Elevate Labs
Cybersecurity Internship Report

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

Submitted by: Namita Rana

Role: Cybersecurity Intern

Company: Elevate Labs

Date of Submission: 12 August 2025

Privacy and Ethical Considerations

When creating and evaluating passwords for this task, it is essential to prioritize both privacy and ethical guidelines to ensure that no sensitive information is compromised. All passwords generated and tested during this exercise must be fictional and created solely for demonstration purposes. Under no circumstances should real passwords, which protect personal accounts, banking services, or work systems, be used. Using genuine credentials in online tools carries the risk of theft or misuse, particularly if the service logs user input.

It is equally important to use only trusted and secure password strength checkers. Tools from reputable sources that clearly state their privacy policies should be chosen, and wherever possible, offline tools should be preferred to minimize the risk of interception. Any passwords recorded in this report should be dummy examples, and screenshots or data containing sensitive information should never be included. Furthermore, the final report file should be stored securely, especially if it contains any form of test results that could be misused.

All activities in this task must align with ethical and legal standards. Cybersecurity practices should follow responsible guidelines recommended by recognized bodies such as (ISC)², ISACA, or OWASP, and comply with applicable privacy laws, including the General Data Protection Regulation (GDPR) and the Information Technology Act in India. No passwords should be collected, tested, or shared without the explicit consent of their owners. Similarly, testing should never involve phishing, guessing, or retrieving passwords from real users, as these methods violate both ethical and legal principles.

Finally, the purpose of this activity is to educate and raise awareness about creating strong passwords, not to exploit security weaknesses. By ensuring that all testing is carried out with fictional credentials, secure tools, and respect for user privacy, this exercise remains a safe, legal, and valuable learning experience.

Acknowledgement

I would like to express my sincere gratitude to my instructor and guide for providing the opportunity to work on this task, *"**Create a Strong Password and Evaluate Its Strength.**"* This activity has helped me gain a deeper understanding of password security, evaluation techniques, and the importance of following best practices for protecting digital information.

I am thankful for the valuable resources and tools made available for conducting the password strength tests, as well as for the guidance that encouraged me to approach this exercise with a strong emphasis on privacy, security, and ethical responsibility. I also appreciate the availability of online password strength checkers, which enabled me to analyse and compare different password complexities effectively.

This task has not only enhanced my technical knowledge but also strengthened my awareness of the ethical considerations involved in cybersecurity practices. I am grateful to all those who supported me during the completion of this work.

— Namita Rana

Table of Content

Chapter 1 – Introduction

1.1 Objective of the Task

The primary objective of this task is to understand the process of creating strong, secure passwords and evaluating their strength using password testing tools. Passwords are the first line of defense in protecting digital identities, online accounts, and sensitive data. Through this activity, the aim is to explore how varying levels of complexity—such as length, character diversity, and unpredictability—impact password strength. By testing and comparing passwords of different complexities, the task also seeks to highlight the importance of adopting strong password practices in real-world cybersecurity.

The task involves generating multiple sample passwords, evaluating them using trusted password strength checkers, analysing the results, and identifying factors that influence password resilience against common attacks. It also focuses on understanding password creation best practices to minimize the risk of compromise.

1.2 Importance of Strong Passwords in Cybersecurity

In today's digital world, where most personal and professional activities are carried out online, passwords play a critical role in safeguarding information. Weak or easily guessable passwords are one of the leading causes of data breaches and unauthorized access. Cybercriminals often exploit predictable patterns, short lengths, and reused passwords through techniques such as brute force attacks, dictionary attacks, and credential stuffing.

Strong passwords—those that are sufficiently long, include a mix of uppercase and lowercase letters, numbers, and special symbols, and avoid common words—are significantly more resistant to such attacks. Implementing strong password policies not only enhances individual account security but also contributes to the overall cybersecurity posture of organizations. By understanding what makes a password strong and testing various examples, this task reinforces the role of password complexity and unpredictability in defending against cyber threats.

Chapter 2 – Tools and Resources Used

2.1 Password Strength Checker Websites

Evaluating the strength of a password requires specialized tools that can simulate the logic attackers use to guess or crack passwords. For this task, only reputable and widely trusted password testing platforms were used to ensure accuracy and reliability of results. These tools not only assess the overall strength of a password but also provide feedback and recommendations for improvement.

1. **Password Meter** – https://passwordmeter.com
    - This tool uses a scoring system where the password is rated based on multiple parameters, including length, presence of different character types, and absence of predictable patterns.
    - It provides both a numerical score and a qualitative assessment (Weak, Good, Strong).
    - Detailed feedback is given for each password, highlighting strengths and weaknesses.
2. **How Secure Is My Password?** – https://www.security.org/how-secure-is-my-password/
    - This platform estimates the amount of time a brute force attack would take to crack the given password.
    - It displays results in a highly visual and easy-to-understand format, making it useful for awareness purposes.
    - While it does not provide as many granular details as Password Meter, its main value lies in showing a clear time-based risk assessment.

Both tools were chosen because they are publicly accessible, do not require account registration, and are widely used for educational and research purposes. Furthermore, both platforms clearly state that they do not store or misuse entered passwords, making them safe for use in a controlled, academic environment.

2.2 Evaluation Criteria

To ensure consistency and fairness in assessing each password, a fixed set of evaluation parameters was used. These parameters align with established cybersecurity standards and password policy recommendations from organizations like NIST (National Institute of Standards and Technology) and OWASP (Open Web Application Security Project).

1. **Length** – The total number of characters in the password. Longer passwords generally provide exponentially greater resistance to brute force attacks. For example, an 8-character password has far fewer possible combinations than a 14-character password, making it much easier to crack.

2. **Character Variety** – The inclusion of different types of characters:
    - **Uppercase Letters** (A–Z)
    - **Lowercase Letters** (a–z)
    - **Numbers** (0–9)
    - **Special Symbols** (!, @, #, $, %, &, etc.)
      A password that combines all four types of characters is typically stronger than one that uses only letters or only numbers.
3. **Predictability** – The degree to which a password follows common or easily guessable patterns. Examples of high-predictability passwords include "123456," "qwerty," "password," or names and birthdates. The less predictable a password is, the harder it is for attackers to guess it using dictionary attacks or social engineering.
4. **Estimated Time to Crack** – The projected duration it would take for a password to be cracked using brute force methods. This figure varies based on computing power, but the tools used provide an estimated time based on standard assumptions about attacker resources.
5. **Tool Feedback** – Recommendations provided by the testing platforms. For example, a tool may suggest increasing length, adding special characters, or avoiding repetitive sequences.

By applying these evaluation criteria consistently across all test cases, it was possible to draw clear comparisons between weak, medium, and strong passwords, and to identify the specific factors that contribute to password security.

Chapter 3 – Password Creation Process

3.1 Levels of Complexity Considered

To analyse password strength comprehensively, five distinct levels of complexity were considered. Each level was defined based on password length, character variety, predictability, and randomness. This approach made it possible to assess the gradual improvement in security as complexity increased.

1. **Very Weak Passwords** –
    - **Characteristics:** Short (4–6 characters), made of only letters or only numbers, often based on personal names, birthdays, or common sequences.
    - **Security Risk:** Extremely vulnerable to brute force and dictionary attacks; can often be guessed manually.
    - **Example:**
        - hacker
2. **Weak Passwords** –
    - **Characteristics:** Slightly longer (6–8 characters), uses letters and numbers, but follows predictable patterns or uses common words.
    - **Security Risk:** Can be cracked in seconds or minutes with automated tools.
    - **Example:**
        - hacker777
3. **Moderate Passwords** –
    - **Characteristics:** 8–10 characters, includes mixed case letters and numbers, may have one special character, but still contains some predictable elements.
    - **Security Risk:** Harder to guess than weak passwords but still crackable in hours or days with advanced tools.
    - **Example:**
        - Hacker@777
4. **Strong Passwords** –
    - **Characteristics:** 12–14 characters, contains uppercase and lowercase letters, numbers, and multiple special symbols, with no dictionary words.
    - **Security Risk:** Highly resistant to brute force and dictionary attacks; estimated cracking time can range from years to centuries depending on attacker resources.

- **Example:**
  - Hacker#777!NotSafe

5. **Very Strong Passwords –**
   - **Characteristics:** 15+ characters, fully random sequence of uppercase and lowercase letters, numbers, and special symbols; no readable patterns or words.
   - **Security Risk:** Nearly impossible to crack within a reasonable time frame with current technology; best suited for highly sensitive accounts.
   - **Example:**
     - X9!pQr7@LmT2$wZ^5

3.2 Examples of Created Passwords

A set of sample passwords from each complexity level was generated for testing. These passwords were designed purely for this experiment and do not belong to any real account.

Password	Complexity Level	Key Features	Predictability
hacker	Very Weak	Only Lowercase, short length	Very High
hacker777	Weak	Lowercase + numbers, short,	High
Hacker@777	Moderate	Mixed case, symbol, numbers	Medium
Hacker#777!NotSafe	Strong	Long, mixed case, multiple symbols, numbers	Low
X9!pQr7@LmT2$wZ^5	Very Strong	Fully random, long, multiple character types	Very Low

These passwords were then evaluated using the tools described in Chapter 2 to measure their resistance to different attack methods and estimate the time required for cracking.

Chapter 4 – Password Strength Testing

4.1 Testing Methodology

The password strength testing process was conducted using a combination of automated and manual tools to assess the robustness of different password formats. The primary tool used was an **online password strength meter**, which evaluates passwords based on criteria such as length, complexity, entropy, and resistance to brute-force attacks.

The methodology followed the steps below:

1. **Password Selection** – A set of passwords was created, each with increasing levels of complexity, ranging from weak to highly secure.
2. **Tool Usage** – Each password was entered into the password strength meter to analyse its score and estimated cracking time.
3. **Complexity Criteria** – Passwords were tested against various factors, including:
    - **Length** (number of characters)
    - **Character Variety** (use of uppercase, lowercase, numbers, symbols)
    - **Unpredictability** (avoidance of common patterns or dictionary words)
4. **Result Documentation** – Strength scores, feedback, and cracking time estimates provided by the tool were recorded for comparison.
5. **Other Tools** – In addition to the password strength meter, supplementary tools were used to cross-check results, such as:
    - **How Secure Is My Password** – For estimating crack time via brute force.
    - **KeePass Password Generator** – For generating highly secure passwords.
    - **LastPass Security Challenge** – For evaluating stored passwords' security.

4.2 Test Results and Observations

The results of the password strength testing revealed a clear relationship between complexity and estimated security. Passwords were tested at five levels of complexity:

Complexity Level	Example Password	Estimated Crack Time	Strength Rating

Level 1 – Very Weak	Hacker	Less than 1 second	Weak
Level 2 – Weak	Hacker777	A few seconds	Weak
Level 3 – Medium	Hacker@777	A few minutes	Fair
Level 4 – Strong	Hacker#777!NotSafe	Several years	Strong
Level 5 – Very Strong	X9!pQr7@LmT2$wZ^5	Trillions of years	Very Strong

Observations:

- **Short passwords**, even with numbers, were cracked almost instantly.
- **Adding special characters** and increasing password length significantly improved strength.
- **Randomly generated passwords** with mixed characters provided the highest level of security.
- **Predictable patterns** (e.g., words + numbers) were rated weaker despite their apparent complexity.

In conclusion, the test confirmed that **length, randomness, and character diversity** are the key factors in creating strong passwords. Tools like password strength meters provide quick and accessible ways to evaluate password security, but for maximum protection, users should also follow best practices such as using unique passwords for each account and regularly updating them.

Chapter 5 – Analysis and Findings

5.1 Comparison of Weak, Medium, and Strong Passwords

Password strength is a crucial aspect of cybersecurity, directly influencing how easily a password can be guessed, cracked, or compromised through brute force or dictionary attacks. In this study, passwords were categorized into five complexity levels to better understand their security posture.

Five Levels of Password Complexity:

1. **Level 1 – Very Weak:**
    - Example: hacker
    - Characteristics: Contains only lowercase or capitalized letters, short in length, no numbers or symbols.
    - Vulnerability: Easily cracked within seconds using brute force or dictionary attacks.
2. **Level 2 – Weak:**
    - Example: hacker777
    - Characteristics: Combination of letters and numbers, but still predictable and often found in leaked password databases.
    - Vulnerability: Can be cracked in minutes using hybrid attacks.
3. **Level 3 – Moderate:**
    - Example: Hacker@777
    - Characteristics: Letters, numbers, and a single special character.
    - Vulnerability: Offers slightly more resistance but still susceptible to targeted dictionary attacks.
4. **Level 4 – Strong:**
    - Example: Hacker#777!NotSafe
    - Characteristics: Longer password, multiple special characters, mix of upper/lowercase letters, and numbers.
    - Vulnerability: Resistant to most brute force attacks but can still be exposed if reused or leaked.
5. **Level 5 – Very Strong:**
    - Example: X9!pQr7@LmT2$wZ^5
    - Characteristics: Randomly generated, high entropy, mix of uppercase, lowercase, numbers, and multiple special characters.

- Vulnerability: Extremely difficult to crack without significant computational resources and time.

This comparison reveals that even small improvements in length and character variety can exponentially increase password strength.

5.2 Factors Affecting Password Strength

The strength of a password is influenced by multiple factors that collectively determine its resistance to unauthorized access attempts:

1. **Length:**
   - Longer passwords significantly increase the number of possible combinations, making brute force attacks less feasible.
2. **Character Variety:**
   - Using uppercase letters, lowercase letters, numbers, and special characters adds complexity, reducing predictability.
3. **Predictability:**
   - Avoiding dictionary words, personal information, or common patterns prevents attackers from guessing passwords quickly.
4. **Uniqueness:**
   - A unique password for each account ensures that even if one password is compromised, others remain secure.
5. **Randomness:**
   - Truly random passwords (often generated by password managers) have high entropy and resist pattern-based attacks.
6. **Avoiding Reuse:**
   - Password reuse across accounts increases the risk of credential stuffing attacks after a single data breach.
7. **Regular Updates:**
   - Changing passwords periodically limits the time window for attackers to exploit compromised credentials.

Conclusion:
The analysis confirms that password security is not just about adding special characters—it is the combination of length, randomness, unpredictability, and uniqueness that ensures maximum resilience against cyber threats.

Chapter 6 – Best Practices for Creating Strong Passwords

In today's cybersecurity landscape, password security remains one of the most critical factors in protecting personal, corporate, and financial data. The following best practices ensure that passwords are not only strong but also resistant to modern hacking techniques.

6.1 Length and Complexity

The strength of a password significantly depends on its length and complexity.

- **Recommended Length**: At least **12–16 characters** for general accounts; **20+ characters** for critical accounts such as banking or administrative access.
- **Complexity Requirements**: Include a mix of uppercase letters, lowercase letters, numbers, and special characters.
- Longer passwords exponentially increase the time required for brute-force attacks to succeed.
- Example:
    - Weak: hacker
    - Strong: X9!pQr7@LmT2$wZ^5

6.2 Use of Special Characters and Case Variations

- Incorporating **special symbols** (! @ # $ % ^ & * ( ) _ +) makes passwords harder to guess.
- **Case variations** (mixing uppercase and lowercase letters) add another layer of complexity.
- Avoid placing symbols only at the end of a password, as this is a common user habit that attackers expect.
- Example progression:
    1. hacker – all lowercase, weak.
    2. Hacker777 – adds capitalization and numbers, moderate.
    3. Hacker@777 – includes a special character, stronger.
    4. Hacker#777!NotSafe – strong but still predictable.
    5. X9!pQr7@LmT2$wZ^5 – strong and random, highly secure.

6.3 Avoiding Predictable Patterns

- Do not use **dictionary words**, **birthdates**, **phone numbers**, or **keyboard patterns** like qwerty or 123456.
- Avoid predictable substitutions (e.g., replacing "A" with "@", "E" with "3") as attackers' tools account for these.
- Randomized sequences of unrelated characters, numbers, and symbols are far harder to crack.
- Example of bad predictable pattern: Password123!
- Example of good unpredictable password: 9v@J7$eW2!pX#Zk3

6.4 Using Password Managers

- Password managers such as **Bitwarden**, **LastPass**, **1Password**, and **KeePass** can securely generate and store unique passwords for every account.
- Benefits:
    - Eliminates the need to remember multiple complex passwords.
    - Reduces password reuse across sites (a major security risk).
    - Can generate extremely long, random passwords impossible to remember manually.
- Example: Instead of memorizing nT4^u2L$wZ!kR7p8, store it in a password manager for auto-fill functionality.

Summary:
By following these practices—emphasizing length, complexity, special characters, avoiding patterns, and using password managers—you can significantly strengthen password security, reducing the risk of compromise from brute-force or guessing attacks.

Chapter 7 – Common Password Attacks

Password security is constantly challenged by various attack methods used by malicious actors to gain unauthorized access to systems, networks, and accounts. Understanding these attack types is essential for building effective defenses. This chapter explains some of the most common password attacks and how they operate.

7.1 Brute Force Attacks

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

Key Characteristics:

- **Speed vs. Complexity:** Short and simple passwords can be cracked within seconds, while long and complex passwords significantly increase the time required.
- **Automation:** Tools such as *Hydra*, *John the Ripper*, and *Hashcat* can automate and speed up the attack process.
- **Defensive Measures:**
    - Enforce strong password policies (minimum 12–16 characters with varied complexity).
    - Implement account lockout after multiple failed attempts.
    - Use CAPTCHA or multi-factor authentication (MFA).

Example Scenario:
A password like pass123 may be cracked in less than a second, whereas X9!pQr7@LmT2$wZ^5 could take billions of years with standard computing power.

7.2 Dictionary Attacks

Dictionary attacks involve using a predefined list of commonly used words, passwords, or leaked credentials to guess the correct password.

Key Characteristics:

- **Wordlist-Based:** Attackers rely on lists containing millions of common passwords (e.g., *rockyou.txt*).
- **Speed:** Much faster than brute force because it avoids testing random combinations.
- **Defensive Measures:**
    - Avoid using real words, phrases, or predictable sequences.

- Combine words with numbers, symbols, and case variations.
- Regularly check credentials against known breach databases.

Example Scenario:
If a user's password is Hacker777, it could be found quickly since such combinations often appear in password dumps.

7.3 Credential Stuffing

Credential stuffing uses stolen username-password pairs from one breached site to gain access to accounts on other platforms.

Key Characteristics:

- **Exploits Password Reuse:** Many people reuse the same password across multiple accounts.
- **Automation:** Bots are used to attempt logins across multiple services simultaneously.
- **Defensive Measures:**
  - Use unique passwords for every account.
  - Enable MFA on all critical accounts.
  - Monitor for login attempts from unusual IP addresses.

Example Scenario:
If user@example.com and Hacker@777 are leaked from a shopping site, attackers might try the same credentials on email, social media, or banking platforms.

7.4 Social Engineering Risks

Social engineering attacks manipulate human behaviour to obtain confidential information, including passwords, without needing to technically "crack" them.

Key Characteristics:

- **Methods:**
  - **Phishing:** Fake emails or websites tricking users into entering credentials.
  - **Pretexting:** Creating a fabricated scenario to request passwords.
  - **Shoulder Surfing:** Observing someone typing their password.
- **Defensive Measures:**
  - User awareness training on phishing and scam techniques.
  - Avoid sharing credentials verbally, over email, or in unsecured chats.

- Use MFA so that stolen passwords alone are not enough for access.

Example Scenario:
An attacker sends a fake “security alert” email prompting the user to log in to a counterfeit banking website, capturing their password in the process.

Chapter 8 – Tips and Recommendations

This chapter provides practical, actionable guidance for individuals and organizations to strengthen password security. By implementing these tips, users can significantly reduce the risk of unauthorized access, data breaches, and other cyber threats.

8.1 Practical Steps for Stronger Passwords

To ensure robust password protection, the following measures should be followed:

1. **Choose Longer Passwords**
    - Aim for a minimum of **12–16 characters**.
    - Each additional character increases the difficulty of brute-force attacks exponentially.
2. **Incorporate Multiple Character Types**
    - Use a combination of uppercase and lowercase letters, numbers, and special characters.
    - Example: T!gr#S1un$et20
3. **Avoid Reusing Passwords Across Accounts**
    - If one account is compromised, reused credentials can expose multiple accounts to attacks.
    - Each account should have a unique password.
4. **Implement Passphrases**
    - Create memorable yet complex sentences.
    - Example: "BlueSkies&Coffee@7AM"
5. **Utilize Two-Factor Authentication (2FA)**
    - Adds a secondary verification layer, such as an OTP or authentication app.
    - Even if the password is leaked, 2FA can prevent unauthorized access.
6. **Avoid Personal Information**
    - Never use easily guessable details like birthdays, pet names, or phone numbers.
    - Hackers often use social media to guess such data.

8.2 Periodic Review and Updates

Maintaining password security is not a one-time task. Regular review and updates are crucial.

1. **Change Passwords Regularly**
    - Update every 3–6 months, especially for sensitive accounts like banking, emails, and corporate portals.
2. **Update Immediately After a Breach**
    - If you suspect a security breach or receive a breach notification, change affected passwords without delay.
3. **Use a Password Manager for Maintenance**
    - Tools like Bitwarden, LastPass, or 1Password help store and organize passwords securely.
    - These tools can also generate strong, unique passwords automatically.
4. **Audit Password Strength Periodically**
    - Use security tools to assess password strength and detect weak or reused credentials.
5. **Stay Informed About New Threats**
    - Cybersecurity threats evolve rapidly; regularly follow trusted sources like **CISA**, **NIST**, or reputable security blogs to update password practices.

Summary:

By following these practical steps and maintaining a consistent update schedule, individuals and organizations can dramatically improve their password security posture. Strong password practices, combined with multi-layered authentication, significantly reduce the likelihood of a successful attack.

Chapter 9 – Conclusion

9.1 Summary of Key Learnings

This project provided a comprehensive understanding of password strength, the importance of secure credential management, and the methods used to evaluate password security. Through practical testing using password strength meters and other evaluation tools, the following key learnings were identified:

1. **Password Length is Critical** – Longer passwords significantly increase resistance to brute-force and dictionary attacks. A minimum of 12–16 characters is recommended for strong protection.
2. **Complexity Enhances Security** – Combining uppercase and lowercase letters, numbers, and special characters creates more difficult combinations for attackers to guess.
3. **Avoiding Predictability is Essential** – Common patterns, sequences, or personal information (e.g., birthdays, names) drastically reduce password strength.
4. **Password Reuse is Risky** – Using the same password across multiple accounts makes all accounts vulnerable if one is compromised.
5. **Tools Aid Awareness** – Password strength meters, password managers, and cybersecurity best practices play a vital role in educating users about security.
6. **Human Factors Matter** – Weak passwords often result from user convenience over security, highlighting the need for ongoing awareness and training.

9.2 Final Thoughts on Password Security

Password security is a cornerstone of digital safety in both personal and professional environments. With cyber threats evolving rapidly, relying solely on basic password practices is no longer sufficient. Attackers now use advanced tools, massive datasets of breached credentials, and AI-powered guessing methods to compromise accounts within minutes if passwords are weak.

To maintain strong password hygiene, users must:

- Create **unique, complex passwords** for every account.
- Use **password managers** to handle multiple secure credentials without relying on memory alone.
- Perform **periodic password audits** to detect and replace outdated or compromised passwords.
- Stay updated on **emerging cyber threats** and adapt password strategies accordingly.

Ultimately, password security is not a one-time action but an **ongoing commitment**. As technology advances, so must our defense mechanisms. By following the best practices outlined in this report, individuals and organizations can significantly reduce the risk of unauthorized access, safeguard sensitive data, and strengthen overall cybersecurity posture.
