

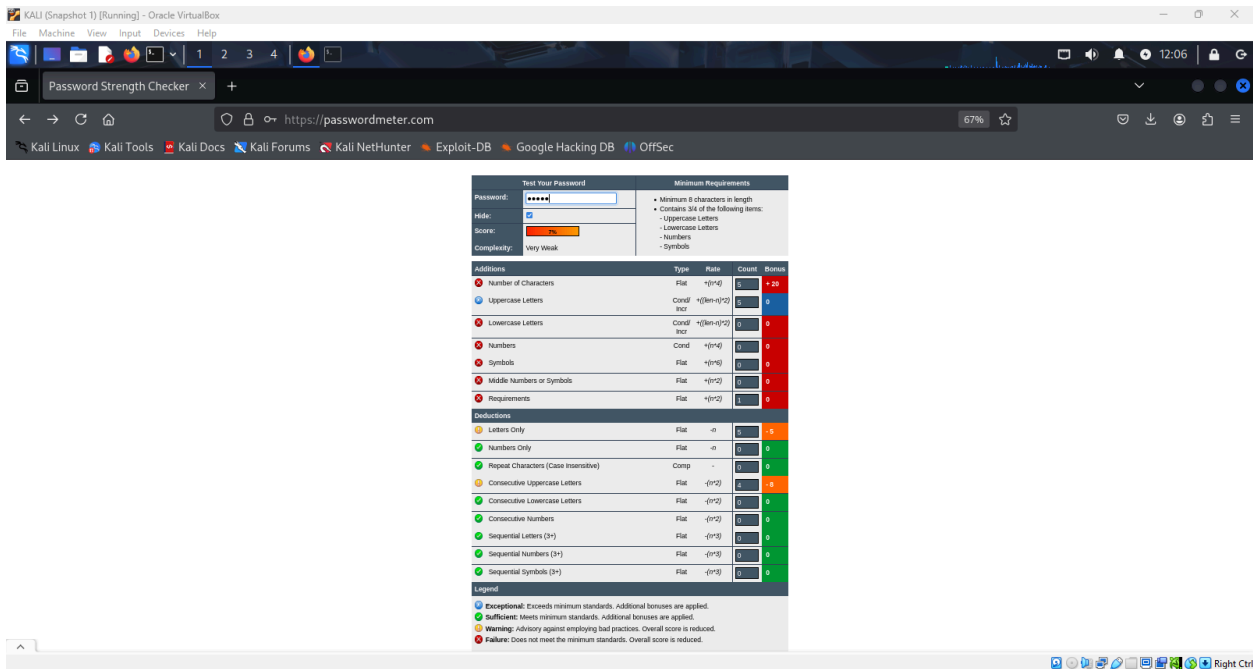
Password Strength Evaluation Report

Cybersecurity Internship

Reported by Thumma Kiranmai

Date: June 03, 2025

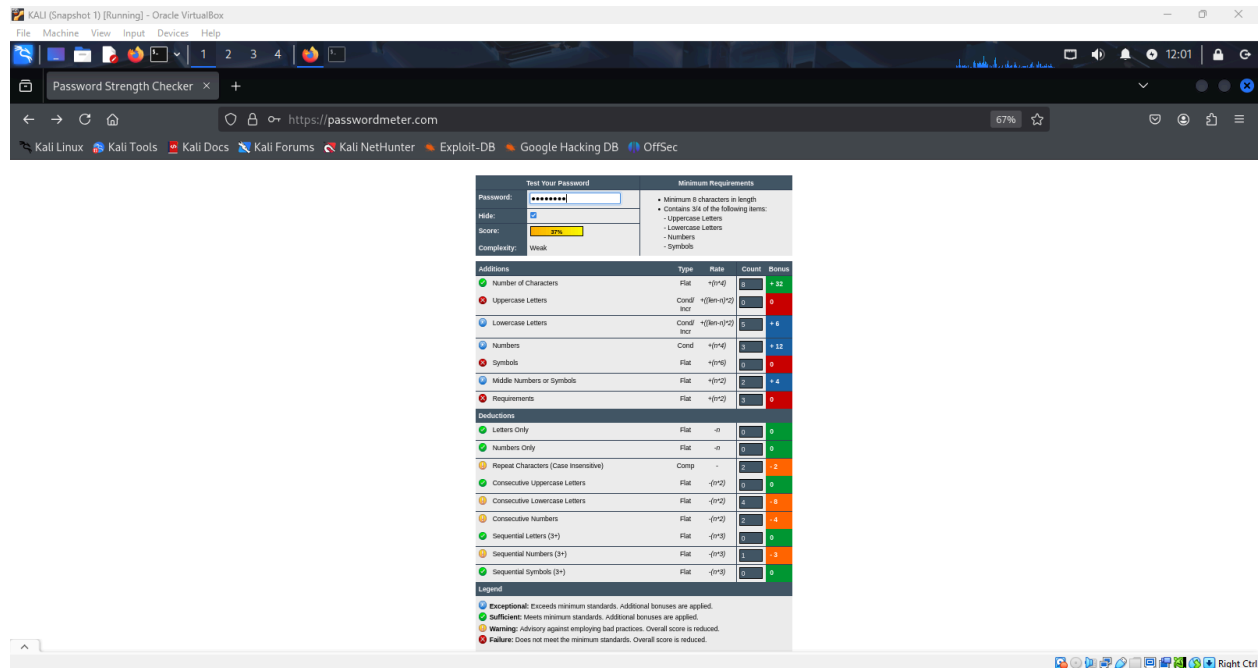
Password admin



- **Score: 7% (Very Weak)**
- **Additions:**
 - Only 5 characters → Minimal bonus for length (+20).
 - Only contains **lowercase letters**.
- **Deductions:**
 - Letters only → -5 points.
 - Fails most requirement checks (no uppercase, numbers, symbols, etc.).

Conclusion: A very basic and insecure password. Easily guessable and doesn't meet most minimum security criteria.

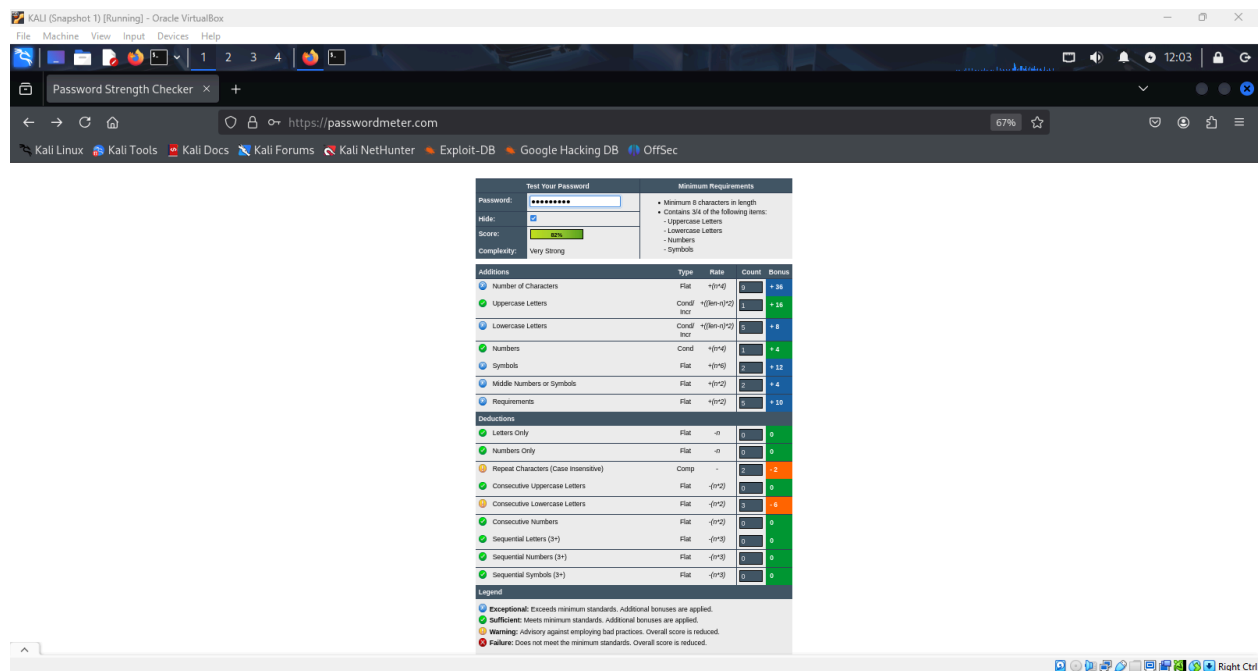
Password **hello123**



- **Score:** 37% (Weak)
- **Additions:**
 - 8 characters long → Moderate bonus (+32).
 - Contains lowercase letters (+6) and numbers (+12).
 - Passes minimum requirements (+4).
- **Deductions:**
 - Contains repeated characters and consecutive lowercase letters (e.g., **ll**, **lo**) → total of -10 points.

Conclusion: A bit stronger due to the mix of letters and numbers, but still weak. Could be brute-forced or guessed.

Password P@ssw0rd!



- **Score:** 82% (Very Strong)
- **Additions:**
 - 9 characters long (+36).
 - Mix of uppercase (P), lowercase (sswrd), number (0), and symbols (@, !) → Large bonus from complexity.
 - Meets all minimum requirements (+10).
- **Deductions:**
 - A minor penalty for a repeated character and consecutive lowercase letters (e.g., ss) → -8 total.

Conclusion: A **very strong password**, thanks to length and complexity. Despite slight repetition, it performs well.

Password Example: h@ckm3n0w!

The screenshot shows a Kali Linux virtual machine with a web browser open to <https://passwordmeter.com>. The password 'h@ckm3n0w!' is entered and analyzed. The score is 78%, categorized as 'Strong'. The analysis shows 9 additions (uppercase, lowercase, numbers, symbols) and 2 deductions (repeated characters 'ss' and consecutive lowercase letters).

Category	Item	Type	Rate	Count	Bonus
Additions	Number of Characters	Flat	+10	10	+40
	Uppercase Letters	Cond	+10	1	+8
	Lowercase Letters	Cond	+10	1	+8
	Numbers	Cond	+10	1	+8
	Symbols	Flat	+10	1	+12
Deductions	Middle Numbers or Symbols	Flat	-10	1	-6
	Requirements	Flat	+10	1	+6
Predictability	Letters Only	Flat	-10	1	-6
	Numbers Only	Flat	-10	1	-6
	Repeat Characters (Case Insensitive)	Comp	-10	1	-6
	Consecutive Uppercase Letters	Flat	-10	1	-6
	Consecutive Lowercase Letters	Flat	-10	1	-6
	Consecutive Numbers	Flat	-10	1	-6
	Sequential Letters (2+)	Flat	-10	1	-6
	Sequential Numbers (2+)	Flat	-10	1	-6
	Sequential Symbols (2+)	Flat	-10	1	-6
	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.				

- **Score**

78% – Strong

A strong password with good complexity and structure.

- **Additions**

9 characters with uppercase, lowercase, numbers, and symbols.

Meets all complexity and security criteria.

- **Deductions**

Minor penalty for repeated characters (**ss**) and consecutive lowercase letters.

Slight deduction due to predictability in structure.

- **Conclusion**

Strong and secure password, suitable for most services.

Minor weaknesses, but overall provides solid protection.

Best Practices for Creating Strong Passwords

1. Use at Least 12–16 Characters

- Longer passwords are significantly harder to crack than short ones.
- Each additional character exponentially increases the number of possible combinations.

2. Mix Different Character Types

- Include:
 - Uppercase (A–Z)
 - Lowercase (a–z)
 - Numbers (0–9)
 - Symbols (!@#\$%^&* etc.)
- Example: T1m3T0\$urviv3!

3. Avoid Personal Information

- Do not use names, birthdates, or usernames.
- These are easily guessable and often exposed in data leaks.

4. Avoid Common Passwords

- Never use passwords like 123456, qwerty, password, or admin123.
- These are first tested in dictionary attacks.

5. Do Not Use Repeated or Sequential Characters

- Avoid patterns like `aaaa1111` or `abcdefg`.
- Predictable patterns reduce password strength.

6. Use Passphrases for Better Memorability

- Create a sentence-like password, such as `Blue_Tree$Falls97!`
- Easier to remember, but still strong if random and long.

7. Use a Password Manager

- Password managers can:
 - Generate strong, random passwords.
 - Store them securely.
 - Automatically fill them on websites.

8. Change Passwords After Breaches

- Always update passwords if a service you use is breached.
- Use tools like haveibeenpwned.com to check.

9. Don't Reuse Passwords Across Sites

- If one password gets compromised, it can be used to access your other accounts (credential stuffing attack).

10. Enable Multi-Factor Authentication (MFA)

- Even if your password is leaked, MFA can stop unauthorized access.
- Use authenticator apps (like Google Authenticator) or hardware keys.

Tips for Creating Strong Passwords

1. Use at least 12 characters:

Short passwords are easier to brute-force. A longer password increases the number of combinations, making it harder to crack.

2. Mix uppercase, lowercase, numbers, and symbols:

Using a combination like P@ssW0rd#123! adds complexity and increases entropy (randomness), making it more secure.

3. Avoid dictionary words or personal information:

Passwords like sunshine or John1999 are easily guessed or cracked using dictionary attacks or social engineering.

4. Never reuse passwords across sites:

If one site is breached, attackers can try your password elsewhere (this is known as credential stuffing).

5. Prefer passphrases:

A passphrase like BlueTiger\$Walks92! is easy to remember but difficult to guess. Passphrases can be random but memorable.

6. Use a password manager:

Password managers can generate and store strong, unique passwords for each account securely, so you don't need to remember them all.

7. Change passwords regularly, especially after a breach:

Frequent updates reduce the window of vulnerability if your credentials are compromised.

Common Password Attacks

1. Brute Force Attack:

A computer tries every possible combination of characters. Simple passwords are cracked within seconds this way.

2. Dictionary Attack:

Uses a list of common words and known passwords. If your password is something like `hello123`, it's likely in the list.

3. Credential Stuffing:

Hackers use leaked username-password pairs from past breaches to try logging in on other sites.

4. Phishing:

Attackers trick users into revealing passwords via fake emails or login pages that look legitimate.

5. Keylogging:

Malware secretly records everything you type, including your passwords, and sends it to the attacker.

How Password Complexity Affects Security (Explained)

- **Higher entropy = higher security:**

Entropy refers to how unpredictable your password is. More varied characters = harder to guess.

- **Character diversity matters:**

A password like `M@rble2025$Sky` is far stronger than `marble2025sky`, even if both are the same length.

- **Avoid common patterns:**

Sequences (`12345`) or repeated characters (`aaaa`) are predictable and penalized by strength checkers.

- **Security tools measure strength:**

Password meters deduct points for simplicity, known patterns, and dictionary matches.

- **Strong passwords resist automated attacks:**

Complex, long passwords with no patterns take years (or more) to crack using modern tools.