Password Strength Evaluation Report

Objective

To create, test, and analyse multiple types of passwords using password strength checkers and understand how various attacks exploit weak passwords.

Password Tested and Results:

Password	**Score (%)**	**Complexity**	**Key Observations**
password	8%	Very Weak	Simple dictionary word, lowercase only
12345678	4%	Very Weak	Only numbers, highly common and predictable
Password@123	93%	Strong	Includes uppercase, lowercase, symbol, and numbers — passes all requirements
Tricky@1358	100%	Very Strong	Randomized with mixed types, strong structure, excellent resistance to attacks

Analysis

- password and 12345678 are both **extremely weak** and crackable in seconds using brute-force or dictionary attacks.
- Password@123 is a **strong password**, but still follows a **predictable structure** — attackers may try similar formats (e.g., Name@123).
- Tricky@1358 scored **100%** due to its ideal length, randomness, and use of all character types — excellent for secure use.

Password Attack Methods:

- Brute Force: Tries every combination of characters.
- Dictionary Attacks: Uses common wordlists or leaked passwords.
- Credential Stuffing: Reuses stolen passwords across sites.
- Keylogging: Malware that records typed keys.

- Phishing: Tricks users into revealing passwords on fake pages.
- Man-in-the-middle: Intercepts and captures passwords in transit.

Best practice to make password stronger:

- Use 12+ characters with uppercase, lowercase, numbers, and symbols
- Avoid dictionary words, names, or patterns like 123 or password
- Create passwords that don’t follow common formats
- Consider using a password manager to store strong passwords securely
- Enable two-factor authentication (2FA) wherever possible