CYBER SECURITY INTERNSHIP

Task 6: Create a Strong Password and Evaluate Its Strength

Submitted by:

Soumen Das

Submission Date:

November 21, 2025

Elevate Labs

Objective

The objective of this task is to understand the fundamental characteristics that contribute to password strength. This involves creating passwords with varying levels of complexity, testing them against standard password strength evaluation tools, and analyzing the resilience of these passwords against common cyber threats such as brute force and dictionary attacks.

Methodology

To evaluate password strength effectively, I created five distinct passwords ranging from very weak to very strong. I tested these passwords against simulated metrics commonly used by online password strength checkers (such as entropy calculations and time-to-crack estimates).

Criteria for Evaluation

- **Length:** Number of characters.
- **Character Set:** Use of Uppercase (A-Z), Lowercase (a-z), Numbers (0-9), and Symbols (!@#).
- **Predictability:** Absence of dictionary words or common sequences.

Password Evaluation Results

The following table summarizes the testing results. Note that for security purposes, the actual passwords listed are examples used for testing structure, not personal passwords.

Password Type	**Example Used**	**Strength Rating**	**Est. Crack Time**
Weak	`password123`	Very Weak	$<$ 1 second
Common Pattern	`Soumen@1`	Weak	Approx. 2 minutes
Medium	`Tr0ub4dor&3`	Medium	3 days
Strong	`Xy9#mP2!qL`	Strong	400 years
Very Strong	`Blue-Horse-Correct-Staple-99`	Excellent	$>$ 1 million years

Table 1: Evaluation of Password Strength and Complexity

Analysis of Common Attacks

1. Dictionary Attack

A dictionary attack involves attempting to guess a password by running through a list of common words and phrases (a ”dictionary”).

- **Vulnerability:** Passwords like `password123` or `Soumen@1` are highly vulnerable because they contain full words or names found in standard wordlists.
- **Defense:** Avoiding recognizable words and names entirely.

2. Brute Force Attack

A brute force attack attempts every possible combination of characters until the correct one is found.

- **Vulnerability:** Short passwords (under 8 characters) are vulnerable because the total number of combinations is low enough for modern GPUs to process in seconds.
- **Defense:** Increasing length is the most effective defense. Each additional character exponentially increases the number of combinations.

Best Practices & Tips

Based on the evaluation, the following best practices have been identified for creating secure passwords:

1. **Length is Key:** Aim for a minimum of 12 characters. A longer password is mathematically harder to crack than a shorter, complex one.
2. **Mix Character Types:** Always combine uppercase, lowercase, numbers, and special symbols to increase the ”entropy” (randomness) of the password.
3. **Avoid Personal Info:** Never use names (e.g., ”Soumen”), birth dates, or pet names. These are the first things attackers guess.
4. **Use Passphrases:** A sequence of random words (e.g., `Correct-Horse-Battery-Staple`) is easier to remember for humans but very difficult for computers to guess due to length.
5. **Unique Passwords:** Never reuse the same password across multiple sites. If one site is breached, all accounts become vulnerable.

Conclusion

Password complexity significantly affects security. While adding complexity (symbols and numbers) helps, increasing the **length** of the password provides the most substantial boost to security against brute force attacks. By adhering to the best practices outlined in this report, users can significantly mitigate the risk of unauthorized access.