Elevate Labs – Cyber Security Internship

Name:Srinivas Atta

Task 6: Create a Strong Password and Evaluate Its Strength

By: Ministry of MSME, Govt. of India

Objective

Understand the characteristics of a strong password, create multiple test passwords with different complexities, evaluate them using online password strength tools, and learn password security best practices.

Tools Required

- Online password strength checker (e.g., passwordmeter.com, howsecureismypassword.net)

Execution Steps / Guide

1. Generate Test Passwords
    - Create at least 4–5 different passwords with variations in:
        - Length (short vs. long)
        - Case (uppercase/lowercase)
        - Numerals and special characters inclusion
        - Use of dictionary words vs. random strings
2. Test in Strength Checker
    - Enter each password into the online tool (do not use real personal passwords).
    - Record the strength score, estimated crack time, and feedback.
3. Compare Results
    - Short/simple passwords will show lower scores and faster crack times.

    - Longer, complex, and random passwords will show higher security ratings.

4. Note Best Practices from Evaluation
    - Identify patterns in what makes passwords strong.
5. Research Common Password Attacks
    - Look into brute force, dictionary attacks, and credential stuffing.
6. Document Security Tips
    - Summarize do’s and don’ts for creating secure passwords.

Findings / Results

Password Example	Length	Components Used	Strength Score	Estimated Crack Time	Tool Feedback
`password123`	11	Lowercase + Numbers	Weak	Few seconds	Common word, easy to guess
`Pa$$w0rd!`	9	Mixed case + Numbers + Symbols	Medium	Minutes/hours	Better complexity but still predictable
`T!ger_1997`	10	Mixed case + Numbers + Symbols	Strong	Days	Uses symbol but has guessable year

`gR7@xLpQ!zK#9%t`	15	Mixed case + Numbers + Symbols	Very Strong	Centuries	High complexity and length
`MyFavColorIsBlueAnd$ky2025`	26	Passphrase + Numbers + Symbol	Very Strong	Millions of years	Easy to remember, hard to guess

Security Analysis

Testing showed that password security increases significantly with length, use of mixed character types, and unpredictability.

- Short, dictionary-based passwords are highly vulnerable to dictionary attacks.
- Common substitutions (like `Pa$$w0rd`) are often included in attacker wordlists.
- Passphrases combining unrelated words with symbols and numbers offer strong and memorable protection.
- Completely random long strings provide maximum security but can be hard to remember without a password manager.

Recommendations

- Make passwords at least 12–16 characters long.
- Use a combination of uppercase, lowercase, numbers, and special characters.
- Avoid dictionary words, predictable patterns, and personal info (birthdays, names).
- Consider using passphrases for memorability and strength.
- Use a password manager to store and generate complex passwords.
- Enable Multi-Factor Authentication (MFA) for additional security.

Outcome

- Learned how password composition affects resistance to attacks.
- Understood how online tools estimate password crack times.

- Identified best practices for creating strong, memorable, and secure passwords.
- Became familiar with common attack methods that exploit weak passwords.

Key Concepts

- Password strength
- Brute force attack
- Dictionary attack
- Passphrase
- Multi-Factor Authentication (MFA)
- Password manager best practices