HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH

HỌC PHẦN: THỰC TẬP CƠ SỞ

MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 3.2
TẤN CÔNG MẬT KHẨU

Sinh viên thực hiện:

PHẠM ĐỨC NAM – B22DCAT206

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HỌC KỲ 2 NĂM HỌC 2024-20

Mục lục

Danh mục hình ảnh

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 nghệ Crack mật khẩu trên các hệ điều hành Linux và Windows

2. Nội dung thực hành

2.1. Cơ sở lý thuyết: công cụ tấn công mật khẩu

a. OphCrack

OphCrack là một phần mềm mã nguồn mở chuyên dùng để khôi phục mật khẩu trên hệ điều hành Windows. Công cụ này tận dụng kỹ thuật tấn công mật khẩu thông qua bảng màu (rainbow tables) để giải mã các mật khẩu đã được băm bằng các thuật toán mã hóa. Với giao diện đồ họa trực quan, OphCrack dễ dàng sử dụng và có tốc độ phá mật khẩu nhanh, mặc dù các bảng màu thường chiếm dung lượng lưu trữ lớn

OphCrack có giao diện đồ họa và rất dễ sử dụng, crack mật khẩu rất nhanh tuy nhiên các rainbow của nó khá tốn dung lượng.

Đặc điểm nổi bật:

• Mã nguồn mở: Mã nguồn công khai, cho phép cộng đồng kiểm tra và tùy chỉnh, đảm bảo tính minh bạch.

• Hỗ trợ đa nền tảng: Hoạt động trên Windows, Linux và macOS, đáp ứng nhu cầu sử dụng linh hoạt.

• Phương pháp kết hợp: Kết hợp tấn công từ điển và bảng mã rainbow, nâng cao khả năng khôi phục mật khẩu.

• Giao diện thân thiện: Giao diện đồ họa đơn giản, phù hợp với người dùng không chuyên sâu về kỹ thuật.

• Hiệu suất cao: Tốc độ khôi phục phụ thuộc vào độ phức tạp mật khẩu và phần cứng, nhưng thường rất hiệu quả.

• Cập nhật thường xuyên: Được cải tiến để tương thích với các phiên bản Windows mới và nâng cao bảo mật.

b. PWDUMP

PWDUMP là một công cụ phần mềm dùng để thu thập thông tin về mật khẩu từ hệ thống Windows. Cụ thể, nó thường được sử dụng để thu thập và trích xuất mật khẩu đã

được mã hóa từ cơ sở dữ liệu của hệ thống Windows. Thông qua việc sử dụng

PWDUMP, người dùng có thể thu thập các mật khẩu này để phục vụ cho các mục đích kiểm tra bảo mật, phân tích hoặc khôi phục mật khẩu.

c. Hashcat:

- Hashcat là một công cụ mạnh mẽ, mã nguồn mở, chuyên dùng để bẻ khóa mật khẩu từ các giá trị băm, hoạt động trên giao diện dòng lệnh.

- Nó hỗ trợ hơn 300 thuật toán băm và cung cấp năm chế độ tấn công khác nhau. Hashcat tương thích với Linux, Windows và macOS, tận dụng CPU, GPU hoặc phần cứng chuyên dụng để tối ưu hóa tốc độ xử lý.

- Tuy nhiên, khi chạy trên máy ảo như Kali Linux trong VirtualBox, hiệu suất GPU thường bị hạn chế. Các chế độ tấn công:

- Từ điển (-a 0): Sử dụng danh sách mật khẩu phổ biến, băm từng giá trị và so sánh với giá trị băm đầu vào.

- Kết hợp (-a 1): Kết hợp hai danh sách (tên người dùng và mật khẩu) để thử các cặp giá trị, phù hợp khi tìm cả tài khoản và mật khẩu. • Mặt nạ (-a 3): Tạo các chuỗi ký tự ngẫu nhiên từ tập hợp ký tự được cung cấp, tương tự vét cạn nhưng có thể tùy chỉnh.

- Lai (-a 6, -a 7): Kết hợp từ điển và mặt nạ, tăng khả năng tìm mật khẩu phức tạp.

- Cú pháp cơ bản:

  hashcat -a -m

hashcat -a <tấn-công> -m <thuật-toán-hash> <file-chứa-hash-đầu-vào> <danh-sách hoặc chuỗi-ký-tự>

Theo đó ta có các thành phần bắt buộc phải có như sau:

- **-a:** Số của hình thức tấn công:

- **-a 0:** Dictionary
- **-a 1:** Combination
- **-a 3:** Mask
- **-a 6 và -a 7:** Dictionary + Mask

- **-m:** Số của thuật toán hash (bất cứ khi nào quên, bạn đều có thể tra cứu lại bằng lệnh **hashcat –help**). Trong ví dụ mình dùng -m 0 để chỉ thuật toán hash MD5.
- File chứa hash đầu vào
- **File chứa danh sách nếu tấn công Dictionary hoặc chuỗi ký tự nếu tấn công Mask**

VD: hashcat -a 0 -m 0 file-chứa-hash file-danh-sách

Chú ý: trên Kali cũng có 1 danh sách mật khẩu: /usr/share/wordlists/rockyou.txt

d. John The Ripper

John The Ripper là một công cụ bẻ khóa mật khẩu miễn phí, hoạt động trên giao diện dòng lệnh, hỗ trợ Linux, Windows và macOS. Điểm nổi bật là khả năng tự động nhận diện thuật toán băm, giúp đơn giản hóa quá trình sử dụng so với Hashcat. Công cụ này hỗ trợ nhiều định dạng mã hóa và phù hợp cho cả tấn công từ điển và vét cạn.

John The Ripper được thiết kế rất dễ sử dụng và có tích hợp cả tính năng tự động nhận diện thuật toán hash, thế nên chúng ta không cần phải xác định thuật toán rồi mới crack giống như Hashcat. Nó cũng hỗ trợ rất nhiều thuật toán mã hóa:

John the Ripper có các chế độ:

• Từ điển: So sánh các mật khẩu từ danh sách với giá trị băm của mật khẩu mục tiêu.

• Vét cạn: Thử mọi tổ hợp ký tự có thể, nhưng mất nhiều thời gian, đặc biệt với mật khẩu dài.Cú pháp sử dụng:

- Không chỉ định thuật toán crack: sẽ rất tốn thời gian
  John path/to/password-file

- Chỉ định thuật toán crack:
  john --format=<Format> path/to/password-file

- Crack mật khẩu sử dụng 1 danh sách từ điển:
  john --format=FORMAT --wordlist=mywordlist.txt path/to/password-file

  Trong đó, **--format=FORMAT** là định dạng của mật khẩu bạn muốn crack (ví dụ:

  --format=md5, **--format=sha512**,...), và **path/to/password-file** là đường dẫn đến tệp chứa mật khẩu.

2.2. Các bước thực hiện

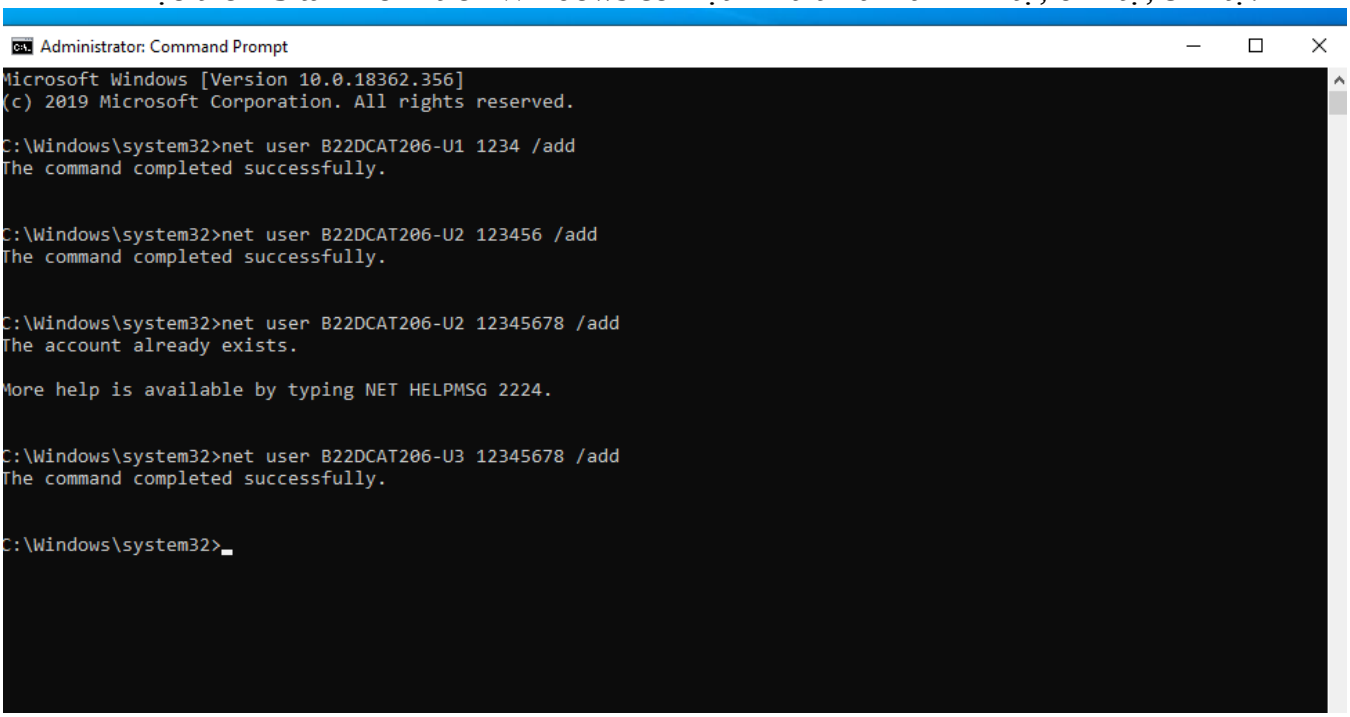
2.2.1 Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa.
- Phần mềm hệ điều hành Linux và Windows.
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Linux
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Windows

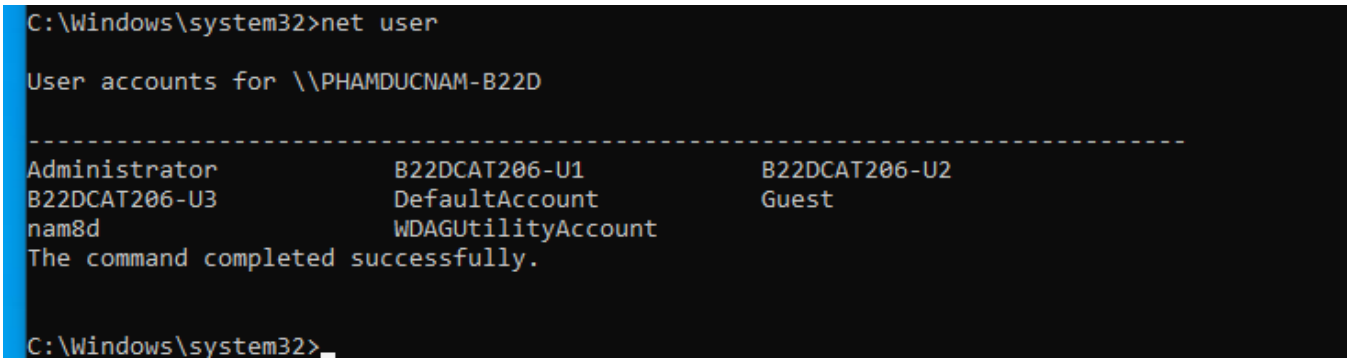
2.2.2 Crack mật khẩu trên Windows

Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,. ....Các tên tài khoản này đều có phần đầu là mã sinh viên.

- Tạo thêm 3 tài khoản trên Windows có mật khẩu thỏa mãn 4 kí tự, 6 kí tự, 8 kí tự:

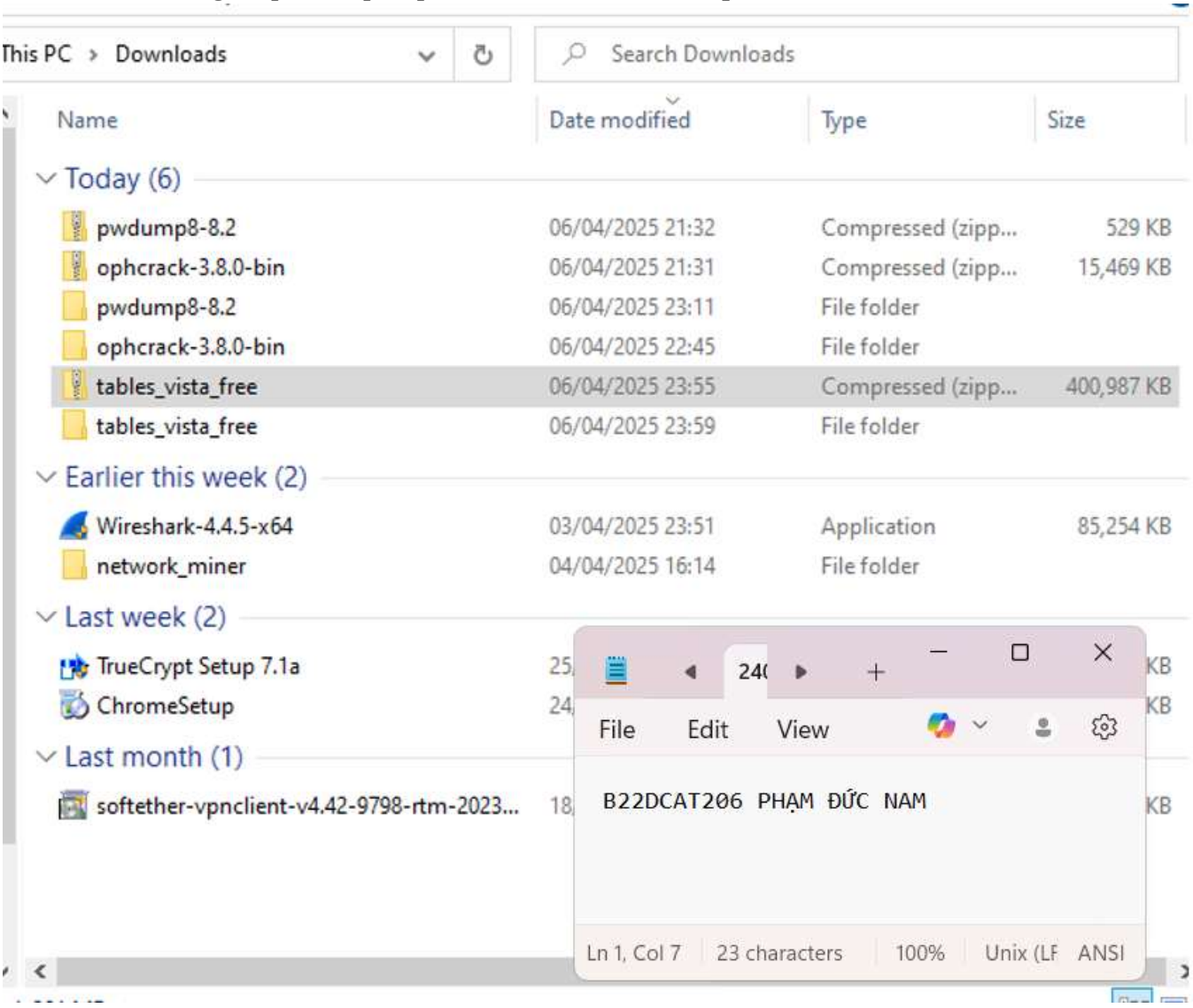


Tạo các Account

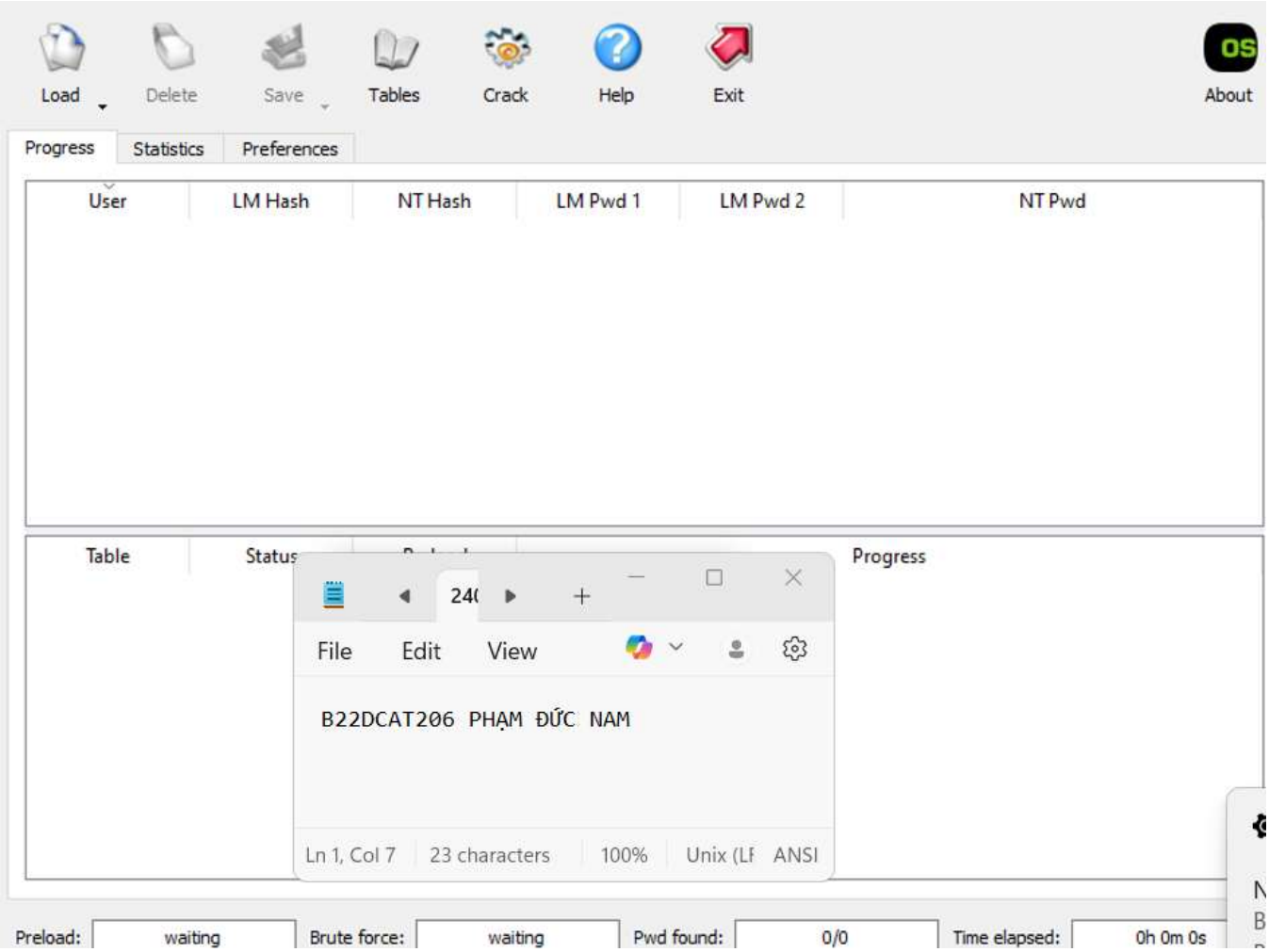


Kết quả

- Tải công cụ pwdump , ophcrack. Giải nén các tập tin đã tải và tiến hành cài đặt.



Các gói cần cài đặt



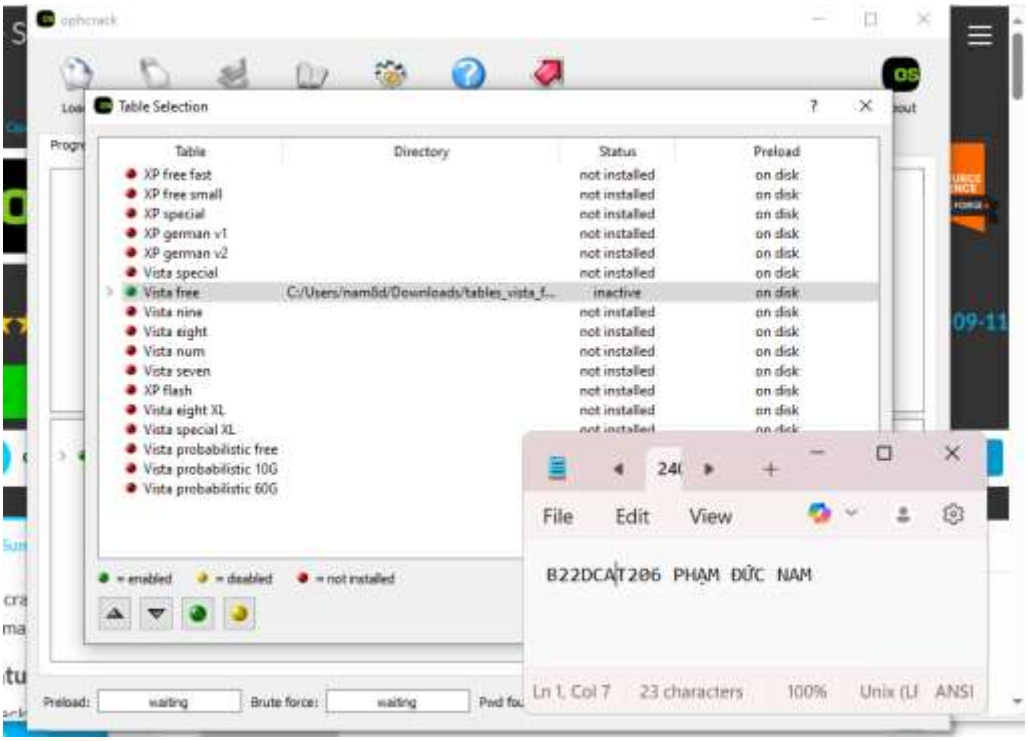
Giao diện OphCrack sau khi tải

- Chạy PwDump với quyền Administrator để trích xuất mật khẩu đăng nhập, đưa nó vào file NamB22AT206.txt

```
C:\Users\nam8d\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe

PwDump v8.2 - dumps windows password hashes - by Fulvio Zanetti & Andrea Petralia @ http://www.blackMath.it

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
DefaultAccount:503:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
WDAGUtilityAccount:504:AAD3B435B51404EEAAD3B435B51404EE:7CCFF9131352C53BD3844F5E715F6EC4
nam8d:1001:AAD3B435B51404EEAAD3B435B51404EE:C53A56E64CA3E837265B13590DE8E82C
B22DCAT206-U1:1006:AAD3B435B51404EEAAD3B435B51404EE:7CE21F17C0AEE7FB9CEBA532D0546AD6
B22DCAT206-U2:1007:AAD3B435B51404EEAAD3B435B51404EE:32ED87BDB5FDC5E9CBA88547376818D4
B22DCAT206-U3:1008:AAD3B435B51404EEAAD3B435B51404EE:259745CB123A52AA2E693AAACCA2DB52


C:\Users\nam8d\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe > NamB22AT206.txt
```

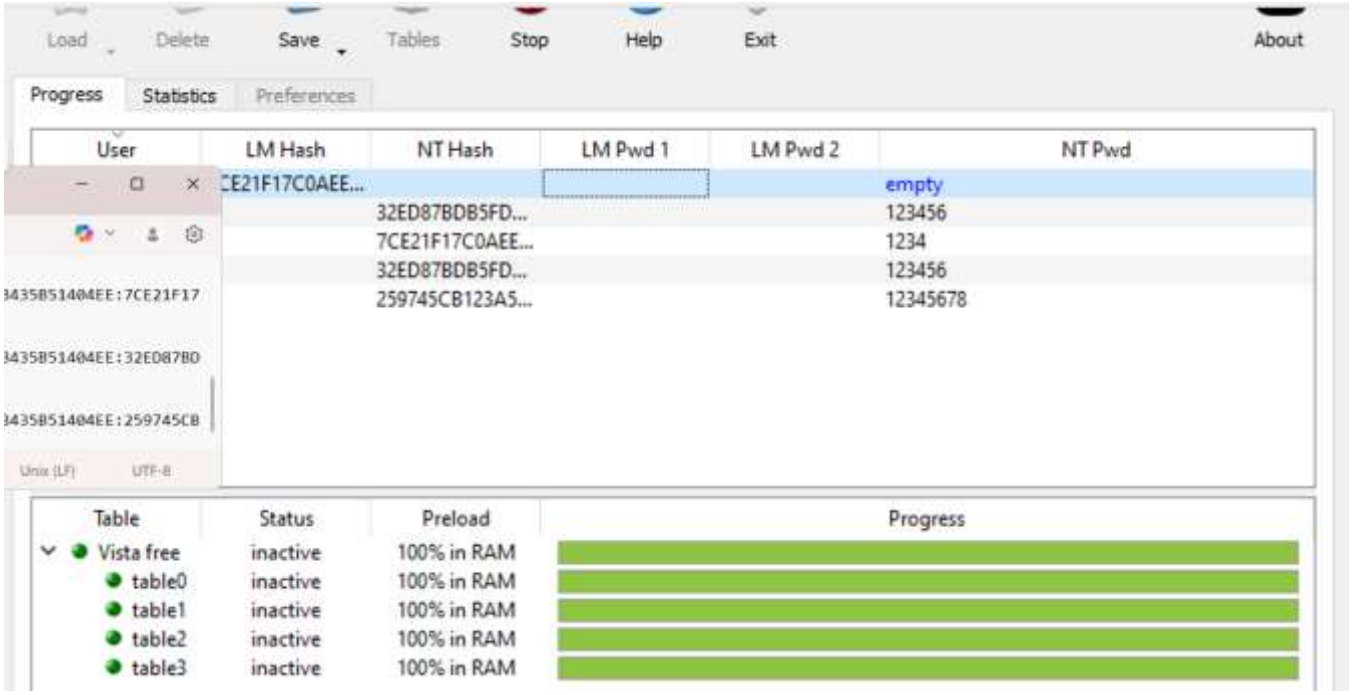
Trích xuất mật khẩu

- Lưu ý, mỗi dòng trong file NamB22AT206.txt cần phải đảm bảo đúng định dạng
- Sử dụng OphCrack để crack mật khẩu:
  + Đầu tiên phải kích hoạt các Rainbow đã tải: Tables → chọn thư mục đã lưu Rainbow



Kích hoạt Rainbow

- Crack các mật khẩu đã lưu trên file NamB22AT206.txt: Load → PWDUMP File → chọn File đã lưu. Đợi file tải hết và chọn Crack để tiến hành bẻ khóa mật khẩu. Kết quả đã bẻ khóa thành công mật khẩu 4 kí tự, 6 kí tự, 8 kí tự, 9 kí tự (cả số cả chữ) (rất nhanh).

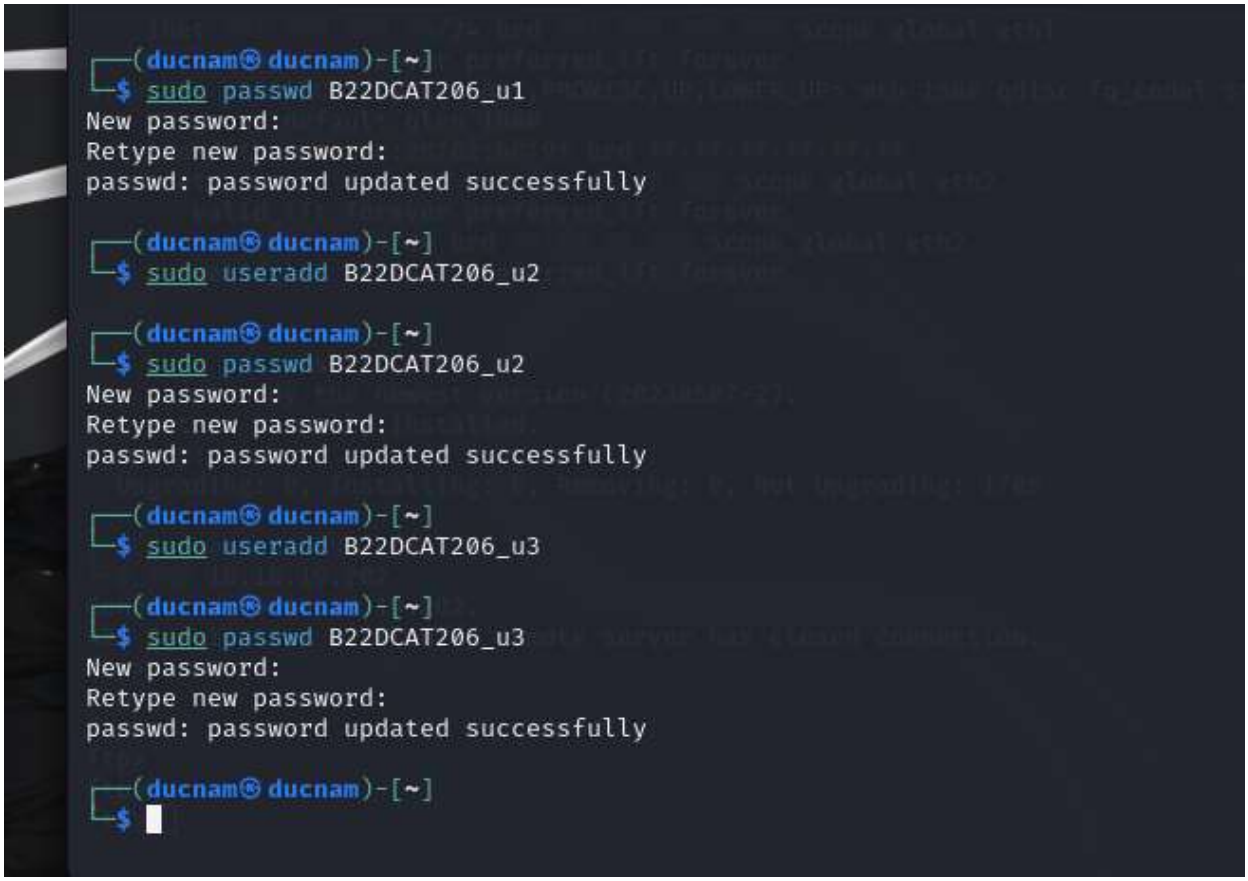


Kết quả

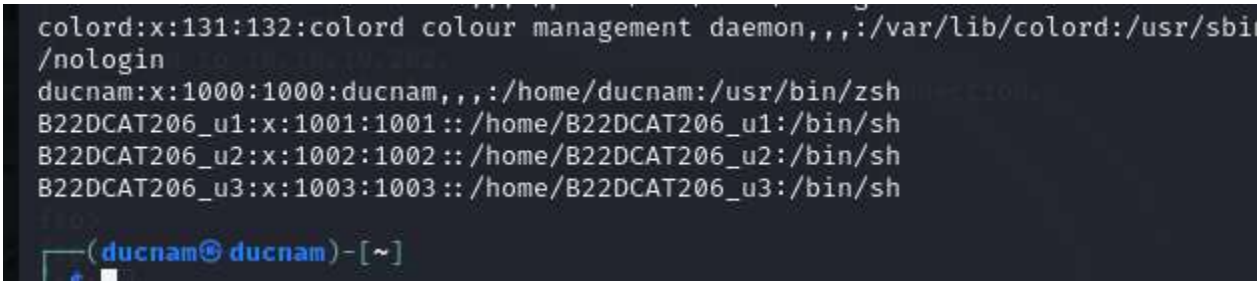
2.2.3 Crack mật khẩu trên Linux

Thử nghiệm crack mật khẩu trên hệ điều hành Linux với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,. ....Các tên tài khoản này đều có phần đầu là mã sinh viên.

- Tạo user và đặt mật khẩu theo yêu cầu



Tạo các User

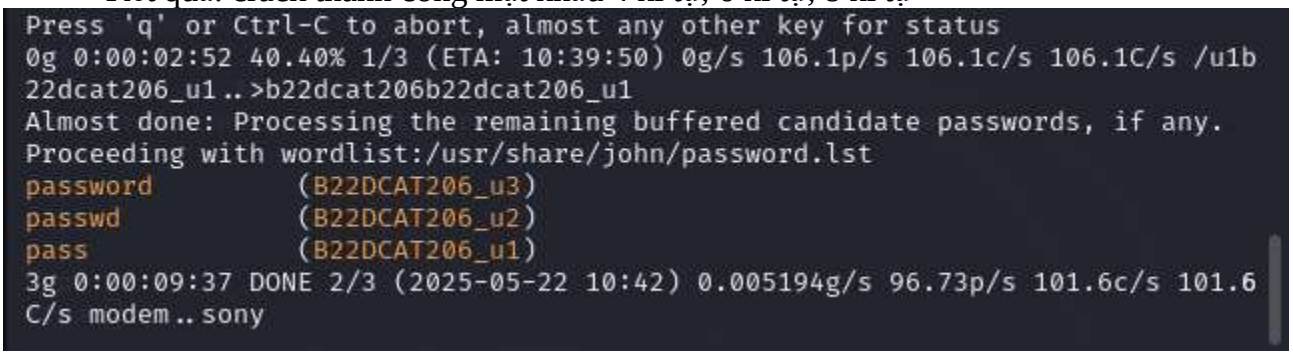


Kiểm tra lại trên file /etc/passwd

- Kết hợp 2 file /etc/passwd và file /etc/shadow để phục vụ cho quá trình crack mật khẩu sử dụng John The Ripper (đây là công cụ có sẵn trên Kali)

Kết hợp 2 file /etc/passwd và file /etc/shadow

- Kết quả: crack thành công mật khẩu 4 kí tự, 6 kí tự, 8 kí tự



Crack thành công mật khẩu 4 kí tự, 6 kí tự, 8 kí tự

3. Kết luận

- Lý thuyết về các công cụ crack mật khẩu trên Windows, Kali Linux
- Crack mật khẩu thành công trên Windows
- Crack mật khẩu thành công trên Kali Linux

4. Tài liệu tham khảo

[1]. Crack mật khẩu trên Windows: xem tại đây [2]. Crack mật khẩu trên Kali: Xem tại đây

[3]. Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.

[4]. Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman