Task 6: Password Strength Analysis Report

Objective

The objective of this task was to understand the principles of strong password creation by testing passwords of varying complexity. The analysis helps in identifying best practices and understanding the risks associated with common password attacks.

Tool Used

- **Password Strength Checker:** PasswordMeter.com

Password Strength Evaluation

A series of passwords were created and tested, ranging from "Very Weak" to "Very Strong." The detailed results and analysis for each are presented below.

Category 1: Very Weak Passwords

These passwords are short, predictable, and lack any complexity. They are extremely vulnerable and would be cracked instantly by an attacker.

Password Tested	Strength Score & Analysis
12345678	Score: 4% (Very Weak) This password consists only of consecutive numbers, which is a major weakness. The tool applies heavy deductions for being "Numbers Only" and for sequential numbers, resulting in a dangerously low score.
password	Score: 8% (Very Weak) This is one of the most common passwords in the world. It contains only lowercase letters and is a dictionary word. The tool penalizes it for "Letters Only" and for consecutive lowercase letters, making it extremely insecure.

Category 2: Moderate Passwords

These passwords introduce some complexity but are still flawed due to short length, predictability, or reliance on common words.

Password Tested	**Strength Score & Analysis**
Admin123	Score: 39% (Weak) Adding a capital letter and numbers is an improvement, but the password is still short and based on a common word ("admin") followed by a simple sequence. Deductions for consecutive and sequential numbers weaken it significantly.
Password1	Score: 54% (Good) The score improves with the inclusion of an uppercase letter and a number. However, it is still based on the word "password" and suffers deductions for consecutive lowercase letters.
P@ssword	Score: 54% (Good) This password uses a common technique called "leetspeak" (substituting symbols for letters). While it adds a symbol, the pattern is predictable and well-known to cracking tools. The score is penalized for repeated characters (ss).
Password123	Score: 75% (Strong) At 11 characters and containing three character types, the score becomes "Strong." However, its predictability (a common word followed by a number sequence) is a weakness that a raw score doesn't fully capture.
Soccer@10	Score: 76% (Strong) This password effectively combines multiple character types. Its main weakness is its relatively short length and the use of a common dictionary word, but it meets the basic requirements for a

	"strong" password.

Category 3: Very Strong Passwords / Passphrases

These passwords achieve a 100% score by combining significant length with high complexity (using all four character types). They are highly resistant to attacks.

Password Tested	Strength Score & Analysis
Tr0ub4dor&3	Score: 100% (Very Strong) This is a classic example of a complex password. It is over 8 characters long and includes uppercase, lowercase, numbers, and a symbol. The use of leetspeak and non-sequential characters results in a perfect score.
Blu3-Sk!es-F0rever	Score: 100% (Very Strong) This is an excellent example of a passphrase. Its strength comes from its significant length (18 characters). It also includes all four character types, making it exceptionally difficult to crack via brute force.
W!nterC0m!ng$25	Score: 100% (Very Strong) At 15 characters, this passphrase combines length and complexity perfectly. It uses multiple symbols, numbers, and capital letters, making it highly secure and earning a top score from the checker.

Summary of Learnings & Best Practices

Based on the evaluation, several key principles for creating strong passwords became clear:

1. **Length is the Most Critical Factor:** The passwords that scored the highest (Blu3-Sk!es-F0rever, W!nterC0m!ng$25) were also the longest. A long password exponentially increases the number of possible combinations, making it resistant to brute-force attacks.
2. **Complexity is Key:** Using a mix of all four character types (uppercase letters, lowercase letters, numbers, and symbols) is essential. The tool consistently awarded higher scores

for passwords that met this requirement.

3. **Avoid Predictability:** Passwords based on common words (even with substitutions), sequences (123), or repetitions (ss) are penalized. True randomness and unpredictability are vital.
4. **Passphrases are Superior:** A long passphrase made of several words can be stronger and easier to remember than a shorter, more complex password. For example, Four-Angry-Trees-Sing2Loudly is often more secure and memorable than aJ7$kL9*pQ2b.

Common Password Attacks

- **Brute-Force Attack:** This is an attack where an automated tool attempts to guess a password by systematically trying every possible combination of characters until the correct one is found. The longer and more complex a password is, the longer a brute-force attack will take, making it impractical.
- **Dictionary Attack:** This is a more targeted type of brute-force attack. Instead of trying random combinations, the attacker uses a predefined list (a "dictionary") of common words, phrases, common passwords, and simple variations (like adding "123" at the end). This is why using words like password or sunshine is so dangerous.
- **Credential Stuffing:** This is a very common attack that leverages password reuse. Attackers take lists of usernames and passwords stolen from a data breach at one company and use automated tools to "stuff" those same credentials into the login pages of other websites (like social media, banking, etc.), hoping to find accounts that reuse the same password.
- **Password Spraying:** This is a "low-and-slow" attack that flips the brute-force method. Instead of trying many passwords against a single user account, the attacker tries a few very common passwords (e.g., Password123, Winter2025) against a large number of different user accounts. This is done to avoid triggering account lockout policies that would normally stop a brute-force attack.

Interview Questions & Answers

1. What makes a password strong?

A strong password is characterized by its **length** and **complexity**. It should be long (ideally 12+ characters), contain a mix of uppercase letters, lowercase letters, numbers, and symbols, and be unpredictable (avoiding common words or personal information).

2. What are common password attacks?

The most common attacks are **brute-force attacks** (trying all possible combinations), **dictionary attacks** (trying common words and passwords),

credential stuffing (using leaked passwords from one site on another), and **phishing** (tricking a user into revealing their password).

3. Why is password length important?

Password length is the single most important factor in its strength. Each additional character exponentially increases the number of possible combinations an attacker must try in a brute-force attack, making the password significantly harder to crack. A 12-character password is exponentially stronger than an 8-character one.

4. What is a dictionary attack?

A dictionary attack is a method of cracking a password where an attacker uses a list of common words, phrases, and previously compromised passwords (a "dictionary") to guess the password, rather than trying every possible combination. It is highly effective against users who choose simple, common words as their passwords.

5. What is multi-factor authentication?

Multi-Factor Authentication (MFA) is a security process that requires users to provide two or more different authentication factors to verify their identity. These factors are typically something you know (a password), something you have (a phone or security key), and something you are (a fingerprint or face scan). MFA adds a critical layer of security, as a compromised password alone is not enough to grant access.

6. How do password managers help?

Password managers help by generating and storing long, complex, and unique passwords for every online account. The user only needs to remember one strong master password to access their "vault." This eliminates the need to reuse weak passwords and ensures that a breach on one website doesn't compromise other accounts.

7. What are passphrases?

A passphrase is a type of password that consists of a sequence of words, often mixed with spaces or symbols. For example, The-cat-ate-all-the-pizza!. They are often more secure than traditional complex passwords because they can be much longer and are easier for humans to remember, while still being extremely difficult for computers to guess.

8. What are common mistakes in password creation?

Common mistakes include: creating passwords that are too short, using personal information (names, birthdays), using common dictionary words or predictable patterns (qwerty, 123456), reusing the same password across multiple websites, and not using a mix of character types.