Internship day- 4

Report

20-01-2026

Password Security Analysis

1. Introduction

Passwords remain the most widely used authentication mechanism for operating systems, applications, and network services. Weak or poorly managed passwords are a major cause of security breaches

2. Objective

To analyse password-related risks, attack methods, weaknesses, and mitigation strategies.

3. Scope

OS-level passwords, application credentials, storage mechanisms, and attack techniques

4. Common Attacks

Brute Force, Dictionary Attacks, Credential Stuffing, Phishing, Keylogging.

5. Weaknesses

Short passwords, reuse, plaintext storage, no lockout policies, shared accounts.

6. Secure Storage

Use strong hashing algorithms like bcrypt, salting, and secure credential storage.

Your String	password
MD5 Hash	5f4dcc3b5aa765d61d8327deb882cf99 Copy
SHA1 Hash	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 Copy

Your String	Hello
MD5 Hash	8b1a9953c4611296a827abf8c47804d7 Copy
SHA1 Hash	f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0 Copy

7. Impact

Unauthorized access, data breaches, financial loss, reputational damage.

8. Defensive Controls

Strong password policy, MFA, least privilege, account lockout, HTTPS, user awareness.

9. Conclusion

Password security requires layered technical and human controls for effective protection