FINAL REPORT

Cyber Security Internship – Task 6

Title: Password Strength Evaluation

Student: Yuvraj Yadav
Date: 28 October 2025

1. Objective

The objective of this task is to understand the factors that determine password strength and to analyze how password complexity affects resistance to common cyber-attacks such as brute-force and dictionary attacks.

2. Tools Used

- Password Meter (passwordmeter.com)
- Kaspersky Password Strength Checker
- NordPass Strength Checker

These tools evaluate password entropy, length, character diversity, and dictionary exposure.

3. Methodology

1. Created multiple passwords of varying complexity (weak → strong).
2. Tested each on three different online tools.
3. Recorded feedback and numerical strength scores.
4. Compared results to identify characteristics of strong passwords.

4. Observations and Results

Password	Strength (%)	Evaluation
`pass123`	20%	Weak — short, predictable, no symbols.
`Password@2025`	55%	Moderate — contains uppercase and symbols, but a predictable pattern.
`Cyb3r$afe@2025!`	95%	Strong — long, mixed characters, uncommon pattern.
`YvR@!92x#ZkLp$21`	100%	Very Strong — high entropy, resistant to brute-force.

5. Analysis

- Password length significantly increases the time required for brute-force attacks.
- Mixed character sets reduce vulnerability to dictionary-based guessing.
- Predictable substitutions like `P@ssw0rd` are easily cracked by hybrid attacks.
- Entropy (randomness) is the most important factor for strength.

6. Common Attacks and Prevention

Attack Type	Description	Prevention
Brute Force	Tries all combinations	Use long, complex passwords
Dictionary	Uses known passwords or words	Avoid dictionary words
Phishing	Tricking users to reveal credentials	Be cautious of suspicious links
Credential Stuffing	Reusing leaked passwords	Use unique passwords per account

7. Best Practices

- Use **12–16+ character passwords** with random symbols.
- Avoid using real words or personal details.
- Enable **Multi-Factor Authentication (MFA)**.
- Use a **password manager** (Bitwarden, KeePass, etc.) to store credentials securely.

8. Outcome

This task provided practical experience in evaluating password strength and understanding how complexity directly impacts security.
By analyzing feedback from password evaluation tools, it became clear that **length, randomness, and diversity of characters** are key to strong passwords.

9. Conclusion

Password complexity plays a crucial role in protecting user accounts and systems from unauthorized access.
A well-structured password policy, combined with MFA and password management tools, forms the foundation of modern cybersecurity hygiene.

10. References

[1] OWASP Foundation. “Authentication Cheat Sheet.” 2025.
[2] PasswordMeter.com, Online Password Strength Evaluation Tool.
[3] Kaspersky Password Strength Checker.
[4] NordPass Password Analysis Tool.