# Password Security & Authentication Analysis

This report analyzes password security mechanisms and authentication practices. The objective is to understand how passwords are stored, how attackers target weak passwords, and how strong authentication mechanisms help protect systems from unauthorized access.

## 1. Password Storage: Hashing vs Encryption

Passwords are stored using hashing algorithms rather than encryption. Hashing is a one-way process, meaning the original password cannot be retrieved from the stored value. Encryption is reversible and therefore unsuitable for secure password storage.

## 2. Common Hash Types

Hashing algorithms such as MD5 and SHA-1 are considered weak due to their speed and known vulnerabilities. Modern systems use adaptive algorithms like bcrypt, which are slower and resistant to brute-force attacks.

## 3. Password Hash Generation

Password hashes can be generated using cryptographic tools for learning purposes. This process demonstrates how plaintext passwords are transformed into secure hash values.

## 4. Cracking Weak Password Hashes

Weak password hashes can be cracked using wordlists that contain commonly used passwords. This shows how predictable passwords are vulnerable to dictionary-based attacks.

## 5. Brute Force vs Dictionary Attacks

Dictionary attacks use predefined password lists, while brute-force attacks attempt every possible combination. Dictionary attacks are faster, whereas brute-force attacks are more resource-intensive.

## 6. Analysis of Weak Password Failures

Weak passwords fail due to short length, reuse, and lack of complexity. Automated tools exploit these weaknesses, leading to frequent account compromises.

## 7. Multi-Factor Authentication (MFA)

Multi-Factor Authentication enhances security by requiring additional verification beyond passwords. MFA significantly reduces the risk of unauthorized access even if passwords are compromised.

## 8. Recommendations for Strong Authentication

1. Use long, unique passwords for each service
2. Avoid common and predictable passwords
3. Use modern hashing algorithms such as bcrypt
4. Implement Multi-Factor Authentication
5. Educate users on password security best practices

## 9. Conclusion

Password security is a fundamental aspect of cybersecurity. Understanding how passwords are stored, attacked, and protected helps in designing secure authentication systems. Strong passwords combined with

MFA significantly improve overall security posture.