# Cyber Security Internship – Task 6

**Task Title:** The Art of Building Unbreakable Passwords

**Submitted By:** Gourav Swaroop

**Date:** 12/08/2025

## Objective

In today's cyber battlefield, passwords are the first (and sometimes last) line of defence. This task dives into the science and art of crafting passwords so secure they make hackers groan in despair.
From creating multiple variations to testing them against industry tools, the mission was simple: turn weak strings into digital fortresses.

---

## Tools of the Trade

- **OS:** Kali Linux (because we're serious about security)
- **Browser:** Firefox / Chromium
- **Password Strength Tester:** PasswordMeter.com

---

## Methodology – How the Magic Happened

1. **Summoned Multiple Passwords** – from the predictable and weak to the fortress-grade masterpieces.
2. **Unleashed Them on the Strength Checker** – watched the score climb (or drop) and took notes.
3. **Analyzed Feedback** – decoded what makes the difference between "meh" and "legendary."

---

## Test Results – The Hall of Fame (and Shame)

| Password | Length | Complexity | Score | Verdict |
|---|---|---|---|---|
| password | 8 | Weak | 8% | Hacker’s delight |
| pa$sword!! | 10 | Medium | 56% | Still guessable |
| G7ntP411 | 8 | Strong | 78% | Now we’re talking |
| H@ckTh3_World | 13 | Very Strong | 100% | Digital Fort Knox |

---

## Secrets of a Strong Password (Lessons Learned)

- **Length = Power** → Aim for 12–16+ characters.
- **Diversity Wins** → Mix uppercase, lowercase, numbers, symbols.
- **No Obvious Choices** → Avoid dictionary words & birthdays.
- **Passphrases are Gold** → “$kyBlues!nTh3M0rning” is better than Sky123.
- **Password Managers = Lifesavers** → Let them remember the chaos for you.

---

## Enemy Tactics – Know Your Opponent

- **Brute Force** – Tries every possible combo until it hits the jackpot.
- **Dictionary Attack** – Uses common words & leaked passwords to guess quickly.
- **Hybrid Attack** – Blends both methods… fast and dangerous.

---

## Conclusion

A strong password is more than a security measure — it’s a warning sign to attackers:
**“You can try, but you won’t get in.”**
This experiment proved that *length* + *complexity* is the unbeatable formula for password resilience.
With just a few smart choices, you can go from a **22% weakling** to a **100% digital fortress**.