**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:Ngô Quang Thắng - B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# **MỤC LỤC**

[**MỤC LỤC** 2](#_Toc196666006)

[**DANH MỤC HÌNH ẢNH** 3](#_Toc196666007)

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 4](#_Toc196666008)

[1.1 Mục đích 4](#_Toc196666009)

[1.2 Tìm hiểu lý thuyết 4](#_Toc196666010)

[1.2.1. OphCrack 4](#_Toc196666011)

[1.2.2. PWDUMP 5](#_Toc196666012)

[1.2.3 Hashcat: 5](#_Toc196666013)

[1.2.4. John The Ripper 6](#_Toc196666014)

[1.2.5.Hash Suite 7](#_Toc196666015)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 11](#_Toc196666016)

[2.1 Chuẩn bị môi trường 11](#_Toc196666017)

[2.2 Các bước thực hiện 11](#_Toc196666018)

[2.2.1. Thử nghiệm crack mật khẩu trên hệ điều hành Windows 11](#_Toc196666019)

[2.2.2.Thử nghiệm crack mật khẩu trên hệ điều hành Linux 15](#_Toc196666020)

[TÀI LIỆU THAM KHẢO 18](#_Toc196666021)

# **DANH MỤC HÌNH ẢNH**

[Hình 1: Tải xuống công cụ Hash Suite 11](#_Toc196665990)

[Hình 2: Tạo các users trên Windows 12](#_Toc196665991)

[Hình 3: Công cụ Hash Suite 12](#_Toc196665992)

[Hình 4: Lựa chọn option 13](#_Toc196665993)

[Hình 5: Chức năng NTLM 13](#_Toc196665994)

[Hình 6: Tấn công mật khẩu 14](#_Toc196665995)

[Hình 7: Tạo user trên Linux 15](#_Toc196665996)

[Hình 8: Kiểm tra lại user 16](#_Toc196665997)

[Hình 9: Chuyển thông tin user vào tệp 16](#_Toc196665998)

[Hình 10: Tấn công bằng john the ripper 17](#_Toc196665999)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   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. 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).

Hash cat 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 đầu hash> <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*

**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.
* John cũng có 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.

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.

**1.2.5.Hash Suite**

**HashSuite: "Dao mổ" mạnh mẽ cho mật khẩu băm**

HashSuite là một bộ công cụ phần mềm đa nền tảng (Windows và Android) được thiết kế chuyên biệt cho việc kiểm toán bảo mật mật khẩu bằng cách thực hiện các cuộc tấn công bẻ khóa mật khẩu băm (password hashes). Nó được phát triển với mục tiêu cung cấp một giải pháp **nhanh chóng, dễ sử dụng, thông minh, mạnh mẽ và có khả năng mở rộng** cho cả người dùng cá nhân và các chuyên gia bảo mật.

**Triết lý thiết kế:**

HashSuite được xây dựng dựa trên triết lý cung cấp một giao diện trực quan, dễ tiếp cận cho người mới bắt đầu, đồng thời cung cấp đủ các tùy chọn cấu hình nâng cao và hiệu suất cao cho người dùng có kinh nghiệm. Nó cố gắng cân bằng giữa sự đơn giản và sức mạnh, giúp người dùng dễ dàng thực hiện các tác vụ kiểm toán mật khẩu một cách hiệu quả.

**Các phiên bản:**

HashSuite có các phiên bản khác nhau để phù hợp với nhu cầu và nền tảng khác nhau:

* **Hash Suite for Windows (Standard - Miễn phí):** Đây là phiên bản cơ bản dành cho hệ điều hành Windows, cung cấp các tính năng cốt lõi để bẻ khóa mật khẩu băm bằng CPU. Nó hỗ trợ nhiều thuật toán băm phổ biến và các kiểu tấn công từ điển, vét cạn cơ bản.
* **Hash Suite for Windows (Pro - Trả phí):** Phiên bản chuyên nghiệp dành cho Windows, mở rộng các tính năng của phiên bản Standard bằng cách hỗ trợ tăng tốc bẻ khóa bằng GPU (Nvidia CUDA, AMD OpenCL, Intel), cung cấp các kiểu tấn công nâng cao hơn (hybrid, rule-based), và có thể có các tính năng khác như báo cáo chi tiết hơn.
* **Hash Suite Droid (Android - Miễn phí/Trả phí):** Phiên bản dành cho hệ điều hành Android, cho phép bạn thực hiện các cuộc tấn công bẻ khóa mật khẩu trực tiếp trên thiết bị di động của mình. Tương tự như phiên bản Windows, có thể có phiên bản miễn phí với các tính năng cơ bản và phiên bản trả phí (thường được mua trong ứng dụng) để mở khóa hiệu suất GPU và các tính năng nâng cao khác.

**Các tính năng nổi bật (chi tiết):**

1. **Hỗ trợ đa dạng thuật toán băm:** HashSuite có khả năng làm việc với nhiều thuật toán băm mật khẩu khác nhau, bao gồm cả các thuật toán cũ và hiện đại. Điều này cho phép nó kiểm toán bảo mật cho nhiều hệ thống và ứng dụng khác nhau. Các thuật toán được hỗ trợ thường bao gồm:
   * **Windows:** LM, NTLM
   * **Phổ biến:** MD5, SHA-1, SHA-256, SHA-512
   * **Salted Hashes:** SSHA, md5crypt, bcrypt, sha256crypt, sha512crypt
   * **Khác:** DCC, DCC2
   * **WiFi:** WPA/WPA2 PSK (thông qua tệp pcap/hccapx)
2. **Phương pháp tấn công linh hoạt:** HashSuite cung cấp nhiều phương pháp tấn công khác nhau để thử bẻ khóa mật khẩu:
   * **Dictionary Attack (Tấn công từ điển):** Sử dụng danh sách các mật khẩu tiềm năng (wordlist) để thử. Rất hiệu quả nếu mật khẩu là một từ phổ biến hoặc nằm trong danh sách.
   * **Brute-Force Attack (Tấn công vét cạn):** Thử tất cả các tổ hợp ký tự có thể trong một phạm vi nhất định. Tốn thời gian nhưng có khả năng tìm ra các mật khẩu phức tạp.
   * **Hybrid Attack (Tấn công kết hợp):** Kết hợp tấn công từ điển với các quy tắc biến đổi (ví dụ: thêm số, ký tự đặc biệt vào cuối từ trong từ điển).
   * **Rule-Based Attack (Tấn công dựa trên quy tắc):** Áp dụng các quy tắc biến đổi lên các từ trong từ điển để tạo ra các mật khẩu tiềm năng. Rất mạnh mẽ để tìm ra các mật khẩu có quy tắc tạo nhất định.
   * **Mask Attack (Tấn công theo mẫu):** Cho phép bạn xác định một mẫu (mask) cho mật khẩu và thử tất cả các mật khẩu phù hợp với mẫu đó.
3. **Quản lý Wordlist mạnh mẽ:**
   * Hỗ trợ nhiều định dạng tệp wordlist (văn bản thuần túy, nén như zip, gz, bz2, 7z).
   * Khả năng tải và quản lý nhiều wordlist cùng lúc.
   * Tích hợp khả năng tải xuống các wordlist phổ biến (tùy thuộc vào phiên bản).
4. **Hỗ trợ Rules (Quy tắc):** Cho phép người dùng sử dụng các tệp quy tắc (thường theo cú pháp của Hashcat hoặc John the Ripper) để tạo ra các biến thể của các từ trong wordlist, tăng khả năng tìm thấy mật khẩu.
5. **Hiệu suất cao và khả năng mở rộng:**
   * Tối ưu hóa cho hiệu suất đa luồng trên CPU.
   * Phiên bản Pro và Droid tận dụng sức mạnh của GPU (card đồ họa) để tăng tốc đáng kể quá trình bẻ khóa, đặc biệt là với các thuật toán băm có thể song song hóa tốt.
   * Có khả năng xử lý một lượng lớn các hash cùng lúc.
6. **Giao diện người dùng thân thiện:**
   * Giao diện đồ họa (GUI) trực quan, dễ sử dụng cho cả người mới bắt đầu.
   * Phiên bản Android được thiết kế tối ưu cho màn hình cảm ứng và kích thước nhỏ.
7. **Tính năng tiếp tục tấn công:** Cho phép bạn tạm dừng và tiếp tục lại quá trình bẻ khóa mà không làm mất tiến trình đã thực hiện.
8. **Quản lý tài nguyên thông minh (phiên bản Android):** Có khả năng tự động dừng tấn công khi pin yếu hoặc nhiệt độ thiết bị quá cao để bảo vệ thiết bị.
9. **Khả năng nhập/xuất cấu hình:** Cho phép bạn lưu và chia sẻ cấu hình (bao gồm cả các wordlist và quy tắc đã chọn) giữa các thiết bị (ví dụ: bắt đầu trên PC và tiếp tục trên điện thoại).
10. **Báo cáo và thống kê:** Cung cấp các thông tin thống kê về quá trình bẻ khóa, bao gồm tốc độ bẻ khóa (hash/giây), số lượng mật khẩu đã thử, thời gian ước tính còn lại và các mật khẩu đã tìm thấy.

**Ứng dụng của HashSuite:**

* **Kiểm toán bảo mật mật khẩu:** Giúp các tổ chức và cá nhân đánh giá độ mạnh yếu của mật khẩu đang sử dụng.
* **Phục hồi mật khẩu bị mất:** Trong một số trường hợp hợp pháp, HashSuite có thể được sử dụng để cố gắng phục hồi mật khẩu bị quên.
* **Nghiên cứu bảo mật:** Là một công cụ hữu ích cho các nhà nghiên cứu bảo mật để phân tích các thuật toán băm và kỹ thuật tấn công mật khẩu.
* **Giáo dục và đào tạo:** Giúp người học hiểu rõ hơn về các nguyên tắc bẻ khóa mật khẩu và tầm quan trọng của việc sử dụng mật khẩu mạnh.

**Lưu ý quan trọng:**

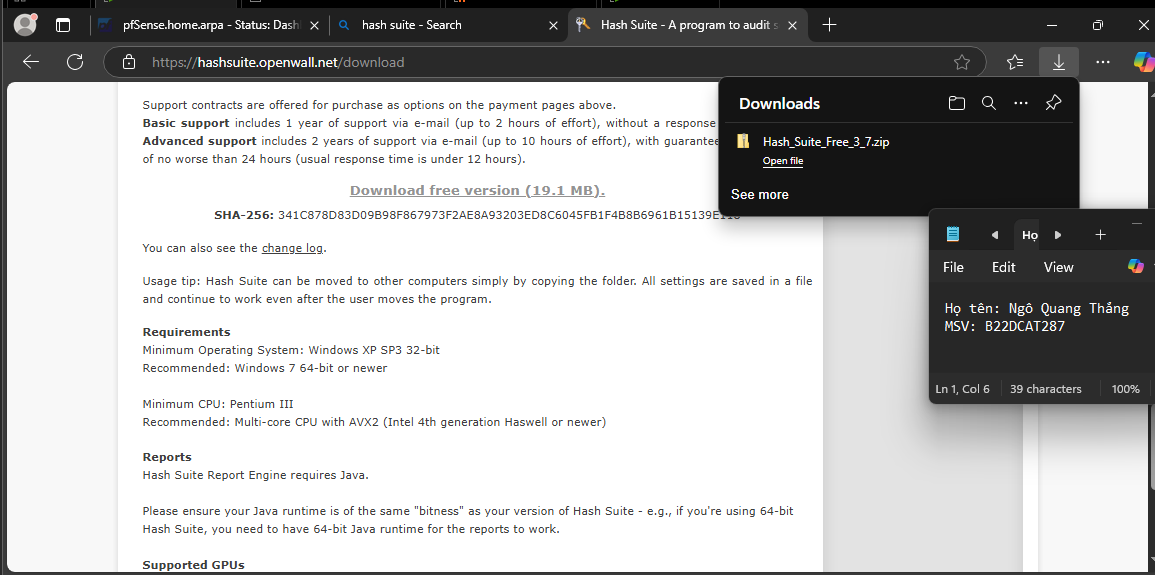
HashSuite là một công cụ mạnh mẽ và cần được sử dụng một cách có trách nhiệm và hợp pháp. Việc sử dụng nó để cố gắng truy cập trái phép vào tài khoản của người khác là bất hợp pháp và phi đạo đức.

1. NỘI DUNG THỰC HÀNH
   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
  1. Các bước thực hiện

**2.2.1. Thử nghiệm crack mật khẩu trên hệ điều hành Windows**

* Tải xuống công cụ Hash Suite:



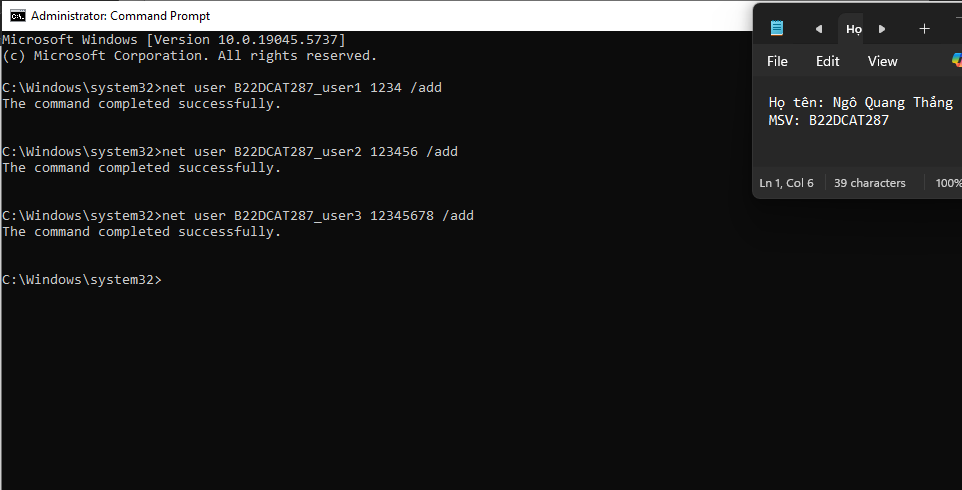
Hình 1: Tải xuống công cụ Hash Suite

* Thêm các user để thực hiện tấn công:

*net user b22dcat287\_user1 1234 /add*

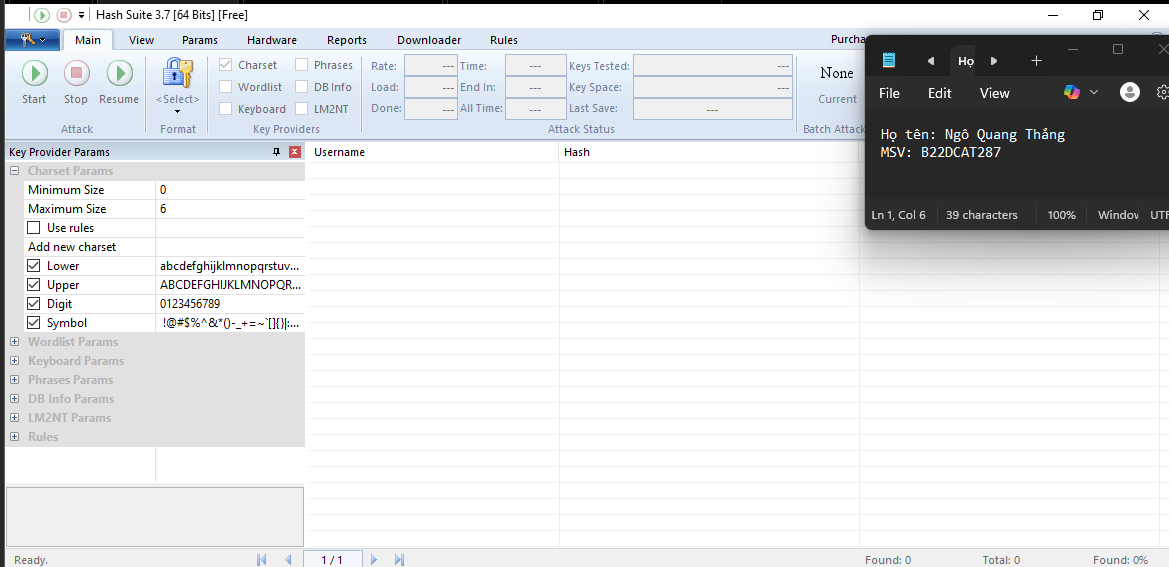
*net user b22dcat287\_user1 123456 /add*

*net user b22dcat287\_user1 123478 /add*



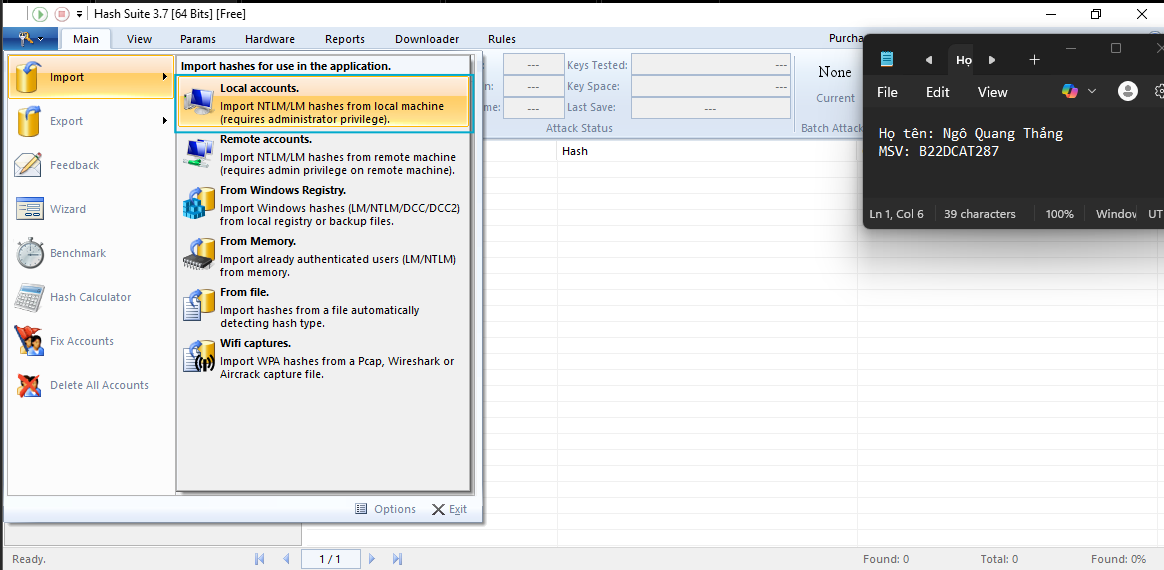
Hình 2: Tạo các users trên Windows

* Thực hiện mở ứng dụng HashSuite:



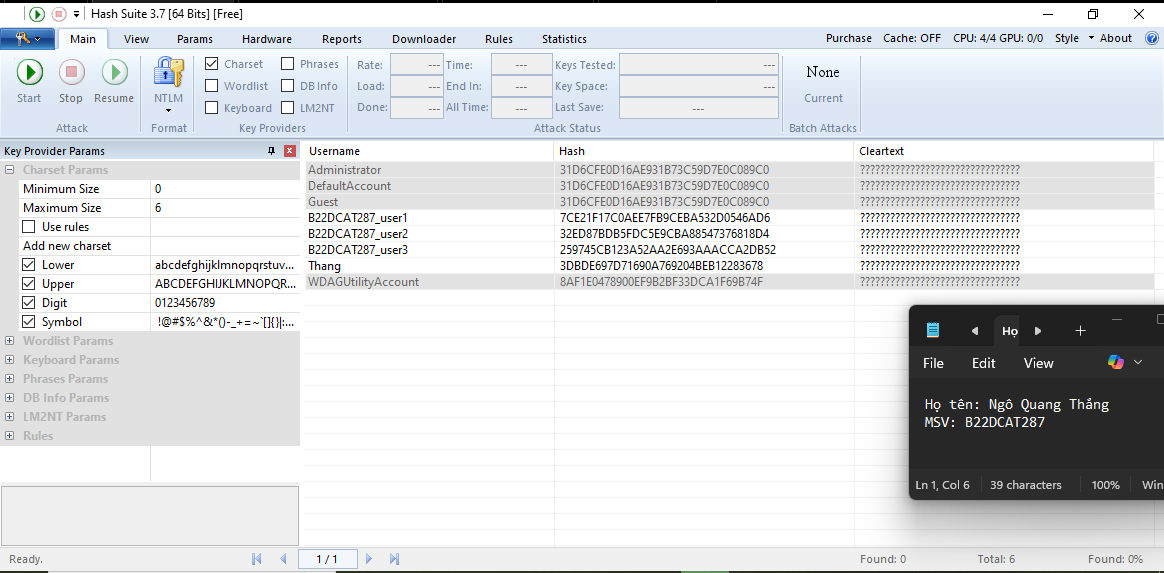
Hình 3: Công cụ Hash Suite

* Click vào chìa khoá -> Lựa chọn *Local accounts*



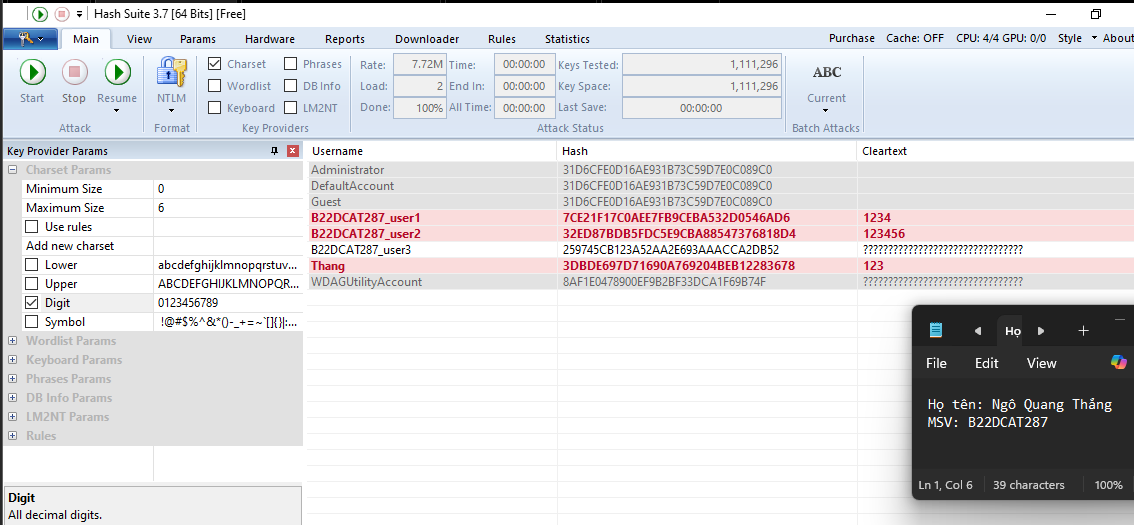
Hình 4: Lựa chọn option

* Lựa chọn Hình khoá+Key : Lựa chọn NTLM:
  + Hiện ra các tài khoàn và hàm băm



Hình 5: Chức năng NTLM

* Click “Start”; thực hiện vét cạn, tấn công mật khẩu
  + Kết quả khi thực hiện vét cạn(Do vét cạn lâu em để vét cạn 2 tài khoản)



Hình 6: Tấn công mật khẩu

**2.2.2.Thử nghiệm crack mật khẩu trên hệ điều hành Linux**

* Tạo các user và độ dài mật khẩu khác nhau

*sudo useradd b22dcat287\_usr1*

*sudo passwd b22dcat287\_usr1*

*password: 1234*

*sudo useradd b22dcat287\_usr2*

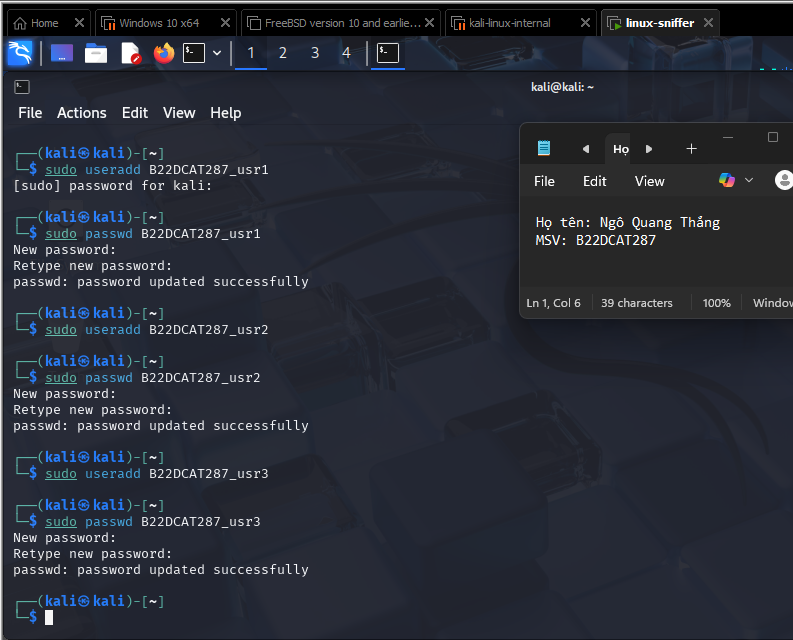
*sudo passwd b22dcat287\_usr2*

*password: 123456*

*sudo useradd b22dcat287\_usr3*

*sudo passwd b22dcat287\_usr3*

*password: 12345678*

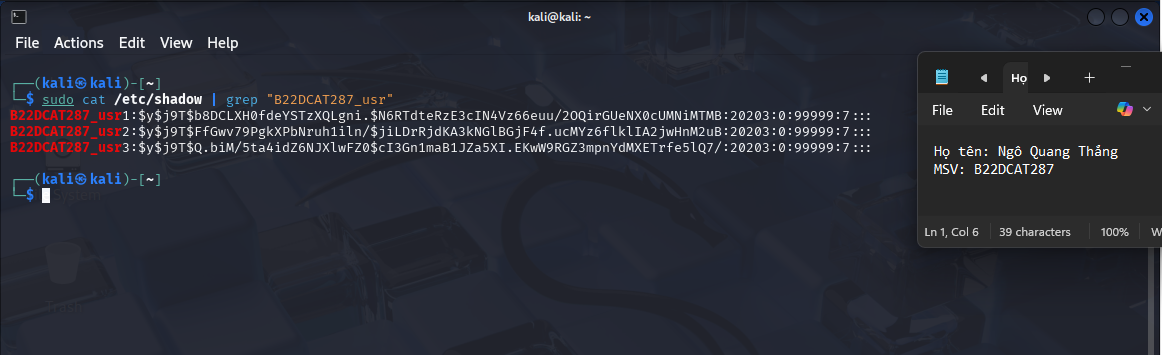


Hình 7: Tạo user trên Linux

* Kiểm tra lại xem đã tạo thành công chưa

*sudo cat /etc/shadow | grep “b22dcat287\_usr”*

* + Hiện ra các user và đoạn mã hoá (mật khẩu)



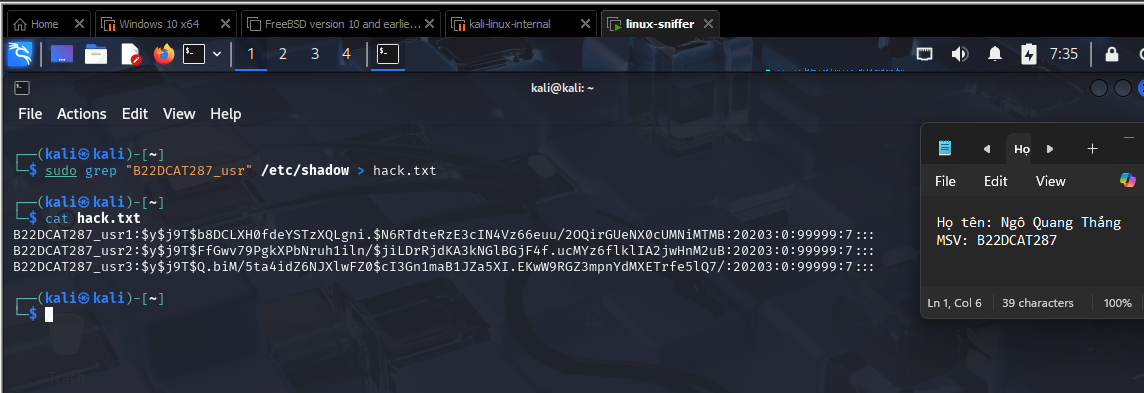
Hình 8: Kiểm tra lại user

* Chuyển vào tệp để thực hiện tấn công mật khẩu

*sudo grep “b22dcat287\_usr” /etc/shadow >hack.txt*

* Kiểm tra lại xem đã có chưa:

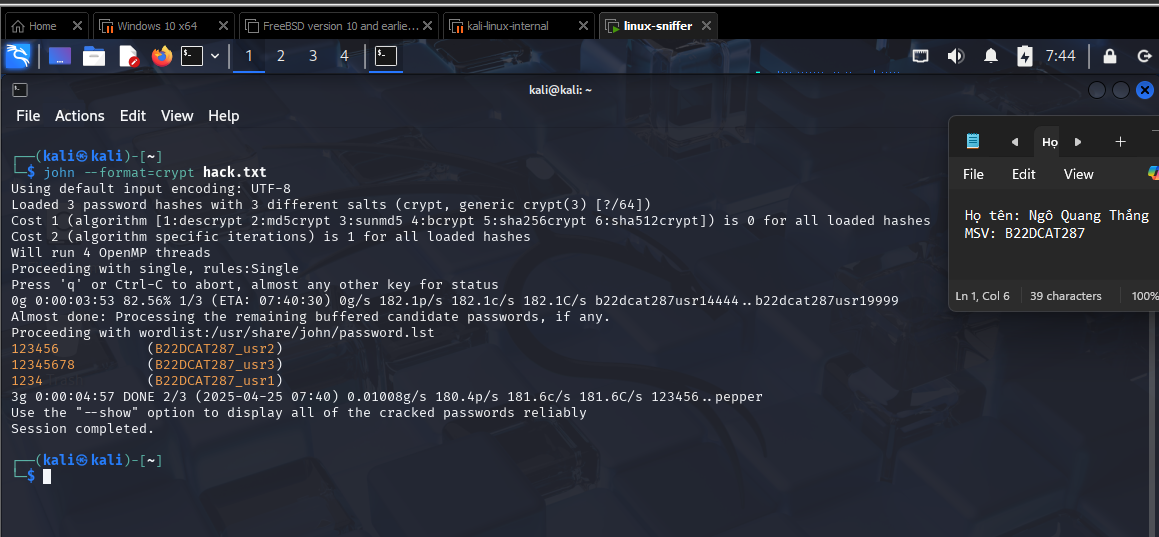
*cat hack.txt*



Hình 9: Chuyển thông tin user vào tệp

* Thực hiện vét cạn

*john -- format-crypt hack.txt*

****

Hình 10: Tấn công bằng john the ripper

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