Common Password Attacks Explained

1. Brute Force Attack

Definition:
A brute force attack is a trial-and-error method where an attacker tries **every possible combination** of characters until the correct password is found.

How it works:

- Attackers use automated tools to try passwords at high speed.
- Short and simple passwords get cracked **within seconds**.

Example:
Trying all combinations like `a`, `aa`, `aaa`, ..., `aA1@zZ9!` until the password matches.

Protection:

- Use **longer passwords (12+ characters)**.
- Include **uppercase, lowercase, symbols, and numbers**.
- Enable **account lockout** after several failed attempts.

2. Dictionary Attack

Definition:
A dictionary attack uses a **predefined list of common passwords, words, and combinations** to guess the password.

How it works:

- Attackers load wordlists like `rockyou.txt` or real-life leaked passwords.
- These wordlists contain millions of commonly used passwords.

Example:
Trying passwords like `password`, `123456`, `qwerty`, `iloveyou`, `admin123`, etc.

Protection:

- Avoid using **real words, names, or predictable sequences**.
- Combine random **letters, symbols, and numbers**.
- Use **passphrases** that are hard to guess.

3. Credential Stuffing

Definition:
This attack uses **leaked username-password pairs** from previous data breaches to try logging into other services.

How it works:

- Many users reuse passwords across platforms.
- Hackers use bots to test leaked credentials on sites like Gmail, Facebook, Instagram, etc.

Protection:

- **Never reuse passwords** on multiple sites.
- Use a **password manager** to store unique passwords.
- Enable **multi-factor authentication (MFA)**.

4. Phishing Attack

Definition:
Phishing tricks users into revealing passwords by impersonating trusted sources like banks, emails, or websites.

How it works:

- Fake websites or emails mimic real ones.
- Users are asked to "verify" login credentials on fake pages.

Protection:

- Never click on suspicious links.
- Always **check the website URL**.
- Use **anti-phishing filters** and email security tools.

5. Keylogger Attack

Definition:
A keylogger is malware that records every keystroke, including passwords.

How it works:

- Installed through malicious downloads or attachments.
- Logs and sends your keystrokes to attackers.

Protection:

- Use **antivirus software** and **keep your OS updated**.
- Avoid installing untrusted programs or browser extensions.

6. Shoulder Surfing

Definition:
This is a physical attack where someone **watches you type your password** (in person or via surveillance).

Protection:

- Use **screen privacy filters**.
- Be aware of surroundings while typing.
- Enable **biometric login** when possible.

7. Social Engineering Attack

Definition:
Attackers **manipulate people into revealing passwords** by pretending to be someone they trust (e.g., IT support).

Protection:

- Never share passwords with anyone, even "support staff."
- Be cautious of unknown callers/emails requesting login info.