**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO ĐỒ ÁN MÔN HỌC**

**(Đồ án phát triển ứng dụng)**

**Lớp: IT003.O21.CTTN**

**SINH VIÊN THỰC HIỆN**

**Mã sinh viên: 23521045 Họ và tên: Nguyễn Hữu Đặng Nguyên**

**TÊN ĐỀ TÀI: ỨNG DỤNG MÔ PHỎNG CÁC MÔ HÌNH PASSWORD CRACKING.**

Mục lục

[I. Giới thiệu đồ án: 2](#_Toc167140881)

[1. Mô tả chung về ứng dụng: 2](#_Toc167140882)

[2. Các CTDL và giải thuật đã được sử dụng: 2](#_Toc167140883)

[II. Quá trình thực hiện 2](#_Toc167140884)

[1. Tuần 1: 3](#_Toc167140885)

[2. Tuần 2: 3](#_Toc167140886)

[III. Kết quả đạt được 3](#_Toc167140887)

[1. Lý thuyết về Password Cracking. 3](#_Toc167140888)

[**a. Khái niệm** 3](#_Toc167140889)

[**b. Phương pháp** 3](#_Toc167140890)

[**c. Hậu quả của việc bị crack password** 3](#_Toc167140891)

[**d. Một vài vụ bẻ khóa mật khẩu nổi tiếng:** 4](#_Toc167140892)

[2. Một vài mô hình Password Cracking phổ biến 4](#_Toc167140893)

[**a. Brute force Attack** 4](#_Toc167140894)

[**b.Dictionary Attack** 4](#_Toc167140895)

[**c.Hybrid Attack** 5](#_Toc167140896)

[**d. Rainbows Attack** 5](#_Toc167140897)

[**e.Phising and Vising** 5](#_Toc167140898)

[**f. Rat and Keylogging** 5](#_Toc167140899)

[3. Chi tiết và giải thích một số mô hình Password Cracking 6](#_Toc167140900)

[**a.** **Các thư viện và ngôn ngữ sử dụng** 6](#_Toc167140901)

[**b.** **Cài đặt môi trường và class** 6](#_Toc167140902)

[**c.** **Brute force Attack** 8](#_Toc167140903)

[**d.** **Dictionary Attack** 9](#_Toc167140904)

[**e.** **Hybrid Attack** 9](#_Toc167140905)

[IV. Tài liệu tham khảo 10](#_Toc167140906)

[V. Phụ lục 1: Giới thiệu (demo) kết quả 11](#_Toc167140907)

[1. Link github sản phẩm: https://github.com/TwinHter/23521045\_DoAnCK 11](#_Toc167140908)

[2. Demo sản phẩm 11](#_Toc167140909)

1. **Giới thiệu đồ án:**
2. **Mô tả chung về ứng dụng:**

Đây là báo cáo trình bày về những nghiên cứu về Password Cracking (bẻ khoá mật khẩu) và những tác động của nó. Đồng thời bài báo cáo cũng cung cấp một tool tổng hợp nhiều phương thức giúp bẻ khoá mật khẩu của một file Zip và đánh giá khách quan các phương thức đó. Về phần Visualization, em có cung cấp một repo github có chứa các file làm việc.

1. **Các CTDL và giải thuật đã được sử dụng:**

Thuật toán sinh ra các tổ hợp từ một bộ ký tự cho trước.

Giải thuật đệ quy để sinh ra các chuỗi phù hợp với mong muốn

Cấu trúc dữ liệu dictionary của Python

Sử dụng các kiến thức về hướng đối tượng trong Python

Một vài kiến thức tổ hợp để áp dụng các công thức toán, …

1. **Quá trình thực hiện**
2. **Tuần 1:**

Hoàn thành phần ý tưởng và một số phần của bài báo cáo bao gồm:

* Lý thuyết Password Cracking (Khái niệm, phương pháp, tác động và ví dụ)
* Một vài mô hình Password Cracking phổ biến
* Gỉải thích chi tiết kèm phần Code của bruteforce attack

1. **Tuần 2:**

* Hoàn thiện phần giải thuật và code cho các mô hình còn lại.
* Thử nghiệm sản phẩm.
* Viết bài báo cáo.

1. **Kết quả đạt được**

**1. Lý thuyết về Password Cracking.**

**a. Khái niệm**

- Password Cracking hay bẻ khóa mật khẩu là quá trình sử dụng nhiều cách thức có thể thủ công hoặc thông qua chương trình máy tính để xác định được mật khẩu của máy tính hay tài nguyên trên mạng.

**b. Phương pháp**

Có nhiều cách để bẻ khóa mật khẩu, một vài cách tiếp cận phổ biến như:

* Đánh cắp trực tiếp mật khẩu từ người dùng.
* Liên tục đoán mật khẩu hay sử dụng một danh sách các mật khẩu phổ biến và kiểm tra với giá trị Hash có sẵn của tài khoản.
* Sử dụng một liên kết hay một tệp có gán các chương trình chi tiết nhằm giả mạo máy tính người dùng hay theo dõi hoạt đồng người dùng từ màn hình, bàn phím từ đó thu thập thông tin.

Tấn công trực tiếp vào cơ sở dữ liệu của máy chủ và lấy thông tin.

**c. Hậu quả của việc bị crack password**

Đa phần người sử dụng Password Cracking vì mục đích xấu. Khi mật khẩu bị các Hacker phát hiện ra, nó có thể gây ra nhiều hậu quả khó lường như:

* Bị lộ thông tin cá nhân, thông tin riêng tư.
* Bị đánh cắp tài khoản ngân hàng.
* Tài khoản bị sử dụng cho các mục đích xấu.

**d. Một vài vụ bẻ khóa mật khẩu nổi tiếng:**

* Gần đây, Streamer Độ Mixi đã bị bẻ khóa mật khẩu nhiều tài khoản mạng xã hội. Đó là do anh đã nhấn vào một file có chứa mã độc từ đó bị đánh cắp thông tin.
* Năm 2012, một hacker mật danh “Peace” đã thực hiện một vụ tấn công mạng vào hơn 100 triệu tài khoản LinkedID. Hắn sử dụng một thuật toán nhằm bẻ khóa mã Hash SHA1 của đa số các tài khoản trên nền tảng này.

**2. Một vài mô hình Password Cracking phổ biến**

**a. Brute force Attack**

Trong mô hình này, hacker sẽ cố gắng đoán mật khẩu thông qua việc thử một cách có hệ thống mọi loại kết hợp ký tự cho đến khi tìm được mật khẩu hợp lệ.

- Ưu điểm:

* Trên lý thuyết, phương pháp này có thể bẻ khóa tất cả mật khẩu và chống lại tất cả loại mã hoá.
* Rất hiệu quả khi chống lại các mật khẩu ngắn và đơn giản

-Nhược điểm

* Tốn rất nhiều thời gian và tài nguyên. Dễ bị phát hiện
* Không hiệu quả với mật khẩu đủ dài và phức tạp.

**b.Dictionary Attack**

Trong mô hình này, hacker sử dụng một danh sách các password phổ biến là từ điển (dictionary) để thử mật khẩu.

-Ưu điểm:

* Có thể bẻ khóa nhanh được các mật khẩu đơn giản
* Sử dụng danh sách có sẵn, không mất công sinh ra mật khẩu.

-Nhược điểm

* + Chỉ hiệu quả với các mật khẩu phổ biến.
  + Nếu mật khẩu được đặt ngẫu nhiên thì phương pháp này coi như vô dụng

**c.Hybrid Attack**

Phương pháp này kết hợp hai phương pháp Brute force attack và Dictionary Attack. Trong mô hình này, Hacker sẽ vẫn sử dụng các mật khẩu có thể từ Dictionary có sẵn. Sau đó hacker sẽ dùng chương trình để thay thế, thêm bớt một vài ký tự bằng các ký tự có liên quan để sinh ra mật khẩu khả thi mới.

**d. Rainbows Attack**

Hiện nay, nhiều máy chủ, hệ thống sử dụng thuật toán Hash(md5, sha) để mã hóa thông tin. Khi người dùng đăng ký tài khoản, server sẽ sử dụng các thuật toán này để mã hóa mật khẩu lại thành một mã Hash. Sau đó khi đăng nhập thì server sẽ tiến hành so sánh với mã Hash thay vì so với mật khẩu thuần. Mô hình Rainbows Attack sử dụng một bảng thống kê gọi là Rainbows Table lưu trữ các giá trị Hash đã được tính toán. Phương pháp này sẽ giống việc Hacker sẽ gian lận bằng việc không nhất thiết đoán chính xác mật khẩu mà là đoán mã Hash của mật khẩu đó. Phương pháp này có thể kết hợp Dictionary Attack.

Ưu điểm:

* Có thể nhanh chóng bẻ khóa được mật khẩu được mã hóa yếu
* Tiền xử lý giúp việc tìm được mã Hash diễn ra nhanh hơn.

Nhược điểm:

* Yêu cầu quy trình xử lý phức tạp và lượng tài nguyên lớn
* Không hiệu quả với mật khẩu được mã hóa mạnh.

**e.Phising and Vising**

Đây được đánh giá là phương pháp dễ dàng, phổ biến và hiệu quả nhất để lấy thông tin về tài khoản. Trong phương pháp này, hacker gửi một trang đăng nhập giả mạo tới nạn nhân. Hacker sẽ gửi trang đăng nhập giả thông qua email, chat ... Khi nạn nhân đăng nhập với username/password, họ sẽ bị hacker phát hiện.

**f. Rat and Keylogging**

Trong phương pháp này, hacker sẽ gửi một keylogger server hoặc RAT server tới nạn nhân. Keylogger sẽ ghi lại mọi thao tác trên bàn phím của nạn nhân và bản ghi này sẽ được gửi tới hacker.

1. **Chi tiết và giải thích một số mô hình Password Cracking**
2. **Các thư viện và ngôn ngữ sử dụng**

Ngôn ngữ sử dụng: Python

Các thư viện sử dụng:

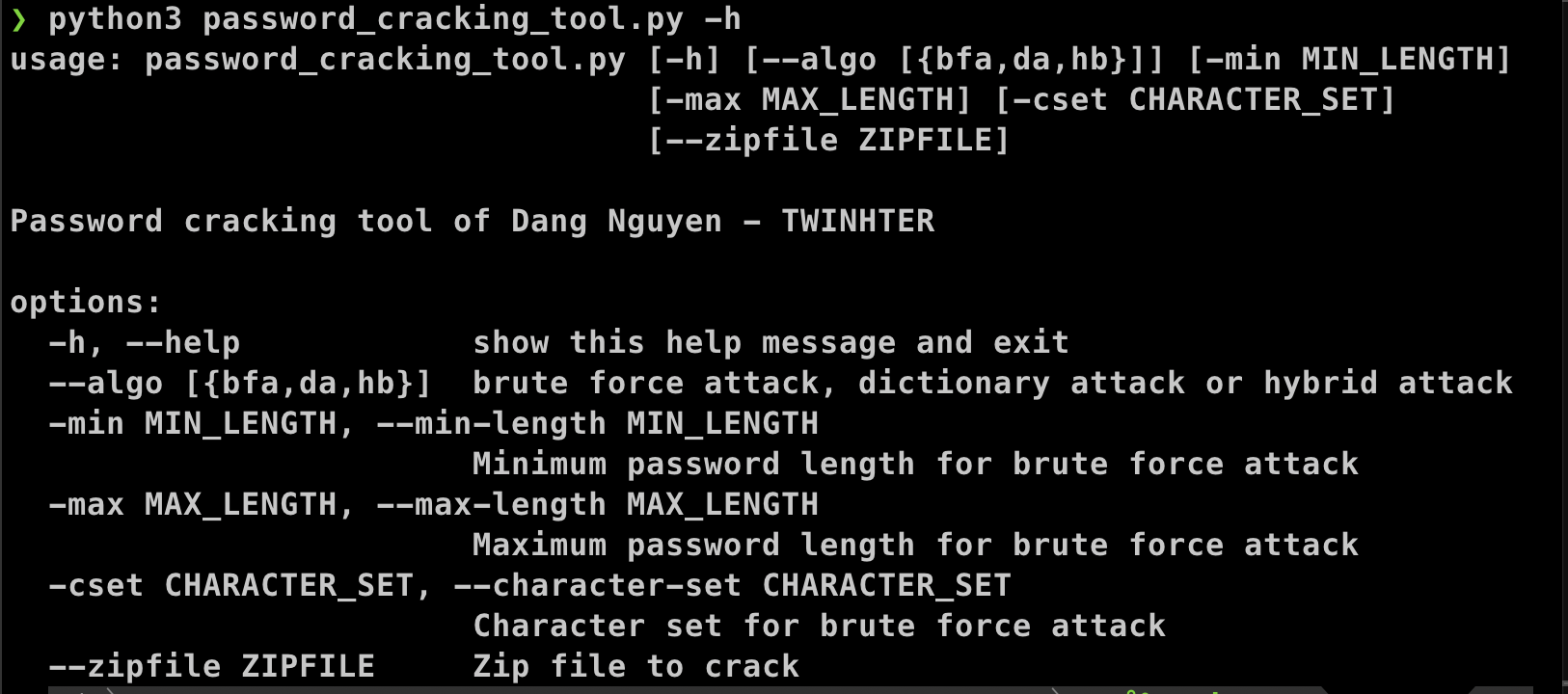
* + - Argparse: Hỗ trợ quá trình tạo tool và làm việc với CLI
    - Itertools: Dùng hỗ trợ cho việc tạo các tổ hợp nhanh chóng
    - Zipfile: Để tương tác và làm việc với file zip
    - Math

1. **Cài đặt môi trường và class**



Các file làm việc gồm có:

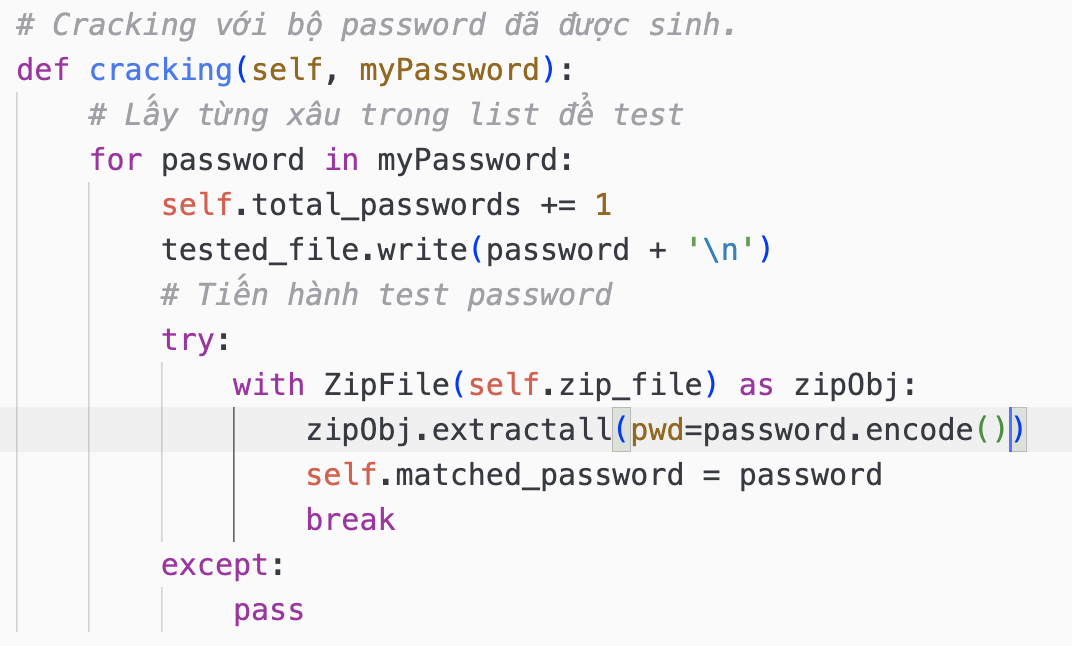
* + - Password\_cracking\_tool.py: Chứa phần code cho sản phẩm
    - Dictionary.txt, hybrid.txt: Chứa phần dữ liệu phục vụ cho dictionary attack và hybrid atack
    - Tested\_password.txt: Chứa phần kết quả đầu ra



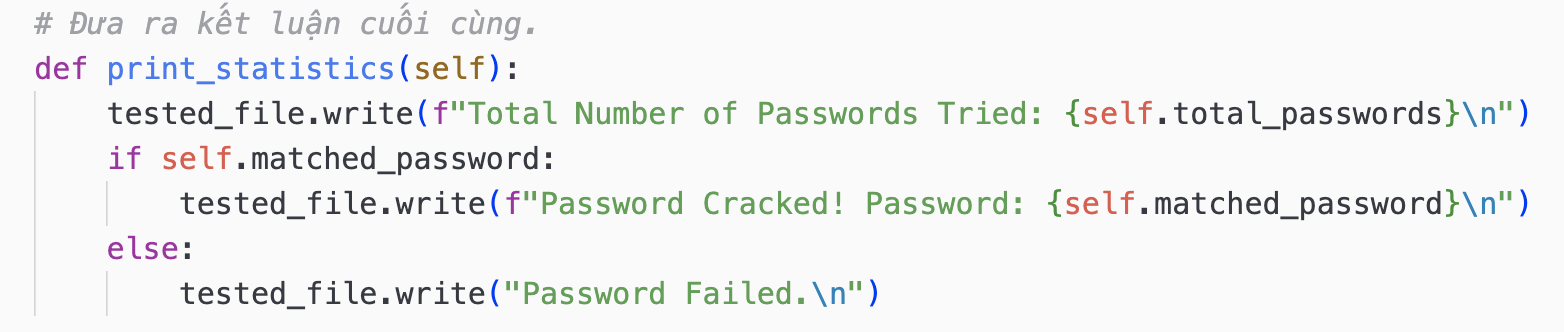
Các module của tool cracking password.



Tổng quan về class Password Cracker

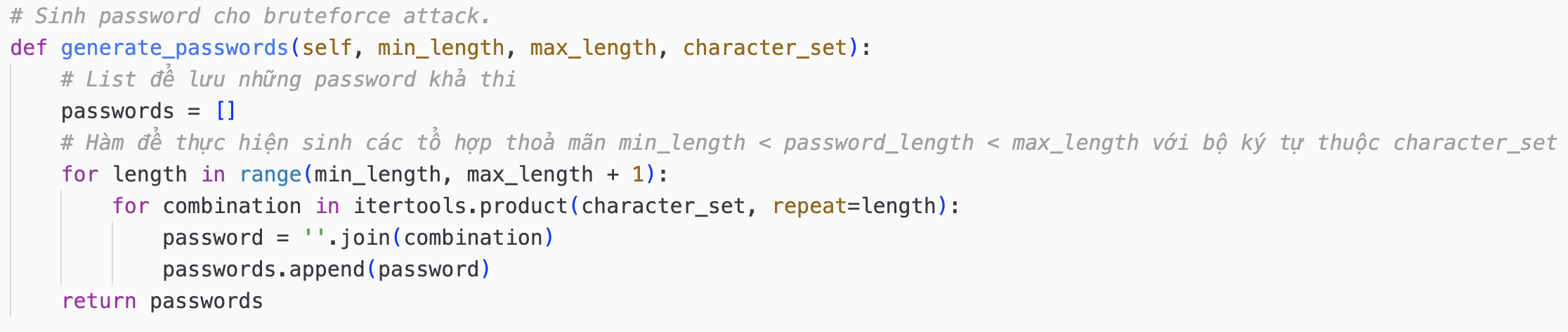


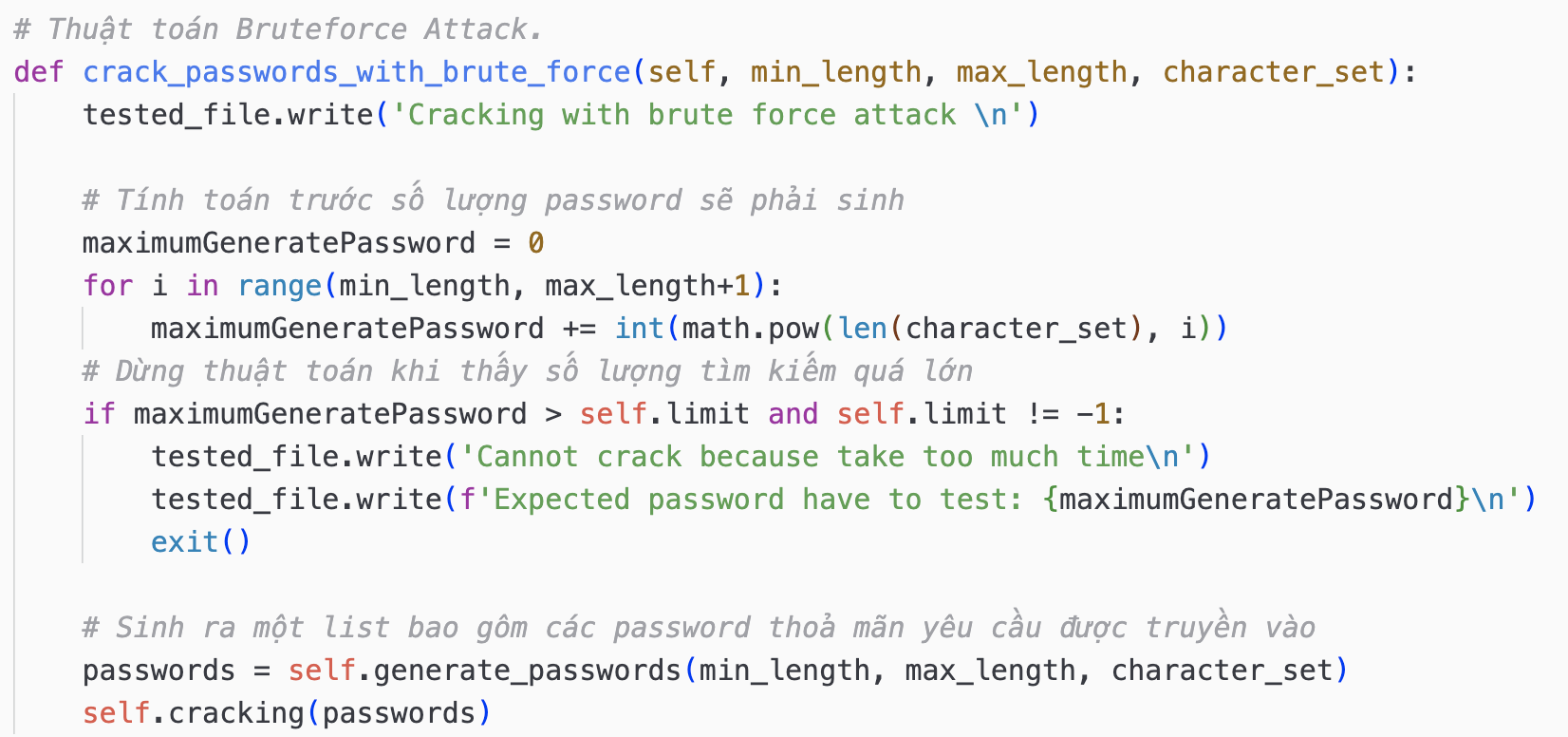
Hàm cracking dùng để crack zip file với một list password đã được sinh ra dựa trên các thuật toán. Hàm sử dụng những function có sẵn được định nghĩa trong thư viện Zipfile để hỗ trợ so khớp mật khẩu.



Hàm dùng để in ra kết quả

1. **Brute force Attack**





-Với các tham số về min length, max length, character set được đưa vào, chương trình sẽ tính trước số tổ hợp ký tự có thể được tạo ra.

maximumGeneratePassword =

-Nếu con số này lớn hơn giới hạn cho trước thì không kiểm tra mà báo ra là không crack vì số lượng password thử là quá lớn. Nếu không thì thực thi hàm generate\_passwords và tiến hành cracking với list password được trả về.

* Nó sẽ tạo ra các password với độ dài lần lượt từ min length đến max length.
* Mỗi độ dài sẽ sử dụng bộ dữ liệu character set cùng hàm product của itertools ( repeat = độ dài đang xét) để tạo ra các tổ hợp password thoả mãn.
* Lưu các password vào một list sau đó return lại.

-**Thời gian dự kiến O(maximumGeneratePassword)**

1. **Dictionary Attack**



* Function trong class: crack\_passwords\_with\_dictionary.
* Sử dụng file chứa các password phổ biến (dictionary.txt). ( > 300000 mật khẩu)
* Đọc các password trong file và lưu vào một list passwords để tiến hành cracking.
* **Thời gian dự kiến: O(len(dictionary.txt))**

1. **Hybrid Attack**





* Sử dụng file chứa các password phổ biến làm không gian chuẩn (hybrid.txt) (> 100 mật khẩu).
* Với mỗi password từ trong file trên, ta tiến hành:
* Tạo ra một list mới từ password đang xét chứa các password tương tự với nó.

Ví dụ admin ⬄ @dmin ⬄ 4dmin.

* Dùng một list num chứa các phần có thể mở rộng của password. Nó là những phần ở phần đầu hoặc cuối hay được thêm vào( VD : ‘123’, ‘111’, ‘abc’, …)
* Tạo ra các tổ hợp password + num và num + password để thử mật khẩu

**Thời gian dự kiến O(len(hybrid.txt) \* len(num) \* A) với A là hằng số với mỗi password cụ thể.**

1. **Tài liệu tham khảo**

StackOverFlow

WhiteHat.vn

Wikipedia

<https://github.com/topics/password-wordlist>

<https://stytch.com/blog/top-10-password-cracking-techniques/>

<https://github.com/HalilDeniz/PassBreaker/tree/main>

1. **Phụ lục 1: Giới thiệu (demo) kết quả**
2. **Link github sản phẩm:** [**https://github.com/TwinHter/23521045\_DoAnCK**](https://github.com/TwinHter/23521045_DoAnCK)
3. **Demo sản phẩm**

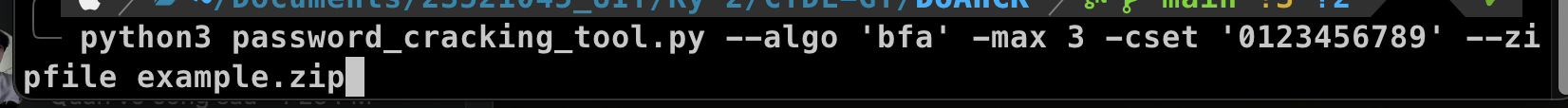
Sử dụng câu lệnh trong terminal để thực hiện sản phẩm

Câu lệnh: python3 password\_cracking\_tool.py <content>

Với content bao gồm:

|  |  |  |
| --- | --- | --- |
| --algo | ‘bfa’, ‘hb’, ‘da’ | Brute force attack, hybrid attack, dicitonary attack (default) |
| --zipfile | Text | Đường dẫn đến file zip cần crack |
| --min-length, -min | Int | Default = 1, độ dài tối thiểu của mật khẩu (dùng cho brute force attack) |
| --max-length, -max | Int | Default = 6, độ dài tối đa của mật khẩu (dùng cho brute force attack) |
| --character-set, -cset | Text | Default = ‘abcdefghijklmnopqrstuvwxyz0123456789’, chứa bộ ký tự của mật khẩu |





Demo sản phẩm: https://youtu.be/QzgecMvyD44 (Kênh Youtube TwinHter - Demo Password Cracking Ver2 – 23521045 UIT)

1. **Nhận xét** 
   * Mô hình chạy tốt với mật khẩu ngắn và bộ ký tự đơn giản.
   * Dictionary và Hybrid attack có thể bao quát được hơn 600000 mật khẩu phổ biến.
   * Với mật khẩu mang tính ngẩu nhiên và dài dòng, mô hình gần như sẽ không đưa ra được kết quả.