Cyber Security Internship – Task 4

Topic: Password Security & Authentication Analysis

Objective

The objective of this task is to understand how passwords are stored, attacked, and protected. This includes studying hashing mechanisms, password cracking techniques, and strong authentication practices.

Tools Used

- Hashcat – for password hash cracking
- John the Ripper – for password auditing
- Online Hash Identifiers – for identifying hash types

Password Storage Concepts

Passwords are not stored in plain text. Instead, they are converted into fixed-length values using hashing algorithms. Hashing is a one-way process, meaning original passwords cannot be directly retrieved from hashes.

Common Hash Types

MD5: Fast but insecure hashing algorithm vulnerable to attacks.
SHA-1: Stronger than MD5 but no longer recommended.
bcrypt: Secure hashing algorithm with built-in salting.

Password Cracking Techniques

- Dictionary Attack – Uses common password lists.
- Brute Force Attack – Tries all possible combinations.

Analysis & Observations

Weak passwords are easily cracked using dictionary or brute force attacks. Strong hashing algorithms and long, complex passwords significantly reduce attack success rates.

Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring more than one verification factor, such as a password and a one-time code. This greatly improves account security.

Recommendations for Strong Authentication

- Use long and complex passwords.
- Avoid common and reused passwords.

- Enable Multi-Factor Authentication.
- Use secure hashing algorithms like bcrypt.

Interview Questions & Answers

What is hashing?
Hashing is a one-way process used to convert passwords into fixed-length values.

Difference between hashing and encryption?
Hashing is irreversible, while encryption is reversible.

What is brute force attack?
An attack that tries all possible password combinations.

Why is MFA important?
It adds an additional security layer beyond passwords.

What makes a strong password?
Length, complexity, and unpredictability.

Deliverables

Password security analysis report documenting hashing, cracking methods, and authentication best practices.

Final Outcome

This task improved understanding of password security weaknesses and modern authentication defenses used to protect user accounts.