Task 6: Create a Strong Password and Evaluate Its Strength

Objective:

To understand what makes a password strong and evaluate its strength using online password strength checkers.

---

Tools Used:

Password Meter

Security.org Password Strength Test

---

|  |  |  |  |
| --- | --- | --- | --- |
| Password | Strength Result | Tool Used | Notes |
| 123456 | Very Weak | Password Meter | Common password; easy to guess |
| Hashini@123 | Medium | Password Meter | Contains uppercase, lowercase, symbol, and numbers |
| H@S#1N!\_S3cuReP@55w0rD | Strong | Password Meter | High complexity; hard to brute-force |
| summer2025! | Medium | Security.org | Better than simple passwords but lacks randomness |
| #L3m0n$Zebra!9021 | Strong | Security.org | Long, random, and includes mixed character types |
|  |  |  |  |

---

Best Practices for Strong Passwords:

Use at least 12–16 characters.

Mix uppercase, lowercase, digits, and special characters.

Avoid using personal information (birthdates, names).

Don’t reuse passwords across different sites.

Consider using passphrases (e.g., Purple$Tiger\_Jumps!99).

---

Insights from Evaluation:

Password length significantly impacts strength.

Adding symbols and numbers boosts complexity.

Dictionary words or predictable patterns make passwords weak.

A password like 123456 was cracked instantly, whereas complex ones showed decades or even centuries of cracking time.

---

Common Password Attacks (Brief Research Summary):

Brute Force Attack: Trying every possible combination.

Dictionary Attack: Trying commonly used words or leaked passwords.

Passwords with low complexity are easy targets.

---

Summary:

Password strength depends on complexity, unpredictability, and length. By using online tools, we evaluated several passwords and learned how even small changes can significantly improve password security. Strong password habits are essential for protecting accounts and data.