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:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng 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 Tổng quan

- Mật khẩu là phương thức xác thực phổ biến nhất dùng để bảo vệ thông tin và tài nguyên. Tuy nhiên, nếu không được bảo vệ đúng cách, chúng trở thành mục tiêu dễ bị tấn công. Tấn công vào mật khẩu là một kỹ thuật mà kẻ tấn công sử dụng để đoán, thu thập, hoặc phá vỡ thông tin xác thực người dùng

1.2.2 Các hình thức tấn công vào mật khẩu phổ biến

1.2.2.1 Tấn công vét cạn (Brute-force Attack)

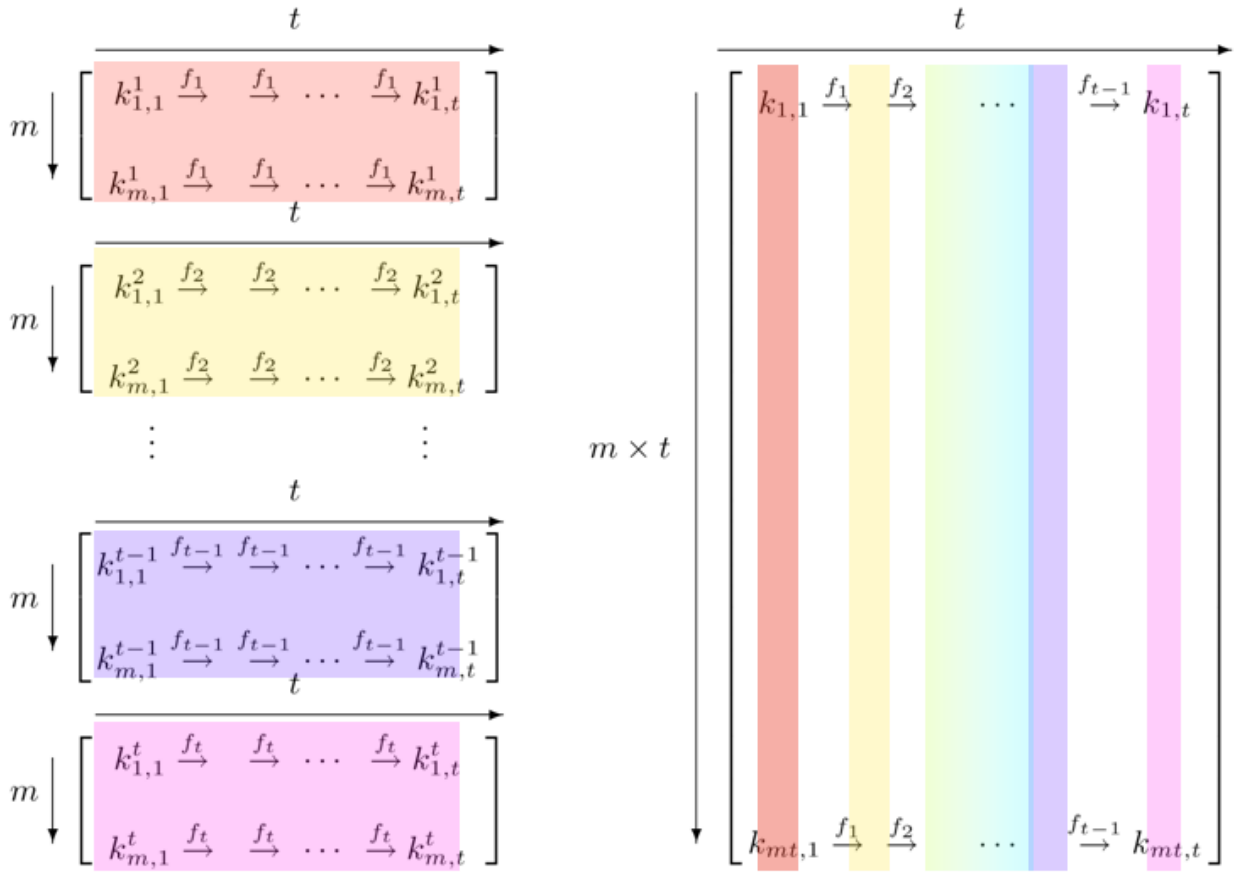
- Đây là hình thức tấn công trong đó kẻ tấn công thử tất cả các tổ hợp có thể của mật khẩu cho đến khi tìm được mật khẩu đúng. Phương pháp này đảm bảo thành công nếu có đủ thời gian và tài nguyên, nhưng sẽ mất rất nhiều thời gian nếu mật khẩu đủ mạnh. Một số công cụ hỗ trợ brute-force phổ biến như: Hydra, John the Ripper, Hashcat.

1.2.2.2 Tấn công từ điển (Dictionary Attack)

- Trong phương pháp này, kẻ tấn công sử dụng một danh sách các mật khẩu phổ biến hoặc có khả năng cao được sử dụng (gọi là từ điển) để thử đăng nhập. Tấn công từ điển nhanh hơn brute-force do giới hạn số lượng mật khẩu cần thử. Tuy nhiên, phương pháp này dễ bị thất bại nếu người dùng sử dụng mật khẩu mạnh và khó đoán.

1.2.2.3 Tấn công bằng bảng cầu vồng (Rainbow Table Attack)

- Bảng cầu vồng là tập hợp các cặp giá trị gồm mật khẩu và hàm băm tương ứng được tính toán trước. Khi tấn công, kẻ tấn công chỉ cần so sánh giá trị băm của mật khẩu lưu trong hệ thống với các giá trị trong bảng để tìm ra mật khẩu tương ứng. Nếu mật khẩu được băm kèm salt, bảng cầu vồng trở nên vô dụng. Vì vậy, việc sử dụng salt và các thuật toán băm an toàn như bcrypt hoặc PBKDF2 là rất quan trọng để phòng ngừa tấn công kiểu này.



Hình 1 Minh họa về Bảng cầu vồng được trình bày tại Crypto 2003 (Wikipedia)

1.2.2.4 Tấn công lừa đảo (Phishing)

- Đây là hình thức tấn công gián tiếp, trong đó kẻ tấn công tạo ra một trang web giả mạo (thường là trang đăng nhập) để lừa người dùng tự nguyện cung cấp tên người dùng và mật khẩu. Hình thức này thường được thực hiện qua email giả mạo hoặc đường dẫn độc hại.

1.2.2.5 Tấn công ghi lại phím gõ (Keylogger)

- Kẻ tấn công cài đặt phần mềm hoặc thiết bị phần cứng để theo dõi và ghi lại toàn bộ các phím mà người dùng nhập vào bàn phím. Qua đó, kẻ tấn công có thể thu được mật khẩu và các thông tin nhạy cảm khác.

1.2.2.6 Nhìn trộm vai (Shoulder Surfing)

- Đây là hình thức quan sát trực tiếp người dùng khi họ nhập mật khẩu, thường xảy ra ở nơi công cộng hoặc không gian làm việc mở. Dù đơn giản, nhưng phương pháp này vẫn khá hiệu quả nếu người dùng không cẩn trọng.

1.2.2.7 Tấn công bằng thông tin bị rò rỉ (Credential Stuffing)

- Kẻ tấn công sử dụng thông tin đăng nhập đã bị rò rỉ từ một dịch vụ khác để thử truy cập vào hệ thống, dựa trên thói quen người dùng sử dụng lại mật khẩu ở nhiều nơi. Đây là một trong những dạng tấn công phổ biến hiện nay.

1.2.3 Biện pháp phòng chống

- Để hạn chế nguy cơ bị tấn công vào mật khẩu, cần áp dụng các biện pháp sau:

- Thiết lập chính sách mật khẩu mạnh: Mật khẩu nên có độ dài tối thiểu và chứa tổ hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Giới hạn số lần đăng nhập sai: Ngăn chặn các cuộc tấn công brute-force và dictionary.
- Sử dụng CAPTCHA: Nhằm phát hiện và ngăn chặn các công cụ tự động tấn công.
- Băm mật khẩu với salt: Tăng cường bảo mật bằng cách sử dụng kỹ thuật băm có salt ngẫu nhiên.
- Xác thực hai yếu tố (2FA): Bổ sung lớp xác thực bằng mã OTP, ứng dụng di động hoặc thiết bị vật lý.
- Theo dõi bất thường trong truy cập: Phát hiện sớm các hành vi đăng nhập trái phép.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

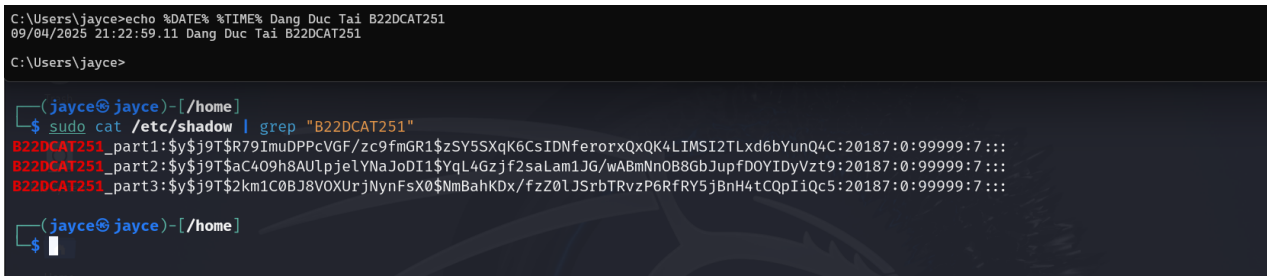
2.1 Chuẩn bị môi trường

- Máy ảo Linux và Windows
- Công cụ crack mật khẩu trên Windows: Hash Suite
- Công cụ crack mật khẩu trên Linux: John the ripper

2.2 Các bước thực hiện

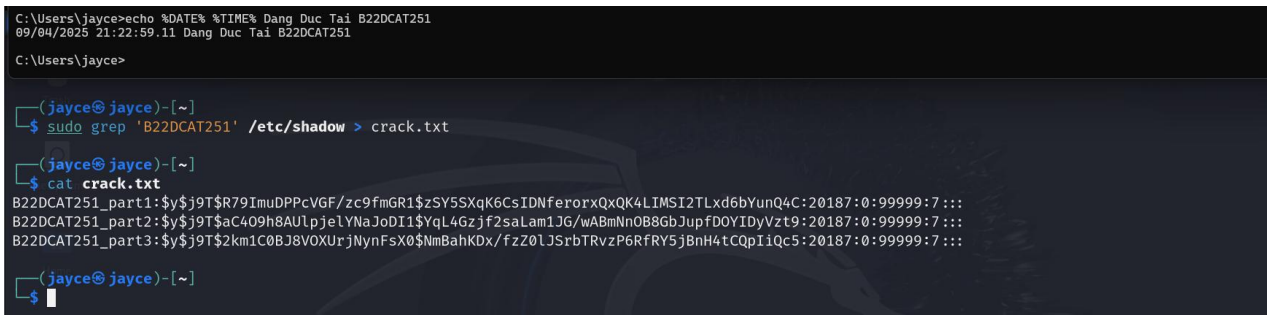
2.2.1 Crack trên Linux

- Tạo các người dùng trên Linux sử dụng các câu lệnh tạo người dùng được học trong bài thực hành số 1.2
  sudo useradd -m USER
  sudo passwd USER
- Xem danh sách mật khẩu dưới dạng hash của người dùng tại file /etc/shadow



Hình 2 Danh sách mật khẩu dạng hash của người dùng

- Chuyển chúng vào file để tiến hành crack mật khẩu. Trong bài này sử dụng 3 mật khẩu của người dùng có độ dài lần lượt 4, 6, 8 ký tự.



Hình 3 Tạo file crack mật khẩu

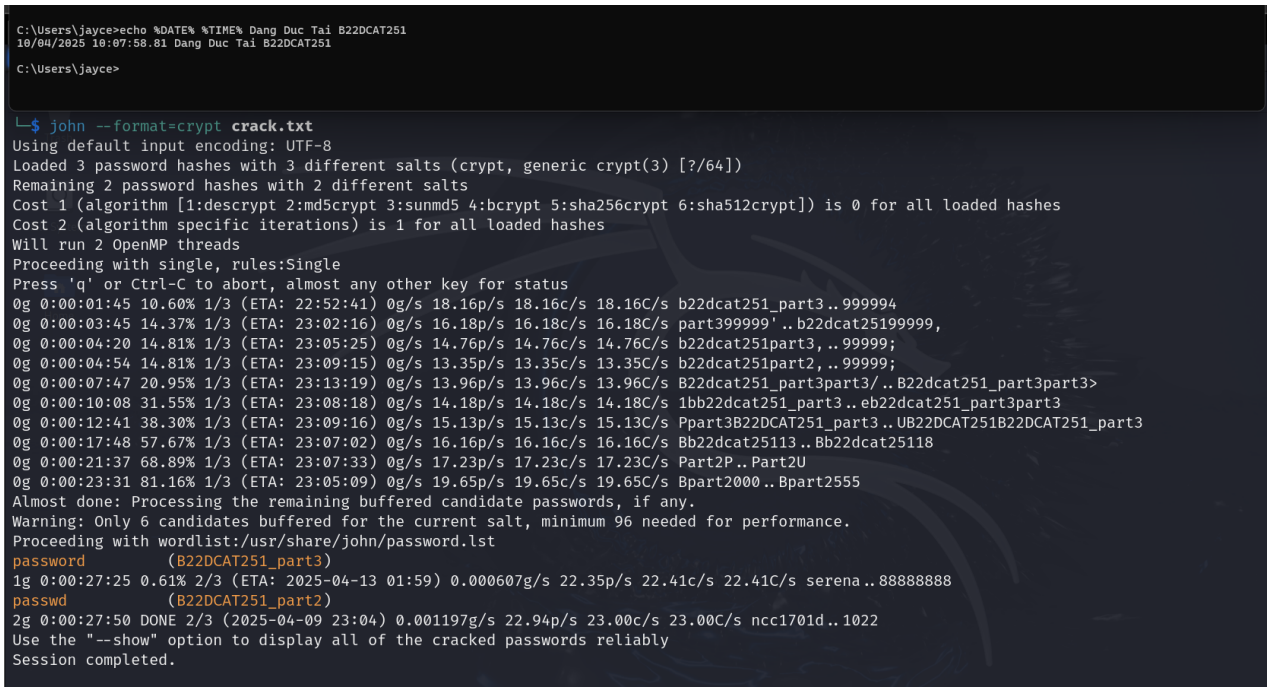
- Sử dụng công cụ john the ripper để tiến hành crack mật khẩu trên Linux

- Tải công cụ bằng câu lệnh:

  sudo apt install john

- Crack file hash vừa tạo

  john –format=crypt crack.txt



Hình 4 Crack mật khẩu với john (1)

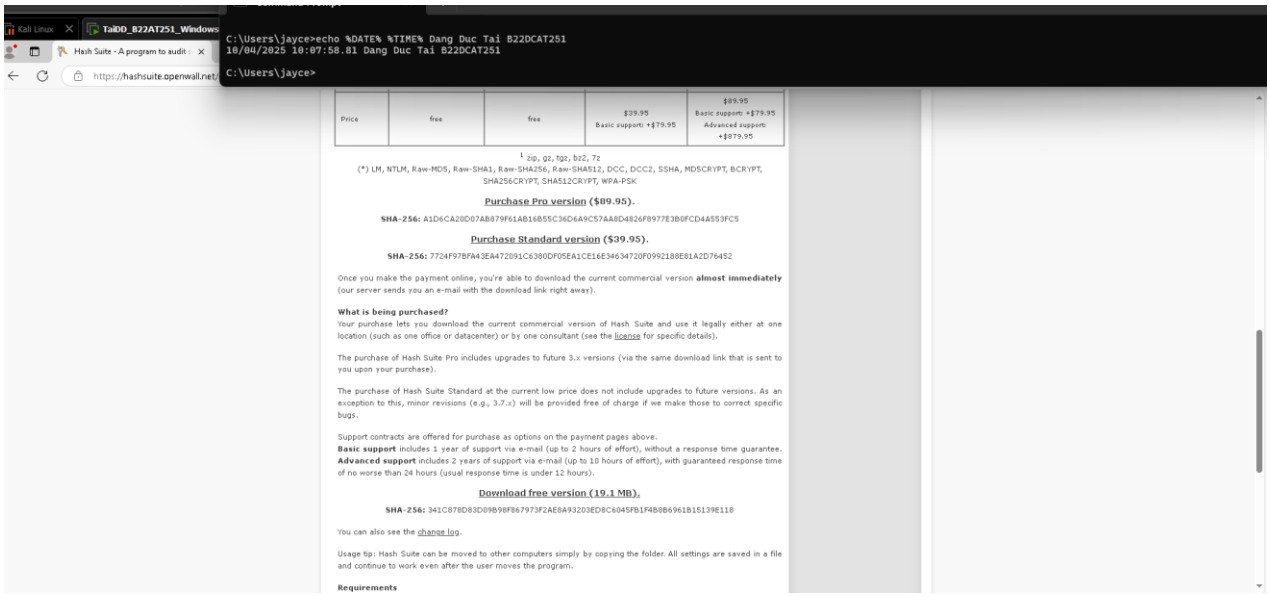
- Các mật khẩu từ 4, 6, 8 ký tự đều được john crack

```
C:\Users\jayce>echo %DATE% %TIME% Dang Duc Tai B22DCAT251
10/04/2025 10:07:58.81 Dang Duc Tai B22DCAT251

C:\Users\jayce>


┌──(jayce㉿jayce)-[~]
└─$ john --format=crypt user1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:42 18.23% 1/3 (ETA: 23:18:03) 0g/s 63.65p/s 63.65c/s 63.65C/s Pb22dcat251h..Pb22dcat251m
0g 0:00:03:36 79.84% 1/3 (ETA: 23:18:43) 0g/s 62.58p/s 62.58c/s 62.58C/s B22dcat251_part1b22dcat25159..b22dcat251_part1b22dcat251000
0g 0:00:03:37 80.28% 1/3 (ETA: 23:18:43) 0g/s 62.60p/s 62.60c/s 62.60C/s bb22dcat251000..bb22dcat251555
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
pass             (B22DCAT251_part1)
1g 0:00:05:40 DONE 2/3 (2025-04-09 23:19) 0.002932g/s 61.69p/s 61.69c/s 61.69C/s modem..sony
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Hình 5 Crack mật khẩu với john (2)

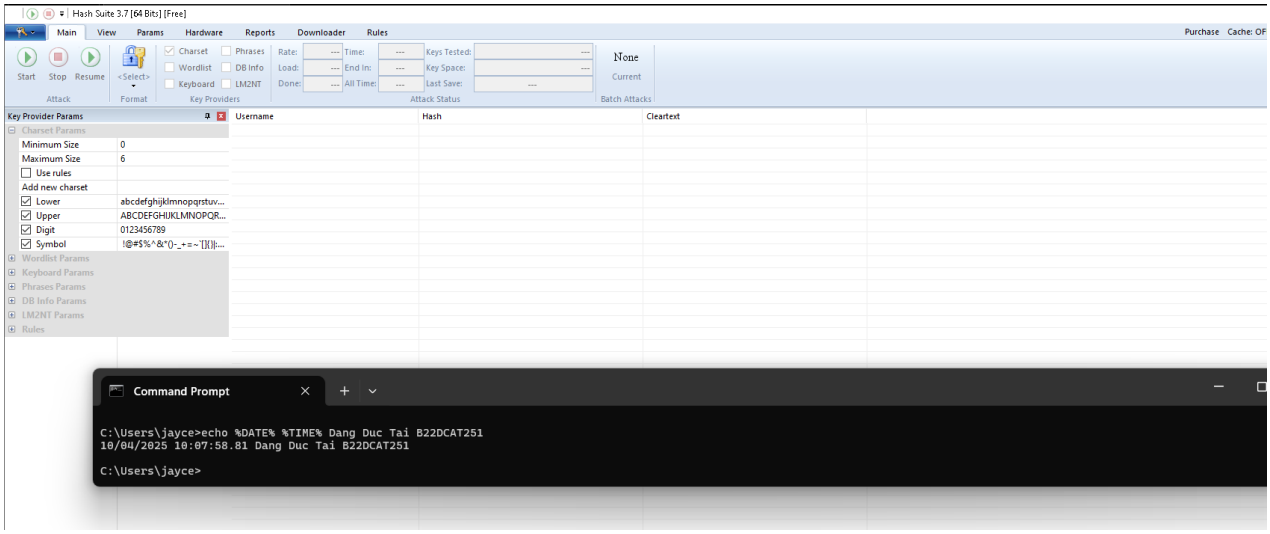
2.2.2 Crack trên Windows

- Tải phần mềm crack mật khẩu Windows Hash Suite https://hashsuite.openwall.net/download



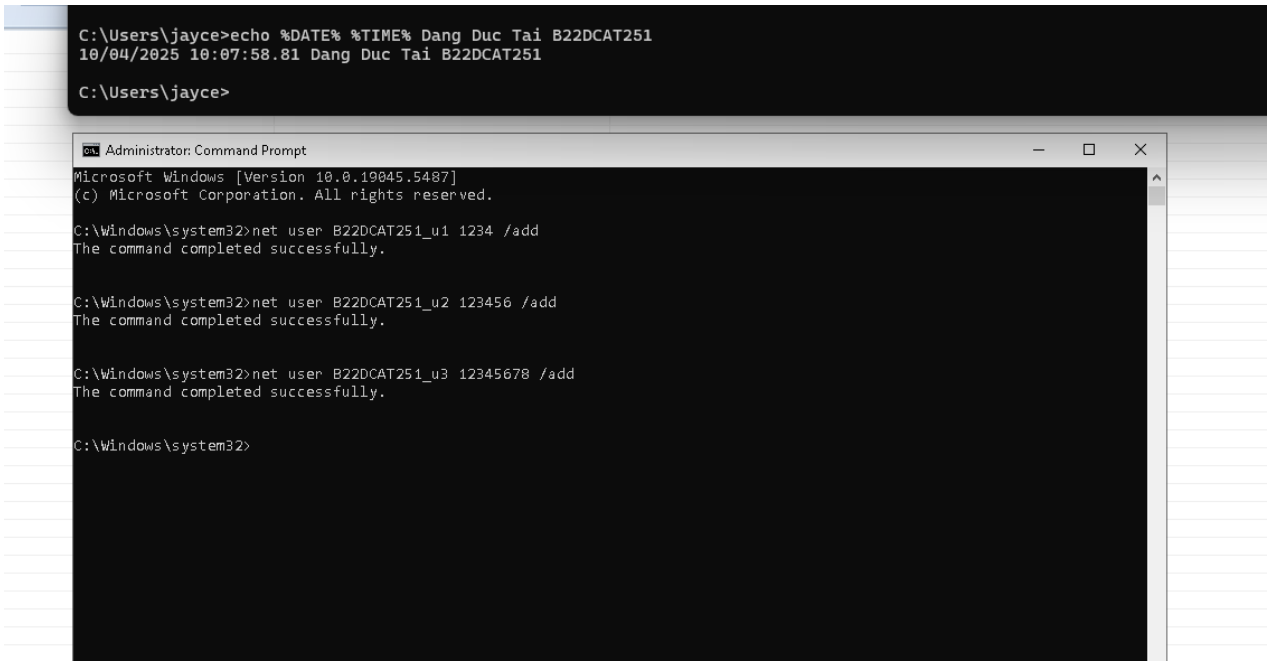
Hình 6 Cài đặt công cụ Hash Suite

- Giao diện đồ họa (GUI) của công cụ Hash Suite



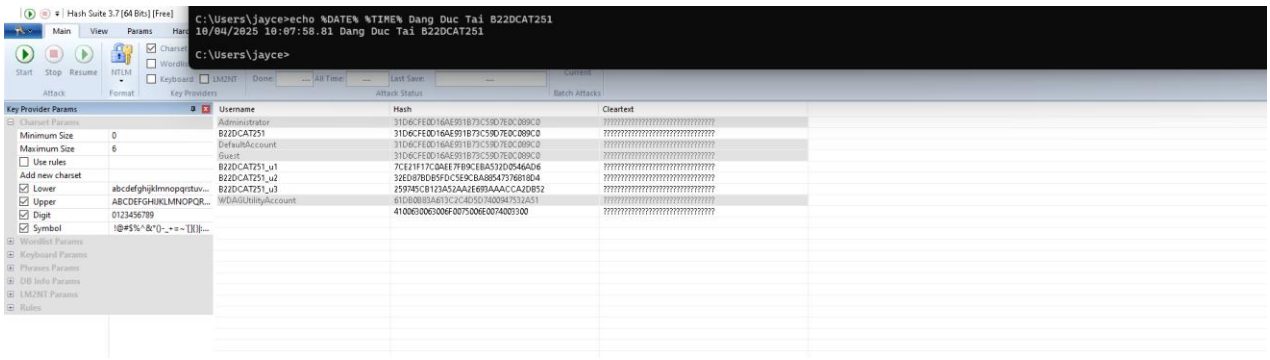
Hình 7 Giao diện đồ họa của công cụ Hash Suite

- Tiến hành tạo người dùng & mật khẩu trên Windows. Trong bài này sử dụng 3 mật khẩu của người dùng có độ dài lần lượt 4, 6, 8 ký tự.
  net user USERNAME PASSWD /add



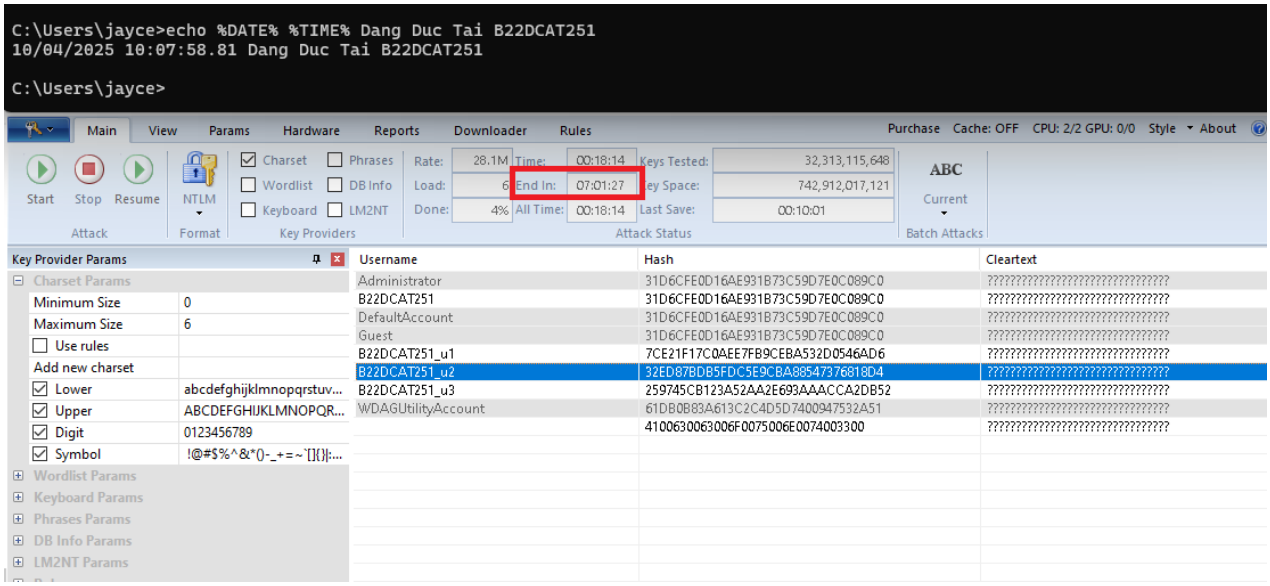
Hình 8 Tạo người dùng trên Windows

- Import file NTLM hash của người dùng Windows lên để công cụ Hash Suite có thể tiến hành crack



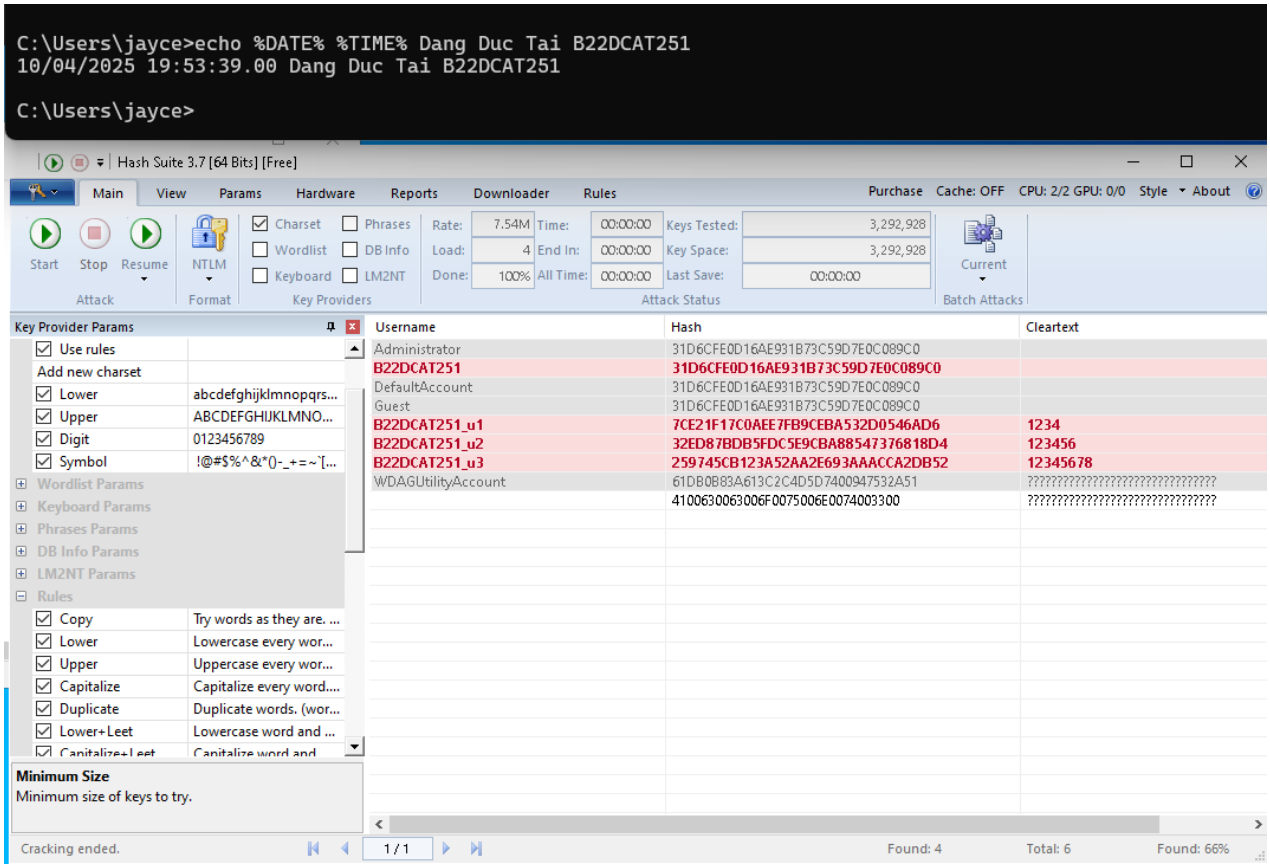
Hình 9 Import file hash và crack bằng Hash Suite

- Với các mã NTLM hash, sẽ tốn khá lâu thời gian để có thể crack được



Hình 10 Thời gian ước tính crack file NTLM hash

- Crack thành công file NTLM hash trên Windows



Hình 11 Crack thành công mật khẩu với Hash Suite

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