Create a Strong Password and Evaluate Its Strength

Introduction

As part of my cybersecurity internship, I was given a very practical and important task — to understand what makes a password truly strong and evaluate various passwords using online password checkers. While I've always known that strong passwords are important, this exercise helped me see exactly how attackers target weak passwords and what I can do to protect myself and others better.

In this task, I created a series of passwords with different complexities, tested them, noted the results, and then reflected on what I learned from the experience.

Step-by-Step Process

Step 1: Creating Passwords

I started by designing 5 different passwords with varying levels of complexity — from extremely basic to highly secure. I intentionally used some common patterns and bad habits to see how weak they actually are, and then contrasted them with stronger formats.

Here are the passwords I tested:

Password -My Reasoning

123456 -The most commonly used weak password.

iloveyou - Simple, emotional, and guessable.

Sunshine22 - Includes a word and digits — semi-predictable.

P@ssw0rd2025! -Includes special characters and a number — average complexity.

B!ue_Monkey!Dr1ft@78 - Long, random, and hard to guess — strong password.

Step 2: Testing with Password Strength Tools

To test these passwords, I used free tools like:

PasswordMeter

Kaspersky Password Checker

HowSecureIsMyPassword.net

Each password was pasted into the checker, and I noted the feedback, strength percentage, estimated time to crack, and improvement suggestions.

Results and Observations

Password	Score	Estimated Time to Crack	Tool Feedback
123456	0%	< 1 second	"Extremely weak, appears

			in most breach lists."
iloveyou	10%	Few seconds	"Common phrase, very easy to guess."
Sunshine22	35%	Few minutes	"Better, but still too predictable."
P@ssw0rd2025!	65%	Hours to days	"Moderate strength, consider more randomness."
B!ue_Monkey!Dr1ft@78	100%	Trillions of years	"Excellent — strong length, complexity, randomness."

I was genuinely surprised at how fast even medium-complexity passwords can be cracked. It was a wake-up call about how important unpredictability and length are.

What I Learned
What Makes a Strong Password?
From the tools and my research, I understood that strong passwords should:

Be at least 12–16 characters long.

Include uppercase and lowercase letters, numbers, and symbols.

Avoid real words, names, or dates.

Be unique — never reused across websites.

How Passwords Get Cracked
I also spent time reading about password attacks, and here’s what I learned:

Brute Force Attack: The attacker tries every possible combination until they succeed.

Dictionary Attack: Uses a list of commonly used passwords and words.

Credential Stuffing: Tries leaked username-password pairs from previous data breaches.

Even complex-looking passwords can fall to these attacks if they follow predictable patterns (like replacing “a” with “@”).

Best Practices I’ll Use Going Forward

Use passphrases: like SmellyCat*2025@CoffeeRain! — long, odd combinations that are memorable but not obvious.

Always enable multi-factor authentication (MFA).

Never reuse passwords across different platforms.

Start using a password manager like Bitwarden or LastPass to safely store my passwords.

Change passwords regularly, especially for sensitive accounts.

Reflections

Before doing this task, I didn’t realize how easy it is for attackers to guess short or common passwords. This wasn’t just about checking scores on a tool — it was about rethinking my personal security habits and recognizing how small oversights can lead to big vulnerabilities.

Honestly, seeing how quickly weak passwords could be cracked made me a little nervous — but also motivated to take password hygiene seriously. This task wasn't just educational — it was a real eye-opener.

Conclusion

This task helped me bridge theory with practice. I now feel confident about identifying weak passwords, explaining why they’re risky, and recommending solutions. Password security seems like a small topic — but it plays a massive role in overall cybersecurity. I’ll carry these lessons with me as I continue this internship and beyond.