Overview

ClatsCracker 1.0 is a cutting-edge password cracking tool designed to help cybersecurity professionals, penetration testers, and security auditors quickly identify and address weak passwords in their systems. With multi-algorithm support, both dictionary-based and brute force attacks, and scalable performance controls, ClatsCracker 1.0 delivers greater versatility, accuracy, and efficiency than many competing tools.

There is a small cost of $10 USD for access to this tool's private repository, so I can continue to allocate time to add new user requested features, fix issues, add and updates in the future. Payment can be sent via PayPal or Interac e-Transfer (if you are located in Canada, anywhere else PayPal is the best option).

Important Note:

Always use this tool ethically and legally, and only on systems you are authorized to test.

Key Advantages

1. **Wide Range of Algorithms**

   ClatsCracker supports eight popular hashing algorithms, including legacy and modern forms:

   - Unsalted: MD5, SHA1, SHA256, SHA512, SHA3-256, Scrypt
   - Salted: Bcrypt, Argon2id

   Unlike other tools that only handle a few algorithms, ClatsCracker provides a one-stop solution to test multiple hashing methods, making it extremely versatile for different scenarios.

2. **Correct Verification of Salted Hashes**

   Salted hashes (like Bcrypt and Argon2id) require special handling. Many tools fail to verify them correctly, rehashing passwords with new salts and never achieving a match. ClatsCracker, however, uses:

   - bcrypt.checkpw() for Bcrypt
   - argon2-cffi's PasswordHasher.verify() for Argon2id

   This ensures proper verification with original salts and parameters, increasing the likelihood of successfully cracking these complex hashes.

3. **Flexible Cracking Methods**

   ClatsCracker offers two main attack strategies:

   - **Dictionary-based Attacks:** Quickly test large lists of known passwords, remove duplicates, and attempt matches efficiently.
   - **Brute Force Attacks:** Systematically try every possible password of a given length and character set, helping you tackle unknown or very strong passwords.

   Having both methods allows you to start with common passwords and escalate to more intensive brute force methods if needed.

4. **User-Friendly Interface & Controls**
   A menu-driven interface, intuitive prompts, and real-time progress updates simplify the process, even for non-experts. ClatsCracker also lets you select the number of threads—1 to 1000—so you can tailor performance to your computer's capabilities.
5. **Threaded Performance & Resource Management**

   Using Python's `ThreadPoolExecutor`, ClatsCracker can run multiple checks in parallel, significantly cutting down cracking time for large datasets. Thread-safe locks ensure accurate progress reporting, and users can choose from preset (Low, Medium, High) or custom thread counts to find the best balance between speed and stability.

6. **Validation & Error Handling**
   The tool validates hash lengths and formats before starting, saving time and reducing confusion. Immediate feedback ensures that any issues with the provided hash are resolved upfront.

7. **Ethical Use & Compliance**
   ClatsCracker includes disclaimers and encourages responsible usage, aligning with legal and ethical standards for penetration testing and security research.

In Practice

- **Penetration Testing & Auditing:** Identify weak passwords quickly and improve your organization's security posture.
- **Research & Development:** Compare and benchmark different hashing algorithms' resistance to cracking.
- **Incident Response & Forensics:** Recover essential passwords and data following security breaches.
-

Technical Requirements

- **Environment:** Python 3.x

- **Libraries:**
  - Built-in: hashlib, itertools, string, sys, os, time, threading, concurrent.futures
  - External: bcrypt, argon2-cffi (install with pip install bcrypt argon2-cffi)
- **Compatibility:** Works on Windows, macOS, and Linux with Python 3.x and required libraries.

Limitations

- Cracking speed depends on hash complexity and system resources.
- Algorithms like Argon2id and Scrypt are intentionally slow to resist brute force attempts.
- Ongoing updates to hashing standards may require future modifications to the tool.

Conclusion

ClatsCracker stands out because it supports more algorithms, handles salted hashes correctly, offers both dictionary and brute force methods, and provides exceptional user control over resources and performance. Its user-friendly interface, robust verification methods, and adherence to best practices make it a superior choice for ethical hacking, cybersecurity research, and password recovery tasks.