Cyber Security Internship – Task 4

Password Security & Authentication Analysis

Objective
To understand how passwords are stored, attacked, and protected using secure authentication methods.

What is Hashing?
Hashing is a one-way cryptographic process that converts passwords into fixed-length values. It cannot be reversed.

Hashing vs Encryption
Hashing is irreversible and used for passwords, while encryption is reversible and used for data protection.

Common Hash Types
MD5 (weak), SHA-1 (deprecated), SHA-256 (stronger), bcrypt (secure and recommended).

Password Attacks
Dictionary attacks use common passwords, while brute force attacks try all combinations. Weak passwords fail easily.

Weak vs Strong Passwords
Weak passwords are short and predictable. Strong passwords are long, random, and unique.

Multi-Factor Authentication (MFA)
MFA adds additional verification steps, making accounts secure even if passwords are compromised.

Recommendations
Use strong hashing algorithms like bcrypt, enable MFA, enforce strong password policies, and educate users.

Final Outcome
Improved understanding of password security, attacks, and defense mechanisms.