**TASK -6**

**Creating a Strong Password and Evaluating Its Strength**

**Objective:** To understand the factors that make a password strong, evaluate various passwords using online tools, and learn best practices for password creation and protection against attacks.

**Step 1: Creating Multiple Passwords**

|  |  |
| --- | --- |
| **Password** | **Description** |
| password123 | Simple, only lowercase and numbers |
| Password@2024 | Moderate complexity |
| P@ssw0rd!2024# | Strong with symbols and variety |
| !F@9kT\*e2L#qW7z% | Very complex, random characters |
| abc123 | Very weak, commonly used |

**Step 2: Using Different Character Combinations** Passwords were created using:

* Uppercase letters (A-Z)
* Lowercase letters (a-z)
* Numbers (0-9)
* Special symbols (!@#$%^&\*)
* Lengths ranging from 6 to 16+ characters

**Step 3: Testing Passwords on Strength Checkers**

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Strength | Estimated Crack Time | Feedback |
| password123 | Weak | Instant | Too common, lacks complexity |
| Password@2024 | Moderate | A few hours | Needs more length and randomness |
| P@ssw0rd!2024# | Strong | Several years | Good use of variety and length |
| !F@9kT\*e2L#qW7z% | Very Strong | Trillions of years | Excellent complexity and randomness |
| abc123 | Very Weak | Instant | Extremely simple, easily guessable |

**Best Practices Identified:**

* Use at least 12 characters
* Include uppercase, lowercase, numbers, and symbols
* Avoid dictionary words or personal information
* Don’t reuse passwords across accounts
* Use a password manager for storing complex passwords
* A **Research on Common Password Attacks:**

1. **Brute Force Attack:** Tries every possible character combination until it finds the correct one.
2. **Dictionary Attack:** Uses a list of common words and phrases to guess passwords.
3. **Phishing:** Tricks users into entering passwords on fake websites.
4. **Credential Stuffing:** Uses leaked credentials from one site to log into others.

**How Complexity Affects Security:**

* Simple passwords (e.g., "abc123") can be cracked in seconds.
* Complex passwords (e.g., "P@ss!Xz#49") can take hundreds of years to crack.
* More characters and randomness make passwords much harder to break.

**Conclusion:** Creating strong passwords is essential for protecting personal and sensitive data. By using a mix of characters, ensuring sufficient length, and avoiding predictability, one can significantly enhance their online security. Regular evaluation and awareness of password attacks further help in building good cybersecurity habits.