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 VÀO MẬT KHẨU

Sinh viên thực hiện:

B22DCAT063 Lê Tiến Dương

Giảng viên hướng dẫn: PGS. TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SAM	Security Account Manager	Cơ sở dữ liệu lưu trữ tài khoản, mật khẩu (dạng hash) trên Windows
GUI	Graphical User Interface	Giao diện đồ họa người dùng

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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.

1.2 Tìm hiểu lý thuyết

1.2.1 OphCrack

OphCrack là một công cụ mã nguồn mở dùng để khôi phục mật khẩu trong hệ thống Windows. Đặc biệt, nó được sử dụng để phá mật khẩu của người dùng trên các phiên bản của hệ điều hành Windows bằng cách sử dụng kỹ thuật khai thác lỗ hổng mật khẩu. OphCrack sử dụng một phương pháp gọi là "bảng màu" hoặc "rainbow table" để tìm kiếm và phục hồi mật khẩu đã mã hóa bằng cách sử dụng thuật toán băm.

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.

OphCrack có một số đặc điểm đáng chú ý sau:

- *Mã nguồn mở*: Ophcrack là một phần mềm mã nguồn mở, điều này có nghĩa là mã nguồn của nó được công bố công khai và có thể được sửa đổi, phát triển bởi cộng đồng người dùng. Điều này tạo điều kiện cho sự minh bạch và kiểm soát mã nguồn.
- *Hỗ trợ đa nền tảng*: Ophcrack có sẵn cho nhiều nền tảng hệ điều hành, bao gồm Windows, Linux và macOS. Điều này cho phép người dùng sử dụng nó trên các hệ thống khác nhau.
- *Tích hợp tấn công từ điển và bảng mã rainbow*: Ophcrack thực hiện việc khôi phục mật khẩu bằng cách sử dụng cả tấn công từ điển và tấn công bảng mã rainbow. Điều này tăng cơ hội khôi phục mật khẩu thành công.
- *Giao diện đồ họa dễ sử dụng*: Ophcrack cung cấp một giao diện người dùng đồ họa (GUI) thân thiện và dễ sử dụng, không yêu cầu người dùng phải có kiến thức kỹ thuật sâu.
- *Hiệu suất và thời gian khôi phục*: Thời gian để khôi phục mật khẩu có thể biến đổi tùy thuộc vào độ phức tạp của mật khẩu và khả năng của máy tính. Tuy nhiên, Ophcrack thường có hiệu suất khá tốt trong việc khôi phục mật khẩu.
- *Cập nhật định kỳ*: Ophcrack thường được cập nhật để hỗ trợ các phiên bản mới của hệ điều hành Windows và để cải thiện hiệu suất cũng như bảo mật

1.2.2 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.

1.2.3 Hashcat

Hashcat là phần mềm crack hash/khôi phục mật khẩu từ hash nhanh nhất và tiên tiến nhất hiện nay trên giao diện dòng lệnh. Hashcat cung cấp cho người sử dụng 5 chế độ tấn công/khôi phục mật khẩu khác nhau áp dụng cho hơn 300 thuật toán hash khác nhau. Hashcat là một phần mềm mã nguồn mở và hoàn toàn miễn phí. Hashcat có thể được sử dụng trên nhiều nền tảng khác nhau như Linux, Windows và MacOS.

Ở thời điển hiện tại, Hashcat có thể sử dụng GPU, CPU và các phần cứng tăng tốc độ tính toán khác trên hệ thống máy tính để tăng tốc độ phá password hash. Tuy nhiên, vì phần lớn chúng ta sử dụng máy ảo Kali Linux trên Virtual Box, nên chúng ta sẽ mất đi sự hỗ trợ đắc lực của GPU (card đồ họa).

Trước khi sử dụng Hashcat, chúng ta phải xác định thuật toán mã hóa, có thể sử dụng công cụ: Hash Identifier (ở ngay trên Kali), Hash Analyzer của TunnelsUP.com (online), Password hash identification (online).

Hashcat hỗ trợ 4 hình thức crack hash:

- *Dictionary (-a 0)*: Bạn sẽ cung cấp cho Hashcat một danh sách (có thể là tập hợp những passwords hay được dùng nhất). Hashcat sẽ sử dụng lần lượt từng giá trị trong danh sách này để hash nó với thuật toán đã chỉ định và so sánh với hash đầu vào, nếu kết quả sai, Hashcat sẽ thử giá trị tiếp theo trong danh sách được cung cấp, nếu đúng thì Hashcat trả lại kết quả đã tạo nên giá trị hash trùng khớp với giá trị hash đầu vào.
- *Combination (-a 1)*: Tương tự như Dictionary attack ở trên, tuy nhiên khi dùng Combination các bạn sẽ phải cung cấp 2 danh sách chứ không phải chỉ 1 danh sách như Dictionary attack. Hình thức tấn công này được sử dụng khi bạn muốn tìm username và password của người dùng. Lúc này bạn sẽ cần 1 danh sách những usernames hay được dùng nhất và 1 danh sách những passwords hay được dùng nhất. Hashcat sẽ lần lượt tạo ra các cặp kết hợp giữa danh sách username và danh sách password và lần lượt thử đăng nhập bằng các cặp kết hợp này cho đến khi tìm ra được username và password chính xác hoặc cho đến khi tất cả các cặp kết hợp đều đã được thử và không có cặp nào chính xác.
- *Mask (-a 3)*: Mask attack tương tự như Bruteforce attack, bạn sẽ cung cấp một loạt các ký tự ví dụ a, b, c, d, e, f, 1, 2, 3, v.v. và từ các ký tự được cung cấp này, Hashcat sẽ tự kết hợp các ký tự lại với nhau và tạo ra các chuỗi ký tự ngẫu nhiên ví dụ như abc123, và các chuỗi này sẽ được dùng để tấn công giống như Dictionary attack. Cách tấn công này sẽ phù hợp để tìm những username và password không nằm trong

danh sách được cung cấp khi tấn công Dictionary attack, tuy nhiên sẽ rất mất thời gian.

- *Hybrid (-a 6 và -a 7)*: Kết hợp cả Dictionary attack và Mask attack.

Cú pháp cơ bản:

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

1.2.4 John The Ripper

John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu miễn phí. Đây cũng là một công cụ trên giao diện dòng lệnh và cũng có thể được cài trên nhiều hệ điều hành khác nhau như MacOS, Windows và Linux.

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:

- *Tấn công từ điển*: Nó lấy các mẫu chuỗi văn bản (trong danh sách từ điển), mã hóa nó theo cùng định dạng với mật khẩu đang được kiểm tra, rồi so sánh đầu ra với chuỗi mật khẩu được mã hóa.
- *Chế độ vét cạn*: nó sẽ thử tất cả các tổ hợp có thể của các ký tự, đem đi mã hóa rồi so sánh mật khẩu đã mã khóa cho đến khi tìm ra mật khẩu chính xác. Cách này rất tốn thời gian.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

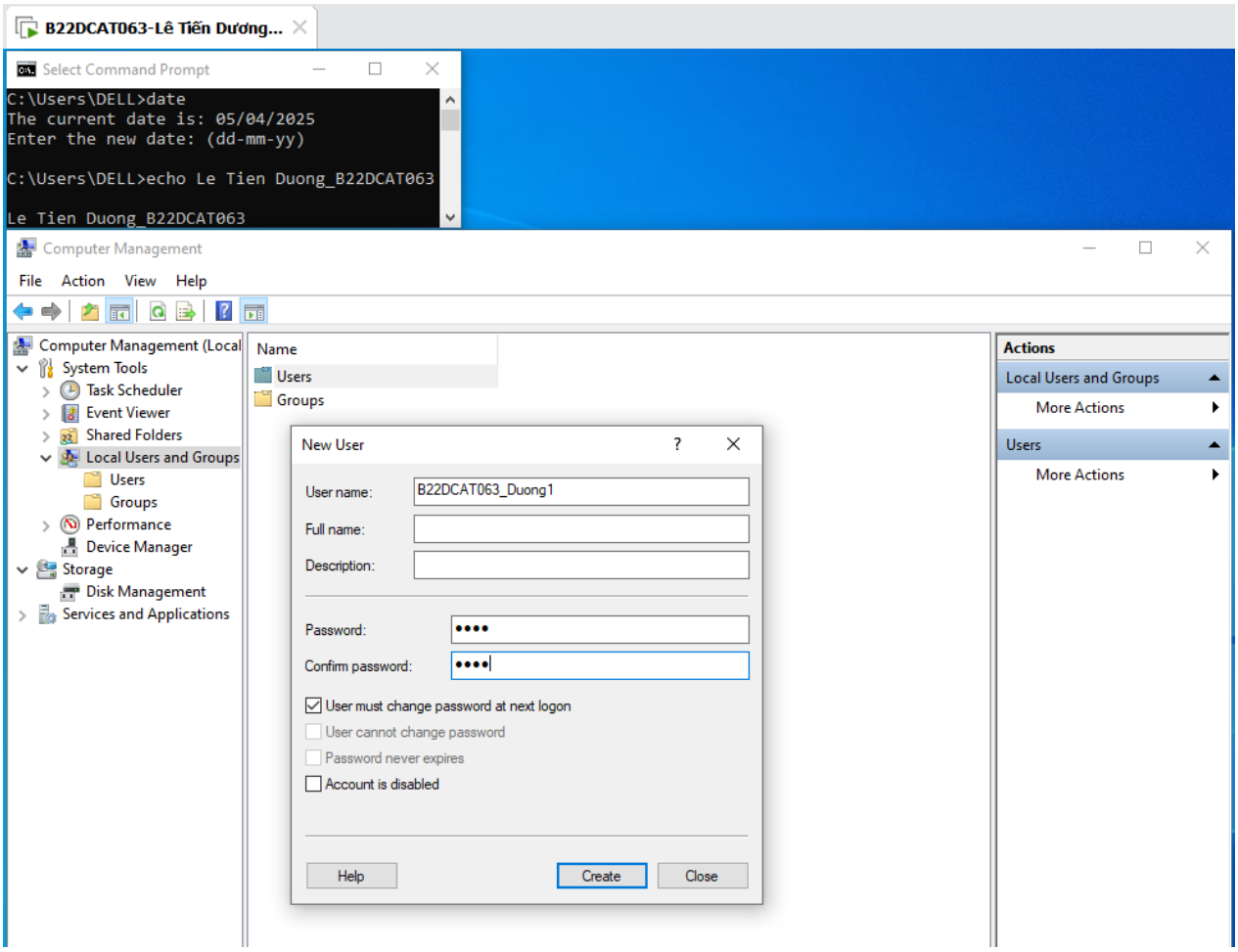
- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Phần mềm hệ điều hành Linux và Windows.
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Linux.
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Windows.

2.2 Các bước thực hiện

2.2.1 Crack mật khẩu trên Windows

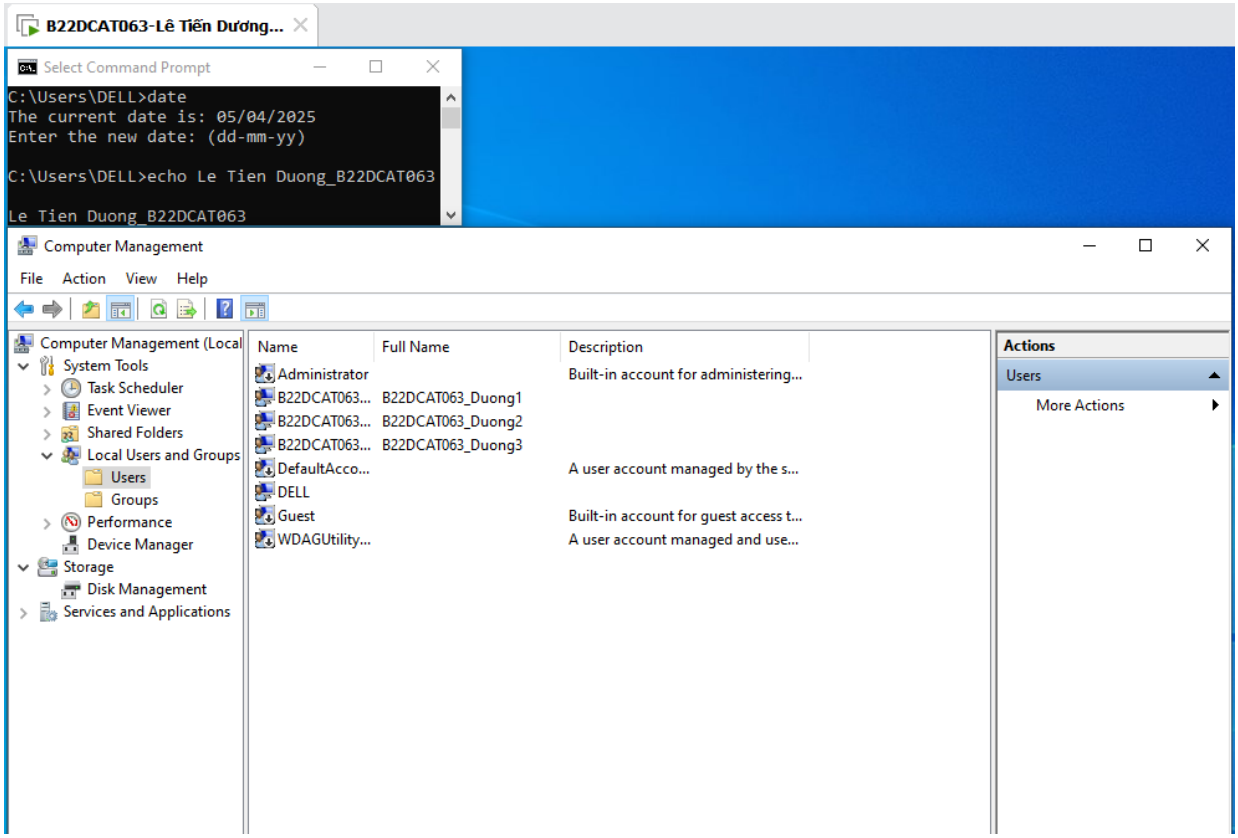
Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,.... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Tạo thêm 3 tài khoản trên Windows có mật khẩu thỏa mã 4 kí tự, 6 kí tự, 8 kí tự: Computer Management -> Local Users and Group -> Chuột phải vào Users -> New User.



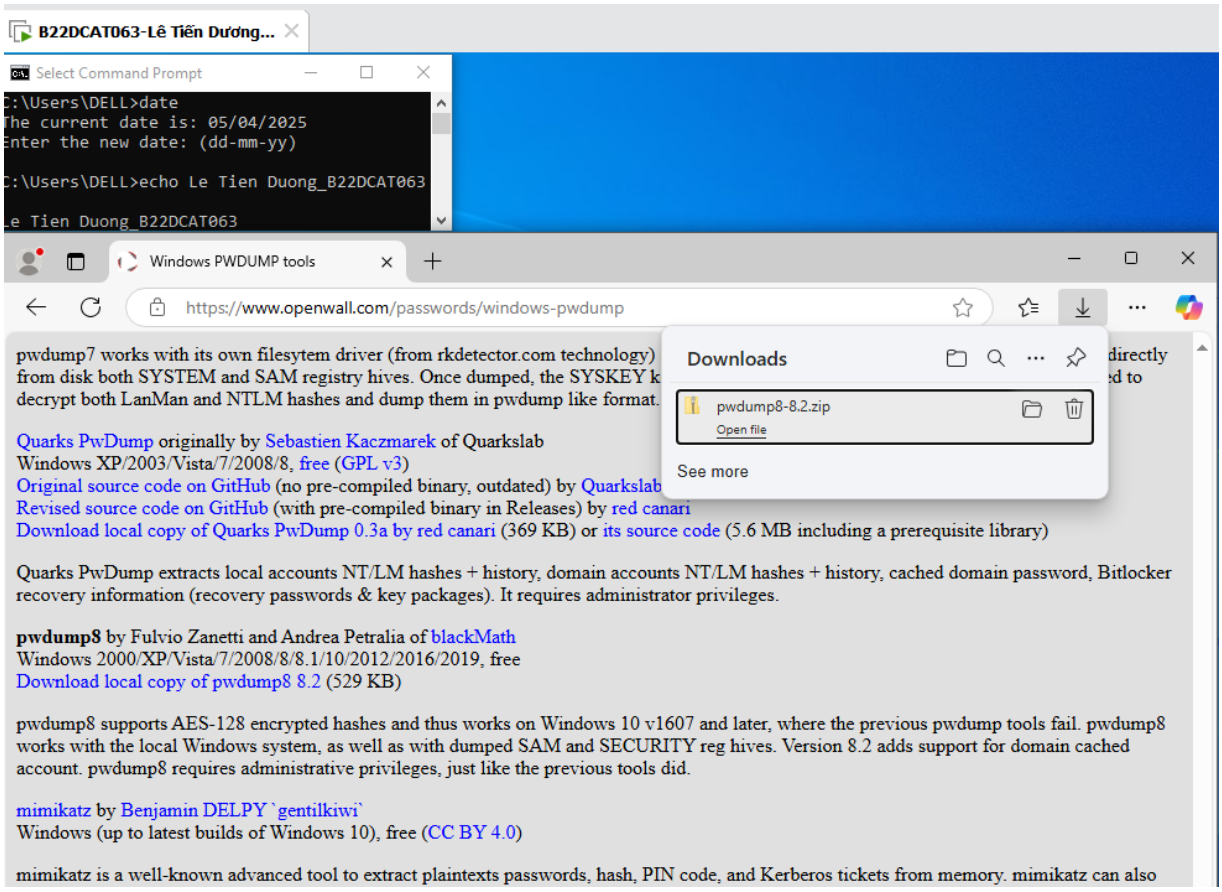
Hình 1 – Tạo người dùng mới

Kiểm tra kết quả sau khi tạo người dùng.

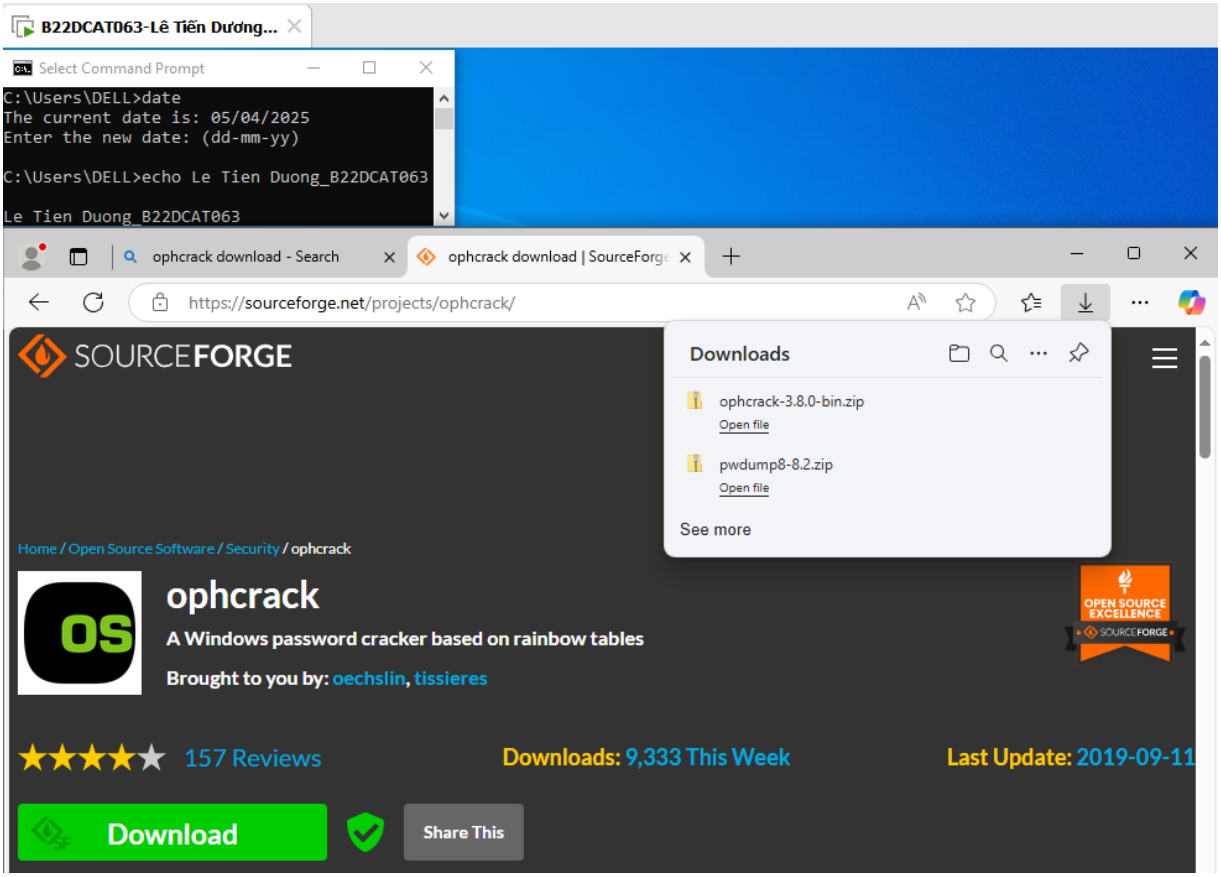


Hình 2 – Kiểm tra kết quả tạo người dùng

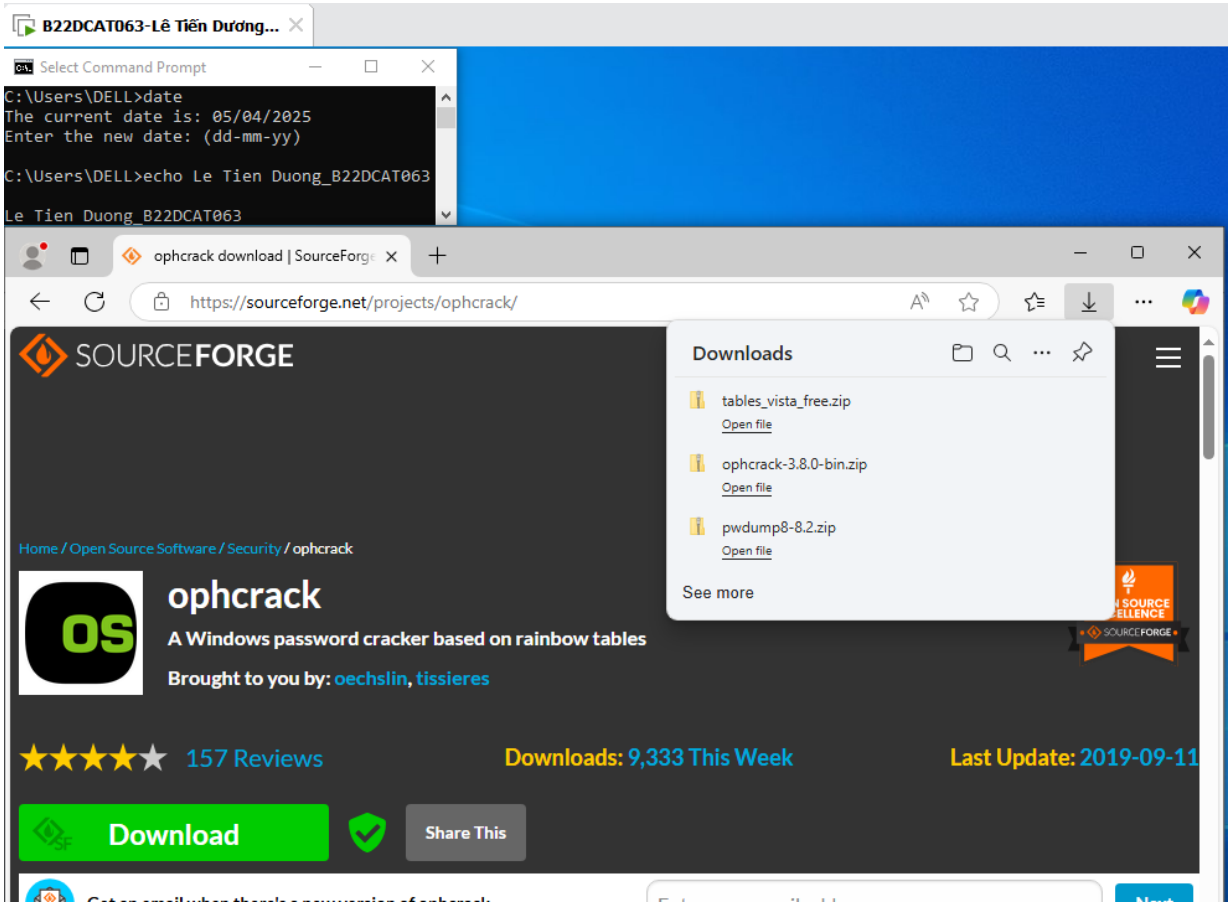
Tải các công cụ PwDump8, Ophcrack (phải tải cả các Rainbow của Ophcrack).



Hình 3 – Tải công cụ PwDump8

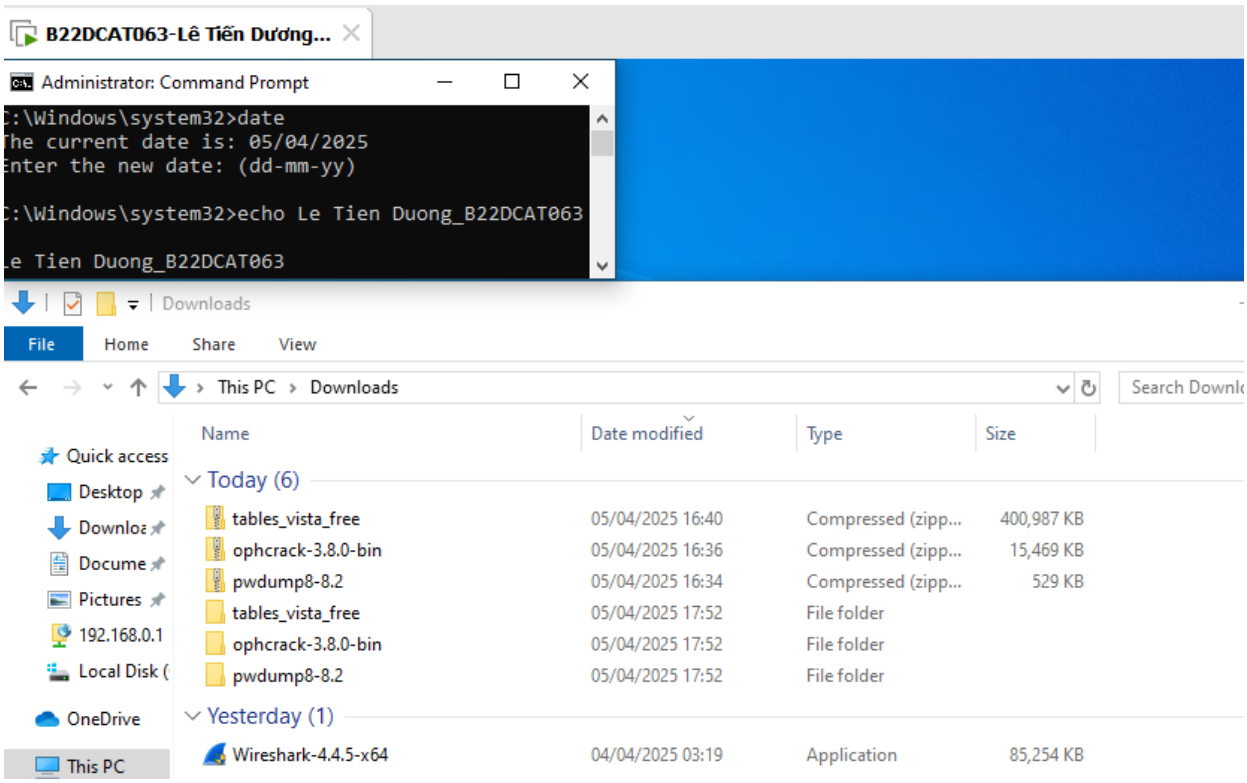


Hình 4 – Tải công cụ Ophcrack

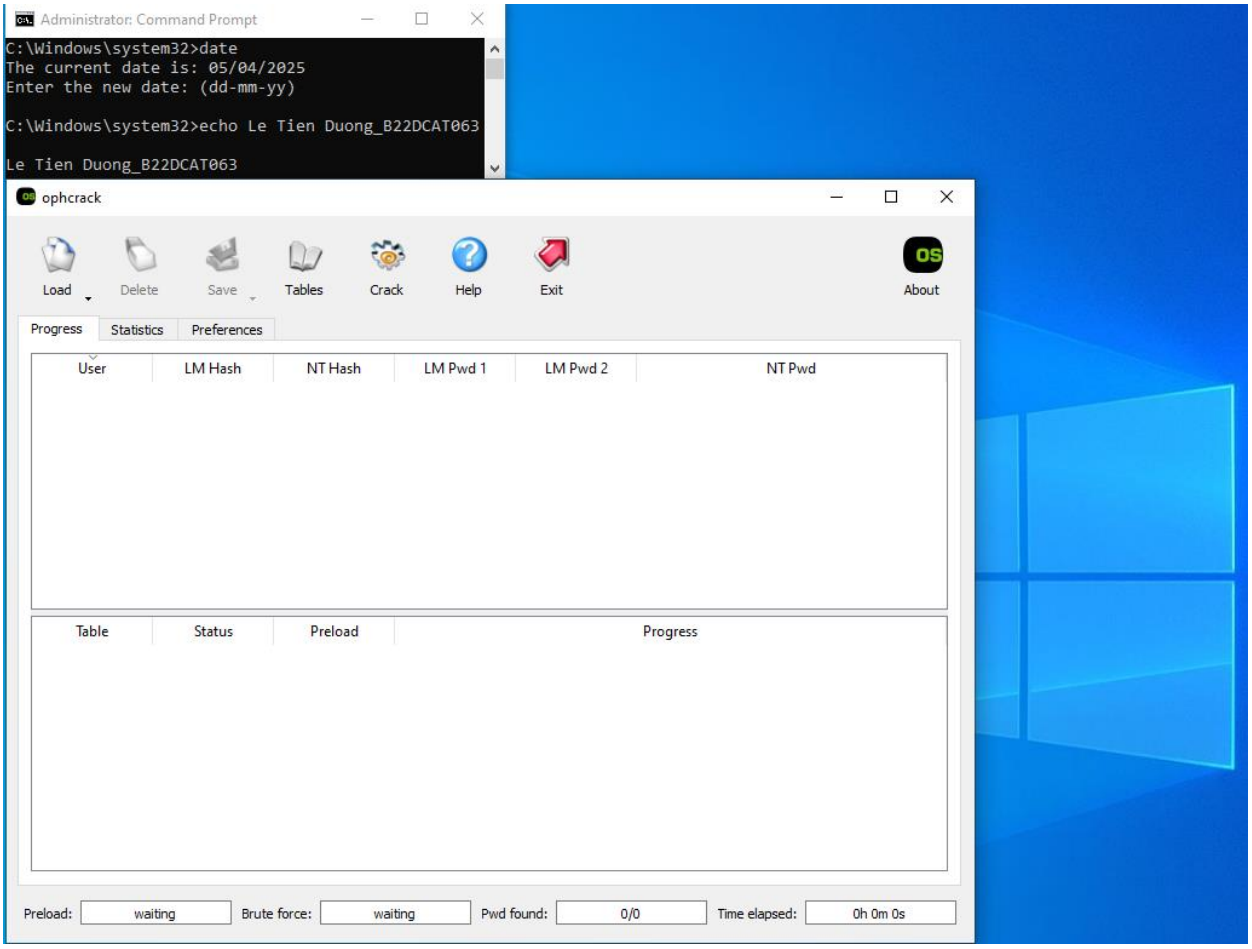


Hình 5 – Tải các rainbow của Ophcrack

Giải nén các tập tin đã tải về và tiến hành cài đặt.

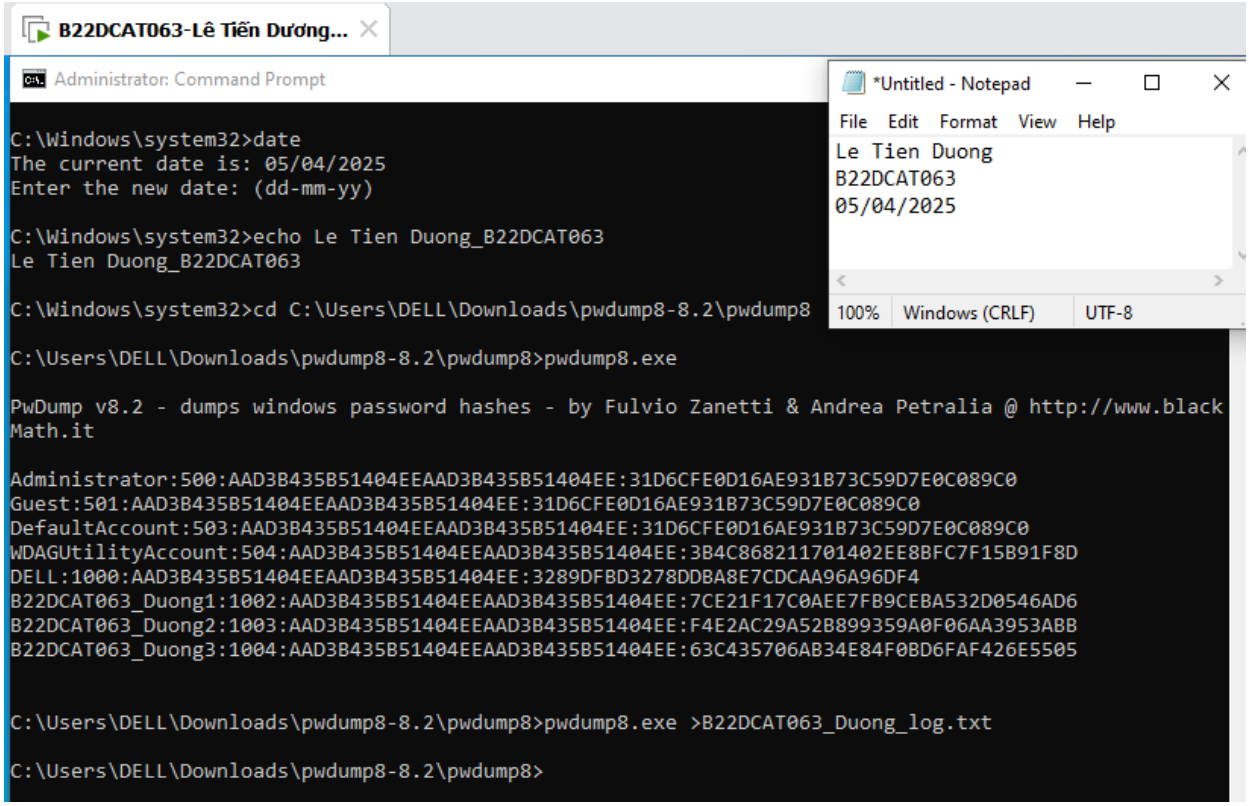


Hình 6 – Giải nén các tập tin vừa tải

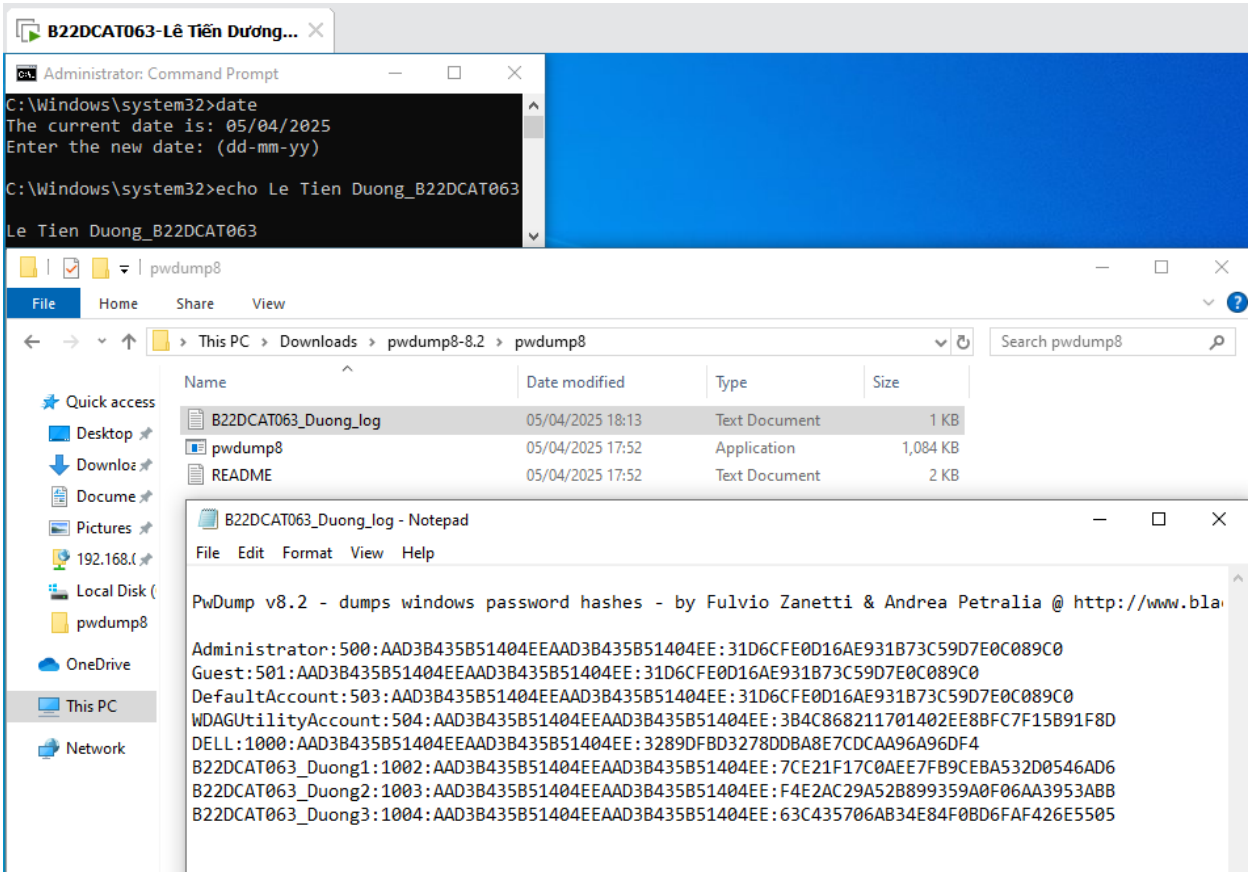


Hình 7 – Giao diện của Ophcrack sau khi cài đặt

Chạy PwDump với quyền Administrator để trích xuất mật khẩu đăng nhập, đưa vào file B22DCAT063_Duong_log.txt.



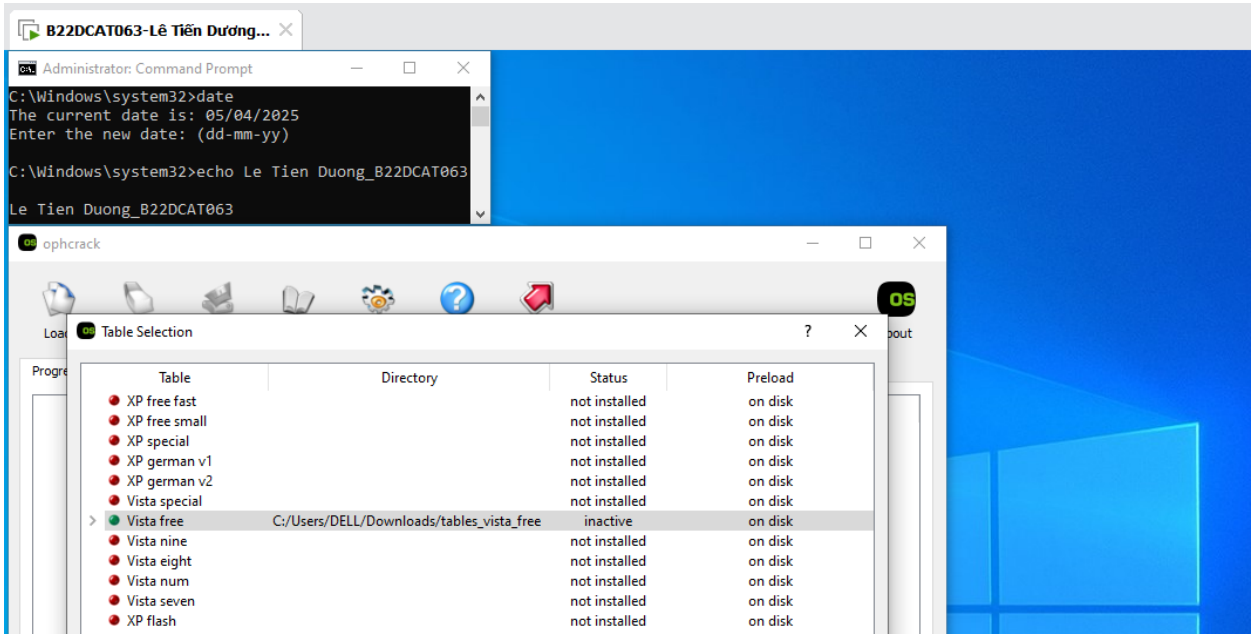
Hình 8 – Trích xuất các mật khẩu đăng nhập



Hình 9 – Kiểm tra lại file B22DCAT063_Duong_log.txt

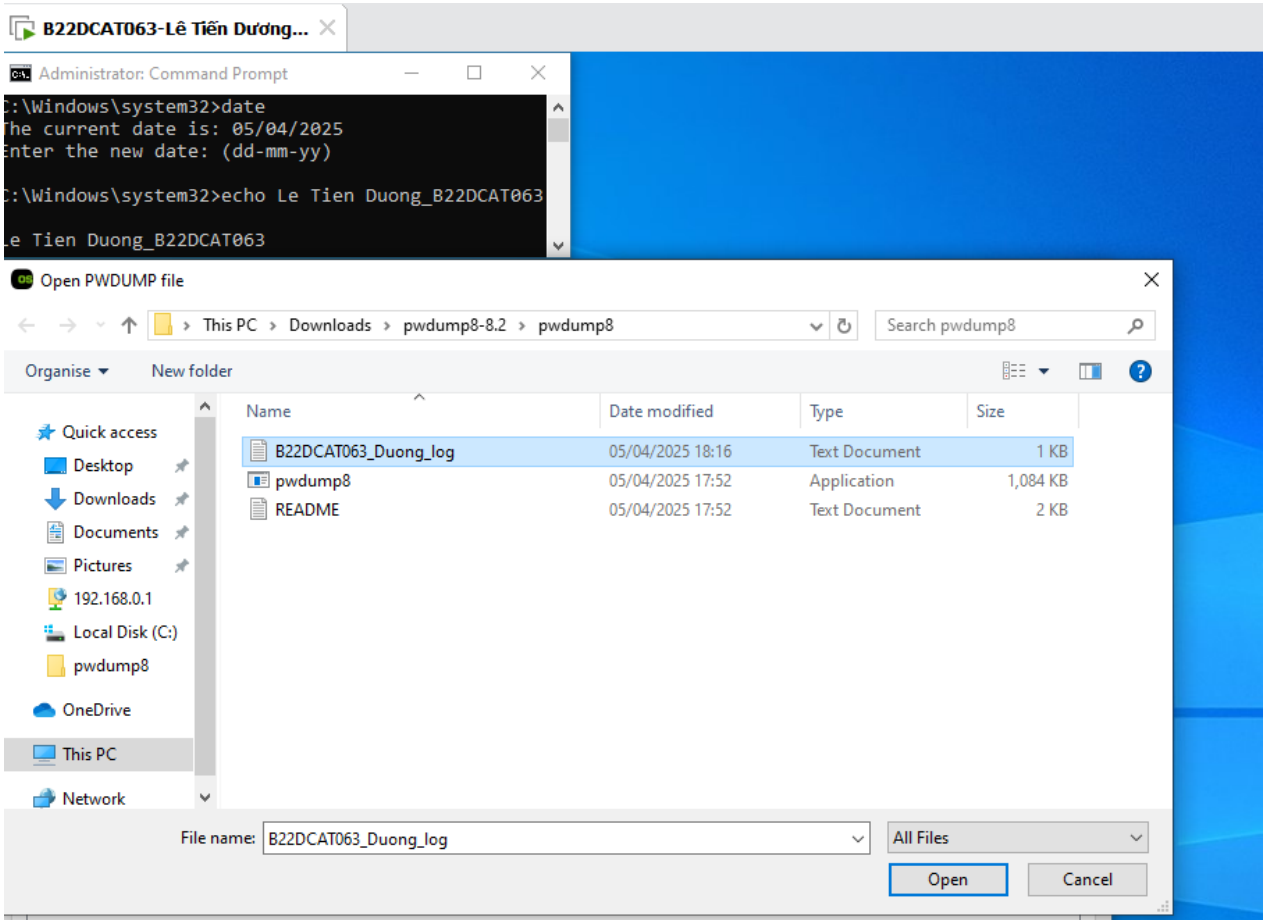
Sử dụng Ophcrack để crack mật khẩu:

Đầu tiên phải kích hoạt các Rainbow đã tải: Tables -> chọn thư mục đã lưu Rainbow.



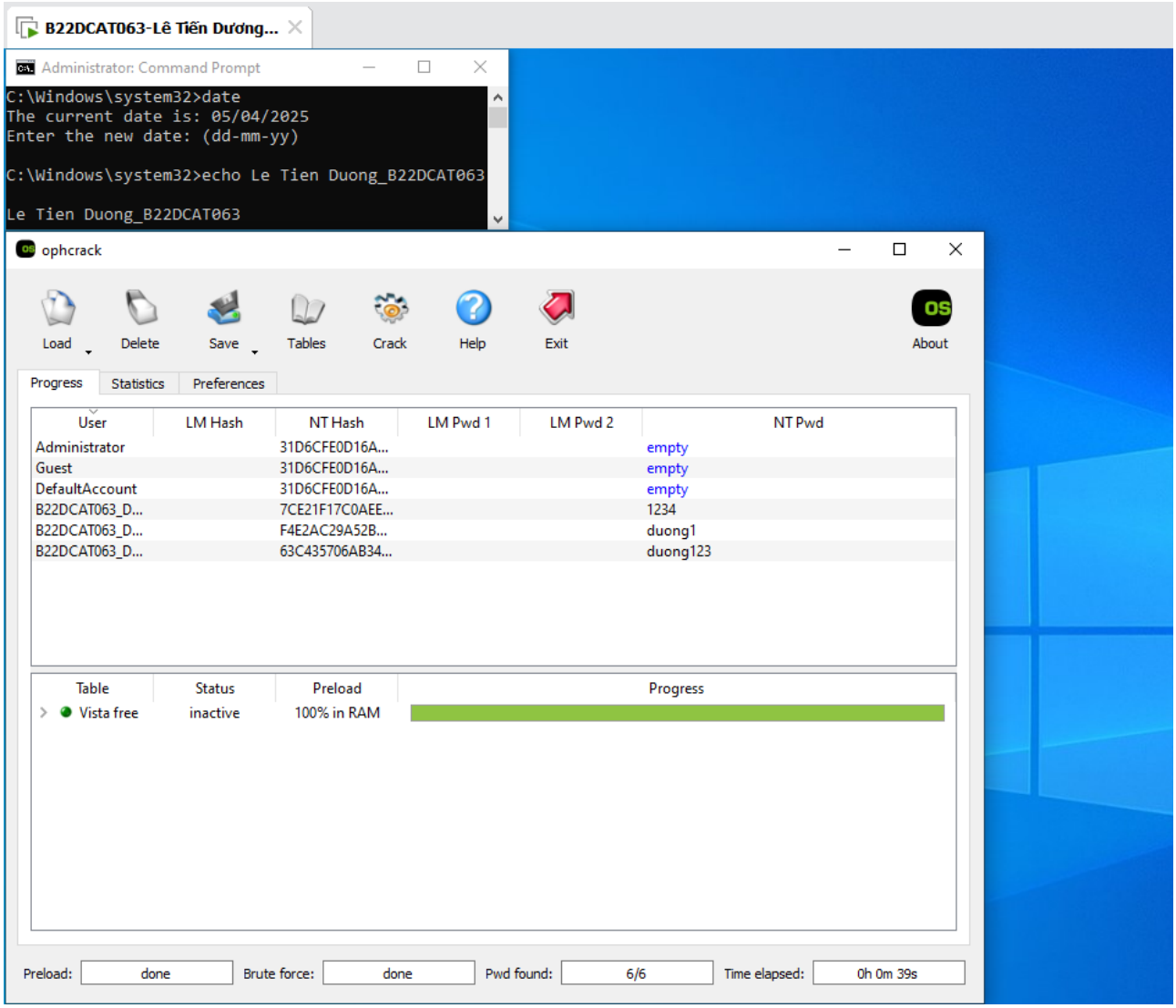
Hình 10 – Kích hoạt Rainbow

Crack các mật khẩu đã lưu trên file B22DCAT063_Duong_log.txt: Load → PWDUMP File → chọn File đã lưu. Đợi file tải hết.



Hình 11 – Chọn file log

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.

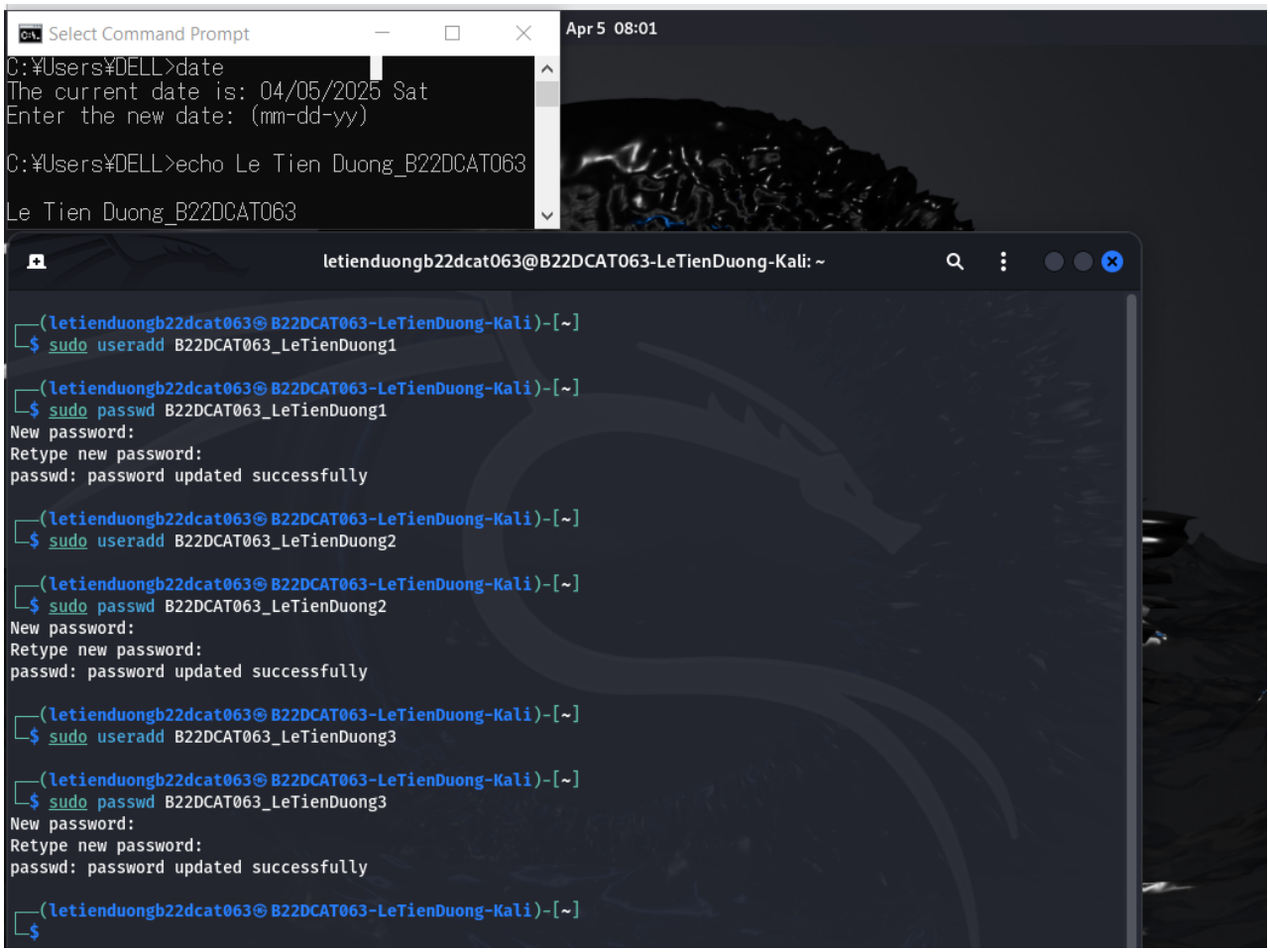


Hình 12 – Kết quả sau khi crack mật khẩu

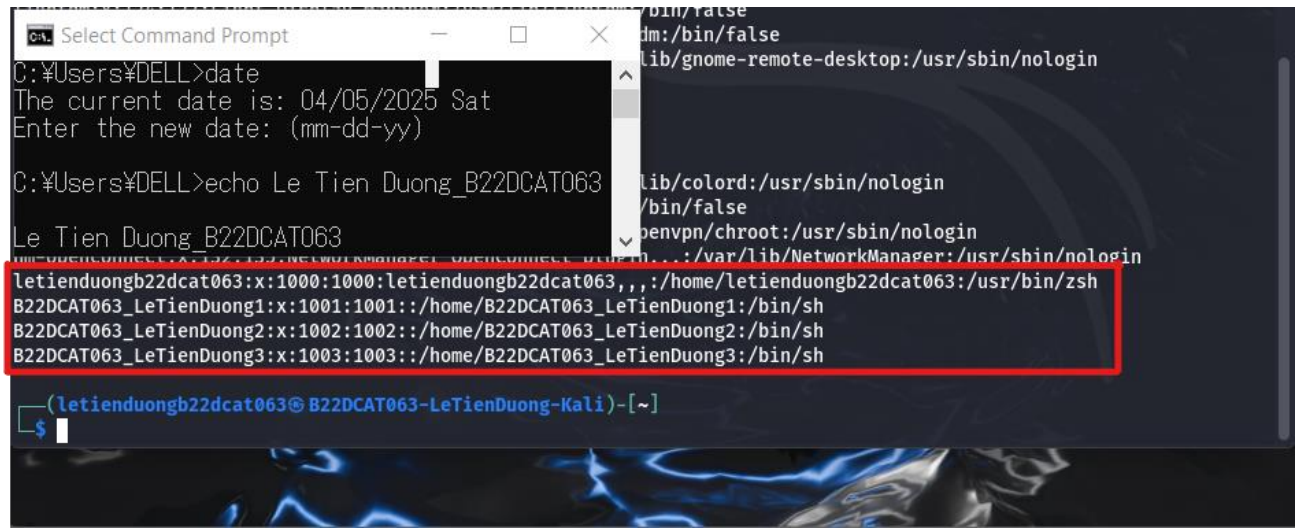
2.2.2 Crack mật khẩu trên Linux

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.

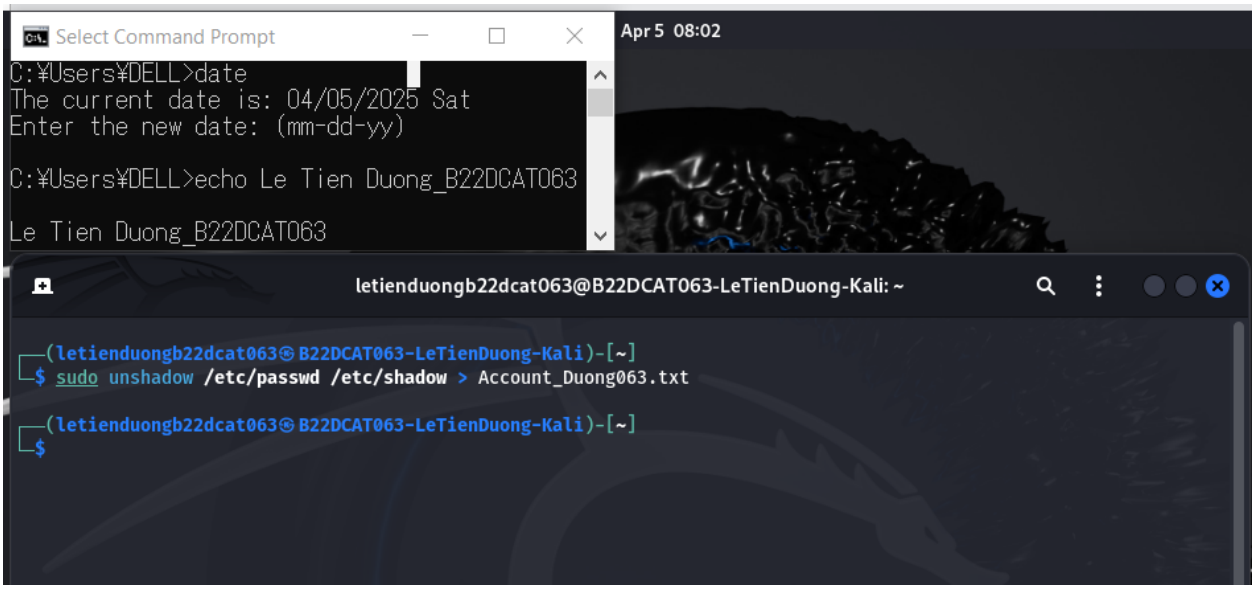


Hình 13 – Tạo các user và đặt mật khẩu



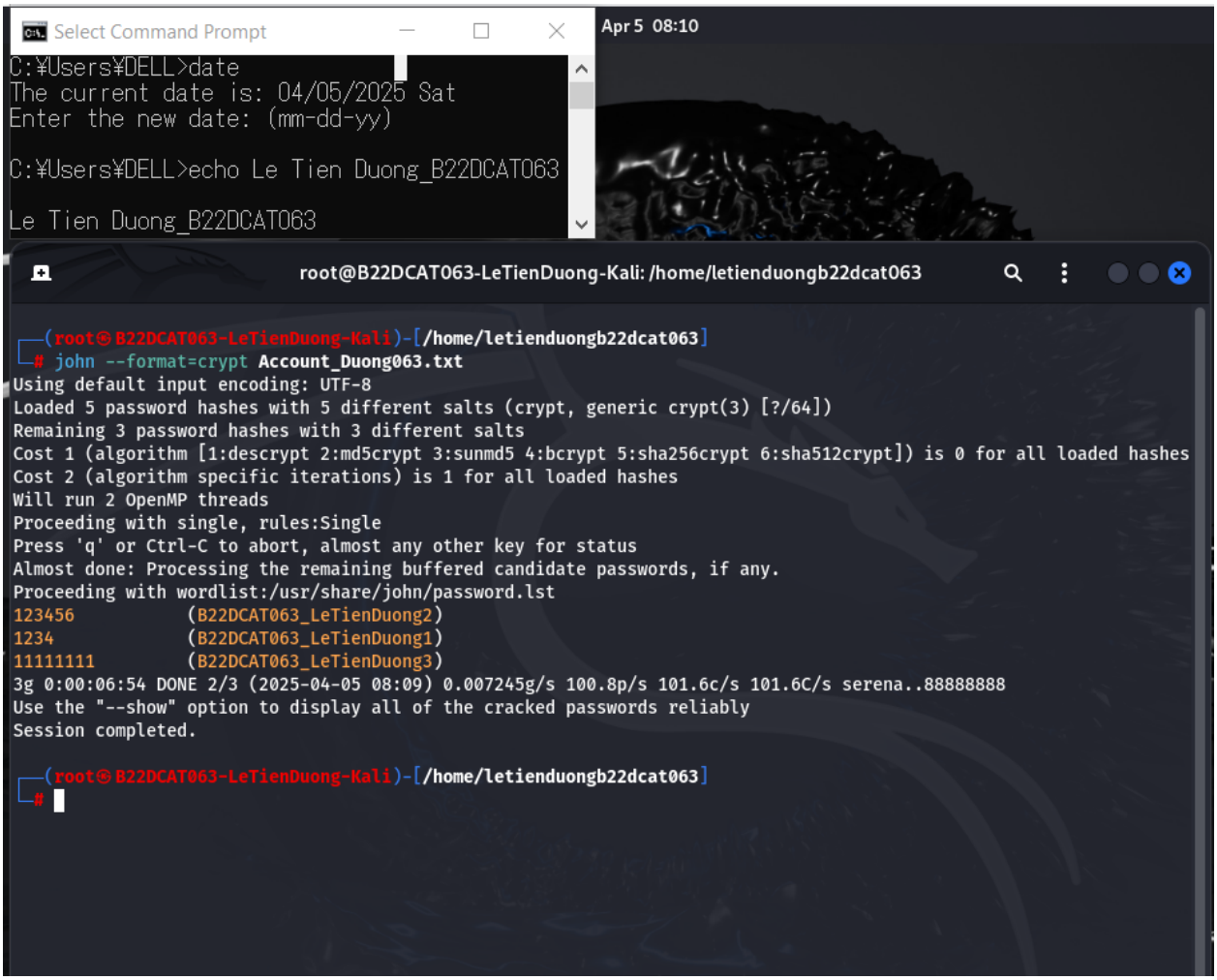
Hình 14 – Kiểm tra lại trên file /etc/password

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).



Hình 15 – 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.



Hình 16 – Crack thành công mật khẩu 4 kí tự, 6 kí tự, 8 kí tự

TÀI LIỆU THAM KHẢO

[1] 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.

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