Elevate Labs - Cybersecurity Internship: Task 6 Report

Task Objective

The objective of Task 6 is to understand what makes a password strong and to test it against password strength tools.

Tools Used :

Passwordmeter.com

1. Password Testing and Results:

Password Example	Complexity Features Used	Strength Score/Rating (from passwordmeter.com or similar)	Feedback/Time to Crack
Weak (e.g., Intern123)	Common word + numbers	Low	Instant/Very short
Medium (e.g., Elevate-Labs2024)	Upper/lowercase, numbers, hyphen. A bit too predictable.	Medium	Hours/Days
Strong (e.g., P@$$wOrdG00d)	Mixed case, numbers, symbols, but contains common substitutions.	High	Years/Decades
Best Practice (e.g., Th!s1sMyL0ngP@ssPhrasE4SecuritY)	**Length** (≥16 characters), mixed case, numbers, symbols, memorable but complex.	Very High/Excellent	Centuries/Millions of Years

2.Best Practices for Creating Strong Passwords

1. **Vary Complexity** : Create passwords that use a mix of different character types.
2. **Use Mixed Character Sets**: Incorporate the following into your password:
    - Uppercase letters
    - Lowercase letters
    - Numbers
    - Symbols
3. **Prioritize Length** : Utilize length variations, as password length is a crucial factor in password strength.
4. **Avoid Common Attacks** : Create passwords that are complex enough to protect against common methods like **brute force attacks** and **dictionary attacks**.
5. **Identify and Apply Learned Tips** : Identify what works best by testing and evaluating different passwords, then write down the best practices and tips learned from that evaluation.

Key Concepts Related to Security

- **Password Complexity Affects Security** : Password complexity directly influences security; a more complex password is harder to crack.
- **Authentication** : Passwords are a primary component **authentication**, which verifies a user's identity.
- **Best Practices** : Adhering to these rules constitutes good **best practices** in cybersecurity.

3. Research on Password Attacks

Common Password Attacks

1. **Brute Force Attack**:
    - **Definition**: The attacker tries every possible combination of characters (letters, numbers, symbols) until the correct password is found.
    - **How Complexity Helps**: Increased **password length** is the primary defense. A longer password takes exponentially more time for a computer to guess, making the attack computationally infeasible.
2. **Dictionary Attack**:
    - **Definition**: The attacker uses a list of common words, phrases, leaked passwords, and simple variations (like substituting '1' for 'l' or '!' for 'i') to test against the system.
    - **How Complexity Helps**: This attack is defeated by **avoiding common words** and not using obvious character substitutions. Using passphrases of random, unrelated words (e.g., `Blue-Dog-Tree-Cloud`) is an effective countermeasure.

4.How Password Complexity Affects Security

Password complexity—defined by

length, character set variety (mixed case, numbers, symbols), and unpredictability—is the core defense against automated attacks. Higher complexity directly translates to a larger

keyspace (the total number of possible combinations). A small keyspace means a password can be cracked instantly; a large keyspace means it would take millions of years, even for the fastest supercomputers, rendering the account effectively secure.

Screenshots :

Test Your Password		Minimum Requirements
Password:	Intren123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	68%	
Complexity:	Strong	

Test Your Password		Minimum Requirements
Password:	Elevate-Labs2024	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Test Your Password		Minimum Requirements
Password:	L0ngP@ssPhrasE4SecuritY	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Test Your Password		Minimum Requirements
Password:	P@$$wOrdG00d	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	