**Cyber Security Internship – Task 6 Report**

**1. Objective**

The purpose of this task is to evaluate the strength and security of various types of passwords by testing them on online password analysis tools.

**2. Tools Used**

1. PasswordMeter.com – Provides a complexity score (0–100%) and feedback.  
2. HowSecureIsMyPassword.net – Estimates how long it would take to crack a password.

**3. Passwords Tested**

1. kritiBsu
2. po3K5/-52
3. Wh3reTh3\*kY\_Blu3?

**4. Results**

|  |  |  |
| --- | --- | --- |
| Password | PasswordMeter Score | Crack Time Estimate |
| kritiBsu | 29% (Too Weak) | 22 min |
| po3K5/-52 | 100%(very strong) | 52 year |
| Wh3reTh3\*kY\_Blu3? | 100% (very strong) | 3quadrillion+ years |

**5. Analysis & Learnings**

I found that password strength increases with length and different character like (uppercase, lowercase, numbers, and symbols). Simple words are easily cracked, while complex password with mixed characters take longer time to break.

**6. Common Password Attacks**

1. Brute Force – Trying all possible combinations.  
2. Dictionary Attack – Using common words and passwords.  
3. Credential Stuffing – Using leaked credentials on other accounts.  
4. Phishing – Trick users into revealing passwords.

**7. Best Practices**

• Use at least 12–16 characters.  
• Mix uppercase, lowercase, numbers, and symbols.  
• Use unique passwords for each account.  
• Enable Multi-Factor Authentication (MFA).  
• Use a password manager.

**8. Interview Q&A**

Q: What makes a password strong?

A: Length, randomness, and variety of characters.

Q: Common password attacks?

A: Brute force, dictionary attacks, credential stuffing, phishing.

Q: Why is password length important?

A: Longer passwords make brute-force attacks exponentially harder.

Q: What is a dictionary attack?

A: An attack using common passwords/words to guess quickly.

Q: What is MFA?

A: Multi-Factor Authentication adds an extra security layer.

Q: How do password managers help?

A: They generate and store strong, unique passwords.

Q: What are passphrases?

A: Random word combinations that are strong and easy to remember.

Q: Common mistakes?

A: Reusing passwords, using patterns, predictable substitutions, no MFA.