Password Strength Report

Best Practices

- Use passwords that are at least 16 characters long.
- Avoid personal details such as names, birthdays, or common dictionary words.
- Include a mix of uppercase letters, lowercase letters, numbers, and special characters.
- Use passphrases instead of single words for better security.
- Enable Two-Factor Authentication (2FA) wherever possible.
- Use a secure password manager to store and manage passwords.

Research on Common Password Attacks

1. Brute Force Attack

- Attackers attempt every possible character combination until the correct password is discovered.
- Longer passwords require significantly more time and computational power to crack.

2. Dictionary Attack

- Uses a list of commonly used words and passwords to guess credentials.
- Simple passwords such as 'password' can be cracked almost instantly.

3. Credential Stuffing

- Uses leaked usernames and passwords from previous data breaches.
- Attackers attempt to reuse stolen credentials on multiple websites.

Final Summary

This task demonstrated the direct relationship between password complexity and security strength. Short or predictable passwords containing common words are highly vulnerable to brute force and dictionary attacks. Increasing password length and combining multiple character types such as uppercase letters, lowercase letters, numbers, and special symbols greatly increases security. Password strength tools assess security based on length, randomness, and character diversity. Long, unique passphrases with high entropy provide stronger protection against cyber threats and unauthorized access.