***Elevate Labs Cyber Security Internship***

***Task 6: Create a Strong Password and evaluate its strength.***

******

**Step 1: Create Passwords**

Start by creating a list of passwords with different levels of complexity. A good way to do this is to vary the length and the types of characters used.

* **Weak:** A short password with only lowercase letters and numbers (e.g., password123)
* **Moderate:** A mix of uppercase, lowercase, and numbers (e.g., P@ssword1)
* **Strong:** A longer password that includes uppercase, lowercase, numbers, and symbols (e.g., \_MySecr3tP@ssw0rd!)
* **Very Strong:** A long, completely random string of characters (e.g., Jk7#wXz$2!qP@9^fR&)

**Step 2: Test Passwords**

Use an online password strength checker to test each of your passwords. Websites like [Security.org](https://www.security.org/how-secure-is-my-password/) or [howsecureismypassword.net](https://howsecureismypassword.net/) are great for this.

1. Navigate to a password strength checker.
2. Enter each of the passwords you created one at a time.
3. For each password, **note the score** or estimated time to crack.
4. **Pay attention to the feedback** provided by the tool. For example, it might tell you to "add more symbols" or that the password is a "common word."

**Step 3: Identify Best Practices & Tips**

Based on the results from the password strength checker, you can identify what makes a password strong. Use these observations to write down your key takeaways.

* The **most important factor** is password **length**. Notice how the estimated crack time increased exponentially with each additional character.
* **Character variety** (uppercase, lowercase, numbers, symbols) makes a password more difficult to guess.
* The **randomness** of the password is key. Avoid using common words or personal information.

**Step 4: Research Password Attacks & Security**

To understand why these best practices are so important, research common password attacks.

* **Brute-Force Attack:** An attacker uses a program to try every possible combination of characters until they find the right password. Your evaluation in Step 2 shows how long this would take for a complex password.
* **Dictionary Attack:** An attacker uses a pre-compiled list of common words, phrases, and leaked passwords to guess a password. The simple passwords you created would be vulnerable to this attack.

**Step 5: Summarize How Complexity Affects Security**

Finally, summarize your findings into a concise report. Explain how a password's complexity directly impacts its security.

A simple password is easy to guess and is vulnerable to both brute-force and dictionary attacks. A complex, long, and random password, on the other hand, makes these attacks **practically impossible**. The more complex a password is, the more time and computational power it requires to crack, which is a major deterrent for hackers.

### *Interview Questions* 1. What makes a password strong?

A strong password is a combination of three key factors: length, variety, and randomness. A password's length is its most important characteristic, as each additional character exponentially increases the time it takes to crack. Character variety, including uppercase and lowercase letters, numbers, and symbols, makes a password harder to guess. Lastly, a strong password avoids predictable information like personal details or common words.

**2. What are common password attacks?**

Common password attacks include:

* **Brute-Force Attack:** An attacker systematically tries every possible combination of characters until the correct password is found.
* **Dictionary Attack:** The attacker uses a list of common words, phrases, and leaked passwords to try to gain access.
* **Phishing:** The attacker tricks a user into revealing their password, often through a fraudulent email or website.

**3. Why is password length important?**

Password length is the single most important factor in its strength. The time it takes a brute-force attack to guess a password increases exponentially with each character added. For example, a 12-character password can take trillions of times longer to crack than an 8-character password.

**4. What is a dictionary attack?**

A dictionary attack is a type of brute-force attack where the attacker uses a pre-compiled list of common words, phrases, and passwords (the "dictionary") to try and guess a password. This method is faster than trying every possible combination but is only effective against passwords that use common or easily guessable words.

**5. What is multi-factor authentication?**

Multi-factor authentication (MFA) is a security method that requires users to provide two or more verification factors to gain access to an account. This typically includes something you know (like a password) and something you have (like a code from your phone or a physical token). MFA significantly increases security, as an attacker would need to compromise both factors.

**6. How do password managers help?**

Password managers are applications that help users generate, store, and manage strong, unique passwords for all their online accounts. You only need to remember one master password to unlock a secure, encrypted vault containing all your other passwords. This allows you to use complex, unique passwords for every service without having to remember them.

**7. What are passphrases?**

A passphrase is a long password made of a sequence of words or a sentence. For example, correcthorsebatterystaple is a famous passphrase. Because of their length, they are highly secure against brute-force attacks while also being easier for humans to remember than a random string of characters.

**8. What are common mistakes in password creation?**

Common mistakes include:

* **Using a simple, short password** that is easy to guess.
* **Reusing the same password** for multiple accounts.
* **Using personal information** that can be easily found, like birthdays or family names.
* **Using common patterns** or dictionary words, even with simple substitutions (e.g., replacing 'e' with '3').