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:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

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 Các công cụ crack mật khẩu trên hệ điều hành Windows

a) Ophcrack

- Mô tả: Một công cụ miễn phí, mã nguồn mở, sử dụng bảng cầu vồng (rainbow tables) để crack mật khẩu Windows dựa trên hash LM và NTLM. Nó đặc biệt hiệu quả với các mật khẩu đơn giản.
- Tính năng:
    - Giao diện đồ họa thân thiện (GUI).
    - Có phiên bản LiveCD để boot và crack mật khẩu mà không cần cài đặt.
    - Hỗ trợ Windows XP, Vista, 7 (ít hiệu quả hơn với Windows 8/10 do cải tiến bảo mật).
    - Cách hoạt động: Tải bảng cầu vồng miễn phí từ trang web chính thức, sau đó phân tích file SAM (Security Accounts Manager) của Windows để lấy hash và crack.
- Ưu điểm: Dễ sử dụng, miễn phí.
- Nhược điểm: Không hiệu quả với mật khẩu dài hoặc phức tạp, không hỗ trợ tốt các phiên bản Windows mới (10/11).

b) Cain & Abel

- Mô tả: Một công cụ mạnh mẽ và miễn phí dành riêng cho Windows, hỗ trợ nhiều phương pháp crack mật khẩu như brute-force, dictionary attack, và cryptanalysis.
- Tính năng:
    - Trích xuất hash từ file SAM.
    - Ghi lại lưu lượng mạng (sniffing) để lấy mật khẩu.
    - Crack mật khẩu Wi-Fi, VoIP, và các giao thức khác.
- Cách hoạt động: Sử dụng GUI để nhập hash từ SAM hoặc bắt gói tin mạng, sau đó áp dụng các kỹ thuật tấn công để tìm mật khẩu.

- Ưu điểm: Đa năng, giao diện dễ dùng.
- Nhược điểm: Chỉ chạy trên Windows, không còn được cập nhật (phiên bản cuối từ 2014).

c) John the Ripper

- Mô tả: Một công cụ mã nguồn mở nổi tiếng, ban đầu phát triển cho Unix nhưng có phiên bản Windows (thường dùng qua command line hoặc GUI như Hash Suite).
- Tính năng:
    - Hỗ trợ hàng trăm loại hash (LM, NTLM, MD5, SHA, v.v.).
    - Các chế độ tấn công: brute-force, dictionary, hybrid.
    - Có phiên bản Pro với tính năng nâng cao.
- Cách hoạt động: Trích xuất hash từ file SAM (dùng công cụ như pwdump), sau đó chạy John để crack.
- Ưu điểm: Linh hoạt, mạnh mẽ, miễn phí (bản cơ bản).
- Nhược điểm: Yêu cầu kỹ năng dòng lệnh, cần danh sách từ (wordlist) tốt để hiệu quả.

d) Hashcat

- Mô tả: Được coi là công cụ crack mật khẩu nhanh nhất thế giới nhờ tận dụng GPU (card đồ họa) để tăng tốc độ xử lý.
- Tính năng:
    - Hỗ trợ hơn 300 loại hash (bao gồm NTLM, SHA, MD5).
    - Các chế độ tấn công: brute-force, dictionary, mask, hybrid.
    - Tối ưu hóa cho cả CPU và GPU.
- Cách hoạt động: Trích xuất hash từ Windows (qua SAM hoặc công cụ như fgdump), sau đó dùng Hashcat để crack với tốc độ cao.
- Ưu điểm: Cực nhanh, miễn phí, mã nguồn mở.
- Nhược điểm: Cần phần cứng mạnh (GPU tốt), không có GUI chính thức (dòng lệnh).

e) L0phtCrack

- Mô tả: Một công cụ thương mại chuyên dụng để kiểm tra và crack mật khẩu Windows, sử dụng các kỹ thuật như dictionary, brute-force, và rainbow tables.
- Tính năng:
    - Trích xuất hash từ SAM hoặc từ mạng.
    - Đánh giá độ mạnh của mật khẩu trong hệ thống.
    - Hỗ trợ Windows XP đến 10/11.

- Cách hoạt động: Quét hệ thống để lấy hash, sau đó áp dụng các phương pháp tấn công để tìm mật khẩu.
- Ưu điểm: Giao diện thân thiện, hiệu quả với hệ thống doanh nghiệp.
- Nhược điểm: Phiên bản đầy đủ phải trả phí, không miễn phí như các công cụ khác.

f) Passware Kit

- Mô tả: Một bộ công cụ thương mại cao cấp để khôi phục mật khẩu, không chỉ cho Windows mà còn cho file Office, PDF, ZIP, v.v.
- Tính năng:
    - Crack mật khẩu Windows (tài khoản local và domain).
    - Tận dụng GPU để tăng tốc.
    - Hỗ trợ Windows 2000 đến 11.
- Cách hoạt động: Tạo USB hoặc đĩa boot để truy cập hệ thống bị khóa, sau đó crack hash từ SAM.
- Ưu điểm: Chuyên nghiệp, hỗ trợ kỹ thuật tốt, giao diện dễ dùng.
- Nhược điểm: Giá cao (từ $49 cho bản cơ bản đến hàng trăm đô cho bản đầy đủ).

g) Offline NT Password & Registry Editor

- Mô tả: Một công cụ miễn phí không crack mật khẩu mà xóa hoặc đặt lại mật khẩu Windows bằng cách chỉnh sửa trực tiếp file SAM.
- Tính năng:
    - Xóa mật khẩu tài khoản local.
    - Hỗ trợ tất cả phiên bản Windows (XP đến 11).
    - Dùng qua USB/CD bootable.
- Cách hoạt động: Boot từ USB/CD, truy cập Registry, và xóa hash mật khẩu trong SAM.
- Ưu điểm: Nhanh, miễn phí, không cần crack mật khẩu gốc.
- Nhược điểm: Không khôi phục được mật khẩu cũ, chỉ xóa hoặc thay mới.

h) THC Hydra

- Mô tả: Một công cụ crack mật khẩu mạng nhanh, hỗ trợ Windows khi tấn công các dịch vụ như RDP, SMB, hoặc HTTP.
- Tính năng:
    - Brute-force và dictionary attack qua mạng.
    - Hỗ trợ nhiều giao thức (FTP, SSH, HTTP, v.v.).

- Cách hoạt động: Nhắm vào dịch vụ mạng trên Windows, thử các tổ hợp mật khẩu từ wordlist.
- Ưu điểm: Nhanh, linh hoạt, miễn phí.
- Nhược điểm: Chủ yếu dùng cho tấn công online, không trực tiếp crack hash SAM.

1.2.2 Các công cụ crack mật khẩu trên hệ điều hành Linux

a) John the Ripper

- Mô tả: Một trong những công cụ crack mật khẩu mạnh mẽ và phổ biến nhất, mã nguồn mở, hỗ trợ cả Linux và nhiều nền tảng khác.
- Tính năng:
    - Crack hash từ /etc/shadow (MD5, SHA-256/512, bcrypt, v.v.).
    - Hỗ trợ dictionary attack, brute-force, và hybrid attack.
    - Có thể tùy chỉnh quy tắc tấn công qua file cấu hình.
- Cách hoạt động:
    - Trích xuất hash: unshadow /etc/passwd /etc/shadow > hashfile.txt.
    - Chạy John: john --wordlist=rockyou.txt hashfile.txt (dictionary) hoặc john --incremental hashfile.txt (brute-force).
- Ưu điểm: Linh hoạt, miễn phí, cộng đồng hỗ trợ lớn.
- Nhược điểm: Dòng lệnh, cần kỹ năng cơ bản.

b) Hashcat

- Mô tả: Công cụ crack mật khẩu nhanh nhất nhờ tận dụng GPU, mã nguồn mở, hoạt động tốt trên Linux.
- Tính năng:
    - Hỗ trợ hơn 300 loại hash (bao gồm SHA-256/512, bcrypt dùng trong Linux).
    - Các chế độ: dictionary, brute-force, mask, hybrid.
- Cách hoạt động:
    - Trích xuất hash từ /etc/shadow (dùng unshadow).
    - Chạy Hashcat: hashcat -m 1800 -a 0 hash.txt rockyou.txt (m 1800 là SHA-512, a 0 là dictionary).
    - Brute-force: hashcat -m 1800 -a 3 hash.txt ?a?a?a?a (thử tổ hợp 4 ký tự).
- Ưu điểm: Cực nhanh với GPU, miễn phí.
- Nhược điểm: Không có GUI, cần phần cứng mạnh.

c) THC Hydra

- Mô tả: Công cụ chuyên crack mật khẩu qua mạng (online attack), hỗ trợ Linux và các nền tảng khác.
- Tính năng:
  - Tấn công các dịch vụ như SSH, FTP, HTTP, SMB, MySQL, v.v.
  - Hỗ trợ dictionary và brute-force.
- Cách hoạt động:
  - Chạy lệnh: hydra -l user -P rockyou.txt ssh://192.168.1.10 (crack SSH với username "user" và wordlist).
  - Brute-force: hydra -l user -p "a-zA-Z0-9" ssh://192.168.1.10.
- Ưu điểm: Hiệu quả với dịch vụ mạng, miễn phí.
- Nhược điểm: Chỉ dùng cho tấn công online, dễ bị chặn bởi firewall.

d) Aircrack-ng

- Mô tả: Bộ công cụ chuyên crack mật khẩu Wi-Fi (WEP, WPA/WPA2), phổ biến trên Linux.
- Tính năng:
  - Bắt handshake WPA/WPA2 và crack bằng dictionary hoặc brute-force.
  - Hỗ trợ giám sát và tấn công mạng không dây.
- Cách hoạt động:
  - Chuyển card Wi-Fi sang chế độ monitor: airmon-ng start wlan0.
  - Bắt handshake: airodump-ng wlan0mon -w capture.
  - Crack: aircrack-ng capture.cap -w rockyou.txt.
- Ưu điểm: Miễn phí, mạnh mẽ với Wi-Fi.
- Nhược điểm: Chỉ dùng cho mạng không dây, cần phần cứng tương thích.

e) chntpw

- Mô tả: Công cụ không crack mà đặt lại hoặc xóa mật khẩu, thường dùng để chỉnh sửa hash trong /etc/shadow (hoặc SAM trên Windows).
- Tính năng:
  - Xóa mật khẩu user hoặc thay bằng hash mới.
  - Hỗ trợ boot từ USB/CD.
- Cách hoạt động:
  - Boot từ USB/CD chứa chntpw.

- Chạy: chntpw -u username /etc/shadow → chọn xóa hoặc đặt lại mật khẩu.

- Ưu điểm: Nhanh, không cần crack mật khẩu gốc.
- Nhược điểm: Cần quyền truy cập vật lý, không khôi phục mật khẩu cũ.

f) Medusa

- Mô tả: Công cụ crack mật khẩu qua mạng tương tự Hydra, hỗ trợ Linux, tập trung vào tấn công online.
- Tính năng:
  - Hỗ trợ SSH, FTP, HTTP, MySQL, Telnet, v.v.
  - Dictionary và brute-force qua nhiều luồng (multithreading).
- Cách hoạt động:
  - Chạy: medusa -u user -P rockyou.txt -h 192.168.1.10 -M ssh.
- Ưu điểm: Nhanh, hỗ trợ nhiều giao thức.
- Nhược điểm: Ít phổ biến hơn Hydra, chỉ dùng online.

g) RainbowCrack

- Mô tả: Công cụ dùng bảng cầu vồng (rainbow tables) để crack hash, hoạt động trên Linux nhưng ít hiệu quả với /etc/shadow do salt.
- Tính năng:
  - Crack hash MD5, SHA-1 nhanh chóng nếu không có salt.
  - Tạo và tra cứu bảng cầu vồng.
- Cách hoạt động:
  - Tạo bảng: rtgen md5 loweralpha 1 8 0 1000.
  - Crack: rcrack *.rt -h hash_value.
- Ưu điểm: Nhanh với hash không salt.
- Nhược điểm: Không hiệu quả với Linux hiện đại (bcrypt, salt).

1.3 Kết chương

Ở chương này đã tìm hiểu và mô tả cách thức áp dụng để crack mật khẩu của các công cụ creack mật khẩu trên hệ điều hành Windows và Linux.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

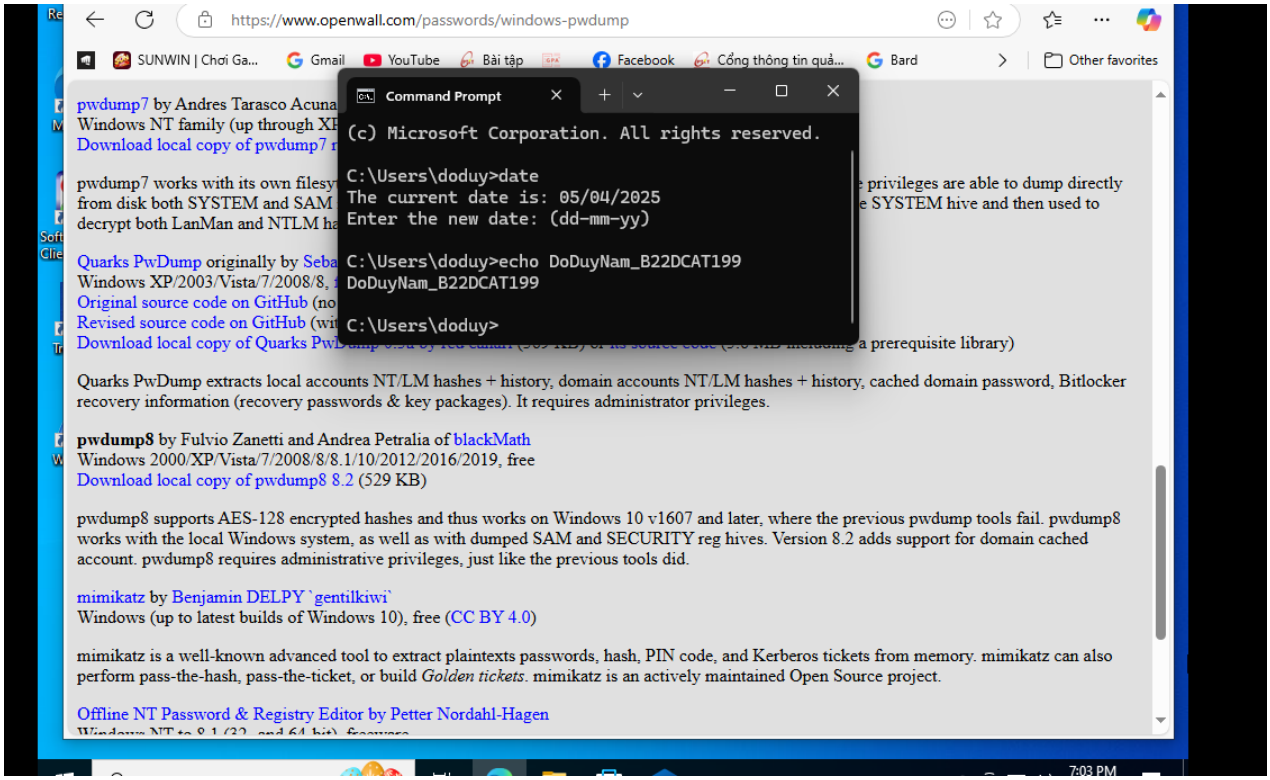
2.1 Chuẩn bị môi trường

- Máy Kali Linux
- Máy Windows

2.2 Các bước thực hiện

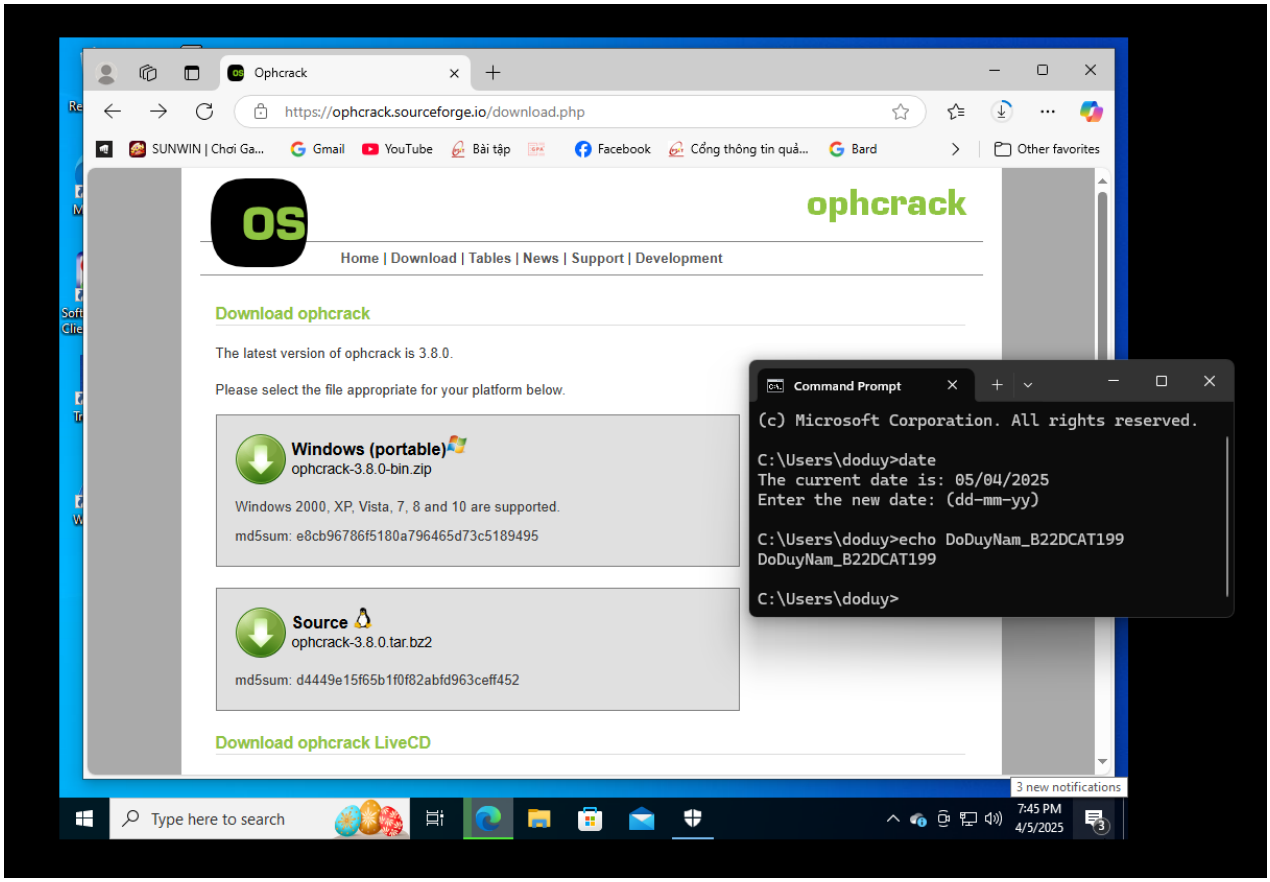
2.2.1 Crack mật khẩu trên hệ điều hành Windows

- 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.
- Tải công cụ pwdump.



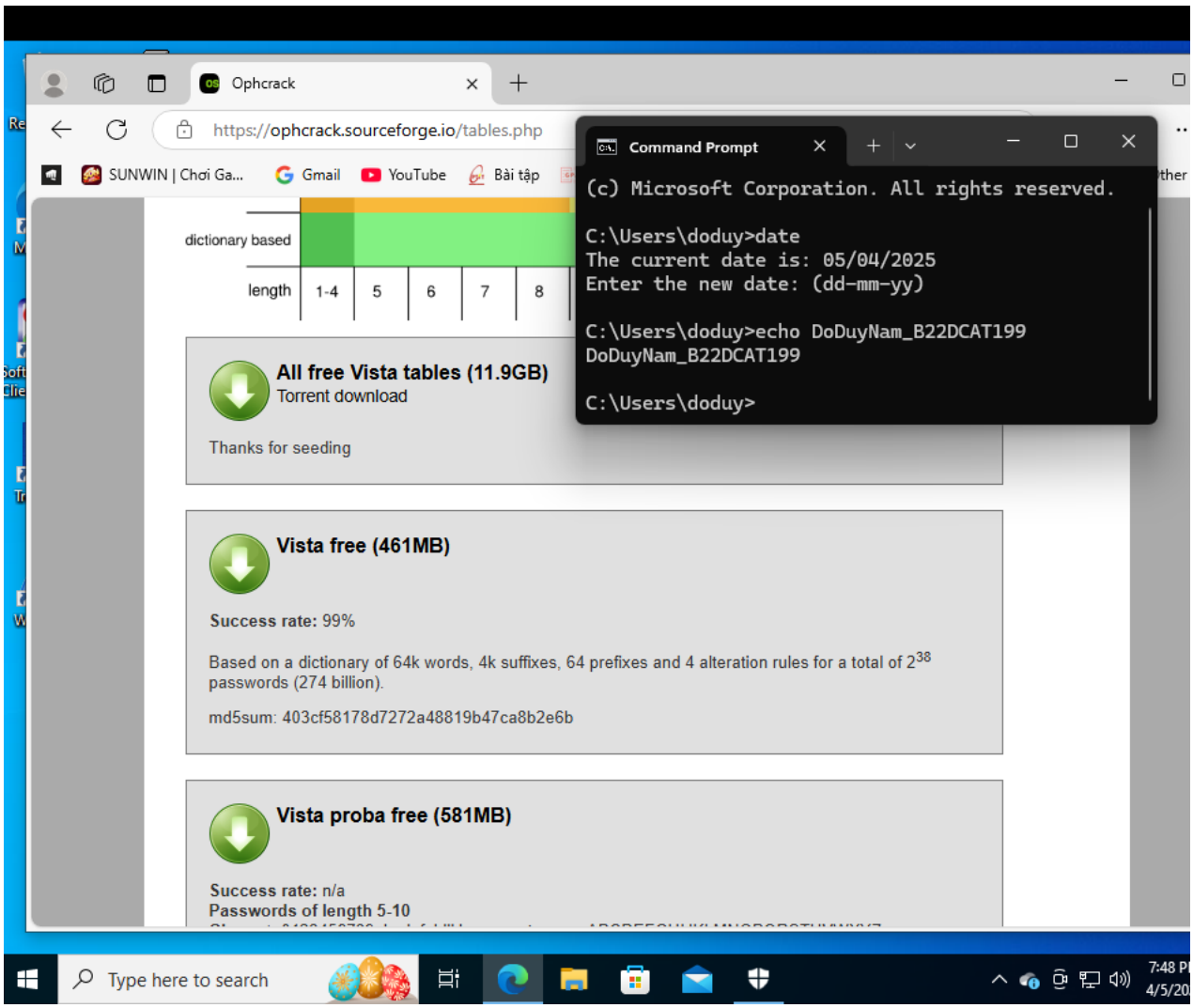
Hình 1 Tải công cụ pwdump

- Tải công cụ ophcrack.



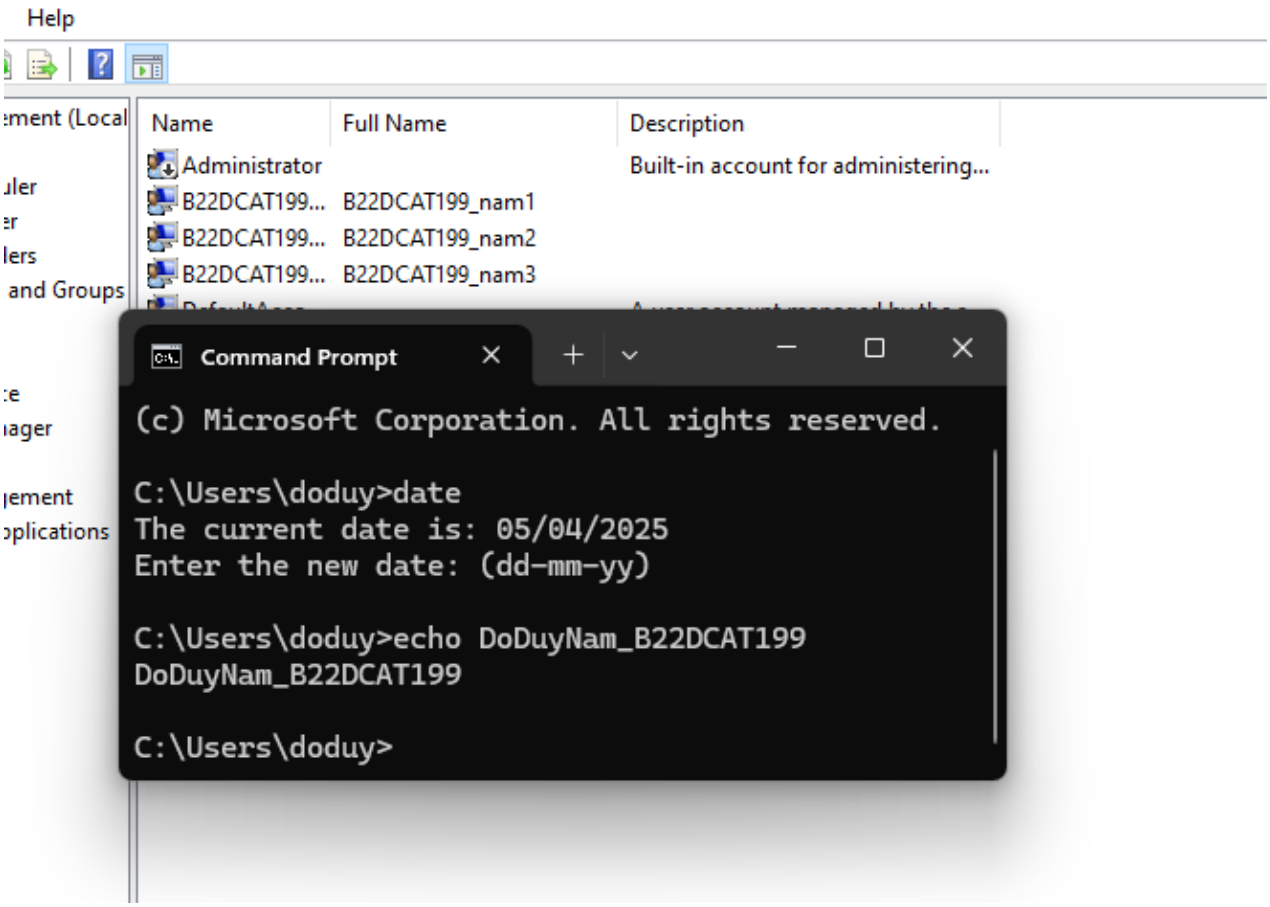
Hình 2 Tải công cụ ophcrack

- Tải Rainbow tables của công cụ ophcrack.



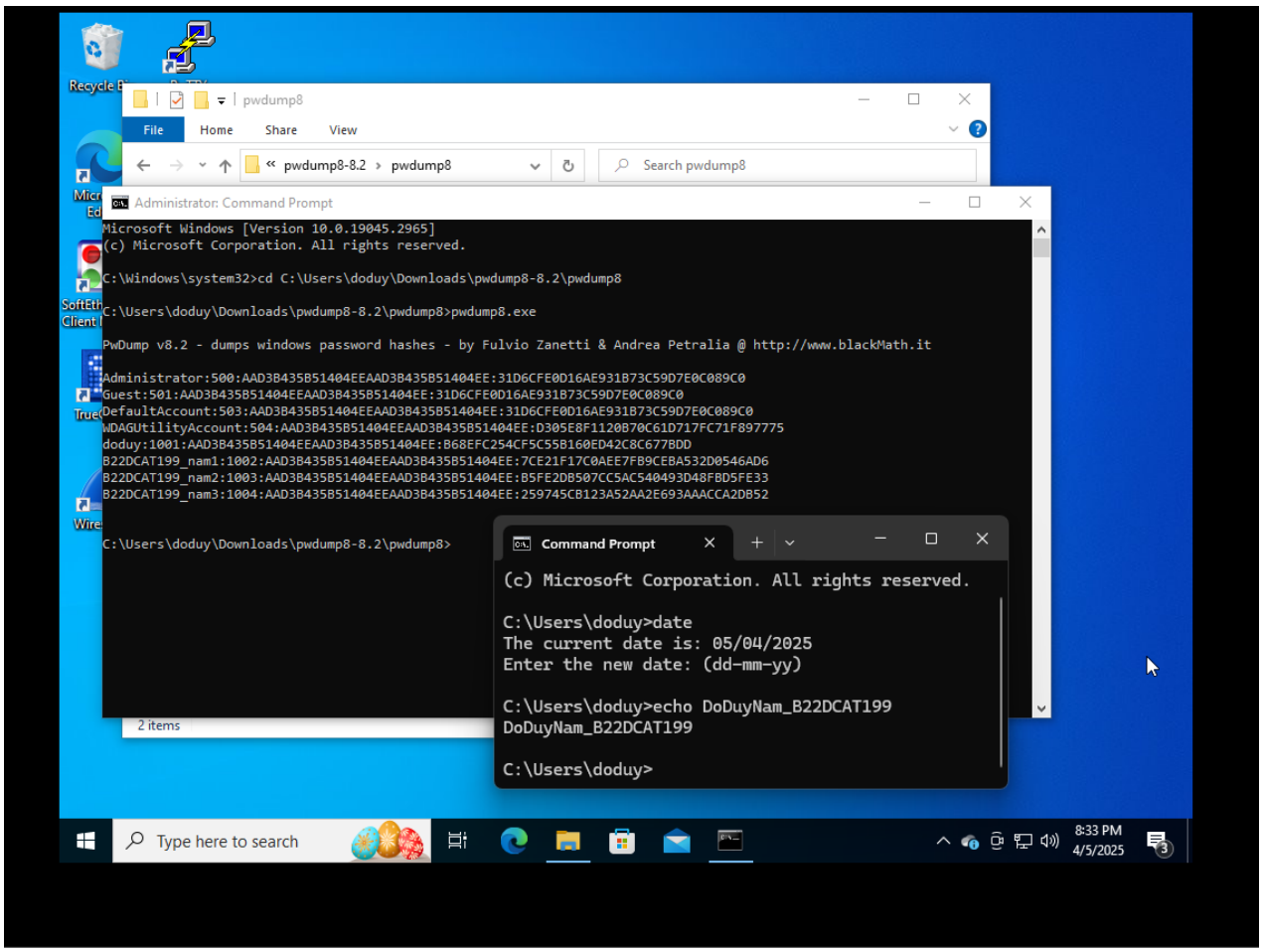
Hình 3 Tải Rainbows tables của công cụ ophcrack

- Tạo các User mới và đặt mật khẩu bằng cách thực hiện mở Computer Management -> Local Users and Groups -> User -> New User.



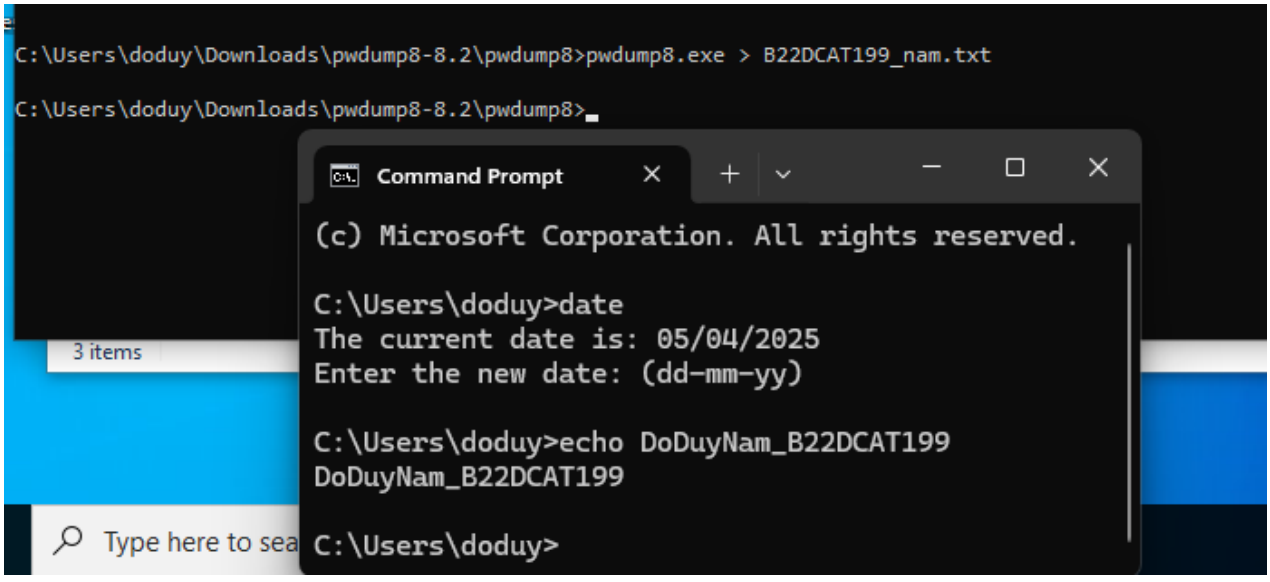
Hình 4 Tạo thành công các user mới có mật khẩu

- Chạy công cụ pwdump trên Terminal



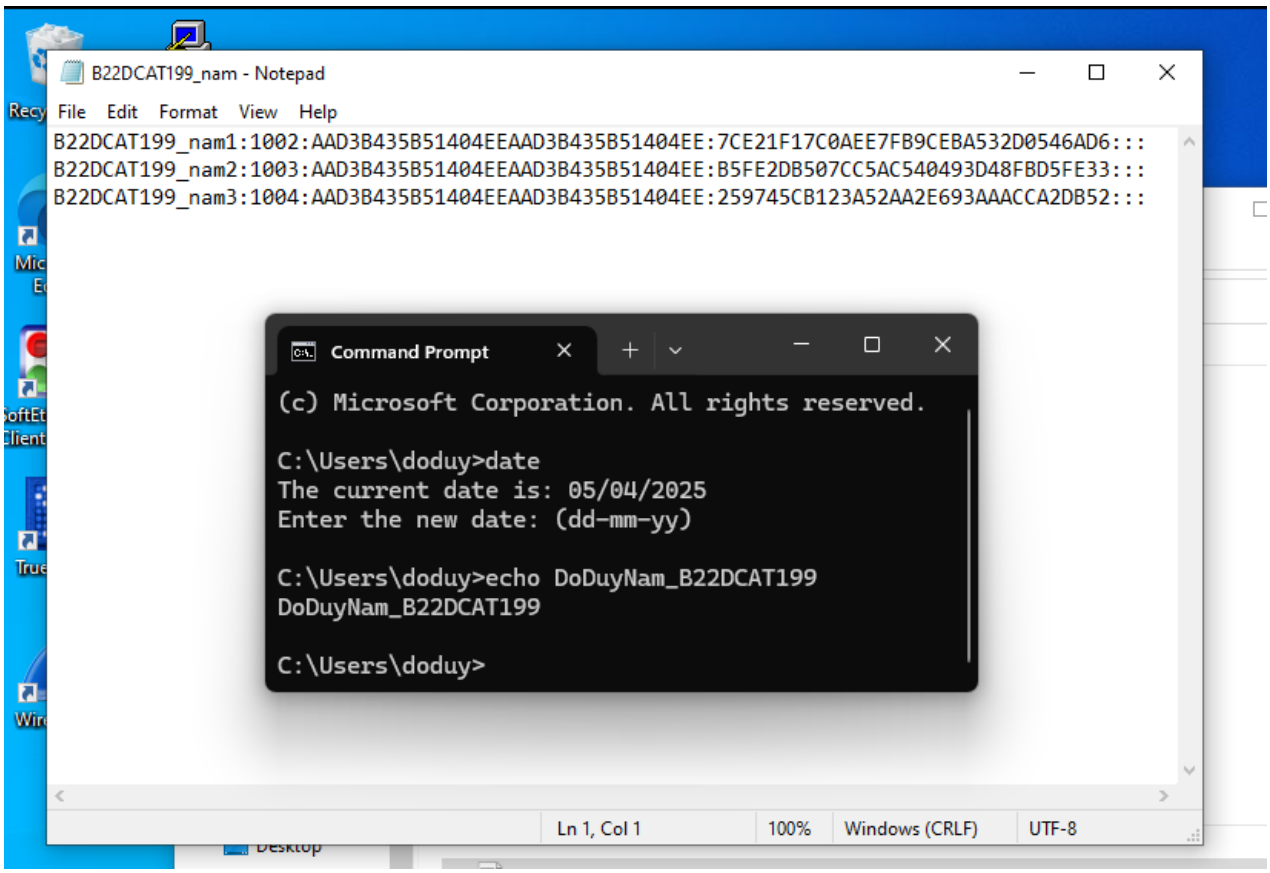
Hình 5 Sử dụng công cụ pwdump

- Lưu lại dữ liệu dump của mật khẩu vào 1 file bất kì.



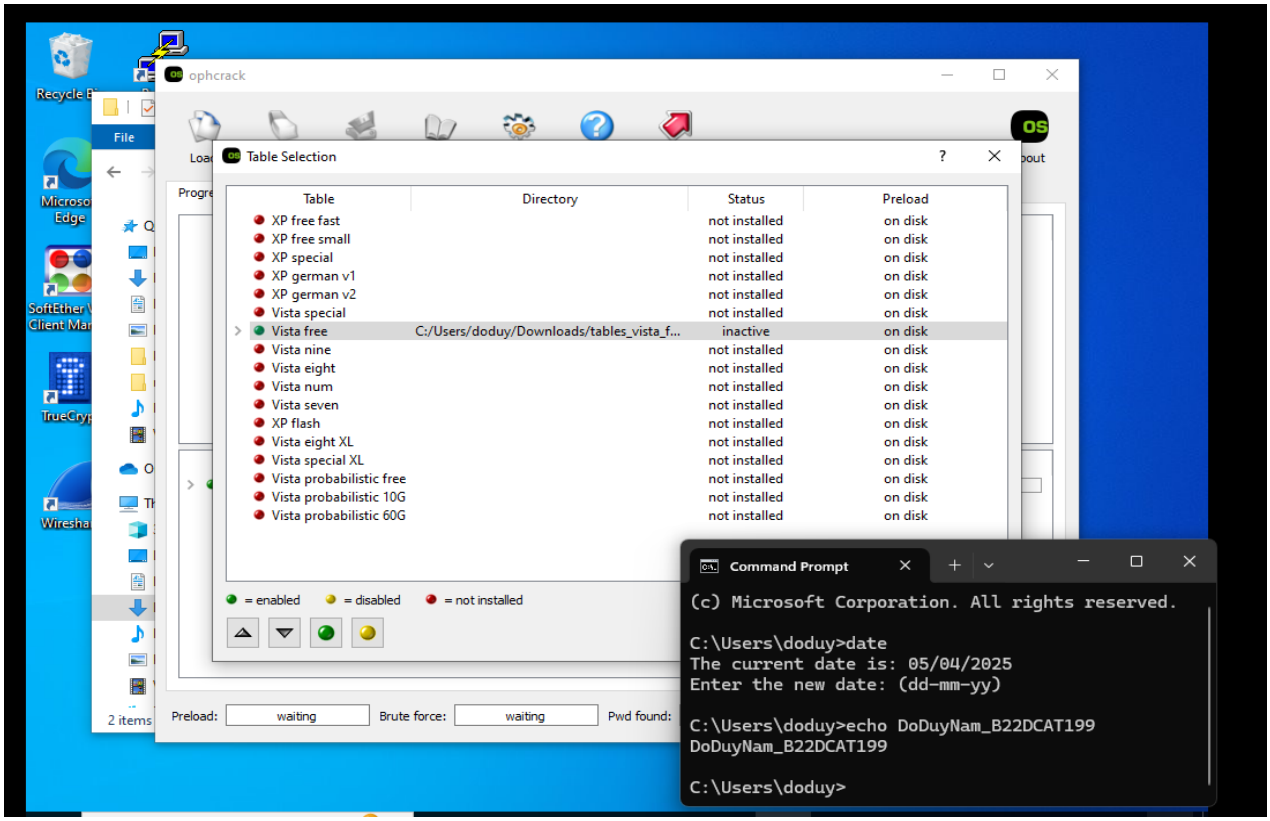
Hình 6 Lưu dữ liệu dump của mật khẩu

- Đảm bảo thông tin lưu có dạng như hình dưới đây.



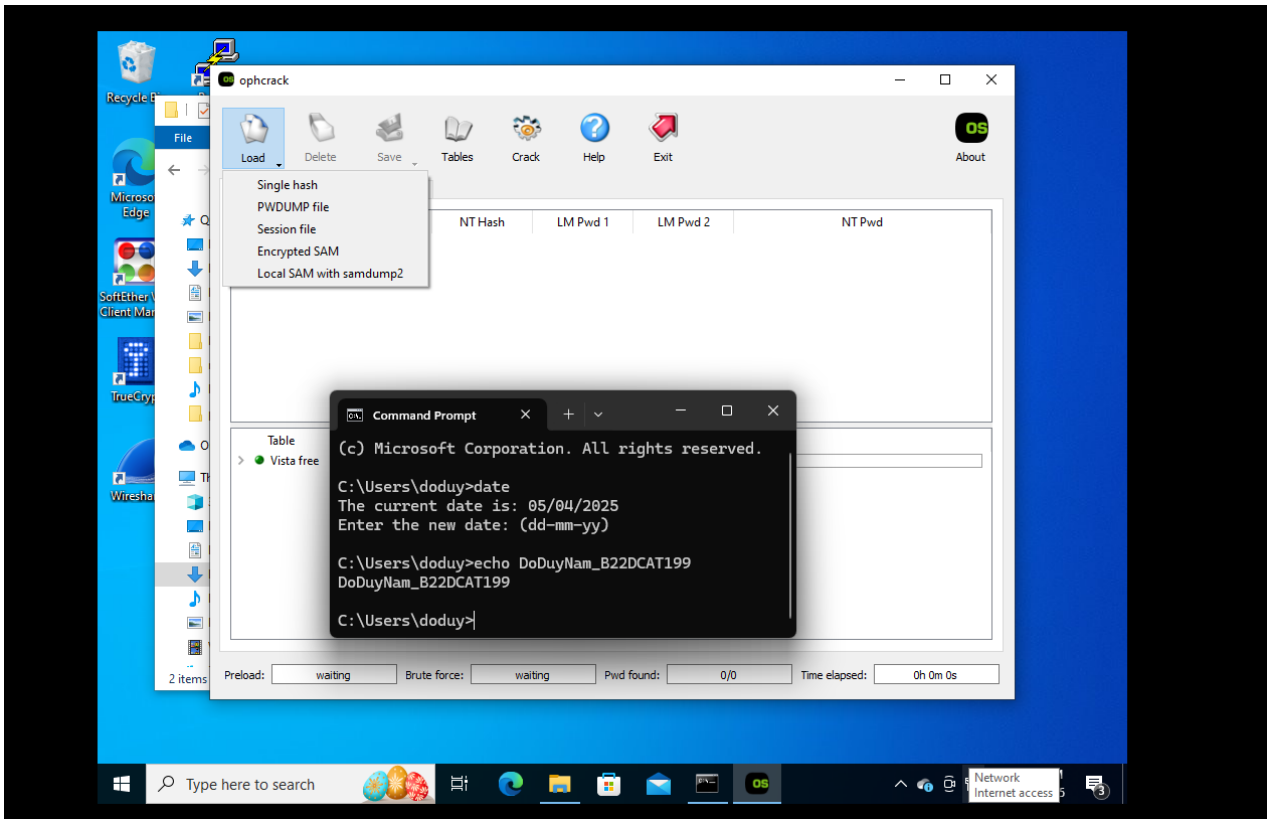
Hình 7 Thông tin đã lưu

- Sử dụng công cụ ophcrack. Chọn Tables -> Install -> File Rainbow đã tải -> table tương ứng chuyển xanh -> thành công.



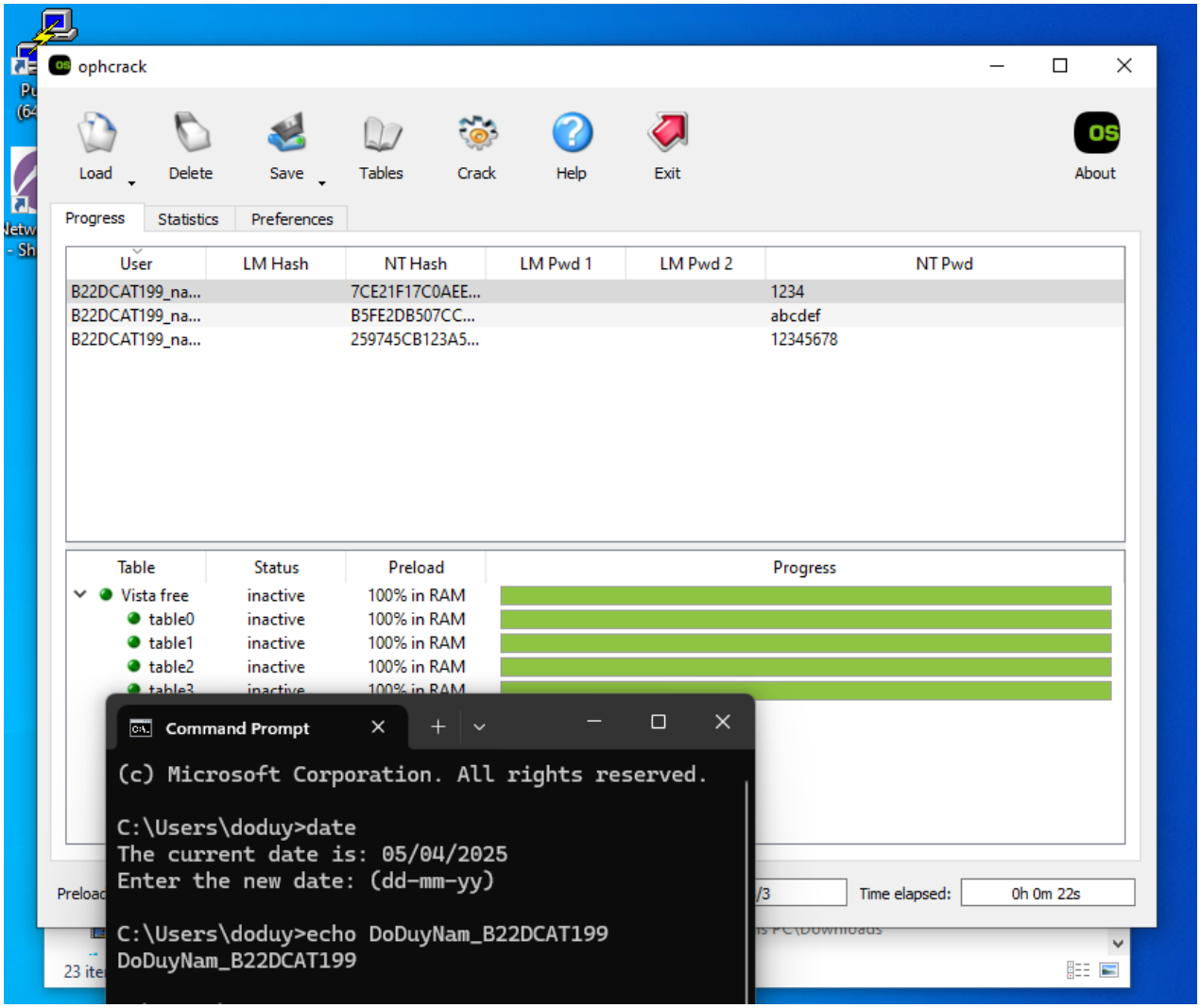
Hình 8 Thành công cài đặt tables trên ophcrack

- Chọn Load -> PWDUMP file để tải file dữ liệu dump đã lưu trước đó.



Hình 9 Thêm file pwdump

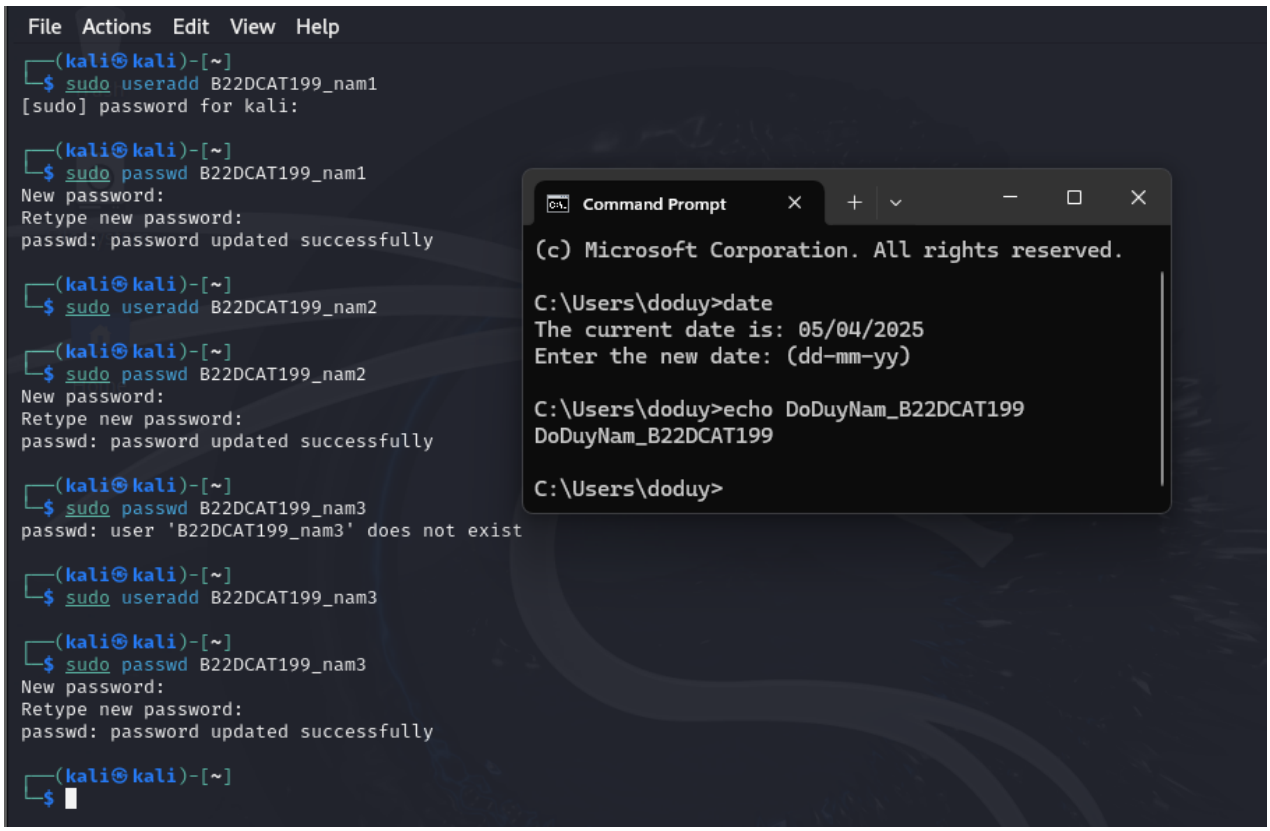
- Sau khi file load chọn Crack để tiến hành bẻ khóa. Chờ công cụ bẻ khóa (thời gian phụ thuộc vào độ khó của mật khẩu).



Hình 10 Bẻ khóa thành công mật khẩu

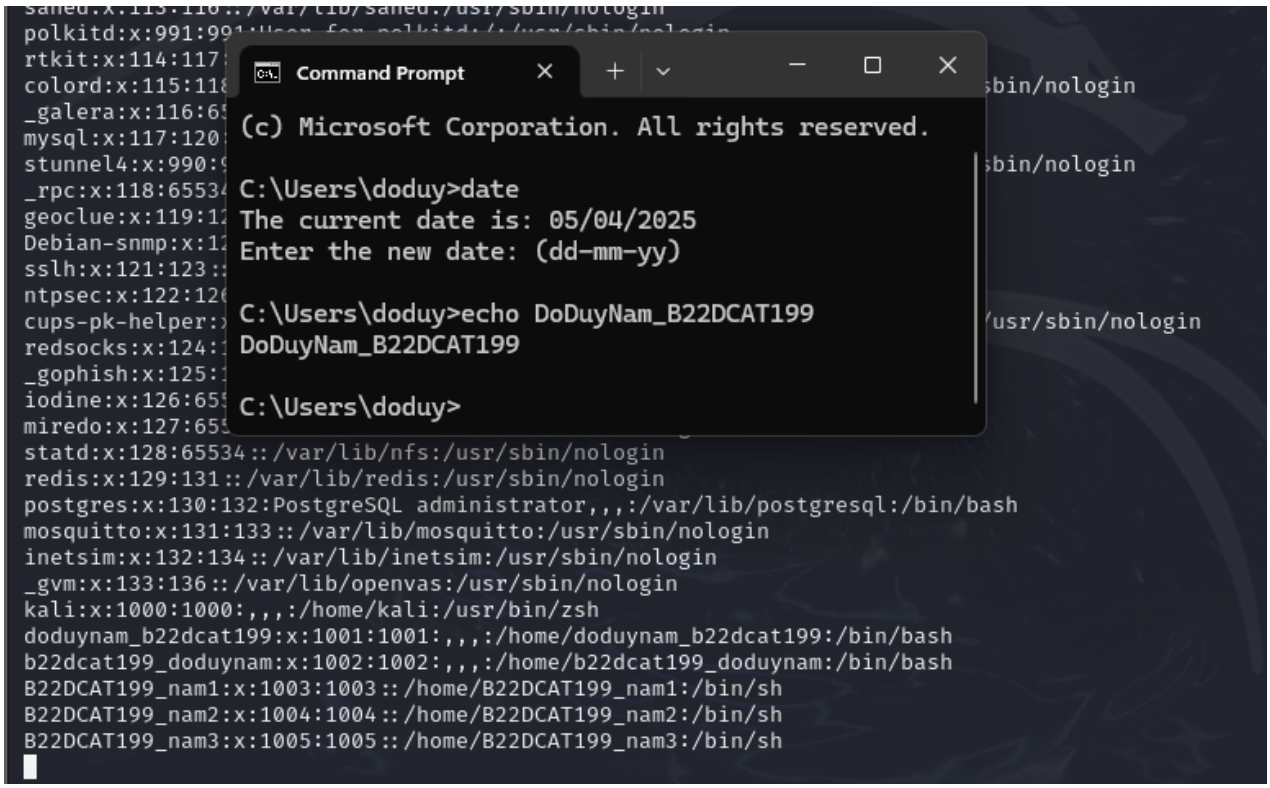
2.2.2 Crack mật khẩu trên hệ điều hành Linux

- 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 các user và mật khẩu theo yêu cầu bằng các câu lệnh *sudo useradd <tên_user>* và *sudo passwd <tên_user>*.



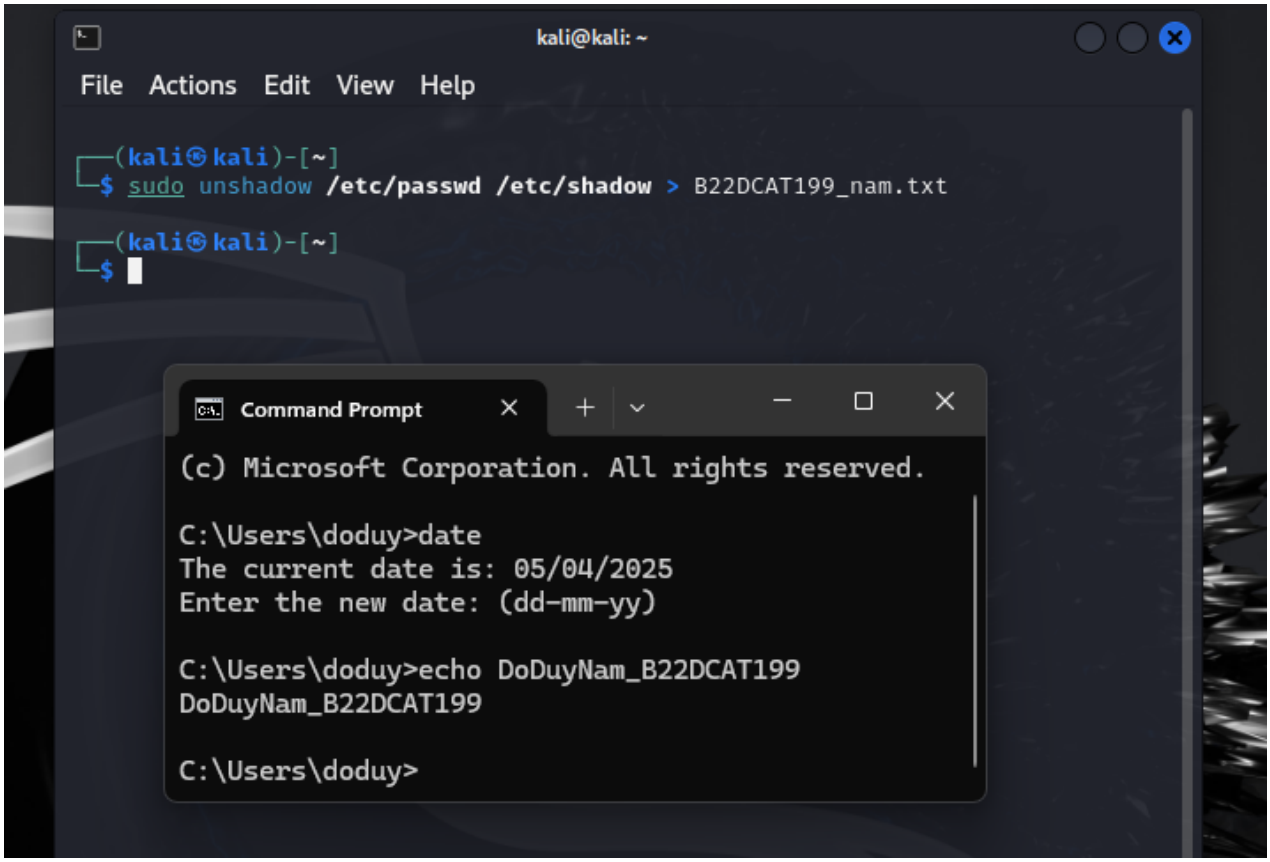
Hình 11 Tạo các user và đặt mật khẩu theo yêu cầu

- Kiểm tra lại để đảm bảo các user đều tạo thành công và có mật khẩu bằng cách xem 2 file /etc/shadow và /etc/passwd



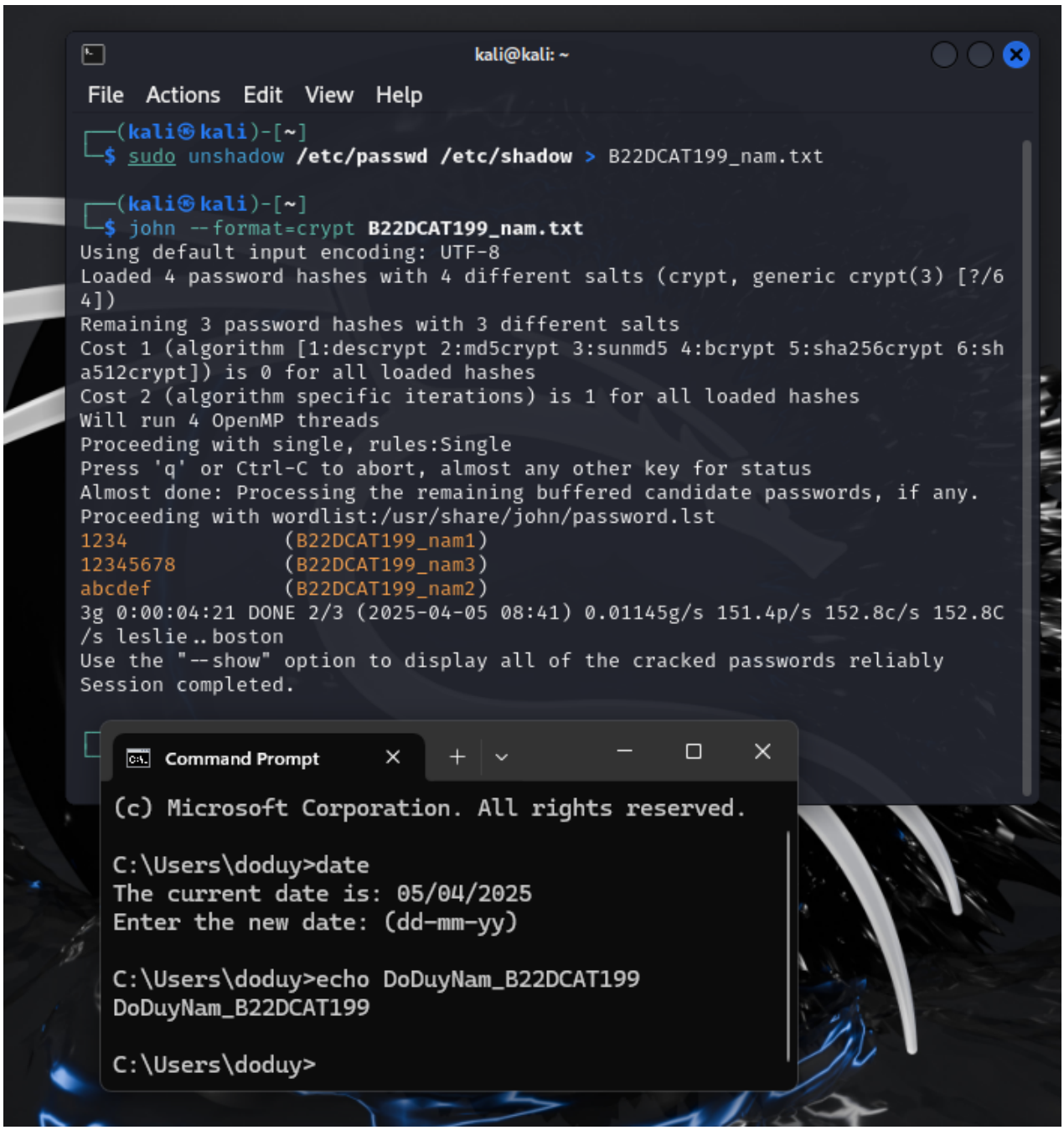
Hình 12 Kiểm tra file /etc/passwd

- Kết hợp 2 file /etc/shadow và /etc/passwd để phục vụ cho quá trình crack mật khẩu sử dụng John The Ripper (công cụ có sẵn trên Kali Linux) bằng sử dụng câu lệnh *sudo unshadow /etc/passwd /etc/shadow > <tên_file>*



Hình 13 Kết hợp 2 file /etc/shadow và file /etc/passwd

- Sử dụng công cụ John The Ripper để tiến hành crack mật khẩu bằng cách dùng lệnh *john –format=crypt <tên_file>*



Hình 14 Crack thành công mật khẩu của các user

2.3 Kết chương

Ở chương này đã thực nghiệm crack mật khẩu trên hệ điều hành Windows và Kali Linux.

KẾT LUẬN

- Tìm hiểu về các công cụ crack mật khẩu trên hệ điều hành Windows và Linux.
- Tìm hiểu về cách thức/phương pháp các công cụ sử dụng để crack mật khẩu trên hệ điều hành Windows và Linux.
- Crack thành công mật khẩu của các User trên hệ điều hành Windows và Linux.

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