Task 6: Create a Strong Password and Evaluate Its Strength

Objective

The goal of this task is to develop an understanding of what constitutes a strong password, evaluate different types of passwords using free online password strength checking tools (such as passwordmeter.com and howsecureismypassword.net), and analyze the results to establish best practices for password creation.

Password Strength Evaluation

We used **howsecureismypassword.net** to assess the strength of various types of passwords. Below is a table showing different passwords with varying complexity levels and the feedback from the tools.

Password	Strength (%)	Estimated Crack Time	Feedback
123456	0%	Instantly	Too short, no variety, very common
password123	20%	<1 second	Common pattern, lacks symbols
SkyFall2024	50%	3 hours	Add symbols for stronger password
C0ffee_Latte!	75%	~2 days	Good symbol/number use, moderate length
T!ger#C@ge908	90%	20 years	Strong mix of characters and length
5uP3r$@f3_P@$$w0rD!	100%	200+ years	Excellent complexity and unpredictability

Learnings and Best Practices

1. **Use Long Passwords**
   Longer passwords are significantly harder to crack. A minimum of 12–16 characters is recommended. The more characters a password has, the more combinations an attacker must try in a brute-force attack, increasing the time and resources needed to break it.
2. **Increase Password Complexity**
   Combine uppercase and lowercase letters**,** numbers**,** and special characters (e.g., !@#$%^&*) to increase complexity. This broadens the character set, making password guessing and brute-force attacks more difficult.
3. **Avoid Common Words and Patterns**
   Do not use dictionary words, names, birthdays, or predictable patterns such as `"password123"`, `"admin"`, or `"qwerty"`. These are commonly used and easily cracked by attackers using dictionary or pattern-based attacks.
4. **Use Passphrases for Memorability and Strength**
   Create passphrases consisting of multiple unrelated words, such as "*PurpleDuckBatterySunset*!". Passphrases are easier to remember than random strings but can still be very secure if the words are chosen randomly.
5. **Use Unique Passwords for Every Account**
   Reusing passwords across different sites is risky. If one site is breached, attackers can use the same credentials to try and access other services (credential stuffing attacks). Always use a unique password per service**.**
6. **Use a Password Manager**
   A reputable password manager (e.g., Bitwarden, 1Password, KeePass, or LastPass) can help generate strong, unique passwords for every account and store them securely, so you don’t have to memorize them.
7. **Enable Multi-Factor Authentication (MFA)**
   Always enable MFA when available. Even if your password is compromised, MFA adds an additional layer of security by requiring a second factor (e.g., a one-time code from your phone).
8. **Avoid Password Hints or Security Questions Based on Public Info**
   Avoid using easily researched answers like your mother’s maiden name or the city you were born in. These can be guessed or found via social media or public records.

9. **Change Default Passwords Immediately**
   Devices like routers, IoT gadgets, and admin dashboards often ship with default login credentials (e.g., admin/admin). Always change these immediately upon setup.
10. **Do Not Share Passwords**
    Never share passwords via email, messaging apps, or verbally. If sharing access is necessary, use secure delegation features or shared vaults in password managers.
11. **Regularly Review and Update Passwords**
    Periodically review your password security. If a service you use has been breached or you suspect any compromise, change the password immediately.

Detailed Overview of 10 Password Attacks

1. Brute Force Attack

An attacker tries every possible combination of characters until the correct password is guessed. The more complex and lengthy the password, the more time it takes. While very effective against short passwords, modern systems often implement account lockouts or throttling to mitigate these attacks.

2. Dictionary Attack

Instead of random combinations, this method uses a list of predefined words and common passwords. Attackers assume users may pick simple words from the dictionary. This method is faster than brute force but ineffective against strong, random passwords.

3. Credential Stuffing

This uses credentials leaked from other websites. Since many users reuse passwords across platforms, an attacker can gain unauthorized access to different accounts without guessing. It's a type of replay attack.

4. Phishing

Tricking users into entering their credentials into fake websites or forms via deceptive emails, SMS, or calls. Once captured, attackers use these credentials immediately. Social engineering plays a major role here.

5. Keylogging
A malicious program records a user’s keystrokes, capturing passwords as they are typed. This malware can be installed via infected downloads, USB devices, or email attachments.

6. Man-in-the-Middle (MitM) Attack
An attacker secretly intercepts communication between two parties. For example, if a user logs in on an unsecured Wi-Fi network, the attacker can capture transmitted credentials unless the data is encrypted (e.g., via HTTPS).

7. Rainbow Table Attack
Attackers use precomputed tables of hashed passwords and compare them against stolen hashed passwords. This method is fast but mitigated by using salted hashes (adding a random string to each password before hashing).

8. Social Engineering
Rather than attacking technology, this attack targets human psychology. Attackers impersonate tech support, coworkers, or authority figures to trick users into revealing passwords over phone or email.

9. Shoulder Surfing
The attacker simply observes the victim typing their password. It can happen in public places, cafes, airports, or even office spaces.

10. Password Spraying
Unlike brute force, which tries many passwords on one account, password spraying attempts one common password on many accounts. This bypasses account lockout mechanisms and exploits weak, shared passwords.

Additional Knowledge on Password Security

In today’s cybersecurity landscape, relying solely on strong passwords is no longer sufficient. Modern systems implement **multi-factor authentication (MFA)** to add an additional layer of defense. MFA combines something the user **knows** (like a password), with something they **have** (like a smartphone or hardware token), or something they **are** (such as a fingerprint or facial recognition). This significantly reduces the risk of unauthorized access, even if a password is compromised.

When storing passwords, secure systems do not save them in plain text. Instead, they use **cryptographic hashing algorithms** to convert passwords into unreadable strings of characters. Advanced algorithms like **bcrypt**, **scrypt**, and **Argon2** are designed specifically for password hashing. These algorithms also apply a **salt**, which is a unique random value added to each password before hashing. Salting ensures that identical passwords result in different hash values, protecting against **rainbow table attacks** (precomputed tables of hash values used to crack passwords).

Furthermore, many organizations are adopting **Zero Trust Architecture (ZTA)** as a security framework. ZTA operates on the principle of "never trust, always verify," meaning that **no user, device, or network segment is inherently trusted**, even if it is inside the corporate perimeter. In a Zero Trust model, systems continuously verify identities and require regular reauthentication to minimize the risk of breaches from compromised credentials or insider threats.

In summary, modern password security incorporates MFA, secure password storage using salted hashes with specialized algorithms, and is reinforced by Zero Trust principles to ensure robust, layered protection of digital assets.

Summary and Recommendations

- Use passwords that are at least 12–16 characters long and include a mix of uppercase, lowercase, numbers, and special characters.
- Avoid reusing passwords across sites or services and Enable multi-factor authentication
- Stay informed about recent data breaches and security news to keep your accounts protected.