

✓ Task 6: Create a Strong Password and Evaluate Its Strength

Objective

To understand what makes a password strong by creating various passwords and testing them using online password strength checkers. This task builds awareness about password complexity, security best practices, and common threats.


Tools Used

- <https://www.passwordmeter.com>

Some Passwords Tested & guess

Some Password Lists	Strength Result	Comments
admin123, shivam	Weak	Common, short, no special characters
qwerty123 , 7896387612	Weak	Predictable, dictionary word, Mobile number
12345678, 111111	Weak	Very common, found in breaches
@Shivam	Moderate	Better, has uppercase + symbol
\$S@chin1	Moderate to Strong	Good mix, still somewhat guessable
ShiVam@2005	Strong	Obfuscated characters, symbols, length
\$S@Ch1n6	Strong	Strong mix of all elements
\$h!vam@7258	Strong	Mix of Upper & lower case, contains symbols
\$ShiVaM_7258	Strong	Long, mix, random
\$S@ch!n-5318	Very Strong	Random words + numbers

Some Password Lists	Strength Result	Comments
B5@kKs!#=d7	Very Strong	Complex and lengthy & random
&D9j!qL7v%T8#Rwz\$U3c@M	Extremely Strong	Random, very long, brute-force resistant

 *Note: Passwords shown here are examples used for testing only.*

□ Key Learnings

- **Longer passwords** (8+ characters) are more secure.
 - Using a **mix of uppercase, lowercase, numbers, and symbols** increases strength.
 - Avoid using **predictable or personal information** (e.g., names, birthdays).
 - **Passphrases** are both secure and memorable.
 - **Password managers** help store and generate strong, unique passwords.
 - Always prefer **multi-factor authentication (MFA)** for enhanced security.
-

♡ Common Password Attacks (Summary)

Brute Force Attack: This method systematically tries every possible combination of letters, numbers, and symbols until the correct password is found. Although time-consuming, it can succeed against short or simple passwords. Longer and more complex passwords exponentially increase the time required for brute force attacks, making them highly resistant. Tools like Hydra and John the Ripper are commonly used for this.

Dictionary Attack: In this attack, the attacker uses a precompiled list of common words, passwords, and phrases (e.g., "123456", "qwerty", "password", etc.) to guess the password. These attacks are faster than brute force and often successful against weak or commonly used passwords. Using unique, non-dictionary phrases can protect against this.

Credential Stuffing: Attackers use leaked username-password combinations from past data breaches and try the same credentials on different websites. Since many users reuse passwords, this method is surprisingly effective. Protection includes using unique passwords for every site and enabling two-factor authentication.

Password Spraying: Unlike brute force that tries many passwords for one account, this attack tries a few commonly used passwords (like "Welcome@123", "Admin123") across

many accounts. It's designed to avoid account lockouts and is effective in corporate environments. It exploits weak but acceptable passwords across multiple users.

Phishing Attacks: Attackers trick users into entering their credentials on fake websites or pop-ups that look legitimate. Phishing is often conducted via email, SMS, or fake login pages. Best defense is awareness, browser security features, and multi-factor authentication.


Keylogging: Malware records keystrokes made by a user to capture login credentials. Keyloggers can be software or hardware-based and are often part of larger malware payloads. Protect yourself using updated antivirus, avoiding unknown downloads, and using MFA.

Shoulder Surfing: A low-tech method where someone watches the user enter their password in a public or semi-private space. Always shield your screen and keyboard in such situations.

Outcome / Result

After testing 15 passwords of varying complexity on multiple password strength tools:

- **Weak passwords** (like admin123) were instantly flagged as insecure.
- **Medium-strength passwords** improved with the addition of symbols and uppercase letters.
- **Strong passwords** were long, randomized, and contained varied character types.
- **Very strong passwords** (e.g., &D9j!qL7v%T8#Rwz\$U3c@M) scored nearly perfect and were marked as "taking centuries to crack" by brute force.

 I now understand how password complexity directly impacts resistance to attacks like brute force, dictionary, and credential stuffing. This task helped reinforce why strong password habits and good practices are essential for personal and organizational cybersecurity.