Task 6: Create a Strong Password and Evaluate Its Strength

Objective:

Understand what makes a password strong and evaluate its effectiveness using online password strength checkers.

Tools Used

- PasswordMeter.com (https://www.passwordmeter.com)
- Security.org Password Strength Checker (https://www.security.org/how-secure-is-my-password/)
- NordPass Password Checker (https://nordpass.com/password-strength-checker/)

Password Samples and Evaluation

Password | Length | Complexity | Score | Time to Crack | Feedback

abc123 | 6 | Lowercase, Numbers | 25% | <1 second | Too short, predictable

Avi@1234 | 8 | Uppercase, lowercase, numbers, symbol | 63% | 5 hours | Medium strength

AviM@nd@l2025 | 13 | All types | 88% | 3 million years | Very strong

Qz!rT7#pLx$9Wd2 | 15 | Complex | 100% | 1 trillion years | Excellent

Tips Learned for Strong Passwords

- Longer is better: Passwords >12 characters are significantly harder to crack.
- Use all character types: Combine uppercase, lowercase, numbers, and symbols.
- Avoid dictionary words: Common words are vulnerable to dictionary attacks.
- No personal info: Don't use names, birthdays, or other personal data.
- Unpredictability is key: Random character placement increases strength.
- Avoid reused passwords: Each account should have a unique password.

Common Password Attacks

- Brute Force: Tries every possible combination until it finds the correct one.
- Dictionary: Uses a precompiled list of common words/passwords to guess quickly.

- Credential Stuffing: Uses previously leaked passwords on multiple sites hoping for reuse.

- Phishing: Tricks users into entering their password on fake websites.

Summary

- Passwords with fewer than 8 characters, no symbols or randomness, are highly vulnerable.

- Adding complexity exponentially increases the time and resources needed to crack them.

- Strong password practices can defend against brute force, dictionary, and credential stuffing attacks.

Outcome

- Understood how password strength is evaluated.

- Learned to create and test strong passwords.

- Gained awareness of password-related attacks and how to defend against them.