Cyber Security Internship – Task 6

Task Name: Create a Strong Password and Evaluate Its Strength

Name: Bhayani Dev
Date: 30 June 2025

Objective

To understand what makes a password strong by creating multiple passwords with varying complexity, testing them using an online password strength checker, analyzing feedback, and learning best practices to avoid weak passwords and common attacks like brute force or dictionary attacks.

Tools Used

- Website: https://passwordmeter.com
- Screenshots captured from each test

- Manual review of security feedback

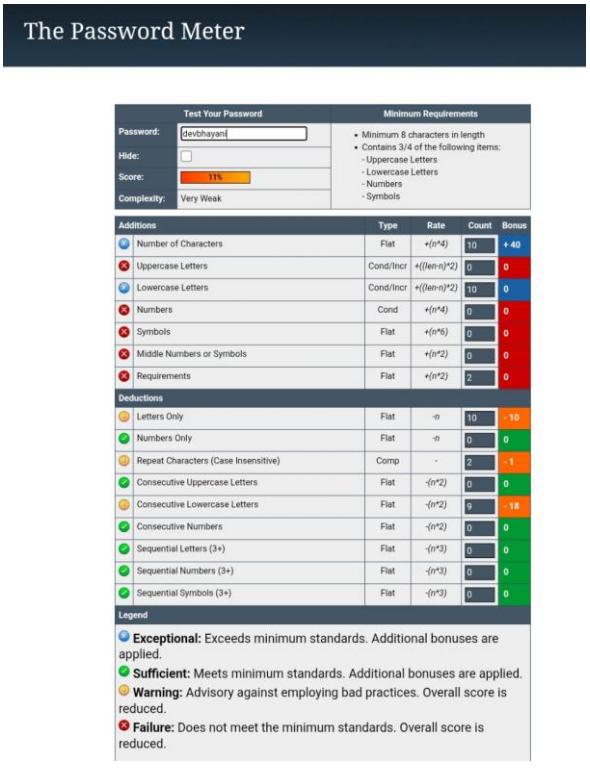
Password Testing and Evaluation

I created and tested five different passwords ranging from very weak to very strong. Below are the full details:

Cyber Security Internship – Task 6

☑ 1. Password: DevBh@y@ni_123

- **Score**: **100%**
- **Complexity**: **Very Strong**
- **Feedback**:
    1. Excellent variety – includes uppercase, lowercase, numbers, and symbols.
    2. Satisfies all minimum requirements (5/5 criteria met).
    3. High character count (14) adds bonus.
- **Result**: **Exceptional**
- **Conclusion**: This password is highly secure. It exceeds minimum standards and is ideal for protecting sensitive accounts. ☑



The Password Meter

Test Your Password		Minimum Requirements
Password:	devbhayani	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	11%	
Complexity:	Very Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	10	+ 40
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	10	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	2	0
Deductions				
Letters Only	Flat	-n	10	- 10
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	9	- 18
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

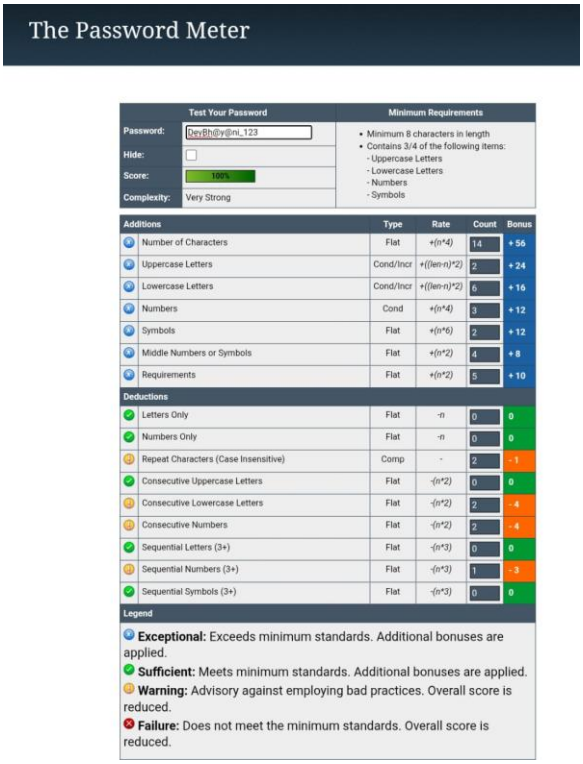
Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Cyber Security Internship – Task 6

☑ 2. Password: Dev@i123

- **Score**: **65%**
- **Complexity**: **Strong**
- **Feedback**:
    1. Good combination of letter cases, numbers, and one symbol.
    2. Fulfills required character types but still has room for improvement (only 7 characters).
    3. Deductions from use of consecutive lowercase and numbers.
- **Result**: **Sufficient**
- **Conclusion**: This is a fairly strong password. Adding more unique symbols and increasing length will make it stronger. 👍



The Password Meter

Test Your Password		Minimum Requirements
Password:	DevBh@y@ni_123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 24
Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 16
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	2	+ 12
Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

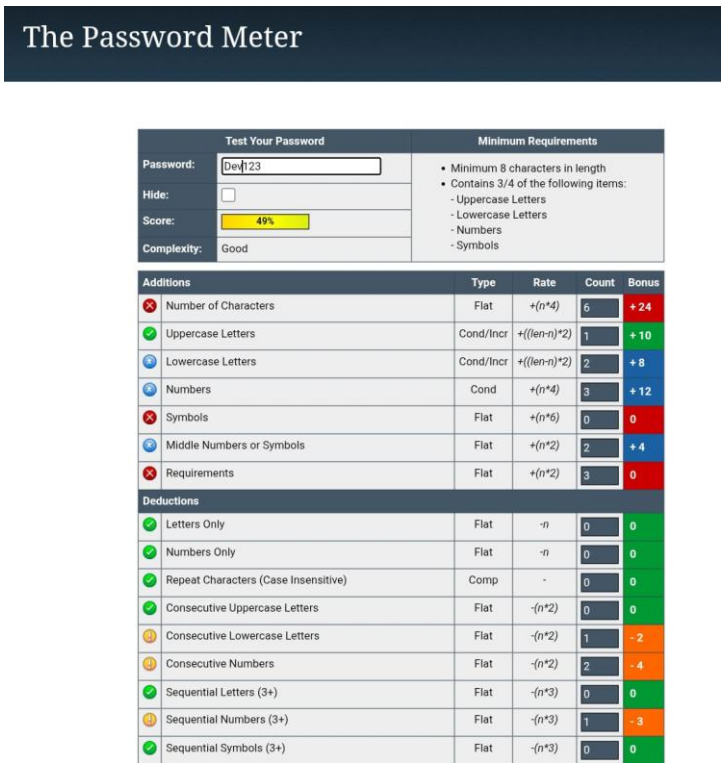
Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Cyber Security Internship – Task 6

⚠ 3. Password: Dev123

- **Score**: **49%**
- **Complexity**: **Good**
- **Feedback**:
    1. Uses upper and lowercase letters, and numbers.
    2. Lacks symbols and is too short (only 6 characters).
    3. Several deductions due to consecutive letters and numbers.
- **Result**: **Warning**
- **Conclusion**: It's better than average, but not good enough for secure use. Add symbols and increase the length to improve. ⚠



The Password Meter

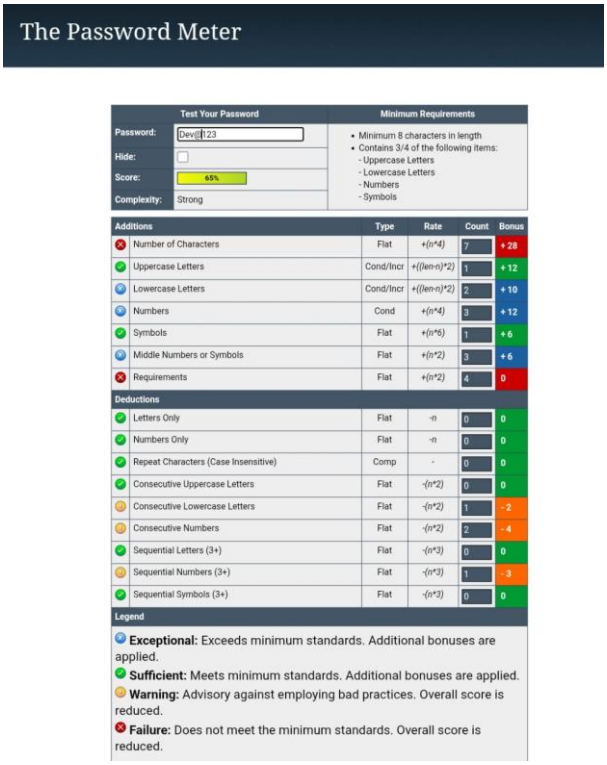
Test Your Password		Minimum Requirements
Password:	Dev123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	49%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	6	+ 24
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 10
Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 8
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Cyber Security Internship – Task 6

❌ 4. Password: devbhayan

- **Score**: **11%**
- **Complexity**: **Very Weak**
- **Feedback**:
    1. Only lowercase letters – no variety.
    2. Deductions due to repetition and lack of character types.
    3. Meets length but fails complexity standards.
- **Result**: **Failure**
- **Conclusion**: Highly insecure password. Needs uppercase, numbers, and symbols. Should not be used in its current form. ❌



The Password Meter

Test Your Password		Minimum Requirements
Password:	Devbh123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	65%	
Complexity:	Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	7	+ 28
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 12
Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 10
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	4	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	1	- 2
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

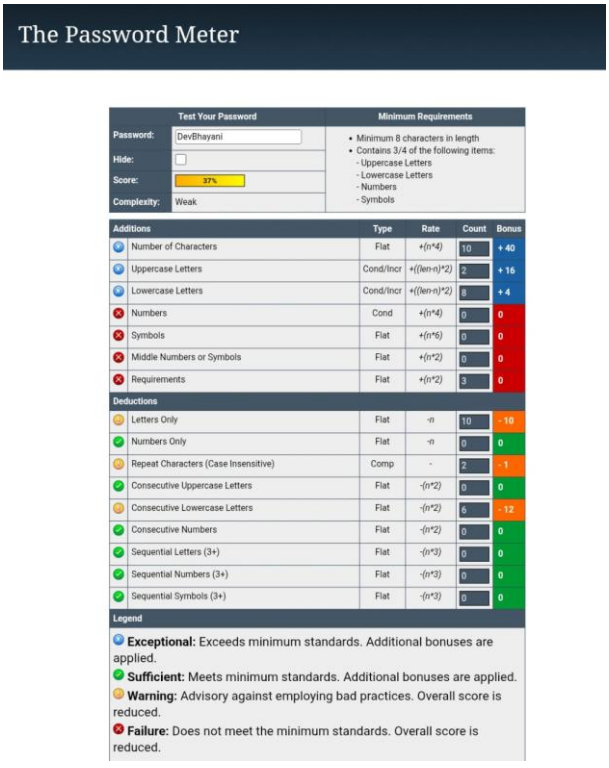
Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Cyber Security Internship – Task 6

❌ 5. Password: DevBhayani

- **Score**: **37%**
- **Complexity**: **Weak**
- **Feedback**:
    1. Contains both uppercase and lowercase letters.
    2. Lacks numbers and symbols.
    3. Consecutive lowercase letters cause deduction.
- **Result**: **Failure**
- **Conclusion**: Slightly better than lowercase-only passwords, but still insecure. Add numbers and symbols to strengthen. ❌



The Password Meter

Test Your Password		Minimum Requirements
Password:	DevBhayani	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	37%	
Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	10	+ 40
Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 4
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	10	- 10
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	2	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
Consecutive Numbers	Flat	-(n*2)	0	0
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	0	0
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Cyber Security Internship – Task 6

Here's a **summary table** comparing all the passwords from the screenshots:

#	Password	Score	Complexity	Result	Key Issues / Strengths
1	DevBh@y@ni_123	100%	Very Strong	☑ Exceptional	Long, uses upper/lowercase, numbers, symbols, satisfies all requirements
2	Dev@i123	65%	Strong	☑ Sufficient	Good mix; lacks more length and has consecutive characters
3	Dev123	49%	Good	⚠ Warning	Too short, no symbols, consecutive patterns
4	devbhayan	11%	Very Weak	✗ Failure	Only lowercase letters, lacks complexity, repetitive
5	DevBhayani	37%	Weak	✗ Failure	No numbers or symbols, some variety but not enough

---

Conclusion:

- **Best Password**: DevBh@y@ni_123 (very strong and secure)
- **Minimum Acceptable**: Dev@i123 (decent for moderate protection)
- **Needs Improvement**: All others, especially devbhayan and DevBhayani – too weak for real use.

Key Tips Learned from Evaluation

- Always use a **minimum of 8–12 characters** for strength.
- Mix **uppercase, lowercase, numbers, and special characters**.
- Avoid using personal names or easily guessed combinations.
- **Passphrases** like `Sunny@Night#2025` are easy to remember yet secure.
- **Avoid repeating characters** or common patterns (e.g., `123`, `abc`).
- Password strength greatly improves with **symbol placement and randomness**.

Cyber Security Internship – Task 6

Common Password Attacks

---

1. Brute Force Attack

Definition:
A brute force attack systematically tries **every possible combination** of characters until it finds the correct password.

How it works:

- Attackers use automated scripts or tools (like Hydra, John the Ripper, or Hashcat).
- It tries `a`, then `aa`, `ab`, `abc`, and so on until the correct password is found.
- Short and simple passwords are cracked **very quickly**.

Defence:

- Use **long and complex passwords** (e.g., 12+ characters).
- Implement **account lockouts** after failed login attempts.
- Enable **multi-factor authentication (MFA)**.

---

2. Dictionary Attack

Definition:
This attack uses a predefined **list of commonly used words or leaked passwords** to guess a password.

How it works:

- The attacker tries passwords like `password`, `123456`, `welcome`, `qwerty`, etc.
- They use large "dictionary files" created from real leaked databases.

Defense:

- Avoid using **common words, names, or patterns**.
- Don’t use simple variations like `Password123!`.
- Use **randomized characters or passphrases** instead.

Cyber Security Internship – Task 6

How Password Complexity Affects Security – Summary

Password complexity plays a **crucial role** in protecting against cyberattacks like brute force, dictionary attacks, and credential stuffing. A complex password is harder to guess, slower to crack, and less likely to be found in leaked databases.

Key Factors of Complexity:

1. **Length:**
   - Longer passwords take exponentially more time to crack.
   - Minimum recommended: **12+ characters**.
2. **Character Variety:**
   - Use a mix of:
     - Uppercase (A–Z)
     - Lowercase (a–z)
     - Numbers (0–9)
     - Symbols (@, #, $, etc.)
   - Increases the number of possible combinations.

3. **Unpredictability:**
   - Avoid names, dictionary words, and keyboard patterns. ○ Use **random phrases** or symbol substitutions (e.g., `@` for `a`).

Why Complexity Matters:

Without Complexity	With Complexity
Easy to guess/crack	Difficult to guess or automate
Vulnerable to dictionary attacks	Resistant to brute force
Found in leaked data	Unique and safer

Example:

- **Weak:** `password123` (easy to guess, short, common)

- **Strong:** `T!m3@R!ver_2025` (long, complex, unique)

Conclusion

This task helped me understand how small changes in a password's structure (length, character variety, and symbols) drastically affect its strength. Tools like PasswordMeter give great feedback on password quality, and this evaluation reinforced why **strong passwords are critical to cyber defence**.

Now I can confidently:

- Build secure passwords
- Analyse weaknesses
- Educate others about password safety
- Avoid common traps that lead to credential leaks
