1.Create multiple passwords with varying complexity. (Using CLI)

```
# simple numeric (weak)

pwgen -1 6 5 > passwords_simple.txt

# medium (letters+numbers)

pwgen -1 10 5 > passwords_medium.txt

# complex (upper+lower+digits+symbols) via openssl

for i in {1..5}; do openssl rand -base64 18 | tr -dc 'A-Za-z0-9!@#$%&*()-_+=' | head -c 16 >> passwords_complex.txt; echo >> passwords_complex.txt; done

# passphrases (3-4 random words)

for i in {1..5}; do shuf -n4 /usr/share/dict/words | tr '\n' ' ' | sed 's/ $//' >> passphrases.txt; done
```

2.Use uppercase, lowercase, numbers, symbols, and length variations.

```
pwgen -1 20 5 > pw_len20.txt   # 20-char passwords
```

3.Test each password on password strength checker.

Use Tools Like :-

-> Passwordmeter

-> HaveIBeenPwned

5.Identify best practices for creating strong passwords.

Best-practice checklist to validate manually:

- ≥12 characters (prefer ≥16 for high-value accounts)
- Mixed case + digits + symbols OR 4-word unique passphrase
- No common words or sequences
- Not reused across accounts

6.Write down tips learned from the evaluation.

- Use a password manager to store unique, complex passwords.

- Prefer length over arbitrary symbols — long passphrases are memorable and strong.

- Avoid reusing passwords across sites.

- Enable MFA wherever possible to mitigate password compromise.

7.Research common password attacks (brute force, dictionary).

Use Tools like :-

-> John The Ripper

```
# using john
john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 test_hash.txt
john --show test_hash.txt
```

-> Hashcat and many more

```
# using Hashcat
hashcat -m 0 -a 0 test_md5.hash /usr/share/wordlists/rockyou.txt --status --status-timer=10
```

8.Summarize how password complexity affects security.

After evaluating multiple passwords of different lengths and complexities using a password strength checker, the results clearly highlighted the relationship between password structure and overall security resilience.

---

1. Strength Evaluation Summary

Password Type	**Composition**	**Average Strength Score**	**Crack Time (Approx.)**	**Remarks**
Simple (only letters/numbers)	6–8 characters	Low (Score 0–1)	Few seconds to minutes	Easily guessed by brute-force or dictionary attacks
Moderate	Mix of letters + numbers	Medium (Score 2–3)	Minutes to hours	Slightly better, but still predictable
Complex	Uppercase + lowercase + numbers + symbols	High (Score 4)	Days to years	Strong protection against common attacks

Password Type	Composition	Average Strength Score	Crack Time (Approx.)	Remarks
Passphrases	3–4 random words	Very High (Score 4)	Decades or more	Long yet memorable and resistant to cracking

---

2. Key Observations

- **Length and randomness** were the most influential factors in password strength. Even simple passwords became significantly stronger when extended beyond 12 characters.
- **Character diversity** (mixing uppercase, lowercase, digits, and symbols) increased resistance to brute-force attacks.
- **Passphrases** performed exceptionally well, combining memorability with high entropy.
- Passwords containing **dictionary words or personal data** (like names or dates) were flagged as weak regardless of length.

---

3. Analysis of Complexity Impact

- **Brute-force Resistance:** Each additional character exponentially increases the number of possible combinations, drastically extending the cracking time.
- **Dictionary Attack Defense:** Random symbols or unrelated word combinations break predictable patterns, making automated attacks ineffective.
- **Human Factor:** Passphrases are easier to remember yet harder to guess, reducing the chance of password reuse or insecure storage.

---

4. Overall Interpretation

The experiment demonstrated that **password complexity directly correlates with security strength**. Weak or short passwords are vulnerable to automated attacks within seconds, while strong, lengthy, and random passwords can withstand years of computational effort.

The ideal balance between **security and usability** is achieved with long passphrases or randomly generated complex strings stored safely in a password manager.

5. Conclusion

The password evaluation confirmed that **length, randomness, and variety** are the pillars of strong password creation. Passwords combining multiple character types and exceeding 12 characters offer robust protection against brute-force and dictionary-based attacks. Using unique passwords along with multi-factor authentication ensures the highest level of account security.