ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-6:

1.Create multiple passwords with varying complexity.

2.Use uppercase, lowercase, numbers, symbols, and length variations.

Very Weak: qwerty
All lowercase, common keyboard pattern, extremely easy to guess.

Weak:qwerty123

Adds numbers, but still predictable and frequently used.

Moderate: Qw3rty!

Uses uppercase and lowercase letters, a number, and a special character, but short in length.

Strong: Qw3rty!92@

Increased length and includes multiple numbers and symbols, making it harder to crack.

Very Strong: Qw3_rT9!$eY@72

Long (14 characters), uses mixed case, numbers, and multiple special characters in a less predictable format.

Ultra Secure:7&Qw3$Ty!_r91*Kz

Very strong due to its 16+ character length, randomness, and full mix of character types.

3.Test each password on password strength checker.

4.Note scores and feedback from the tool.

Password	Score	Time to Crack	Feedback
qwerty	Very Weak	Instant	Common password, lowercase only, easily guessed
qwerty123	Weak	<1 second	Predictable pattern, found in breach lists
Qw3rty!	Moderate	A few hours	Better mix of characters, but too short
Qw3rty!92@	Strong	Centuries	Good complexity and decent length
Qw3_rT9!$eY@72	Very Strong	Trillions of years	Excellent length and complexity, rare pattern
7&Qw3$Ty!_r91*Kz	Extremely Strong	Longer than the universe	Ideal password: long, random, and hard to guess

5.Identify best practices for creating strong passwords:

To create a strong password, it's best to make it at least 12 characters long and use a mix of uppercase and lowercase letters, numbers, and special symbols. Avoid using personal information or common patterns like “123456” or “qwerty.” It’s also important not to reuse the same password across different accounts. Using a few random words together, along with symbols or numbers, can make a password both strong and easier to remember. For extra security, consider using a password manager and enabling two-factor authentication whenever possible

6.Write down tips learned from the evaluation.

From the evaluation, I learned that strong passwords are long, use a mix of characters (uppercase, lowercase, numbers, and symbols), and avoid common patterns or personal info. Simply changing letters to symbols isn't enough—randomness and length matter more. Reusing passwords is risky, and even short complex ones can be weak. Passphrases with

random words work well, and using a password manager and enabling two-factor authentication makes things much more secure.

7.Research common password attacks (brute force, dictionary).

1. **Brute Force Attack:** Tries every possible combination until the correct one is found. Longer, complex passwords take exponentially longer to crack.
2. **Dictionary Attack:** Uses lists of common words, phrases, and substitutions (like password, p@ssw0rd) to guess passwords quickly.
3. **Credential Stuffing:** Uses leaked username-password pairs from previous data breaches to access other accounts with reused credentials.
4. **Phishing:** Tricks users into giving up passwords through fake websites or messages.
5. **Keylogging:** Malware records everything typed on a keyboard, including passwords.

8.Summarize how password complexity affects security.

Password complexity directly increases security by making passwords harder to guess or crack using automated tools. A simple password like qwerty123 can be cracked instantly, while a longer, complex password like 7&Qw3$Ty!_r91*Kz could take trillions of years. Adding a mix of character types, avoiding common words, and increasing length all significantly reduce the chance of successful brute force or dictionary attacks. In short, the more random and complex a password is, the more secure your account will be.