Password Security and Authentication Analysis

Final Report

1. Introduction Passwords are the most widely used authentication mechanism in computer systems.
2. Despite their popularity, passwords remain one of the weakest security controls due to poor human choices and improper storage mechanisms.
3. This project focuses on understanding password security from both attacker and defender perspectives using deep theoretical analysis and practical experiments performed in a VMware-based Kali Linux environment.

Objectives –

- Understand authentication and password fundamentals - Study password hashing mechanisms - Analyze password attack techniques - Perform controlled offline password analysis - Learn modern defensive strategies.
- Environment and Tools - VMware - Kali Linux - Hashcat - RockYou wordlist
- Authentication and Password Theory Authentication verifies user identity.
- Passwords belong to the knowledge-based authentication factor.
- Human behavior such as password reuse and predictable patterns makes passwords vulnerable.

- Hashing Concepts Hashing converts passwords into fixed-length irreversible values.
- Secure systems store hashes instead of plain passwords to prevent disclosure during data breaches.

Hashing vs Encryption Encryption is reversible and requires a key, while hashing is irreversible.

Passwords must always be hashed, not encrypted.

- Password Attacks Offline attacks allow attackers to guess passwords without system restrictions.
- Dictionary attacks are most effective due to human password habits.
- Salting and Secure Hashing Salting ensures identical passwords produce different hashes.
- Bcrypt and Argon2 are recommended due to slow computation and built-in salting.

  Practical Analysis All experiments were performed using **self-generated passwords inside Kali Linux**

Findings - Weak passwords fail rapidly - Fast hash algorithms are insecure - Salting is critical – MFA significantly improves security

Recommendations - Use bcrypt or Argon2 - Enforce long passwords - Enable Multi-Factor Authentication - Apply rate limiting and monitoring

Conclusion Password security requires layered defenses. Hashing, salting, MFA, and monitoring together reduce risk and impact of compromise.

Ethical Note All experiments were conducted ethically using self-created data only.