong passwords should be long, unique, and randomly generated. Organizations should enforce MFA and avoid weak hashing algorithms.

Conclusion

Understanding password attacks and defenses is essential for cybersecurity. Strong authentication practices significantly reduce the risk of unauthorized access.