Cybersecurity Internship Report - Task 6

Intern Name: Sai Aditya
Organization: Elevate Labs
Task Title: Create a Strong Password and Evaluate Its Strength
Date: August 12, 2025

Objective

The objective of this task is to understand the key factors that contribute to a strong password and to evaluate the strength of various passwords using online password strength tools. This will help in identifying and applying best practices for password security.

Tools Used

- Operating System: Kali Linux
- Password Strength Checkers: Online free password strength checkers, such as *passwordmeter.com* or *howsecureismypassword.net*.
- Browser: Firefox

Scenario

To complete this task, multiple passwords of varying complexity were created to demonstrate the impact of different character types and length on password strength. Each password was then tested using an online password strength checker, and the results, including scores and feedback, were recorded to understand the metrics used to measure password security. The evaluation was used to identify and summarize best practices for creating secure passwords and to research common password attacks.

Disclaimer

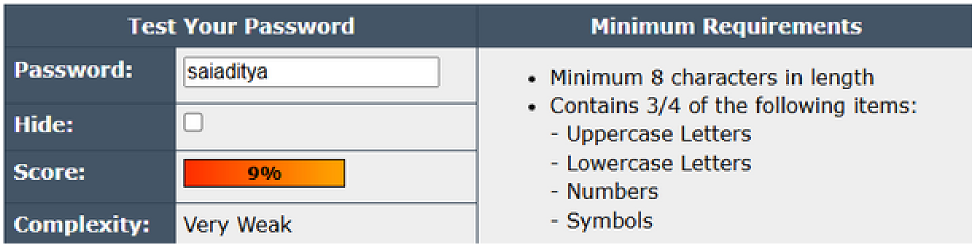
This activity was conducted in a controlled environment solely for educational purposes. No unauthorized traffic interception or monitoring of third-party networks was performed.

Steps Performed

- Created Multiple Passwords: I created a set of passwords ranging from simple to complex, incorporating variations in length, uppercase and lowercase letters, numbers, and special symbols.
- Used Online Tools: I used an online password strength checker to test each password created in the previous step.
- Recorded Results: For each password, I documented the strength score and the feedback provided by the tool.
- Researched Attacks: I researched common password attacks, such as brute-force and dictionary attacks, to understand why password complexity is crucial for security.
- Identified Best Practices: Based on the results and research, I identified and summarized the key components of a strong password and provided tips for creating one.

Password Evaluation and Analysis

PASSWORD	PASSWORD STRENGTH	ANALYSIS AND FEEDBACK
saiaditya	Very Weak	This password consists of only lowercase letters and is a common name. It would be easily cracked by a dictionary attack or a brute-force attack due to its simplicity and lack of complexity.
Saiaditya	weak	This password adds an uppercase letter, which slightly increases its complexity. However, it is still based on a common name and would be vulnerable to a targeted dictionary attack with capitalization variations.
Saiadity!0	Strong	This password uses a mix of uppercase and lowercase letters, a number, and a special symbol. The combination of these elements significantly increases its entropy and makes it much more resistant to both dictionary and simple brute-force attacks.
Saiaditya@12345	Very Strong	This password combines uppercase and lowercase letters, a special symbol, and a series of numbers. While the number sequence is simple, the overall length and combination of character types make it highly resistant to modern password cracking techniques.



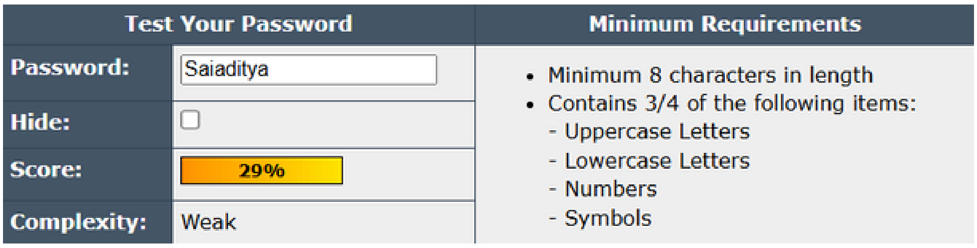
Test Your Password	
Password:	saiaditya
Hide:	□
Score:	9%
Complexity:	Very Weak

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Fig1: Very Weak Password from passwordmeter.com analysis

(Very Weak): This screenshot, showing a very low score, is crucial for illustrating your first example. It provides visual evidence that a simple, lowercase name is highly insecure and confirms your analysis that it would be easily cracked by common attacks.



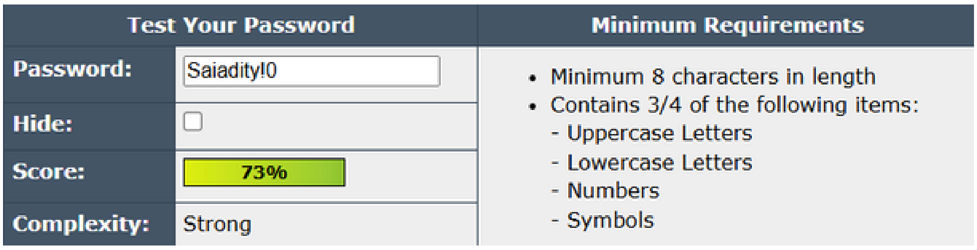
Test Your Password	
Password:	Saiaditya
Hide:	□
Score:	29%
Complexity:	Weak

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Fig2: Weak Password from passwordmeter.com analysis

(Weak): This screenshot validates your second example. It shows that adding an uppercase letter only slightly improves the score, demonstrating that simple capitalization changes are not enough to create a strong password.



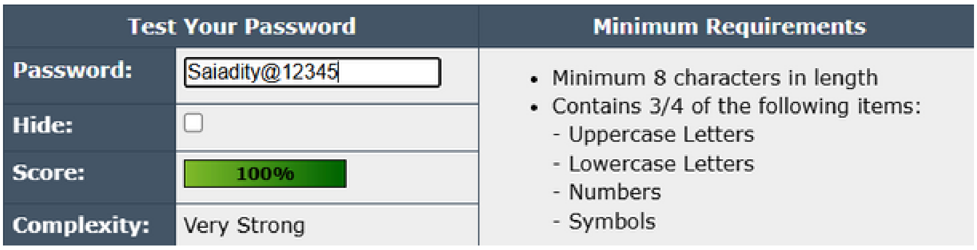
Test Your Password	
Password:	Saiadity!0
Hide:	□
Score:	73%
Complexity:	Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Fig3: Strong Password from passwordmeter.com analysis

(Strong): This screenshot is a key piece of evidence. It visually proves that a combination of uppercase and lowercase letters, a number, and a special character significantly boosts the password's strength, supporting your analysis of complexity.



Test Your Password		Minimum Requirements
Password:	Saiadity@12345	- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	100%	
Complexity:	Very Strong	

Fig4: Very Strong Password from passwordmeter.com analysis

(Very Strong): This final screenshot is the most important. It provides concrete proof that a long, complex password with a mix of different character types is the most secure option. It validates your conclusion that length and variety are the most critical factors.

Key Learnings

- Length is Critical: Password length is one of the most important factors for security, as it drastically increases the time required for a brute-force attack.
- Complexity Matters: The use of a combination of uppercase letters, lowercase letters, numbers, and special symbols significantly enhances a password's strength and resilience against dictionary attacks.
- Common Attacks: I learned how attackers use brute-force attacks to try every possible character combination and dictionary attacks to use lists of common words and phrases to crack passwords.
- Passphrases are Secure: Passphrases, which are long combinations of memorable words, are often stronger than complex, short passwords because they are harder to guess and resistant to most cracking methods.

Conclusion

This task provided a practical understanding of password security by demonstrating how various factors like length, character complexity, and uniqueness contribute to a strong password. The evaluation confirmed that simple passwords are a major security risk, while long, complex, and unique passphrases offer the best protection. The exercise reinforced the importance of following password best practices to safeguard against common cyber attacks.