Password Strength Evaluation Report

Objective

Understand what makes a password strong and test it against online password strength tools.

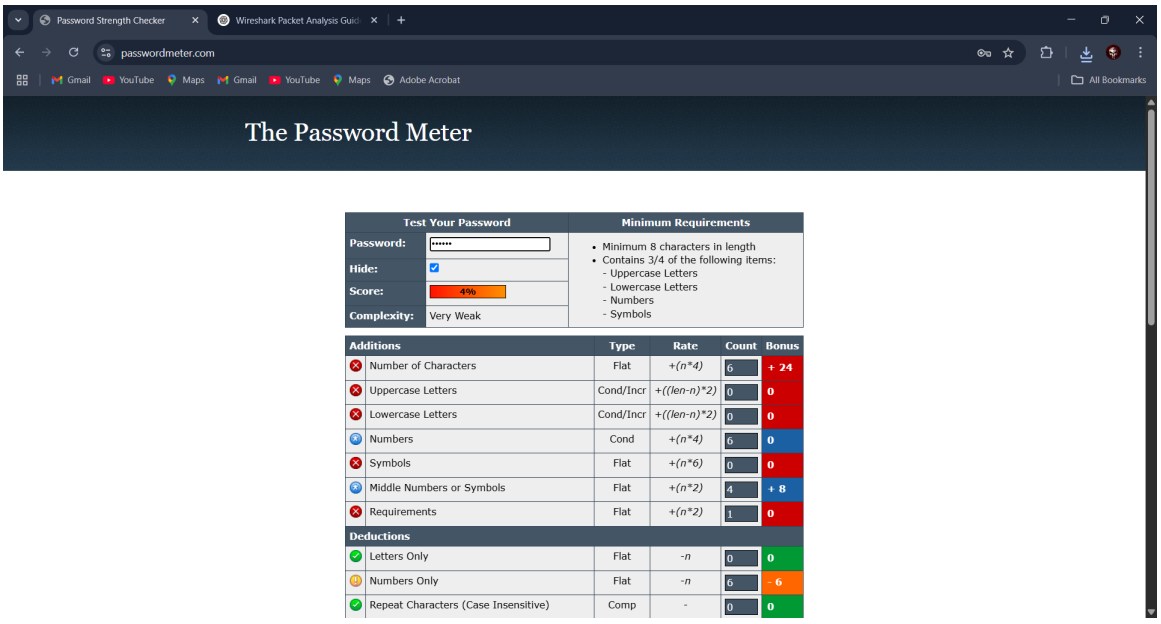
Tools Used

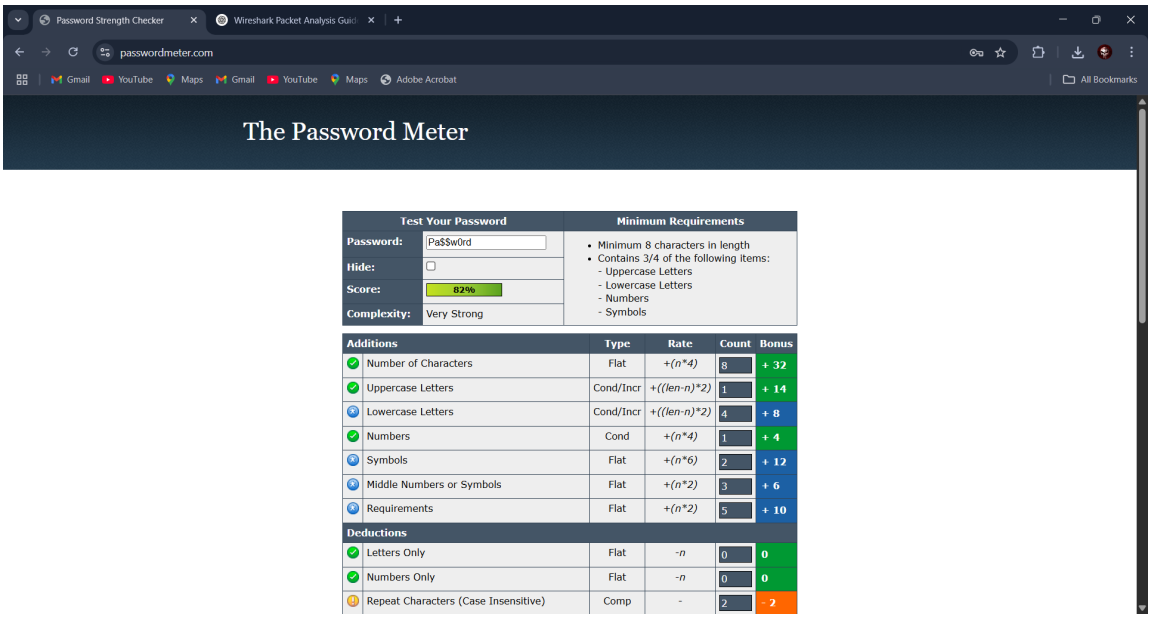
• Online Password Strength Checkers https://passwordmeter.com/

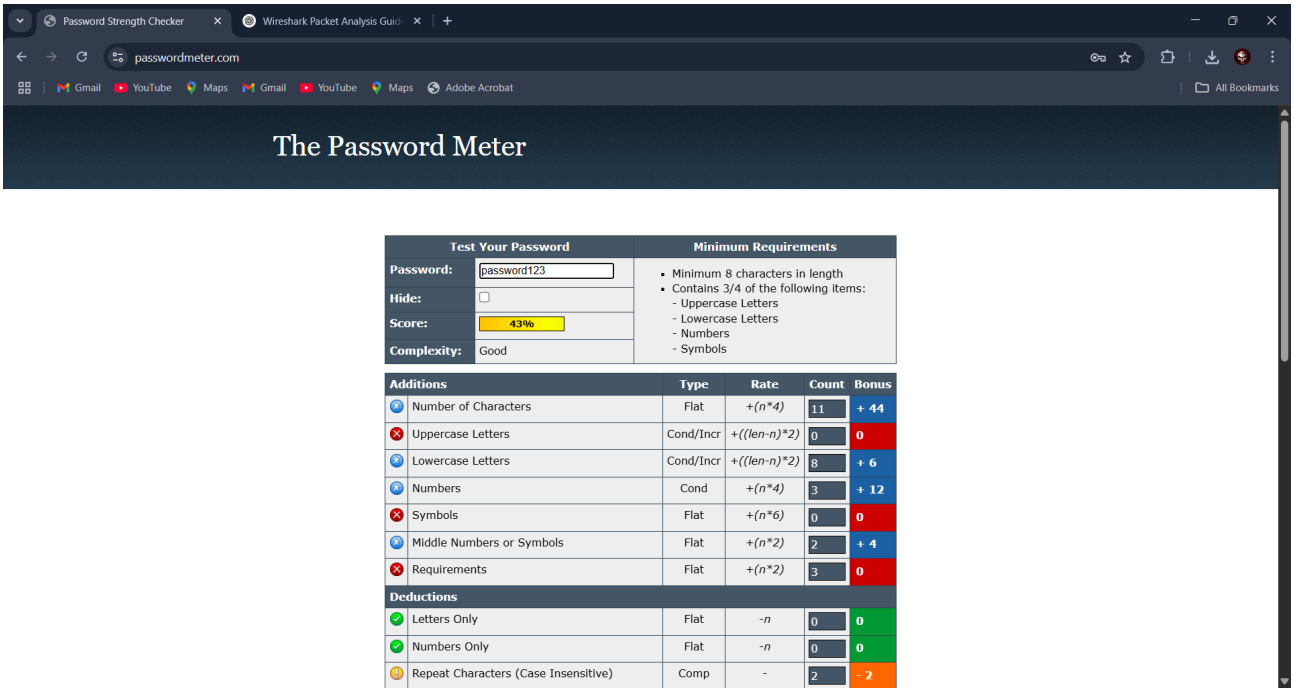
Procedure

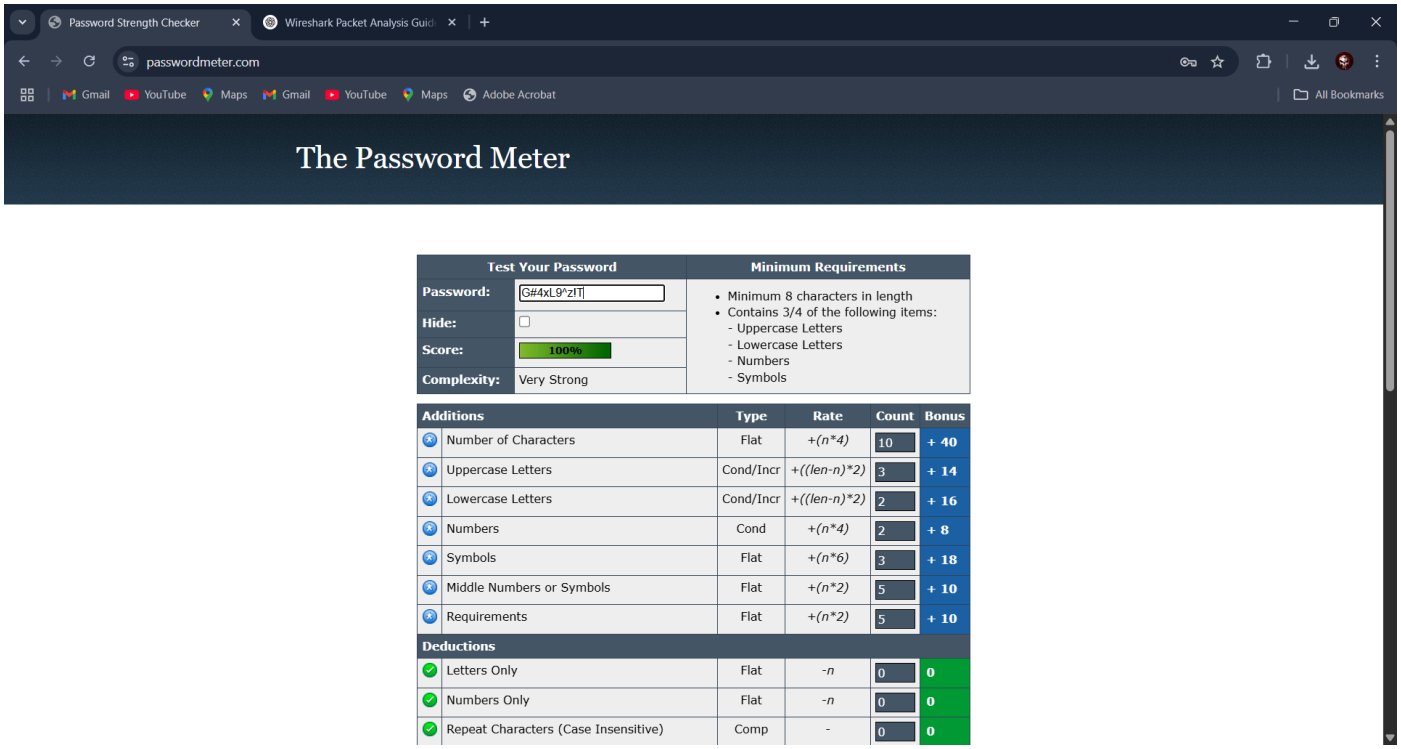
1. 1. Created a list of passwords with varying complexity, including differences in length, use of uppercase and lowercase letters, numbers, and symbols.
2. 2. Tested each password using an online password strength checker.
3. 3. Recorded the score, rating, and feedback provided by the tool.
4. 4. Analyzed which patterns and characteristics contributed to higher strength ratings.
5. 5. Compiled tips and best practices based on results.
6. 6. Conducted research on common password attacks such as brute force and dictionary attacks.
7. 7. Summarized how password complexity affects password security.

Screenshots (Placeholders)




Password Strength Checker
Wireshark Packet Analysis Guid
passwordmeter.com
Gmail YouTube Maps Gmail YouTube Maps Adobe Acrobat
All Bookmarks
The Password Meter
Test Your Password
Password: Pa$$w0rd
Hide:
Score: 82%
Complexity: Very Strong
Minimum Requirements
• Minimum 8 characters in length
• Contains 3/4 of the following items:
- Uppercase Letters
- Lowercase Letters
- Numbers
- Symbols
Additions | Type | Rate | Count | Bonus
Number of Characters | Flat | +(n*4) | 8 | + 32
Uppercase Letters | Cond/Incr | +((len-n)*2) | 1 | + 14
Lowercase Letters | Cond/Incr | +((len-n)*2) | 4 | + 8
Numbers | Cond | +(n*4) | 1 | + 4
Symbols | Flat | +(n*6) | 2 | + 12
Middle Numbers or Symbols | Flat | +(n*2) | 3 | + 6
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 | - 2


Password Strength Checker
Wireshark Packet Analysis Guid
passwordmeter.com
Gmail YouTube Maps Gmail YouTube Maps Adobe Acrobat
All Bookmarks
The Password Meter
Test Your Password
Password: password123
Hide:
Score: 43%
Complexity: Good
Minimum Requirements
• Minimum 8 characters in length
• Contains 3/4 of the following items:
- Uppercase Letters
- Lowercase Letters
- Numbers
- Symbols
Additions | Type | Rate | Count | Bonus
Number of Characters | Flat | +(n*4) | 11 | + 44
Uppercase Letters | Cond/Incr | +((len-n)*2) | 0 | 0
Lowercase Letters | Cond/Incr | +((len-n)*2) | 8 | + 6
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 | - | 2 | - 2



Sample Passwords and Evaluation

Below are examples of passwords tested and their respective strength scores:

Password	Strength Score/Rating	Tool Feedback
password123	Weak	Too common, lacks symbols
Pa$$w0rd	Moderate	Includes symbols and numbers
G#4xL9^z!T	Strong	High entropy, excellent complexity

Best Practices for Strong Passwords

• Use a mix of uppercase and lowercase letters.

• Include numbers and special characters.

- Avoid common words and predictable patterns.
- Make the password at least 12–16 characters long.
- Do not reuse passwords across multiple accounts.
- Consider using a password manager to store complex passwords.

Password Attacks and Importance of Complexity

Common password attacks include brute force attacks, where every possible combination is tried, and dictionary attacks, which use a list of common words and phrases. Password complexity significantly affects how long it would take to crack a password. More complex and longer passwords are exponentially harder to break, making them more secure against these attacks.

Conclusion

This evaluation highlighted the importance of using strong, complex passwords. Using online tools helped visualize weaknesses in simpler passwords and guided best practices for creating secure credentials.