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:

B22DCAT018 – Nguyễn Hoàng Anh

Giảng viên hướng dẫn: ThS. Ninh Thị Thu Trang

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. TÌM HIỂU LÝ THUYẾT

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

Trên Windows:

- Cain & Abel: Công cụ đa năng dùng để phục hồi mật khẩu bằng cách sniffing, brute-force, dictionary, và phân tích hash từ file hệ thống.
- Ophcrack: Crack mật khẩu Windows bằng kỹ thuật Rainbow Table, không cần đăng nhập vào hệ điều hành.
- Mimikatz: Trích xuất thông tin xác thực như mật khẩu plaintext, hash, ticket từ bộ nhớ hệ thống.
- Hash Suite: Là công cụ kiểm thử độ mạnh của mật khẩu bằng cách phân tích và crack hash từ file SAM của Windows. Giao diện đồ họa thân thiện và hỗ trợ nhiều thuật toán hash khác nhau. Thường được sử dụng để đánh giá chính sách mật khẩu trong môi trường doanh nghiệp.

Trên Linux:

- John the Ripper (JtR): Crack hash mật khẩu được lưu trong hệ thống Linux (thường trong file /etc/shadow). Hỗ trợ nhiều chế độ tấn công.
- THC-Hydra: Công cụ brute-force mạnh mẽ dùng để crack mật khẩu qua nhiều giao thức mạng như SSH, FTP, Telnet, HTTP...
- Hashcat: Công cụ crack mật khẩu bằng GPU, tốc độ rất cao, hỗ trợ nhiều định dạng hash như MD5, NTLM, SHA1, WPA...

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

Các công cụ crack mật khẩu hoạt động dựa trên một số phương pháp chính sau:

1. Brute-force attack (Tấn công vét cạn)

Thử tất cả các tổ hợp ký tự có thể để tìm ra mật khẩu đúng. Phương pháp này đảm bảo tìm được mật khẩu nếu đủ thời gian, nhưng rất tốn tài nguyên và thời gian nếu mật khẩu phức tạp.

→ Hashcat, John the Ripper, THC-Hydra và Hash Suite đều hỗ trợ brute-force.

2. Dictionary attack (Tấn công từ điển)

Sử dụng một danh sách các mật khẩu phổ biến hoặc do người dùng định nghĩa để thử lần lượt. Hiệu quả với các mật khẩu yếu hoặc thông dụng.

→ Hầu hết các công cụ như Cain & Abel, John the Ripper, Hash Suite, Hydra đều hỗ trợ.

3. Rainbow Table attack (Tấn công bảng cầu vồng)

Dựa trên bảng ánh xạ sẵn giữa hash và mật khẩu đã biết để tra ngược nhanh chóng.

→ Ophcrack là công cụ tiêu biểu sử dụng phương pháp này.

4. Credential dumping (Trích xuất thông tin xác thực)

Khai thác thông tin như mật khẩu, hash, token... từ bộ nhớ hệ thống hoặc file hệ thống.

→ Mimikatz có khả năng truy xuất mật khẩu plaintext, hash từ bộ nhớ (LSASS) hoặc các file như SAM trong Windows.

5. Hash cracking (Giải mã hash ngoại tuyến)

Crack mật khẩu từ các hash đã trích xuất (thường là NTLM trên Windows hoặc SHA trên Linux) mà không cần truy cập trực tiếp hệ thống.

→ Hashcat, John the Ripper, Hash Suite đều rất mạnh trong phương pháp này.

6. Online attack (Tấn công trực tiếp qua giao thức mạng)

Thử đăng nhập nhiều lần vào dịch vụ mạng như SSH, FTP, HTTP bằng nhiều mật khẩu khác nhau.

→ THC-Hydra nổi bật trong loại tấn công này, hỗ trợ nhiều giao thức.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

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

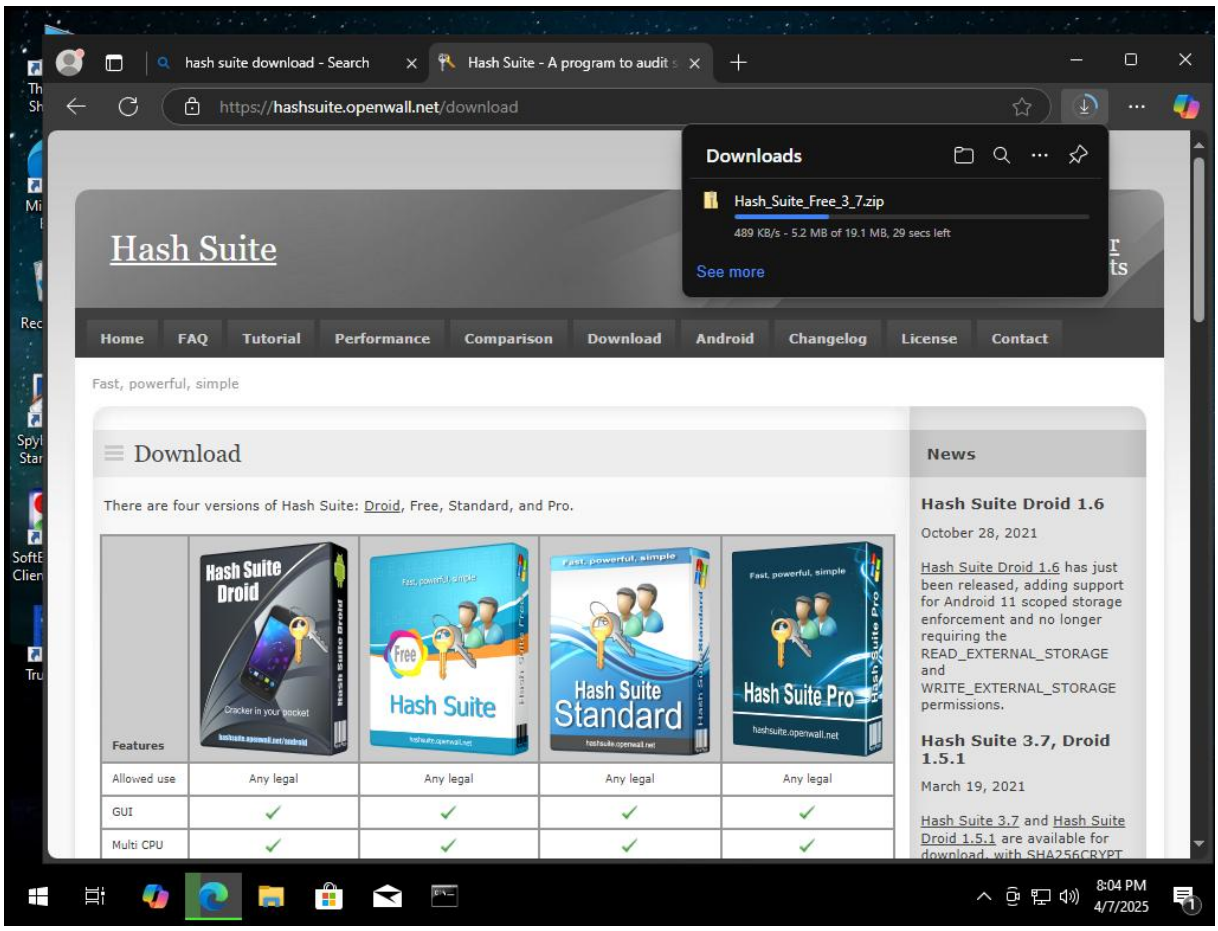
Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Windows

2.2 Các bước thực hiện

2.2.1 Trên máy Windows

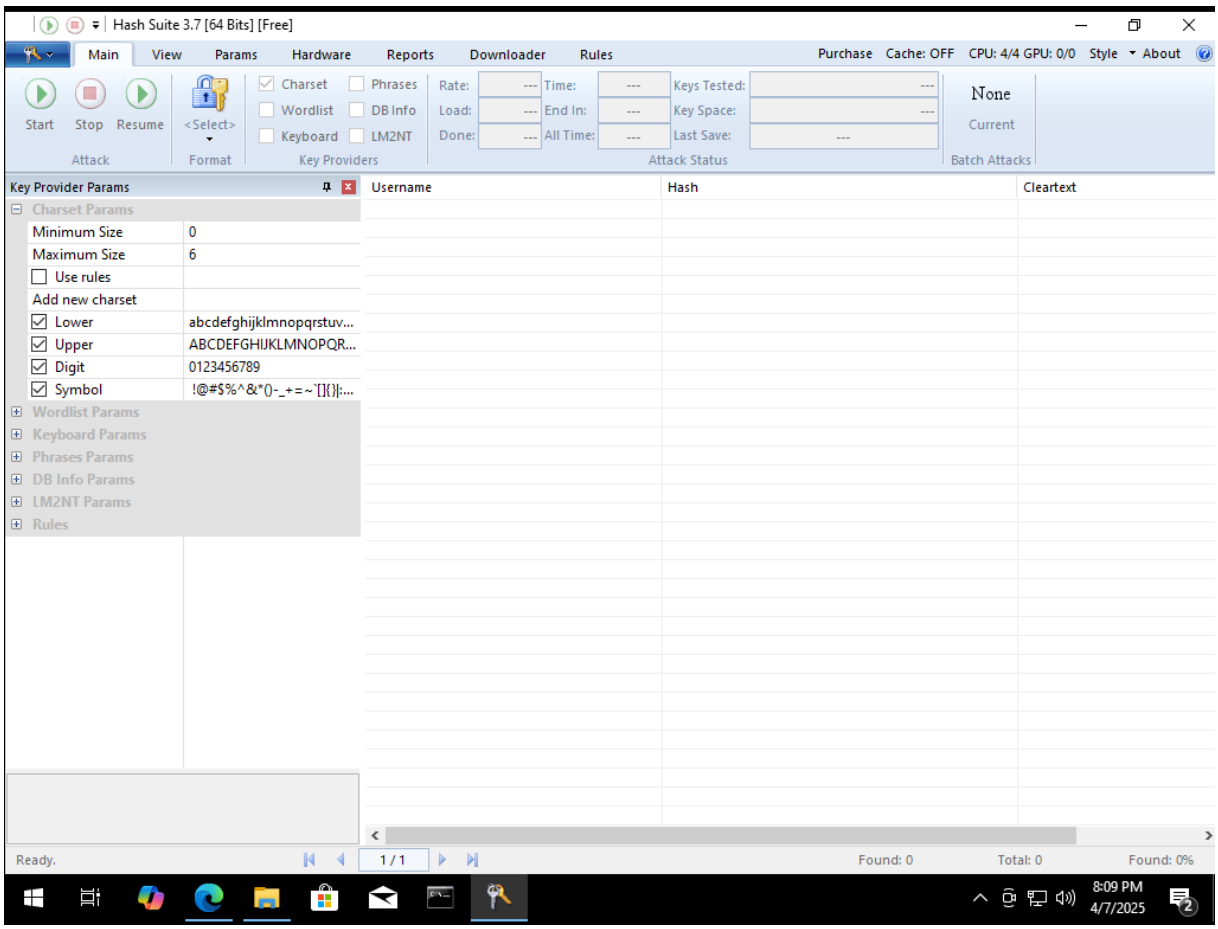
Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,.... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Tải công cụ Hash Suite để crack mật khẩu:



Hình 1 - tải hash suite

Sau khi tải về và giải nén, đây là giao diện của Hash Suite:



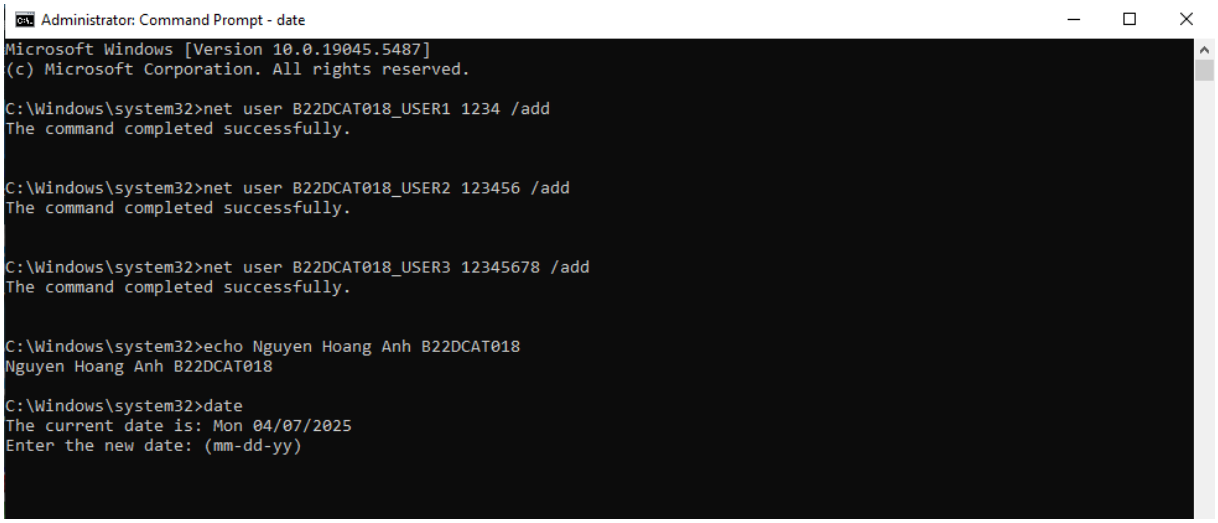
Hình 2 - giao diện hash suite

Tạo 3 người dùng mới với tài khoản và mật khẩu lần lượt là:

B22DCAT018_USER1 – mật khẩu: *1234*

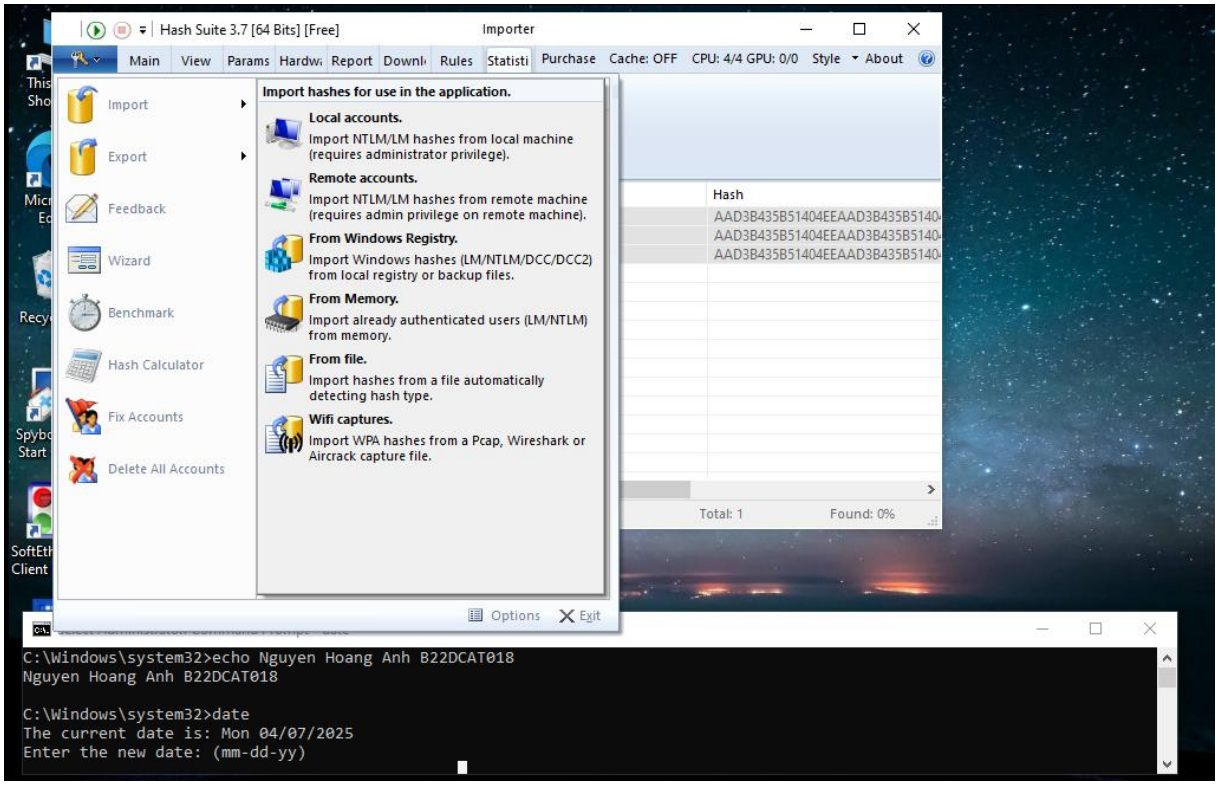
B22DCAT018_USER2 – mật khẩu: *123456*

B22DCAT018_USER3 – mật khẩu: *12345678*



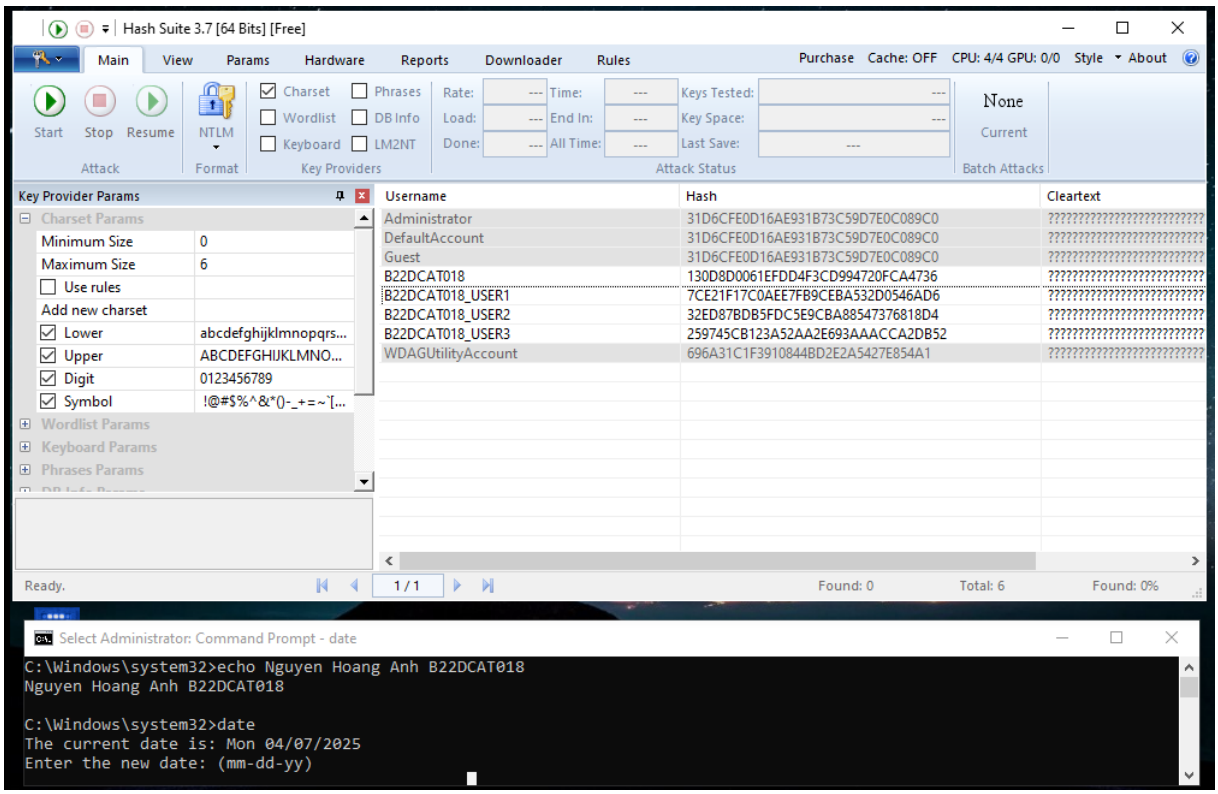
Hình 3 - tạo 3 người dùng mới

Chọn “import” → “local accounts”



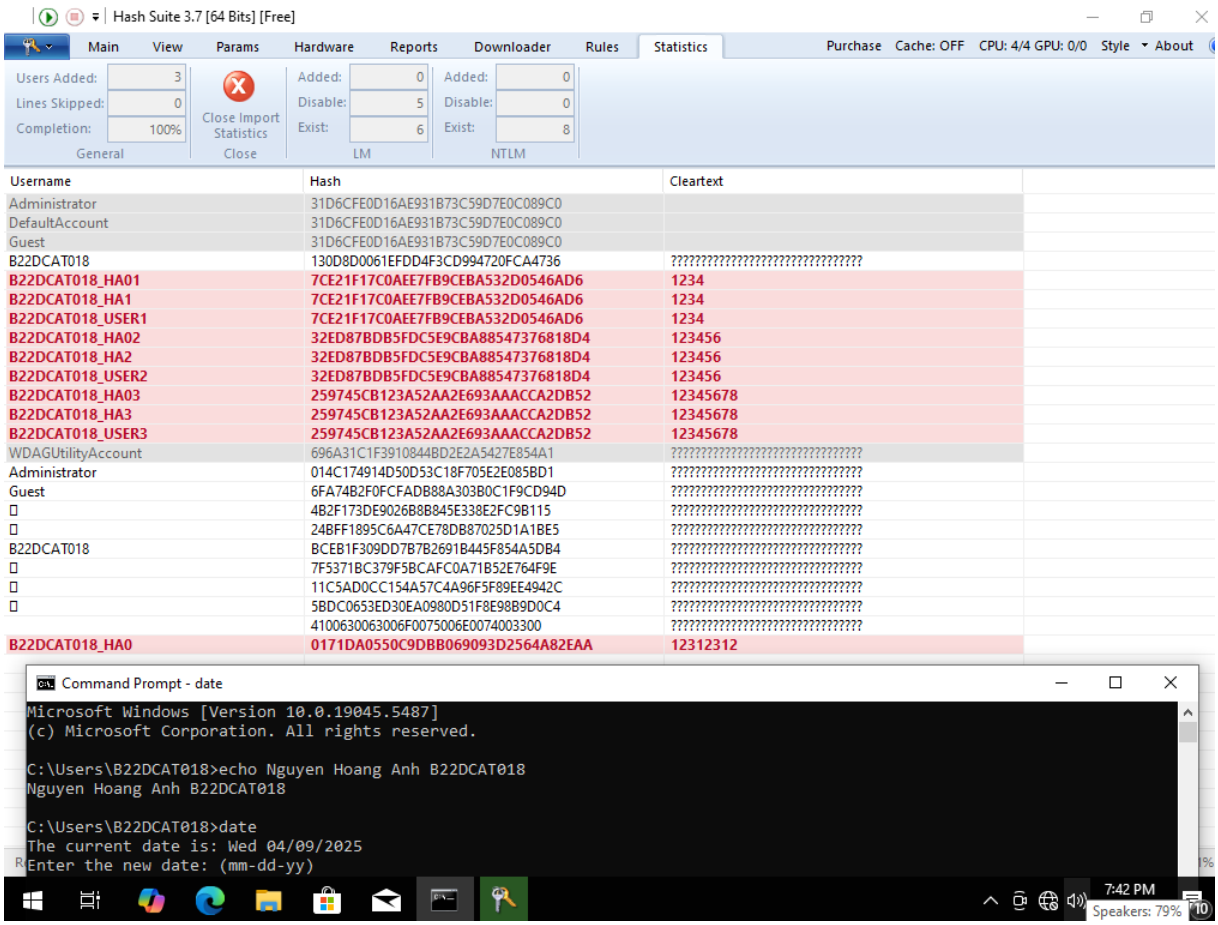
Hình 4 - import danh sách người dùng

Sau khi import sẽ hiện ra danh sách các user, trong đó có 3 user vừa tạo



Hình 5 - danh sách người dùng sau khi import

Chọn “start” để crack mật khẩu



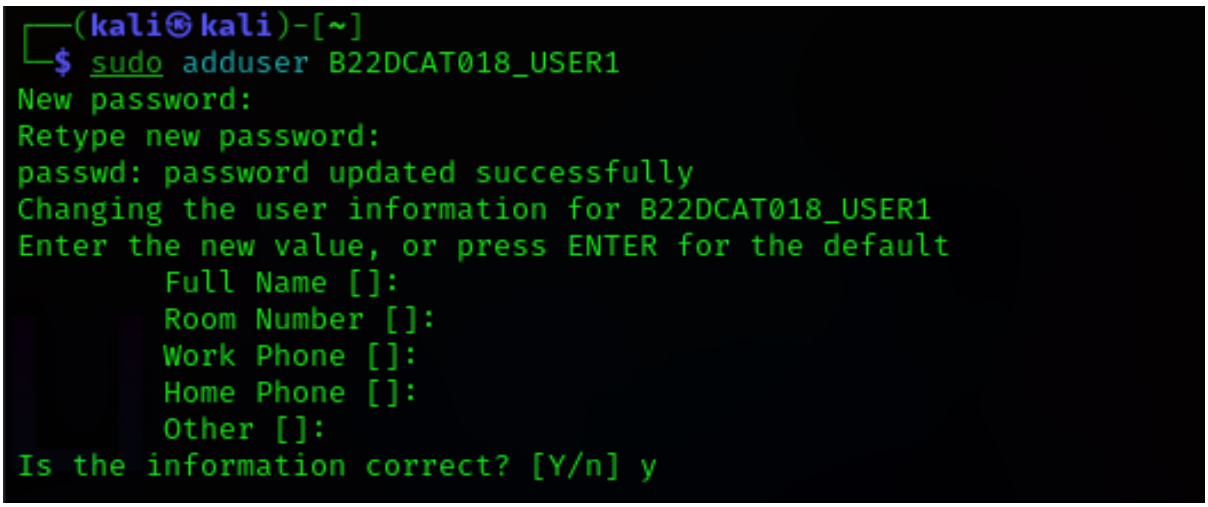
Hình 6 - crack mật khẩu

→ tìm ra được mật khẩu của 3 user *B22DCAT018_USER1*, *B22DCAT018_USER2*, *B22DCAT018_USER3* là: 1234, 123456, 12345678

2.2.2 Trên máy Linux

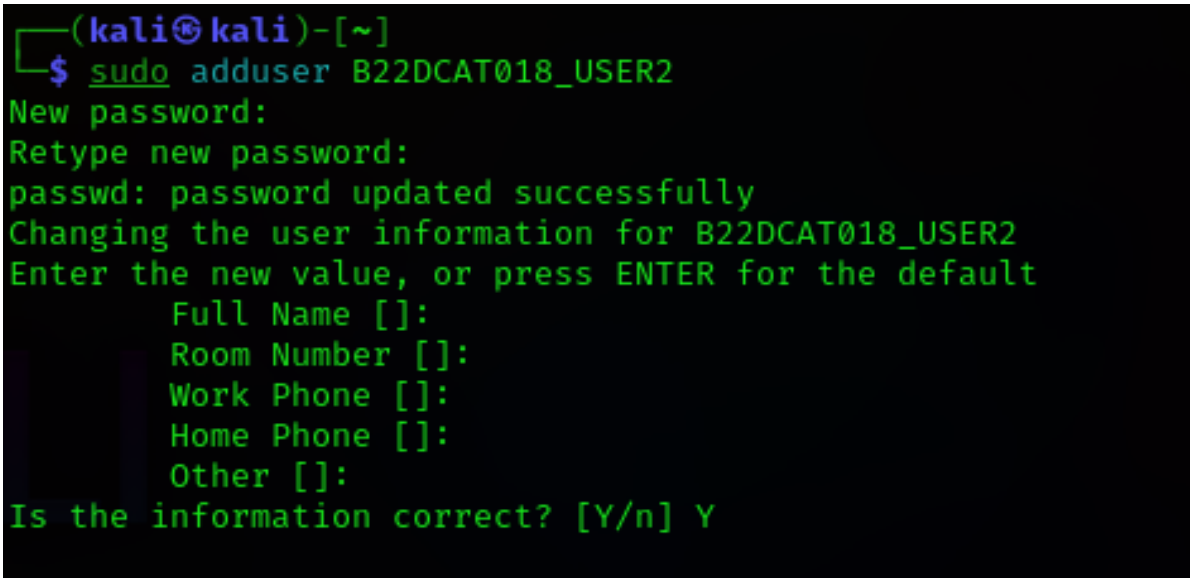
Thử nghiệm crack mật khẩu trên hệ điều hành Linux với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,.... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Tạo người dùng 1 tên là: *B22DCAT018_USER1*, mật khẩu là: *1234*



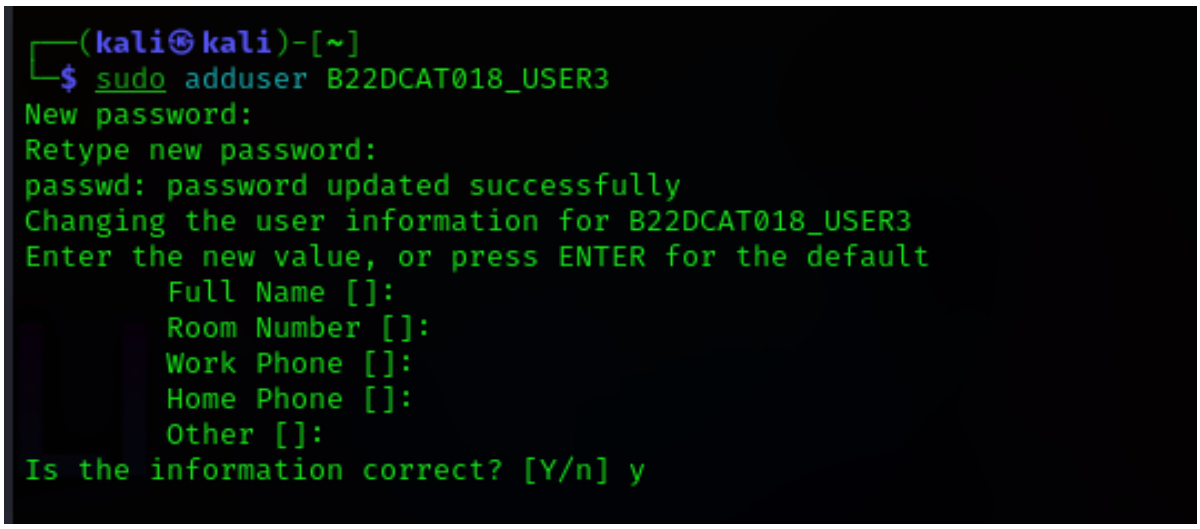
Hình 7 - tạo người dùng 1

Tạo người dùng 2 tên là: *B22DCAT018_USER2*, mật khẩu là *123456*



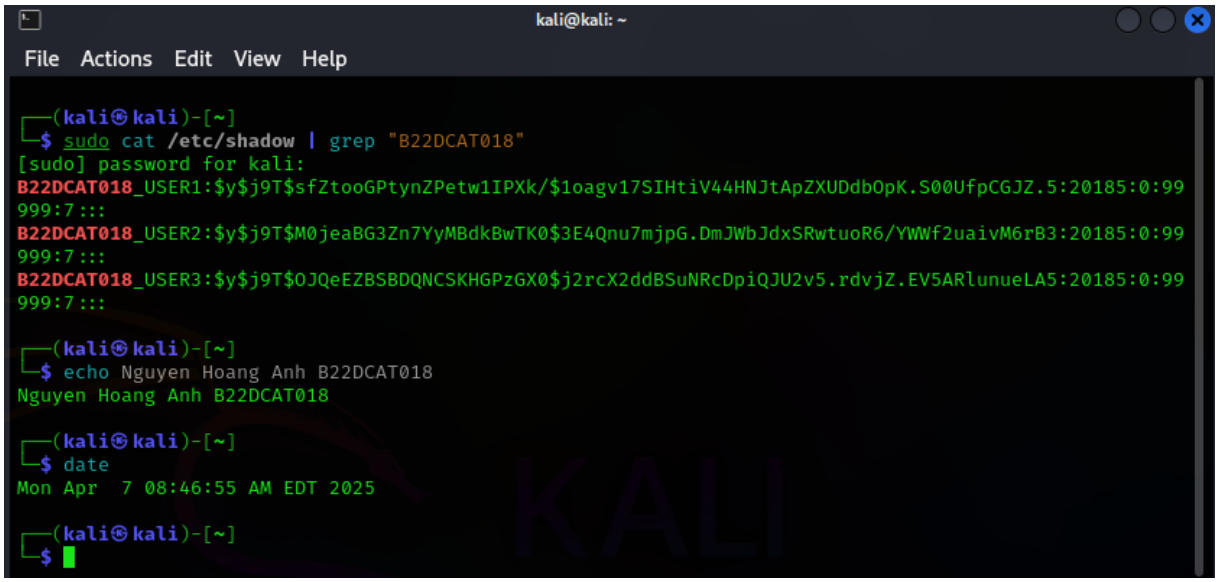
Hình 8 - tạo người dùng 2

Tạo người dùng 3 tên là: *B22DCAT018_USER3*, mật khẩu là: *12345678*



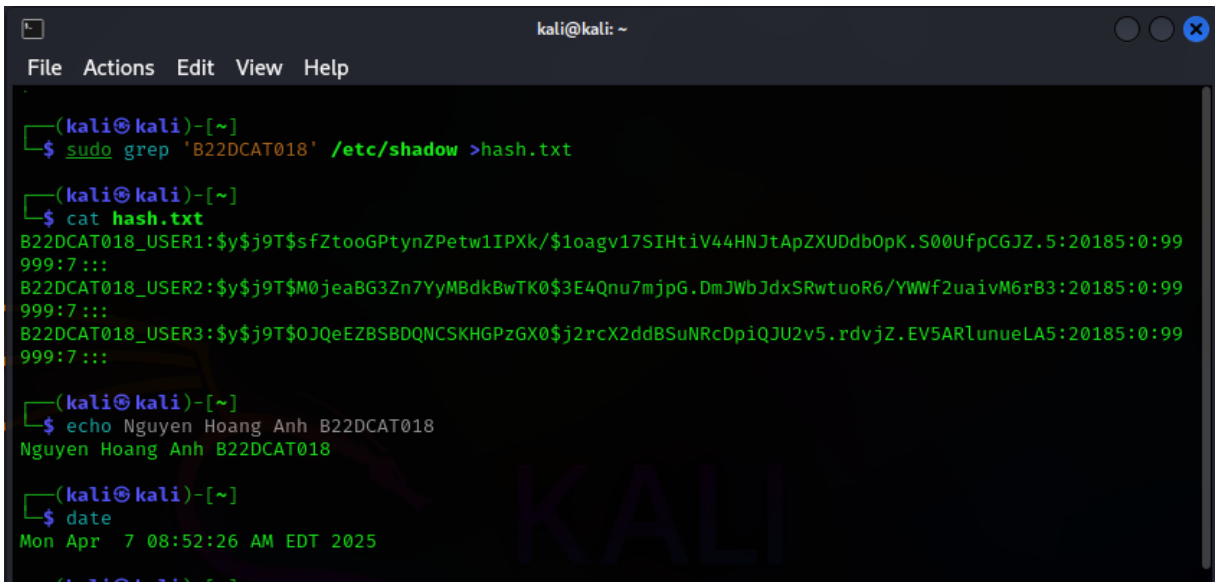
Hình 9 - tạo người dùng 3

Danh sách cả 3 người dùng đã tạo và mã hash mật khẩu:



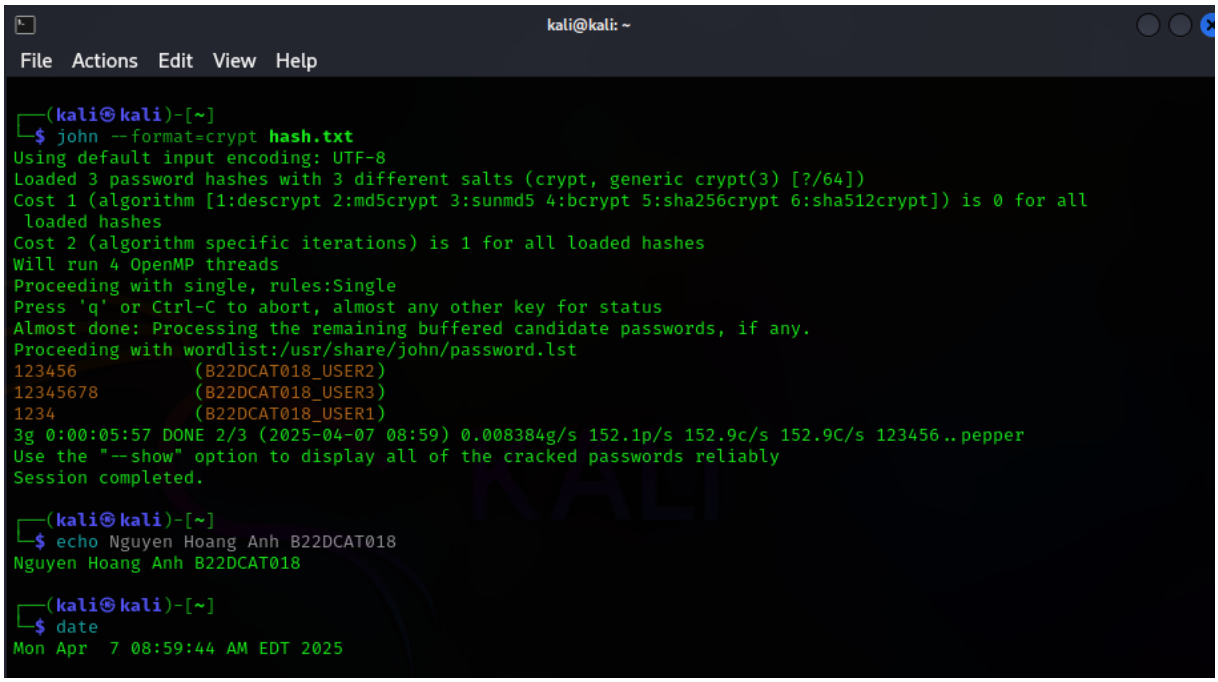
Hình 10 - danh sách 3 người dùng vừa tạo

Lưu 3 người dùng đó vào tệp “hash.txt”:



Hình 11 - lưu danh sách người dùng vào tệp "hash.txt"

Sử dụng công cụ john the ripper để crack mật khẩu của 3 người dùng vừa tạo:



Hình 12 - sử dụng john the ripper để crach mật khẩu

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