INTERN NAME – IMAM ASHRAF

Cyber Security Internship: Task 6 - Password Strength Evaluation Report

Objective

This task aims to understand the elements that make a password strong and test various passwords using online password strength checkers. This task also aims to explore common password attacks and best practices for creating secure passwords.

Passwords Created and Tested

Password	Complexity Elements	Password Strength Result (Passwordmeter.com)
imam123	Lowercase, Numbers	Very Weak
Imam@2025	Uppercase, Lowercase, Numbers, Symbol	Weak
ImAm!@#$	Uppercase, Lowercase, Numbers, Multiple Symbols	Medium
AMITYup2526!@	Uppercase, Lowercase, Numbers, Symbol	Very strong
AmRTref!@#523	Uppercase, Lowercase, Numbers, Multiple Symbols	Very Strong

Observations

- Passwords that only use lowercase and numbers (e.g., password123) are easily crackable using dictionary or brute force attacks.
- Passwords that combine uppercase, lowercase, numbers, and symbols (e.g., Pass@2024) show moderate security but can still be vulnerable if the pattern is simple.
- Passwords that are longer and use multiple types of characters and special symbols (e.g., X!v9@qT7#bL2) are significantly stronger.
- Passwords that resemble passphrases with added complexity (e.g., Hello@world2024) offer strong security and are easier to remember.

Screenshot taken during observation


How Secure is Your Password?
Take the Password Test
Tip: Avoid the use of dictionary words or common names, and avoid using any personal information
Show password:
ImAm!@#$
Medium
8 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
8 hours
Review: Hmm, using that password is like locking your front door, but leaving the key under the mat. Your password is of medium strength because it contains 2 dictionary words and a combination of characters that are close together on the keyboard.
Your passwords are never stored. Even if they were, we have no idea who you are!


How Secure is Your Password?
Take the Password Test
Tip: Avoid the use of dictionary words or common names, and avoid using any personal information
Show password:
AMITYup2526!@
Very Strong
13 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
10 years
Review: Fantastic, using that password makes you as secure as Fort Knox.
Your passwords are never stored. Even if they were, we have no idea who you are!

Best Practices for Creating Strong Passwords

1. Use at least 12-16 characters.
2. Combine uppercase, lowercase, numbers, and special characters.
3. Avoid using dictionary words, names, or predictable sequences.
4. Use passphrases that are easy to remember but hard to guess.
5. Change passwords regularly and never reuse passwords across critical accounts.
6. Consider using a password manager to generate and store complex passwords.
7. Enable multi-factor authentication (MFA) wherever possible.

Common Password Attacks

1. Brute Force Attack

- **Definition:** Attackers try **every possible combination** of characters until the correct password is found.
- **Example:** Attempting all combinations like "aaa", "aab", "aac", ... until the correct one is guessed.
- **Prevention:**
    - Use long, complex passwords.
    - Implement account lockout after multiple failed attempts.
    - Use rate-limiting and multi-factor authentication (MFA).

---

2. Dictionary Attack

- **Definition:** Attackers use a **precompiled list of common words, phrases, and known passwords** to quickly guess passwords.
- **Example:** Trying passwords like "password", "123456", "admin" from a common password list.
- **Prevention:**
    - Avoid using predictable words and simple patterns.
    - Use unique combinations with symbols, numbers, and uppercase letters.

---

3. Credential Stuffing

- **Definition:** Attackers use **previously leaked username-password pairs** from other websites to try to log into different platforms.
- **Example:** If your social media password was leaked, attackers will try the same login on your email, bank, etc.
- **Prevention:**
    - Always use **unique passwords** for each account.
    - Enable **multi-factor authentication** (MFA).
    - Monitor for breach notifications.

---

4. Phishing

- **Definition:** A social engineering attack where attackers **trick users into providing their passwords** by pretending to be a trusted source.

- **Example:** Fake emails or websites asking users to "verify" their login credentials.
- **Prevention:**
    - Always verify URLs and sender details.
    - Avoid clicking on suspicious links.
    - Use email filters and security awareness training.

---

5. Rainbow Table Attack

- **Definition:** Attackers use **precomputed tables of hashed passwords** to reverse password hashes and quickly discover the original passwords.
- **Example:** Matching a hashed password like 5f4dcc3b5aa765d61d8327deb882cf99 to "password" using a rainbow table.
- **Prevention:**
    - **Salt passwords** (add random strings before hashing).
    - Use modern hashing algorithms like **bcrypt, scrypt, or Argon2**.
    - Regularly update security hashing practices.

Key Learnings

- Password length and complexity directly increase security.
- Passphrases provide a balance between memorability and strength.
- Using MFA adds a crucial layer of protection beyond password security.
- Password managers help in maintaining unique, complex passwords for every account.