Cyber Security Internship – Task 6 Report

Objective: Create multiple passwords, evaluate their strength using standard criteria, and recommend best practices.

Sample Passwords Created (varied complexity):

Password	Notes & Expected Strength
p@ssw0rd	Common substitution, short (8) — weak
Summer2025	Mixed-case + numbers, no symbols (10) — moderate
Tr0ub4dor&3	From famous example — moderate
G4rbAge!HorseBlu3#7	Long, mixed types (18) — strong
correcthorsebatterystaple	Long passphrase, all lowercase (25) — strong by length
X9$vQ#8pL!z7Dm3	Random-like with symbols (16) — strong
LinkedIn2025!	Contains service name and year — guessable by targeted attack
P@$$w0rd123456	Common pattern with sequences — weak

Evaluation Criteria / Methodology:

1. Length: Longer passwords increase entropy exponentially. Aim for 12+ characters; 16+ for high-value accounts. 2. Character set: Use uppercase, lowercase, numbers, and symbols to increase possible combinations. 3. Avoid common words, repeated patterns, or predictable substitutions (e.g., 'p@ssw0rd'). 4. Use passphrases or random passwords generated by password managers for high entropy. 5. Entropy estimation (bits) approximate: entropy = length * log2(character_set_size). Typical set sizes: lowercase=26, lower+upper=52, digits=62, with symbols ~95 possible printable.

Estimated Entropy for Each Sample:

Password	Length	Charset size approx.	Entropy (bits)	Strength (qualitative)
p@ssw0rd	8	68	48.7	Moderate
Summer2025	10	62	59.54	Moderate
Tr0ub4dor&3	11	94	72.1	Strong
G4rbAge!HorseBlu3#7	19	94	124.54	Very Strong
correcthorsebatterystaple	25	26	117.51	Very Strong
X9$vQ#8pL!z7Dm3	15	94	98.32	Very Strong
LinkedIn2025!	13	94	85.21	Very Strong
P@$$w0rd123456	14	94	91.76	Very Strong

Best Practices & Recommendations:

- Use a password manager to generate and store unique, random passwords per account. - Prefer long passphrases (4+ random words) or 16+ character random passwords for important accounts. - Enable multi-factor authentication (MFA) wherever possible. - Avoid reusing passwords across sites; change passwords immediately if a breach is suspected. - Do not include obvious personal info (birthdays, pet names) or service names for targeted accounts. - Regularly review accounts and use breach-check tools (HaveIBeenPwned) to check exposures.

Common Password Attacks:

- Brute-force attack: attempt every possible combination — mitigated by length and account lockouts. - Dictionary attack: tries words from lists and common variations — mitigated by avoiding dictionary words. - Credential stuffing: uses leaked username/password pairs — mitigated by unique passwords and MFA. - Hybrid attacks: dictionary + common substitutions and appended numbers — mitigated by randomness.

How to Test Passwords Safely:

- Use reputable online checkers (e.g., passwordmeter.com) but avoid entering real passwords. - Instead, use a representative sample or check locally with tools like 'zxcvbn' library for offline testing. - If you must use an online tester, append or modify the password slightly and then apply the same rule locally.

Interview Questions & Short Answers:

What makes a password strong? — Length, randomness (entropy), and uniqueness. Use MFA for extra security.

What are common password attacks? — Brute-force, dictionary attacks, credential stuffing, hybrid attacks.

Why is password length important? — Each extra character increases entropy exponentially, making brute force harder.

What is a dictionary attack? — An attack that tries words from a dictionary and common permutations.

What is multi-factor authentication (MFA)? — An authentication method requiring additional verification factors beyond a password.

How do password managers help? — They generate/store unique passwords, so users don't reuse weak passwords.

What are passphrases? — Long sequences of words (e.g., 'correct horse battery staple') that are easier to remember and strong.

Common mistakes in password creation? — Reusing passwords, short length, predictable substitutions, using personal info.

Report generated by: Nitin Saini Rathor