Report by AISWARYA S

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

Objective:

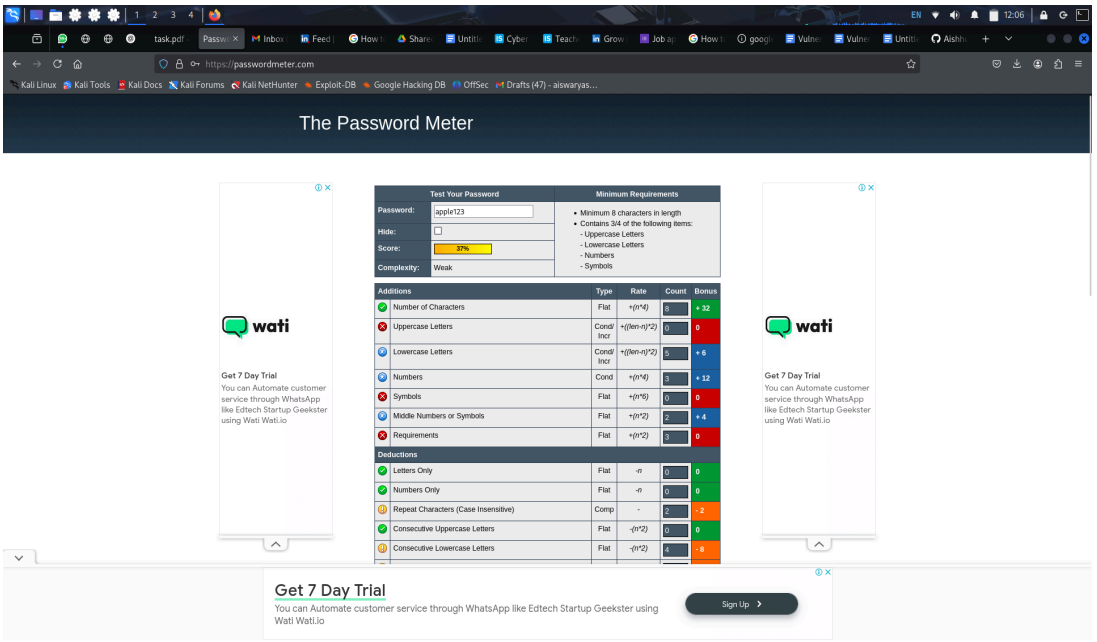
To understand what makes a password strong and to evaluate the strength of various passwords using online tools.

Step 1: Passwords Created

Password	Complexity Level	Expected Strength
apple123	Weak	Very Low
AppLe_2025	Medium	Medium
$ecur3!tY	Strong	High
H@ckTh3W0rld!	Very Strong	Very High
123456789	Very Weak	Extremely Low
M@nGo_C#ke.98	Strongest	Very High

Step 2: Tool Used

- Website: https://www.passwordmeter.com



Step 3: Password Strength Results

Password	Score (%)	Tool Feedback
1. apple123	**37%**	Too short, lacks complexity, dictionary word
2. AppLe_2025	**53%**	Better, but still predictable
3. $ecur3!tY	**70%**	Good use of special characters & case
4. H@ckTh3W0rld!	**85%**	Excellent complexity & length
5. 123456789	**15%**	Very common, easy to guess
6. M@nGo_C#ke.98	**88%**	Very strong, good variety and length

Step 4: Tips Learned

1. Longer = Stronger: Passwords above 12 characters are harder to crack.
2. Mix Elements: Combine uppercase, lowercase, numbers, and special characters.
3. Avoid Common Patterns: "123456" or names are easily cracked.
4. Use Passphrases: Eg. "G0Crazy@Midn!ght123" is both secure and memorable.
5. No Reuse: Always use different passwords for different accounts.

Step 5: Password Attacks Researched

- **Brute Force Attack**: Tries every possible combination. Short/simple passwords fall fast.
- **Dictionary Attack**: Uses common wordlists. Real words = risky.
- **Credential Stuffing**: Reuses passwords from data breaches.

Step 6: How Complexity Affects Security

Passwords with more randomness, longer length, and a mix of character types take **millions of years** to crack compared to simple ones, which can be cracked in seconds.