**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOAN AN TOÀN THÔNG TIN**


# BÁO CÁO THỰC HÀNH

## Bài 12: Tấn công mật khẩu

**Họ và tên: VũThành Long**

**Mã sinh viên: B21DCAT012**

**Nhóm: 06**

**Môn học: Thực tập cơ sở**

**Giảng viên giảng dạy: Nguyễn Hoa Cương**

**Hà Nội, 2024**

# Mục lục

# I. Tìm hiểu lý thuyết:

## 1. Phần mềm bẻ khoá mật khẩu:

- John the Ripper là một công cụ bẻ khóa mật khẩu miễn phí, có mặt trên nhiều họ hệ điều hành như Unix, DOS, Windows.
- Được phát triển bởi OpenWall, John là một trong những chương trình kiểm tra và phá mật khẩu phổ biến nhất vì nó kết hợp nhiều kĩ năng bẻ khoá mật khẩu vào một phần mềm và có khả năng tự động phát hiện các loại mã băm mật khẩu.
- John có thể phá mật khẩu được băm bởi nhiều thuật toán mã băm khác nhau như DES, MD5 hay Blowfish.
- Hash Suite là một công cụ bẻ khoá mật khẩu khác, được phát triển bởi một người đóng góp (contributor) của John.
- Hash Suite chỉ có mặt trên Android và Windows. Khác với John, Hash Suite có giao diện đồ hoạ (GUI).

## 2. Phương pháp bẻ khoá mật khẩu:

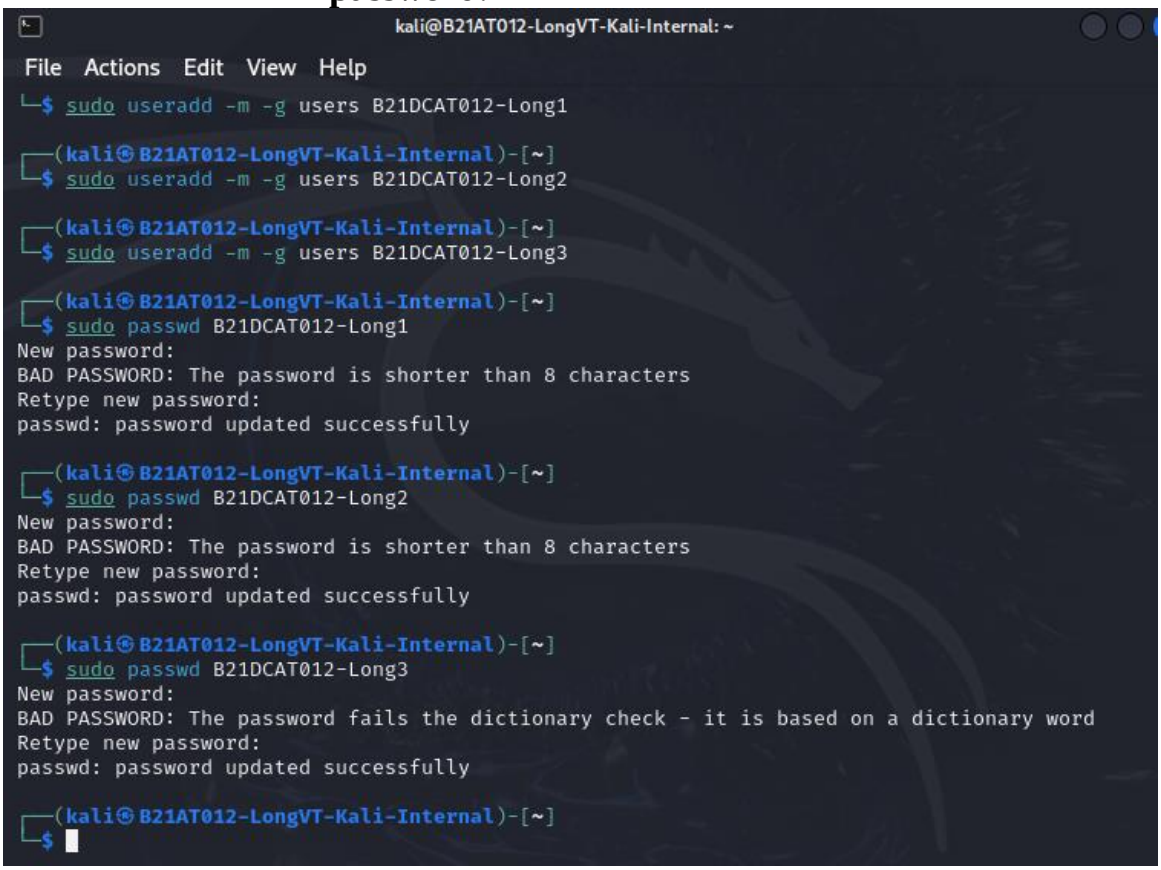
- Hầu hết các phần mềm bẻ khoá mật khẩu đều hỗ trợ hai phương pháp phổ biến nhất là Brute-force attack và Dictionary attack.
- Brute-force attack là kiểu tấn công mà kẻ tấn công thử tất cả các trường hợp có thể của mật khẩu để tìm ra mật khẩu đúng. Trong John, mỗi trường hợp của mật khẩu sẽ được băm sau đó John so sánh mã băm này với mã băm lấy được từ máy tính.
- Ưu điểm của Brute-force attack là chắc chắn sẽ tìm ra mật khẩu đúng nếu thời gian cho phép. Tuy nhiên, nhược điểm của brute-force là thời gian giải mã sẽ rất lâu nếu độ dài của khoá lớn. Ví dụ, thời gian bẻ khoá AES-256 lớn hơn 2^128 lần so với AES-128. Nếu một siêu máy tính có thể thử 10^14 trường hợp trong 1 giây, sẽ phải mất 3.67 * 10^55 năm để kiểm tra tất cả các trường hợp trong AES-256.
- Dictionary attack, hay còn gọi là tấn công bằng từ điển, là khi kẻ tấn công thay vì thử tất cả các trường hợp có thể của mật khẩu, thì chỉ thử những mật khẩu thông dụng nhất. Danh sách các mật khẩu thông dụng được lưu trong một tệp văn bản gọi là wordlist. John sẽ lấy từng mật khẩu trong wordlist, băm rồi so sánh với mã băm lấy được từ máy tính. Ngoài ra, John cũng thử thay đổi một chút mật khẩu trong wordlist khi băm, ví dụ như thử mật khẩu "password" rồi không dừng lại mà thử tiếp "passw0rd" hay "password1".

- Một số mật khẩu thông dụng có thể kể đến như: password, pass, 123456, 12345678, qwerty, anhyeuem, matkhau, admin, root, v.v

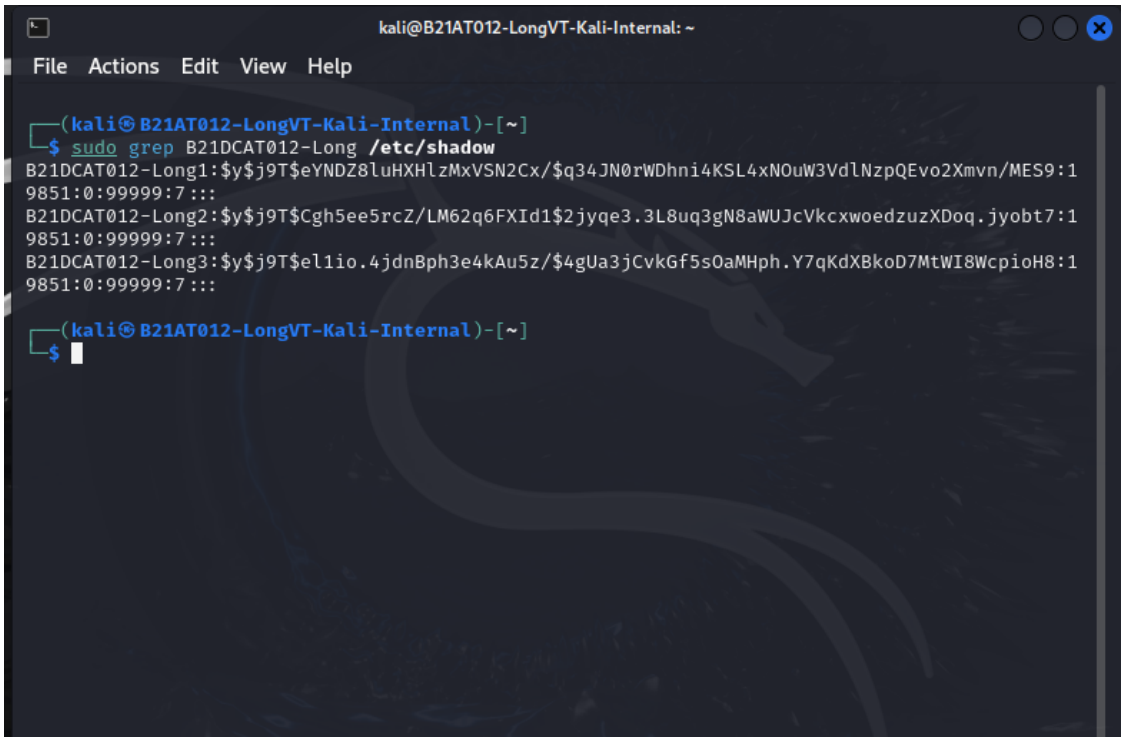
## II. Mô tả cài đặt & kết quả:

### 1. Trên Linux:

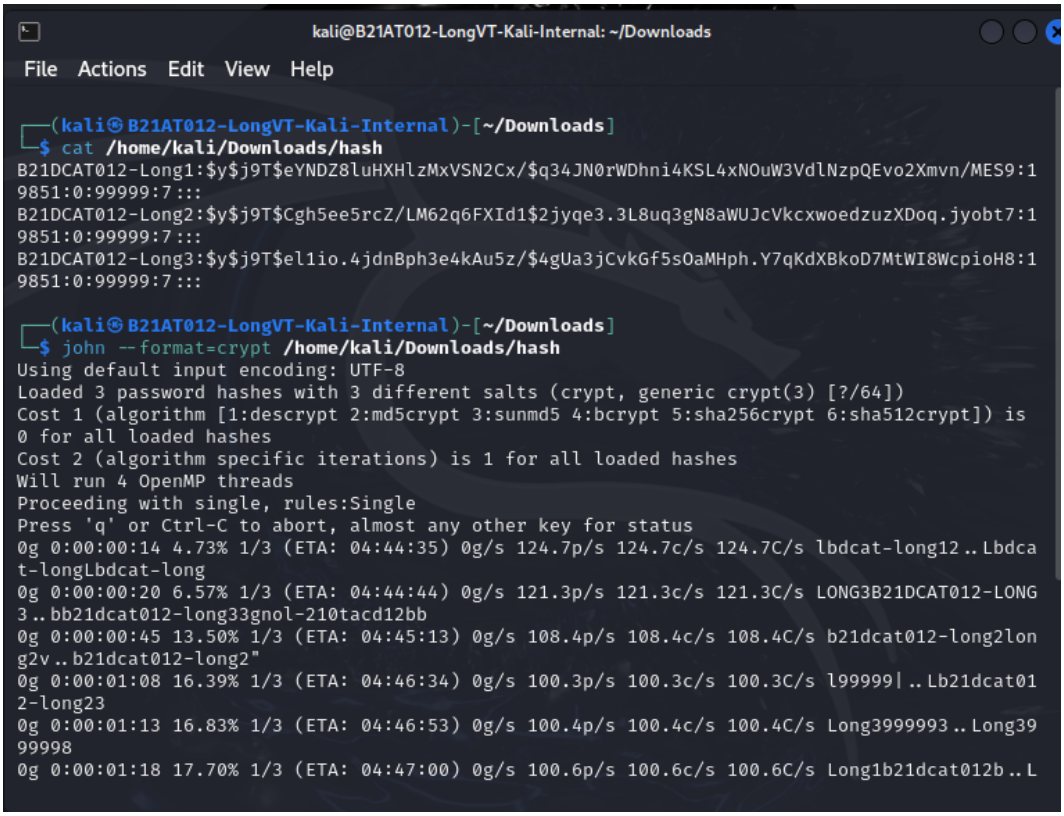
- Sinh viên sử dụng công cụ **john** có cài sẵn trên hệ điều hành Kali Linux.
- Trước hết, sinh viên tạo các người dùng mới bằng lệnh useradd và passwd:
  - Người dùng **B21DCAT012-Long1** mật khẩu **pass**.
  - Người dùng **B21DCAT012-Long2** mật khẩu **passwd**.
  - Người dùng **B21DCAT012-Long3** mật khẩu **password**.



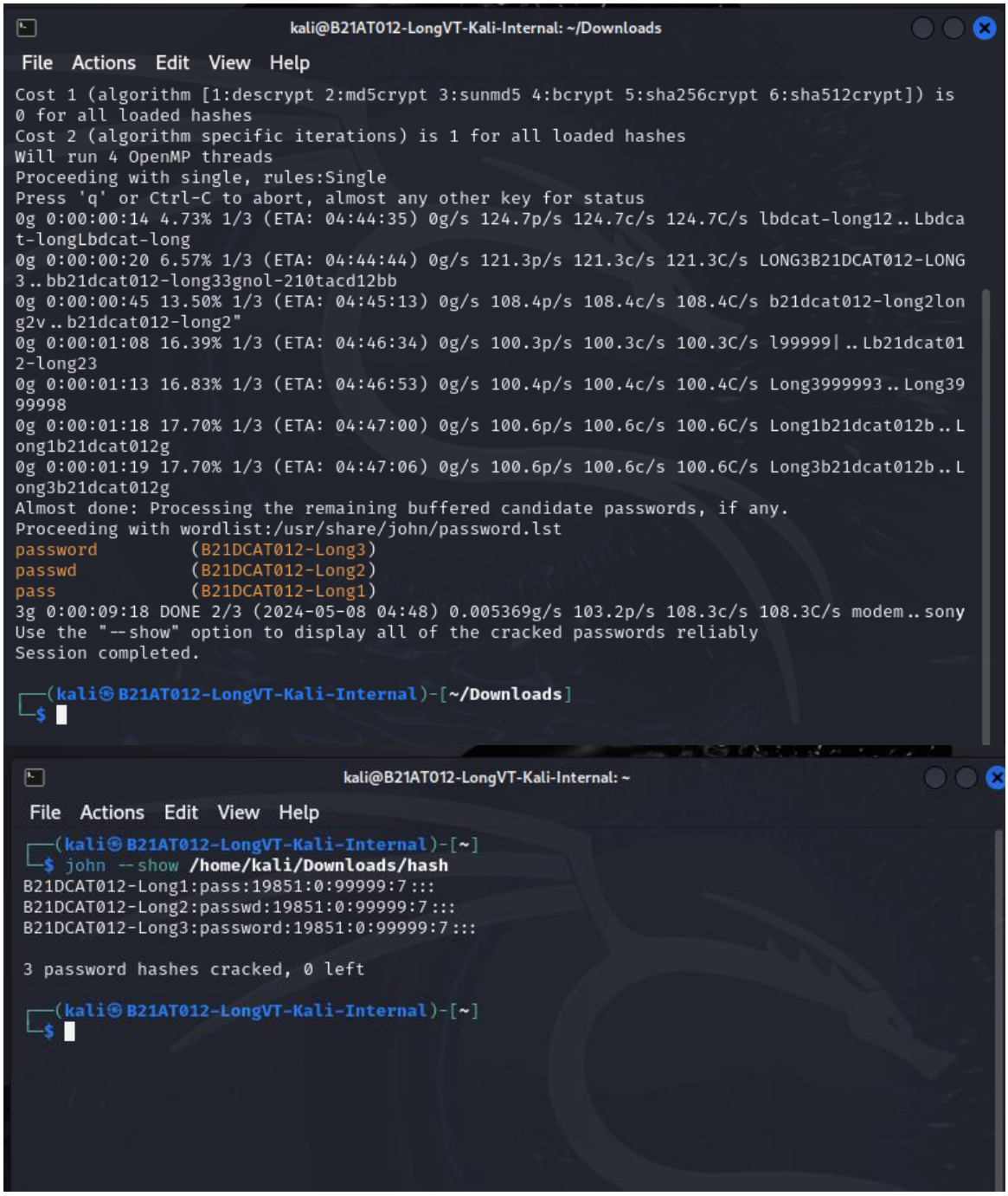

- Mật khẩu đã được mã hoá trên Linux được lưu ở /etc/shadow. Sinh viên thực hiện tìm và copy dòng chứa tên người dùng và mật khẩu đã mã hoá ở tệp tin này.




- Tiếp theo, sinh viên lưu dữ liệu trên vào một tệp văn bản (trong ví dụ là /home/kali/Downloads/hash).
- Tiếp theo sinh viên khởi động john để phá mật khẩu. Để ý thấy trên đoạn mật khẩu mã hoá có các kí tự **$y$**. Điều này có nghĩa là Kali Linux sử dụng thuật toán **yescrypt** để mã hoá mật khẩu.
- Trên terminal, điền lệnh **john --format=crypt /home/kali/Downloads/hash** và kiên nhẫn chờ đợi.

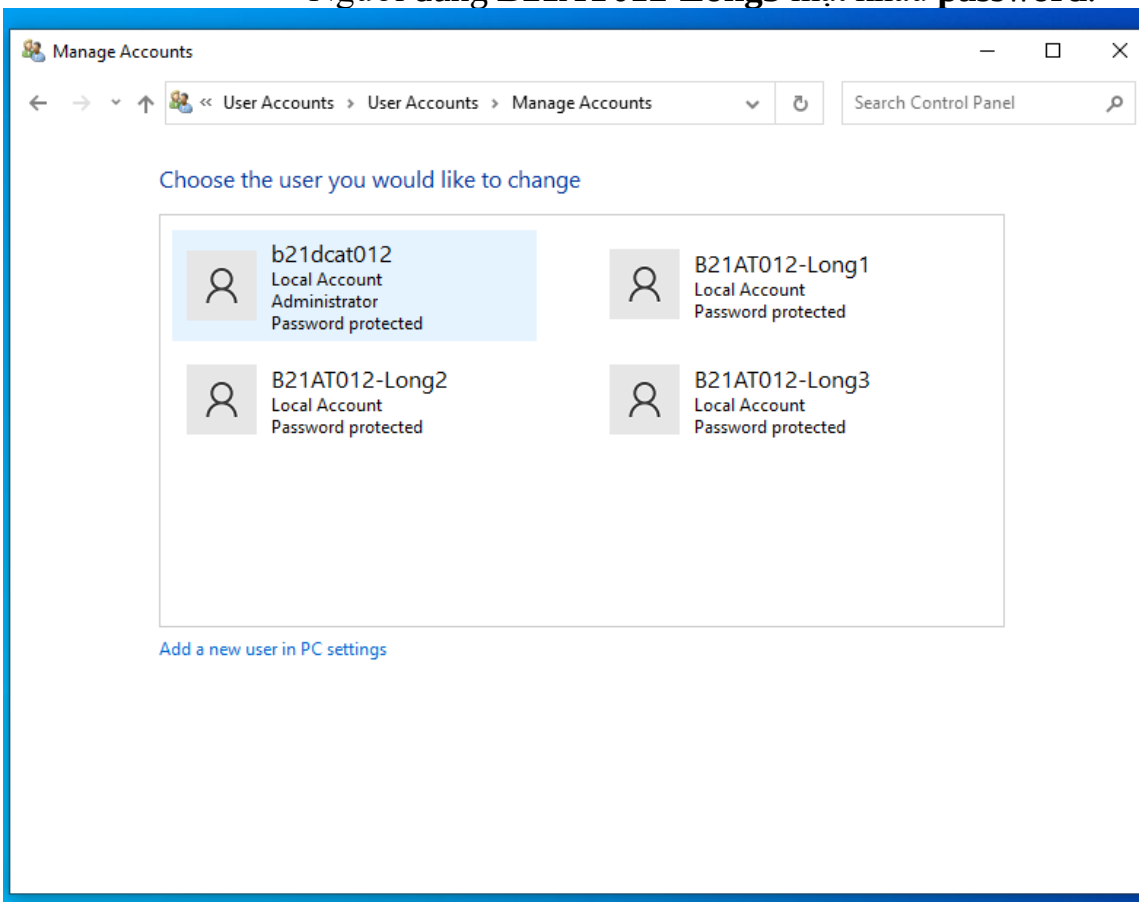



- Hình bên dưới là kết quả phá mật khẩu thành công. Mật khẩu và tên người dùng được in màu cam. Ngoài ra có thể dùng lệnh **john --show /home/kali/Downloads/hash** để in ra tên người dùng và mật khẩu.

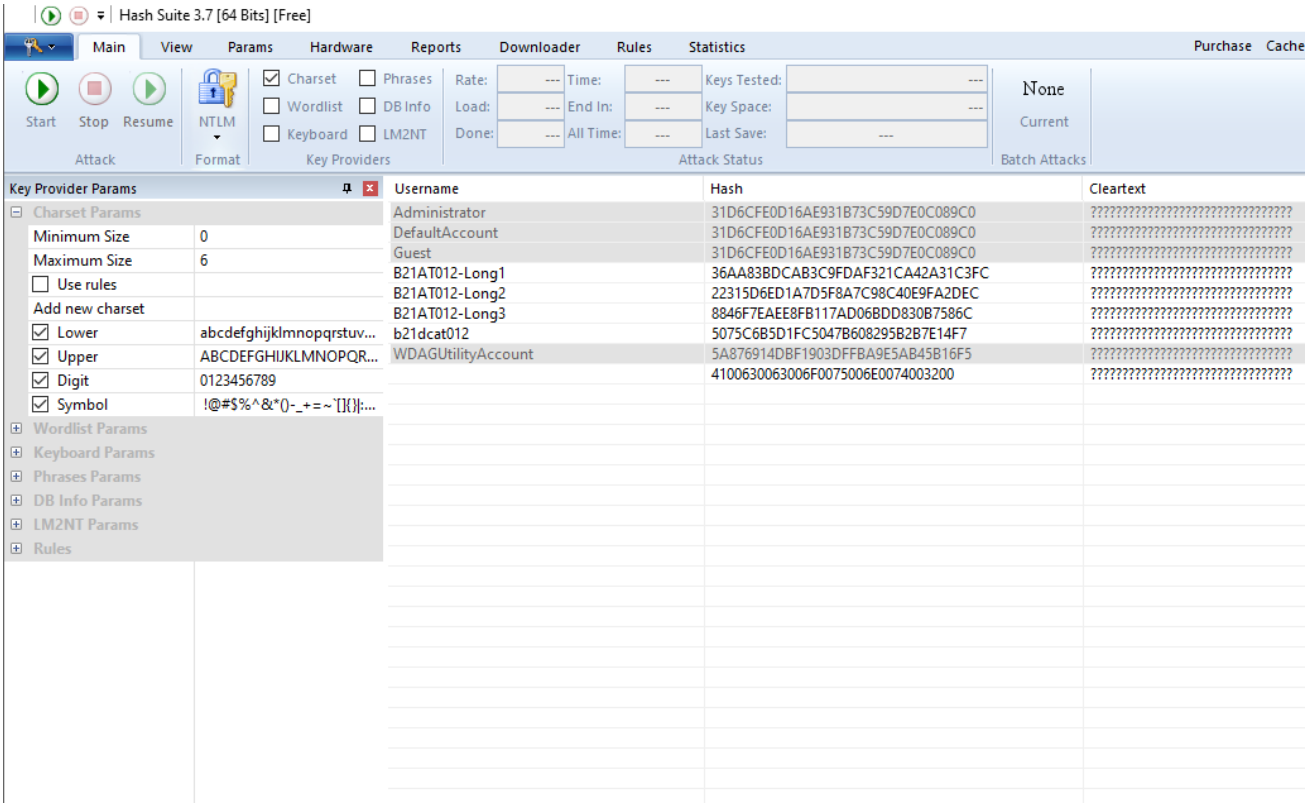



2. Trên Windows:
   - Sinh viên sử dụng phần mềm Hash Suite. Tải và giải nén Hash Suite từ https://hashsuite.openwall.net/download
   - Trên Windows, sinh viên tạo các tài khoản như sau:
     - Người dùng **B21AT012-Long1** mật khẩu **pass**.
     - Người dùng **B21AT012-Long2** mật khẩu **passwd**.

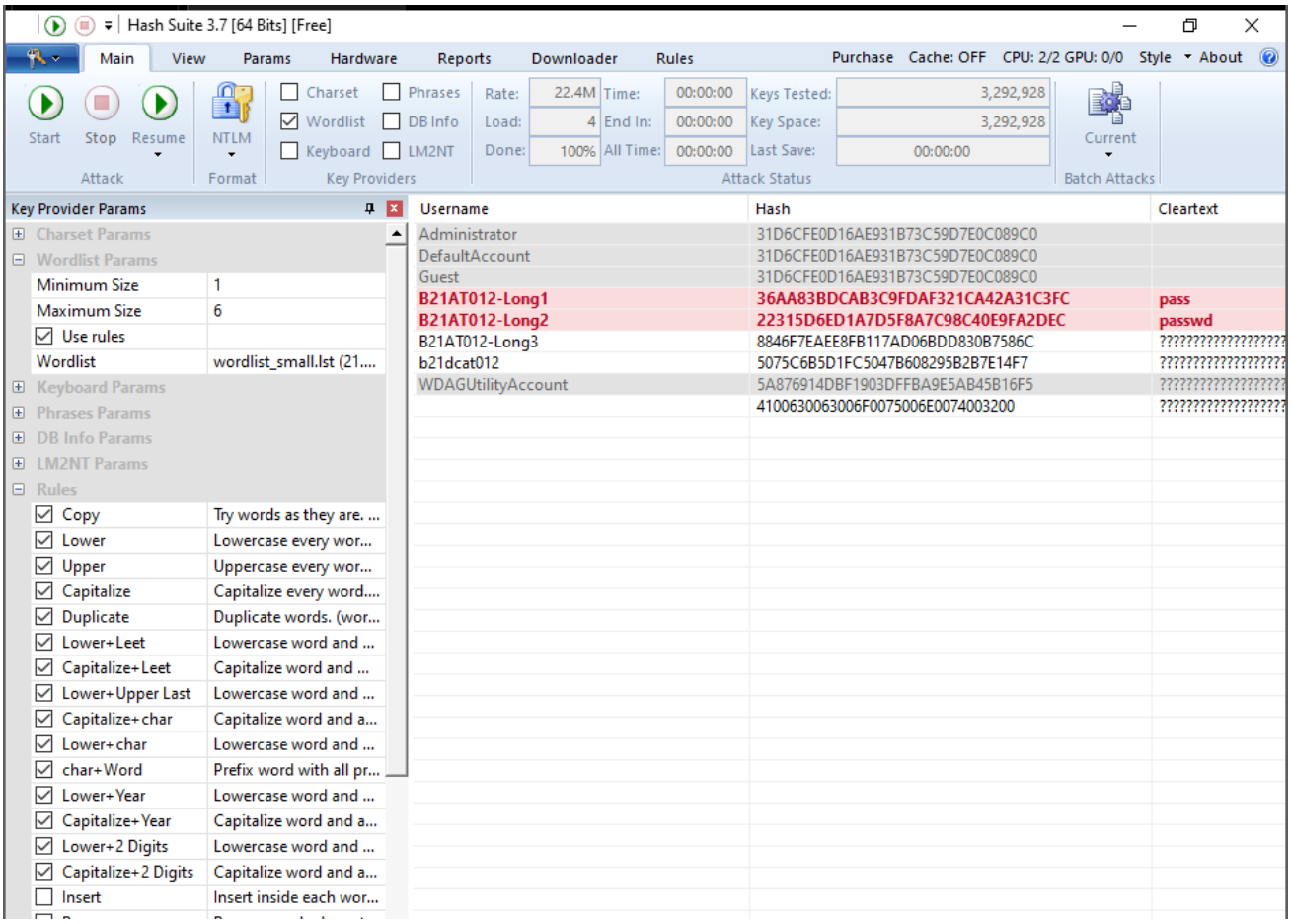
- Người dùng **B21AT012-Long3** mật khẩu **password**.




– Trên giao diện chính của Hash Suite, bấm vào nút màu xanh nước biển ở góc trên bên trái màn hình, chọn Import để nạp dữ liệu người dùng và mật khẩu đã mã hoá từ hệ điều hành.
– Ở tab Main, mục Format chọn NTLM thay vì LM.
– Kết quả hiển thị như hình dưới.




- Tại đây, người dùng có thể chọn các phương pháp bẻ khoá mật khẩu khác nhau như charset, wordlist, keyboard, phrases, v.v
- Để việc bẻ khoá mật khẩu diễn ra nhanh, sinh viên chọn wordlist vì pass, passwd, password đều là các từ thông dụng. Tất nhiên trong trường hợp thực tế thì kẻ tấn công không biết mật khẩu nên không thể biết phương pháp bẻ khoá nào là tối ưu nhất. Tuy nhiên vì đây là môi trường thử nghiệm, trên máy ảo có tài nguyên ít nên mong giảng viên thông cảm.




– Kết quả, Hash Suite bẻ khoá được mật khẩu của 2 tài khoản như hình trên. Phần mềm này là phiên bản miễn phí nên bị giới hạn bẻ khoá mật khẩu dưới 8 kí tự, nên sinh viên không thể bẻ khoá B21AT012-Long3. Mong giảng viên thông cảm.

## III. Tài liệu tham khảo:


– Bài thực hành 1 bộ môn An toàn hệ điều hành, TS. Hoàng Xuân Dậu.