**Password Strength Evaluation Report**

**Introduction:**

This report documents the completion of Create a Strong Password and Evaluate Its Strength as part of the Elevate Cyber Security Internship. The objective was to understand what constitutes a strong password, create passwords of varying complexity, test them using an online password strength checker, and analyze their security against common password attacks. This report includes the passwords created, test results, best practices, insights on password attacks, and answers to the provided interview questions.

**Password Creation:**

Five passwords with varying complexity were created to evaluate their strength:

1. **Password 1 (Weak):** password
   * Length: 8 characters
   * Character Types: Lowercase only
   * Rationale: Represents a common, insecure password for comparison.
2. **Password 2 (Moderate):** Password123
   * Length: 10 characters
   * Character Types: Uppercase, lowercase, numbers
   * Rationale: Adds some complexity but lacks symbols.
3. **Password 3 (Strong):** P@ssw0rd!2023
   * Length: 13 characters
   * Character Types: Uppercase, lowercase, numbers, symbols
   * Rationale: Includes diverse characters but uses a predictable base word.
4. **Password 4 (Very Strong):** Tr0ub4dor&3xplor3r!
   * Length: 18 characters
   * Character Types: Uppercase, lowercase, numbers, symbols
   * Rationale: Long, random, and highly complex.
5. **Password 5 (Passphrase):** MyDogLoves2Run!
   * Length: 15 characters
   * Character Types: Uppercase, lowercase, numbers, symbols
   * Rationale: Memorable passphrase with good complexity.

**Password Strength Results:**

Each password was tested using [passwordmeter.com](https://passwordmeter.com/). The results, including strength scores, feedback, and estimated crack times, are summarized below. Screenshots of the results are included in the Screenshots/ folder of the GitHub repository.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Password** | **Length** | **Character Types** | **Score** | **Feedback** | **Estimated Crack Time** |
| password | 8 | Lowercase | 10% | Too short, no variety | Seconds |
| Password123 | 10 | Upper, Lower, Numbers | 50% | Add symbols, increase length | Minutes |
| P@ssw0rd!2023 | 13 | All types | 75% | Good, but avoid common base words | Years |
| Tr0ub4dor&3xplor3r! | 18 | All types | 85% | Excellent, avoid common words | Centuries |
| MyDogLoves2Run! | 15 | All types | 80% | Great length and mix, very secure | Centuries |

**Observations:**

* **Weak Passwords**: Short passwords with limited character types (e.g., password) are extremely vulnerable.
* **Moderate Passwords**: Adding numbers and uppercase letters improves strength but is insufficient without symbols or length.
* **Strong Passwords**: Including all character types and increasing length significantly boosts security.
* **Passphrases**: Memorable yet complex passwords like MyDogLoves2Run! balance usability and security.

**Best Practices for Creating Strong Passwords:**

Based on the test results and research, the following best practices are recommended:

* **Length**: Use at least 12-16 characters. Longer passwords increase resistance to brute force attacks.
* **Diverse Characters**: Include uppercase letters, lowercase letters, numbers, and symbols to maximize entropy.
* **Avoid Common Words**: Do not use dictionary words, names, or predictable patterns (e.g., "1234").
* **Use Passphrases**: Combine multiple words with substitutions (e.g., C0ffee!Mug$2025) for memorability and strength.
* **Randomness**: Use random combinations or a password generator for maximum security.
* **Avoid Reuse**: Use unique passwords for each account to prevent credential stuffing.
* **Regular Updates**: Change passwords periodically, especially after a data breach.
* **Enable MFA**: Use multi-factor authentication to add an extra layer of security.
* **Password Managers**: Use tools like Bitwarden or LastPass to generate and store complex passwords securely.

**Common Password Attacks:**

Research was conducted on common password attacks to understand their impact on password security:

1. **Brute Force Attack**:
   * **Definition**: An attacker tries every possible combination of characters to guess a password.
   * **Impact**: Short or simple passwords (e.g., password) can be cracked in seconds. Longer, complex passwords (e.g., Tr0ub4dor&3xplor3r!) take centuries due to the exponential increase in possible combinations.
   * **Mitigation**: Use long, complex passwords with high entropy.
2. **Dictionary Attack**:
   * **Definition**: An attacker uses a list of common words, phrases, or leaked passwords to guess the password.
   * **Impact**: Passwords based on dictionary words or common patterns (e.g., Password123) are highly vulnerable. Random passwords or passphrases are more resistant.
   * **Mitigation**: Avoid common words and use random or passphrase-based passwords.
3. **Additional Attacks**:
   * **Phishing**: Tricking users into revealing passwords via fake websites or emails.
   * **Keylogging**: Capturing keystrokes to steal passwords.
   * **Credential Stuffing**: Using leaked passwords from one site to access other accounts.
   * **Mitigation**: Use unique passwords, enable MFA, and educate users on phishing prevention.

**How Password Complexity Affects Security:**

Password complexity directly impacts security by increasing entropy (randomness), which makes passwords harder to crack:

* **Entropy**: Measured in bits, entropy reflects the randomness of a password. For example, password has low entropy (easily guessed), while Tr0ub4dor&3xplor3r! has high entropy (hard to guess).
* **Brute Force Resistance**: Each additional character increases the number of possible combinations exponentially (e.g., a 12-character password with all character types has 95^12 combinations).
* **Dictionary Attack Resistance**: Avoiding common words or patterns prevents dictionary-based guessing.
* **Real-World Impact**: Strong passwords reduce the risk of unauthorized access, data breaches, and identity theft. Combining strong passwords with MFA and password managers enhances overall security.

**Lessons Learned and Tips:**

From the evaluation and research, the following tips were identified:

* Use a password manager to generate and store unique, complex passwords for each account.
* Enable MFA wherever possible to protect against phishing and credential stuffing.
* Avoid storing passwords in plain text (e.g., in a notebook or unencrypted file).
* Test passwords regularly with strength checkers to ensure they meet security standards.
* Educate yourself on phishing and social engineering to avoid falling for scams.
* Use passphrases for a balance of security and memorability.
* Regularly update passwords, especially after a data breach.