**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN 1**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 12**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 12: Crack mật khẩu.**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

Crack mật khẩu

**1. Mục đích**

- Hiểu được mối đe dọa về tấn công mật khẩu.

- Hiểu được nguyên tắc hoạt động của một số công cụ Crack mật khẩu trên các hệ điều hành Linux và Windows.

- Biết cách sử dụng công cụ để Crack mật khẩu trên các hệ điều hành Linux và Windows.

**2. Nội dung thực hành**

**2.1 Tìm hiểu lý thuyết**

**Mô tả ngắn gọn lý thuyết về các công cụ các công cụ crack mật khẩu trên hệ điều hành Windows và Linux**

- Các công cụ crack mật khẩu sình ra để bẻ khóa, khám phá mật khẩu máy tính. Điều này thường được thực hiện bằng cách khôi phục mật khẩu từ dữ liệu được lưu trữ hoặc vận chuyển từ hệ thống máy tính. Việc bẻ khóa mật khẩu được thực hiện bằng cách liên tục đoán mật khẩu, thường thông qua thuật toán máy tínhtrong đó máy tính thử nhiều kết hợp cho đến khi mật khẩu được phát hiện thành công.

- Danh sách các Tools Password:

* Crackers o Lophtcrack – WebCracker
* John The Ripper – Munga
* Bunga o Brutus – ReadCookies
* Obiwan – SnadBoy
* Authforce – WinSSLMiM
* Hydra - RAR o Cain & Abel Gammaprog

- Hầu hết các tools này đều miễn phí và nếu có phí thì hoàn toàn crack được một

cách dễ dàng. Hầu hết chúng đều có khả năng sử dụng tất cả các loại tấn công trên, đều có thể Export Username Password từ một hệ thống Local hay Remote.

- Cain & Abel là một tools vừa có thể Crack Password trên windows khingồi tại máy tính hay có thể tóm các gói tin trên mạng và giải mã ngược lại sử dụng: 4 Dictionary và Bruforce Attack. Ngoài ra Cain & Abel còn nằm trong số các phần mềm Sniffer.

- John the Ripper đây là phần mềm chuyên phá mật khẩu trong môitrường Unix và sử dụng mã hóa DES, Extend DES, MD5 cũng tích hợp nhiều phương pháp giải mã.

- Brutus là một chương trình Online hay Remote Password Cracker. Tấn công tới một hệ thống như máy chủ IIS, Windows, Modem ADSL....Chúng thử lần lượt Username và Password nhất định để tấn công vào máy chủ.

- Obiwan khắc phục nhược điểm của Brutus là có độ trễ khi sử dụng Username

Password sai.

- Authforce dựa vào HTTP Basic Authentication hỗ trợ việc thử Username Password tới một site nhất định o MessenPass có thể giải nénđược hầu hết các tài khoản chát như Yahoo, MSN...

* Mô tả cách thức hoặc phương pháp các công cụ sử áp dụng để crack mật khẩu trên hệ điều hành Windows và Linux

- Hầu hết các chương trình quản lý Password đều mã hóa Password theo một phương thức nào đó. Mật khẩu sau khi được tạo ra và lưu vào trong hệ thống sẽ được mã hóa, hệ thống sẽ chứa Key để giải mã mật khẩu. Những phần mềm Password Cracker sẽ tìm cách lấy được các đoạn mật mã đó. Sau khi đã lấy được các đoạn mật mã trên máy của nạn nhân chúng sẽ tiến hành giải mã mật khẩu bằng những phương thức cụ thể cho từng tình huống.

- Có 2 phương thức để tìm mật khẩu đơn giản là:

* Đoán mật khẩu
* Thay thế đoạn URL

- Các dạng Password Cracker

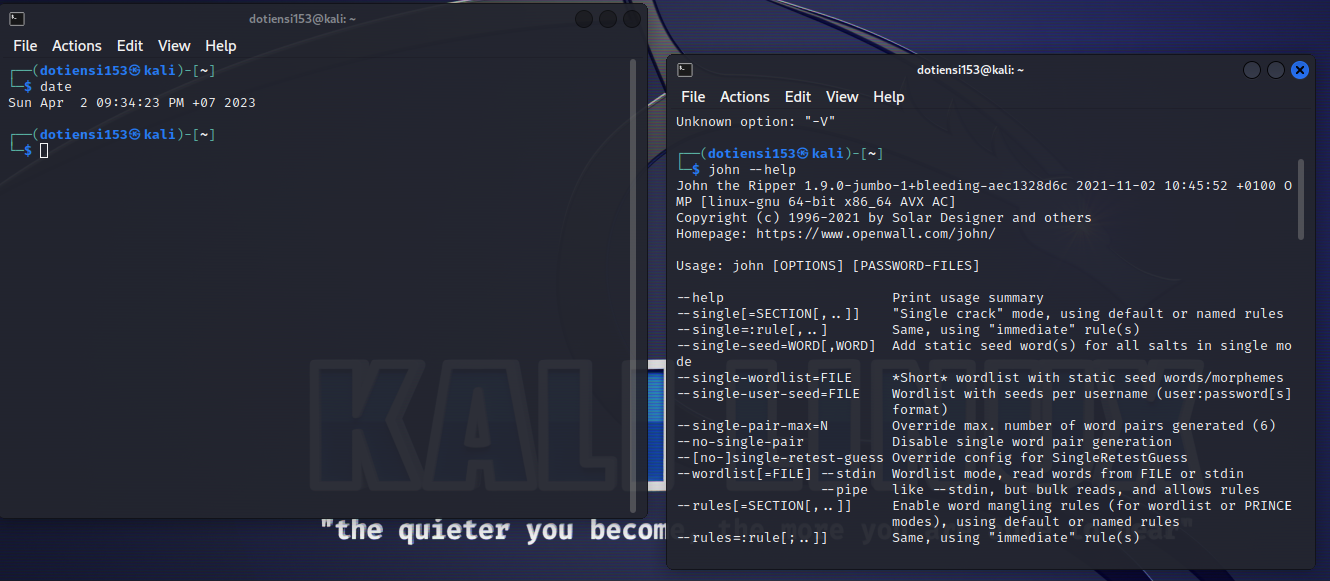
* Brute Force Attack: Tìm mật khẩu bằng cách tổ hợp các ký tự
* Hybird Attack: Lai giữa hai phương thức trên
* Smart Table Recovery Attack: Phương thức tấn công tìm mật khẩu thông minh nhất dựa trên các bảng dữ liệu – Khoảng 700MB dữ liệu text

**2.1 Bước thực hiện:**

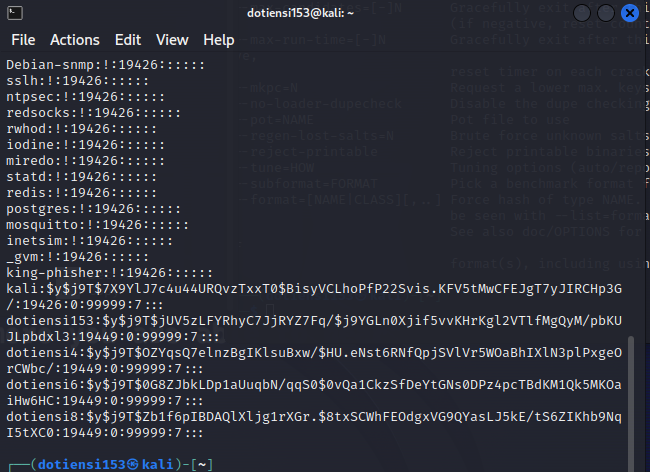
- Trên Windows và Kali Linux tạo 3 người dùng có tài khoản và mật khẩu như dưới

|  |  |
| --- | --- |
| Tài khoản | Mật khẩu |
| dotiensi4 | 1111 |
| dotiensi6 | 111111 |
| dotiensi8 | 11111111 |

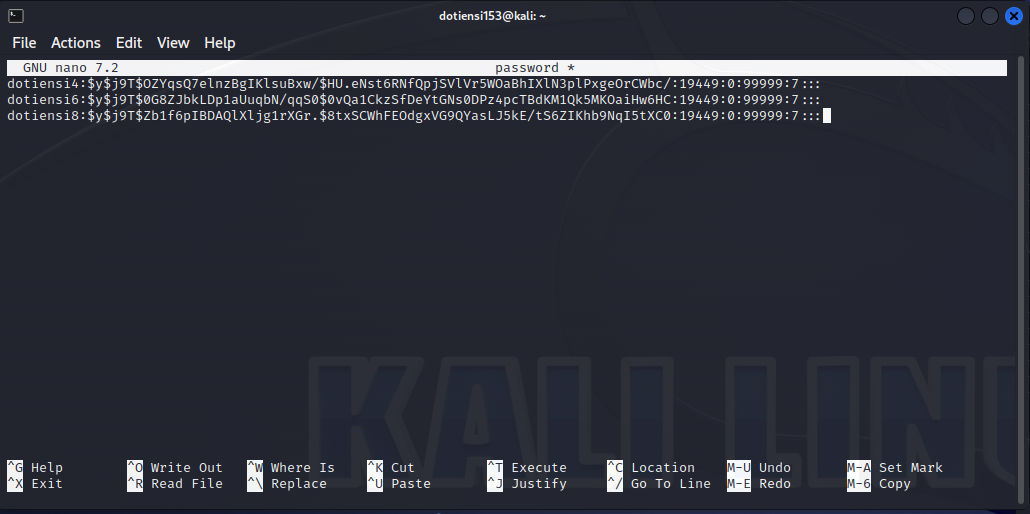
* Trên kali tải john(đã được hỗ trợ sẵn trên kali linux)

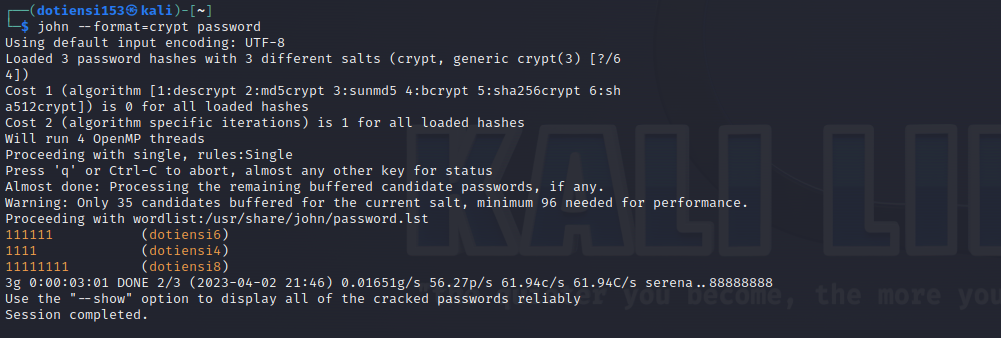


Người dùng đã được tạo, dùng **sudo cat /etc/shadow** để xem tài khoản mật khẩu người dùng



Copy vào file password



- Crack mật khẩu bằng john

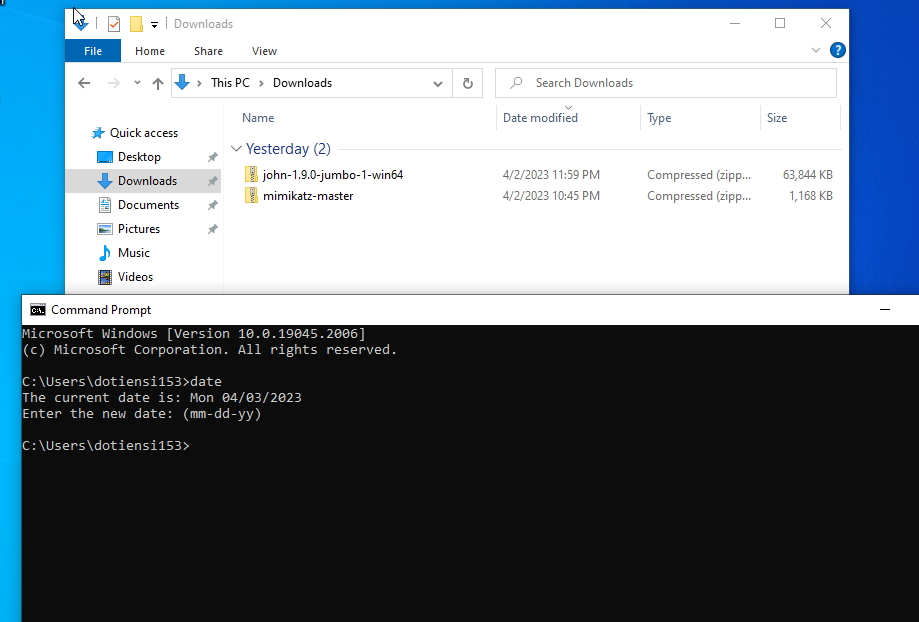
- Kết quả

Text

Description automatically generated with medium confidence

b, Crack mật khẩu trên máy ảo Windows

Tải mimikatz và John the ripper cho Windows



giải thích: các thông tin tài khoản người dùng được lưu trữ trong registry key

HKEY\_LOCAL\_MACHINE\SAM và HKEY\_LOCAL\_MACHINE\SECURITY.

Tuy nhiên, các thông tin này được mã hóa và bảo vệ chặt chẽ để đảm bảo an toàn cho người dùng

Text

Description automatically generatedText

Description automatically generated

- Tài khoản mật khẩu được lưu ở file hash.txt

Graphical user interface, text, application

Description automatically generated - Xóa dữ liệu thừa trong file, để lại tài khoản và mật khẩu dạng hash

Graphical user interface, text, application

Description automatically generated

* Crack mật khẩu

Text

Description automatically generated