Elevate Labs (Cyber-Security Internship)

Task 6 : Create a Strong Password and Evaluate Its Strength.

Objective: Understand what makes a password strong and test it against password strength tools.

Tools: Online free password strength checkers (e.g., passwordmeter.com).

Deliverables: Report showing password strength results and explanation.

Report:

Password	Length	Uppercase	Lowercase	Numbers	Symbols	Score	Strength Feedback
hello123	8	No	Yes	Yes	No	35%	Too short, lacks complexity, easily guessable.
HelloWorld12	12	Yes	Yes	Yes	No	64%	Better length, but lacks symbols.
H3llo@2025	10	Yes	Yes	Yes	Yes	78%	Strong, includes all character types, moderate length.
H#2r!9eL@8zP	12	Yes	Yes	Yes	Yes	90%	Strong — high complexity, less predictable.
V9$tX7#rQ!m2@1W	15	Yes	Yes	Yes	Yes	100%	Very strong — long, high randomness, all character types.

The Password Meter

Test Your Password		Minimum Requirements
Password:	V9$tX7#rQIm2@1W	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	4	+ 22
Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 24
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	4	+ 24
Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
Requirements	Flat	+(n*2)	5	+ 10

Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	0	0
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

- **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
- **Sufficient:** Meets minimum standards. Additional bonuses are applied.
- **Warning:** Advisory against employing bad practices. Overall score is reduced.
- **Failure:** Does not meet the minimum standards. Overall score is reduced.

Quick Footnotes

- **Flat:** Rates that add/remove in non-changing increments.
- **Incr:** Rates that add/remove in adjusting increments.
- **Cond:** Rates that add/remove depending on additional factors.
- **Comp:** Rates that are too complex to summarize. See source code for details.
- **n:** Refers to the total number of occurrences.
- **len:** Refers to the total password length.
- Additional bonus scores are given for increased character variety.
- Final score is a cumulative result of all bonuses minus deductions.
- Final score is capped with a minimum of 0 and a maximum of 100.
- Score and Complexity ratings are not conditional on meeting minimum requirements.

Disclaimer

PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☑

#G@@gIE&H#LL0_W@rLD&

Very Strong

20 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

230 billion trillion years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Your passwords are never stored. Even if they were, we have no idea who you are!

❖ **Best Practice, to BUILD-STRONG Password:**

- ✓ **Length matters** — At least **12–16 characters** are recommended.
- ✓ **Mix character types** — Use **uppercase, lowercase, numbers, and symbols**.
- ✓ **Avoid patterns** — Do not use 12345, abed, or repeated letters.
- ✓ **Do not use personal info** — No names, birthdays, or common words.
- ✓ **Use passphrases** — Combine random words with symbols (**e.g., Pine#Ocean7!Cloud**).
- ✓ **Randomness is king** — Avoid dictionary words without modification.
- ✓ **Unique for every site** — Never reuse passwords across accounts.
- ✓ **Consider password managers** — They can generate and store complex passwords.

❖ **Common Password Attack's:**

1. **Brute Force Attack**
   - ➢ The attacker tries every possible combination until the password is found.
   - ➢ Weak passwords: Can be cracked in seconds.
   - ➢ Strong passwords: Take millions of years with current computing power.
2. **Dictionary Attack**
   - ➢ Uses a precompiled list of common words/passwords.
   - ➢ Adding symbols and numbers breaks dictionary matches.
3. **Hybrid Attack**
   - ➢ Combines dictionary words with predictable modifications (Password123!).
   - ➢ Randomized characters reduce this risk.

❖ **Summary:**

- ✓ Password strength is determined by **length, complexity, and unpredictability**.
- ✓ The strongest tested password (**V9$tX7#rQ!m2@1W**) scored **100%** and would be **extremely difficult** to crack.
- ✓ Complex passwords defend against **Brute-Force** and **Dictionary** attacks by making the possible combinations astronomically high.