HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI THỰC HÀNH
THỰC TẬP CƠ SỞ
Bài 12: Crack mật khẩu

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Giảng viên: Nguyễn Hoa Cương

Hà Nội – 2023

MỤC LỤC

I. Tìm hiểu lý thuyết

1. Tìm hiểu về John the Ripper

- Được phát hành lần đầu vào năm 1996, John the Ripper (JtR) là một công cụ bẻ khóa mật khẩu ban đầu được sản xuất cho các hệ thống dựa trên UNIX. John the Ripper hỗ trợ một danh sách khổng lồ các loại mật mã và hàm băm. Nó 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.
- Đây là một trong những chương trình kiểm tra và phá mật khẩu được sử dụng thường xuyên nhất vì nó kết hợp một số trình bẻ khóa mật khẩu vào một gói, tự động phát hiện các loại băm mật khẩu và bao gồm một trình bẻ khóa có thể tùy chỉnh.
- Nó có thể chạy với các định dạng mật khẩu được mã hóa khác nhau bao gồm một số kiểu băm mật khẩu thông dụng nhất trên các phiên bản Unix khác nhau (dựa trên DES, MD5 hoặc Blowfish), Kerberos AFS và Windows NT / 2000 / XP / 2003 LM hash.
- Các mô-đun bổ sung đã mở rộng khả năng bao gồm mã băm mật khẩu dựa trên MD4 và mật khẩu được lưu trữ trong LDAP, MySQL và các mô-đun khác.
- Ví dụ về John the Ripper

```
quangnh@Quang-B20DCAT144:/$ john password --format=crypt
Loaded 3 password hashes with 3 different salts (crypt, generic cryp
t(3) [?/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:59 91% 1/3 0g/s 125.6p/s 125.6c/s 125.6C/s 999991972..n99
9991996
0g 0:00:01:00 92% 1/3 0g/s 125.6p/s 125.6c/s 125.6C/s quang1441982..
999992005
123456           (nguyenhuyquang)
12345678         (quang144)
1234             (nhq144)
3g 0:00:01:12 100% 2/3 0.04136g/s 122.5p/s 125.2c/s 125.2C/s 123456.
```

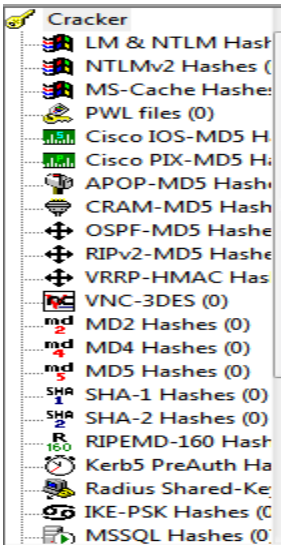
- Một trong những chế độ mà John có thể sử dụng là tấn công từ điển. Nó lấy các mẫu chuỗi văn bản (thường từ một tệp, được gọi là danh sách từ, chứa các từ được tìm thấy trong từ điển hoặc mật khẩu thực đã được bẻ khóa trước đó), mã hóa nó ở định dạng giống như mật khẩu đang được kiểm tra (bao gồm cả thuật toán mã hóa và khóa), và so sánh đầu ra với chuỗi được mã hóa.
- Nó cũng có thể thực hiện nhiều thay đổi đối với các từ trong từ điển và thử những từ này. Nhiều thay đổi này cũng được sử dụng trong chế độ tấn công đơn lẻ của John, chế độ này sửa đổi bản rõ được liên kết (chẳng hạn như tên người dùng với mật khẩu được mã hóa) và kiểm tra các biến thể so với các hàm băm.
- Brute-force Attack:
    + Trong mật mã, brute force attack bao gồm một kẻ tấn công gửi nhiều mật khẩu hoặc cụm từ mật khẩu với hy vọng cuối cùng đoán chính xác.

Kẻ tấn công kiểm tra một cách có hệ thống tất cả các mật khẩu và cụm mật khẩu có thể có cho đến khi tìm thấy mật khẩu chính xác.

+ Ngoài ra, kẻ tấn công có thể cố gắng đoán khóa thường được tạo từ mật khẩu bằng cách sử dụng chức năng dẫn xuất khóa. Đây được gọi là một tìm kiếm khóa toàn diện.

2. Tìm hiểu về phần mềm Cain

- Cain and Abel là bộ công cụ giúp việc dò tìm, phát hiện và giải mã các mật khẩu trên hệ điều hành Microsoft Windows.
- Công cụ này được viết bởi Montoro, một lập trình viên nổi tiếng với hi vọng rằng nó sẽ là công cụ hỗ trợ đắc lực cho việc quản trị mạng giúp nhân viên điều tra có thể dễ dàng truy cập vào các hệ thống máy tính.
- Chương trình này không khai thác những lỗ hổng chưa được vá của bất kỳ phần mềm nào. Nó tập trung vào điểm yếu, khía cạnh hiện có trong các chuẩn giao thức, các phương pháp đăng nhập và các kỹ thuật đệm.
- Một số tính năng của Cain:
  + Dò tìm và phát hiện mật khẩu: Công cụ này cho phép người dùng có thể dò tìm mật khẩu của người sử dụng trên máy tính hoặc internet bằng các phương pháp như Dictionary, Brute-Force và Cryptanalysis.
  + Giải mã và khôi phục mật khẩu.
  + Ghi lại cuộc đàm thoại VoIP: hỗ trợ việc ghi âm lại cuộc đàm thoại thông qua VoIP và lưu dưới dạng mp3.
  + Hỗ trợ giả mạo ARP: với tính năng làm cho người sử dụng công cụ có thể liên kết với một máy tính trong mạng nội bộ mà rất khó bị phát hiên hay theo dõi.
  + Hỗ trợ việc hack mật khẩu wifi.
  + Chạy trên nhiều hệ điều hành như Windows 7,8,XP.
- Password Cracker: Thao tác với hầu hết hàm băm thông thường và một vài phương thức mã hóa cơ sở: MD2, MD4, MD5, SHA1, SHA2 (384bit – 512 bit)



- Brute-force password cracker: là phương pháp phá vỡ một thuật toán mã hóa bằng thử tất cả các trường hợp có thể. Tính khả thi của brute force attack phụ thuộc vào độ dài key của thuật toán mã hóa và thông tin tính toán trước đó của kẻ tấn công. Brute-force password cracker kiểm tra tất cả các kết hợp có thể của ký tự trước một ký tự xác định hoặc tùy chỉnh thiết lập lại các mật khẩu.

II. Nội dung thực hành

1. Chuẩn bị môi trường

- 1 máy Ubuntu
- 1 máy Windows 7
- Phần mềm VMWare WorkStation

2. Nội dung thực hành

2.1. Crack mật khẩu trên hệ điều hành Linux sử dụng John the Ripper

- Mở terminal, tạo 3 user với tên lần lượt là **quangnh, nguyenhuyquang, nhq144**

```
quangnh@Quang-B20DCAT144:~$ sudo su
root@Quang-B20DCAT144:/home/quangnh# useradd quangnh
useradd: user 'quangnh' already exists
root@Quang-B20DCAT144:/home/quangnh# useradd nguyenhuyquang
root@Quang-B20DCAT144:/home/quangnh# useradd nhq144
root@Quang-B20DCAT144:/home/quangnh#
```

- Xem tất cả tài khoản người dùng có trong hệ thống
  cat /etc/passwd | grep home

```
root@Quang-B20DCAT144:/home/quangnh# useradd nhq144
root@Quang-B20DCAT144:/home/quangnh# cat /etc/passwd | grep home
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-he
lper:/usr/sbin/nologin
quangnh:x:1000:1000:nguyenhuyquang,,,:/home/quangnh:/bin/bash
quangnh144:x:1001:1001::/home/quangnh144:/bin/sh
quang144:x:1002:1002:NguyenHuyQuang-B20DCAT144,,,:/home/quang144:/bin/bash
nguyenhuyquang:x:1003:1003::/home/nguyenhuyquang:/bin/sh
nhq144:x:1004:1004::/home/nhq144:/bin/sh
root@Quang-B20DCAT144:/home/quangnh#
```

- Đặt mật khẩu cho các tài khoản vừa tạo: quang144 (12345678), nguyenhuyquang (123456), nhq144 (1234)

```
root@Quang-B20DCAT144:/home/quangnh# passwd quangnh
New password:
Retype new password:
passwd: password updated successfully
root@Quang-B20DCAT144:/home/quangnh# passwd nguyenhuyquang
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
root@Quang-B20DCAT144:/home/quangnh# passwd nhq144
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
root@Quang-B20DCAT144:/home/quangnh#
```

- Lấy mã băm mật khẩu của các tài khoản vừa tạo và copy vào clipbroad
  tail –n 6 /etc/shadow

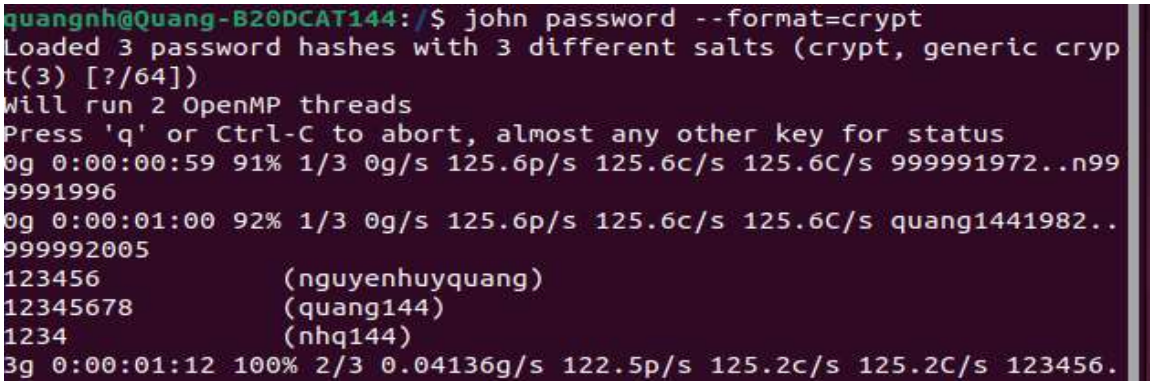
```
quangnh@Quang-B20DCAT144:/$
hplip:*:19213:0:99999:7:::
gdm:*:19213:0:99999:7:::
quangnh:$y$j9T$I32AE6Dn2UtbzxNk/Bo1s.$vl5sv2oEFzKLkmD54oIUY0Dql1qJ/k
Iu.aEzlUnkQ60:19426:0:99999:7:::
fwupd-refresh:*:19410:0:99999:7:::
sshd:*:19410:0:99999:7:::
quangnh144:$y$j9T$14UBFNNBmseDu6rAjk2BV.$QvZjTtEjUqkoGvMBl6Cxr92Z4ss
7Esf02P1Qs/V7/ZD:19427:0:99999:7:::
ftp:*:19424:0:99999:7:::
quang144:$y$j9T$MU1IDzhmdq1Amu71bW4uo0$c/zrLVS.fGTASMPfztuGN9ksJy/YZ
RCl465O3VeE7E5:19427:0:99999:7:::
nguyenhuyquang:$y$j9T$FLKM8mdToKacklGsUuJOw1$zaTo5X6n43Bt1mcnxIllX/I
AautPlGaskgd6dIREUR3:19427:0:99999:7:::
nhq144:$y$j9T$z2dakrc0wliGQRuS9bx9q1$qlESUPU6f7rJgFalh3OPNONCaKpM4Vp
9uEUMx7dNYr2:19427:0:99999:7:::
```

- Copy những mã băm trên vào file password

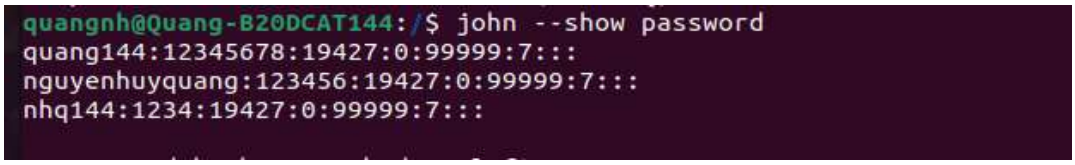
  nano password

- Sử dụng John the Ripper để tiến hành crack mật khẩu

  john password --format=crypt

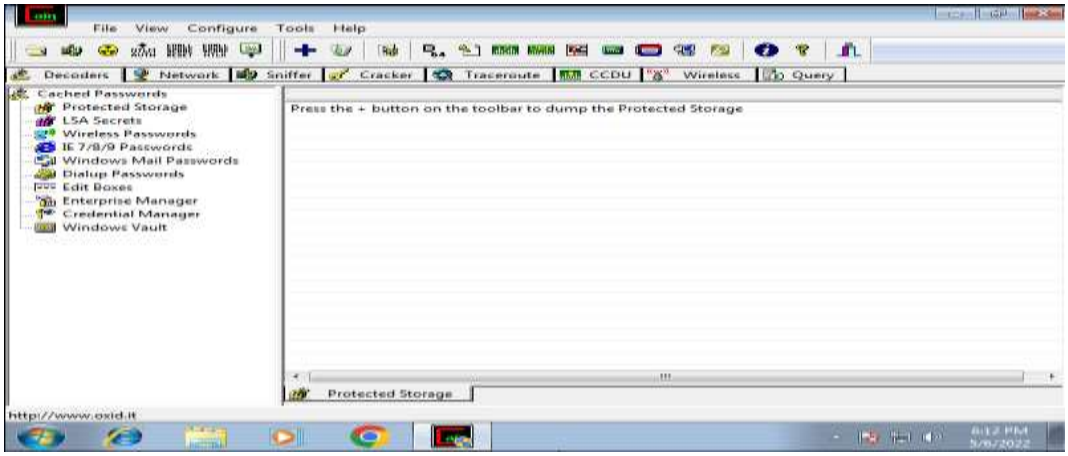


  john --show password

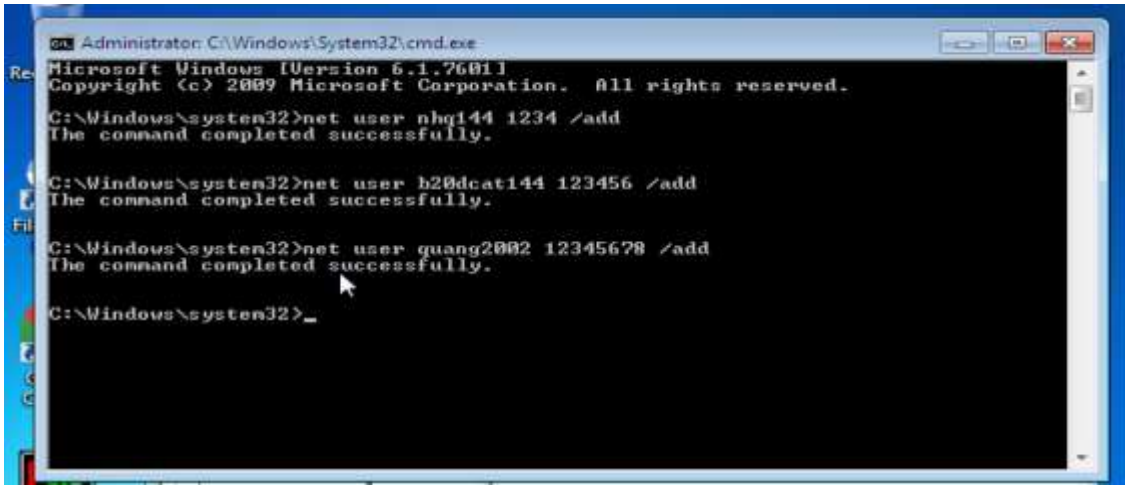


2.2. Crack mật khẩu trên hệ điều hành Windows sử dụng Cain

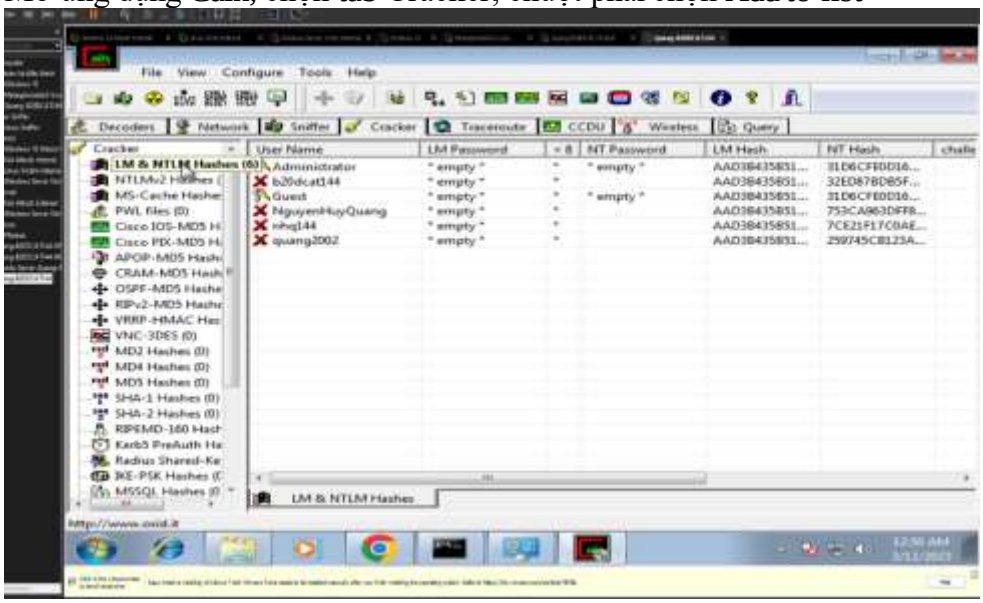
- Download Cain từ trang www.oxid.it, giao diện của Cain sau khi được cài đặt thành công



- Mở cmd, tiến hàng tạo 3 user và password lần lượt như sau: nhq144 (1234), b20dcat144 (123456), quang2002 (12345678)

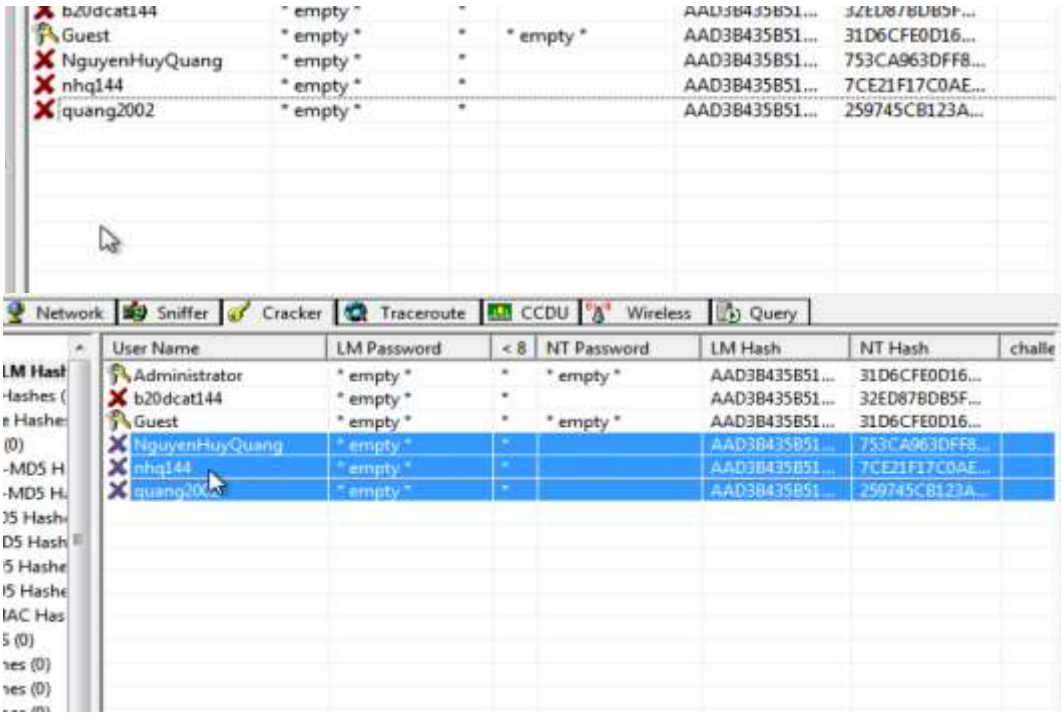


Mở ứng dụng Cain, chọn tab Cracker, chuột phải chọn Add to list

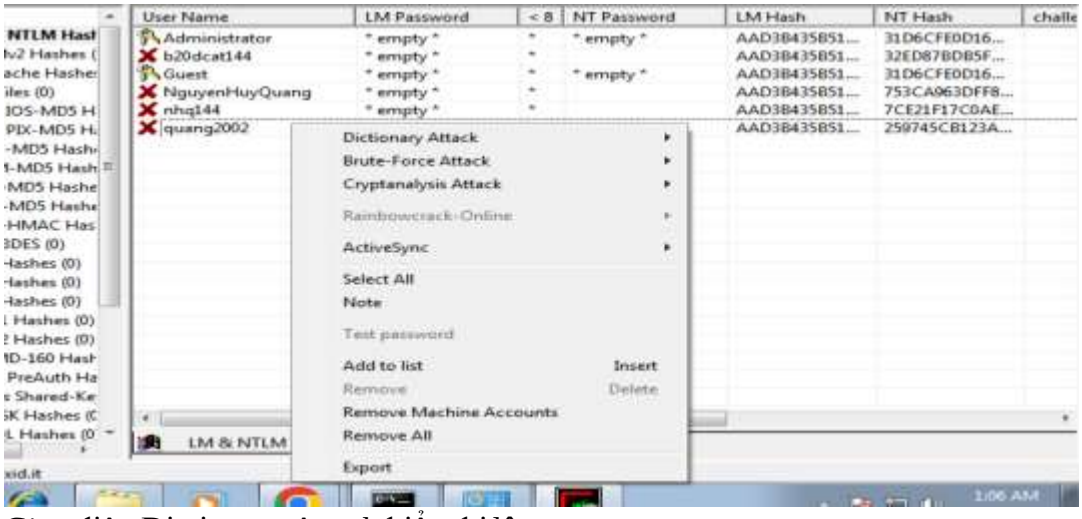


- Chọn Import Hashes from local system

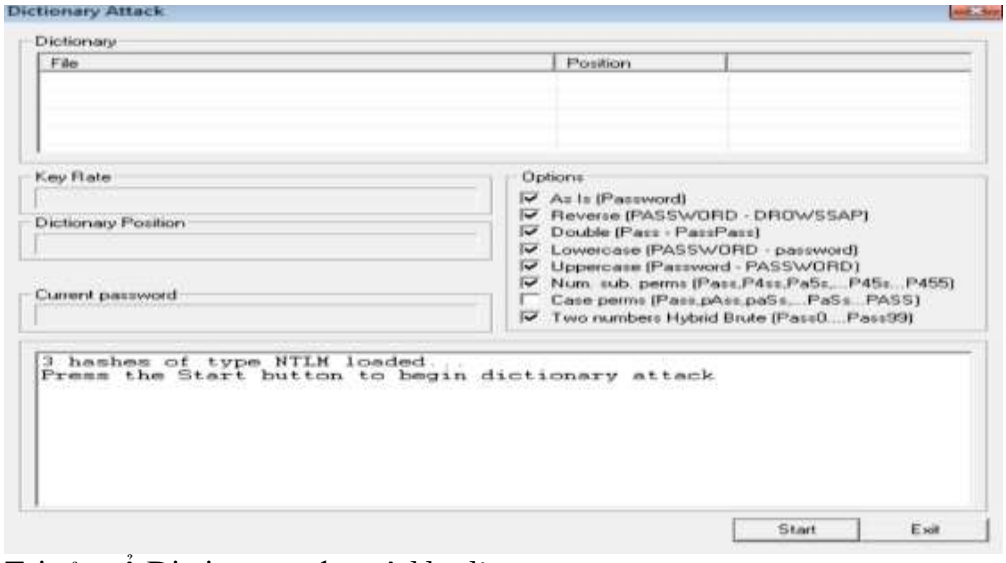
- Sau khi hiển thị ra các user trên hệ thống, click chọn 3 user vừa tạo để tiến hành crack mật khẩu



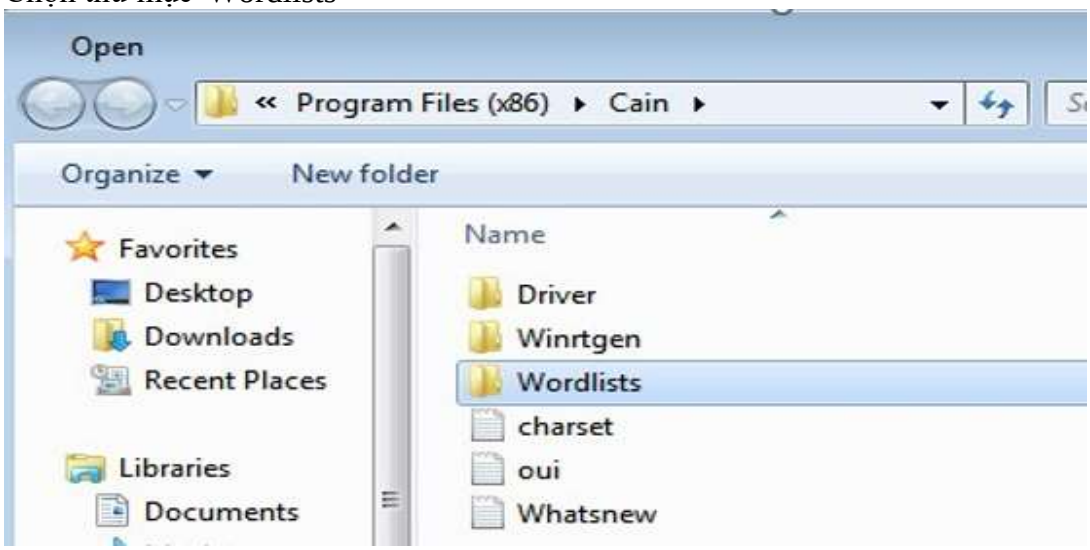
- Chuột phải chọn Dictionary Attack -> Chọn NTLM Hashes



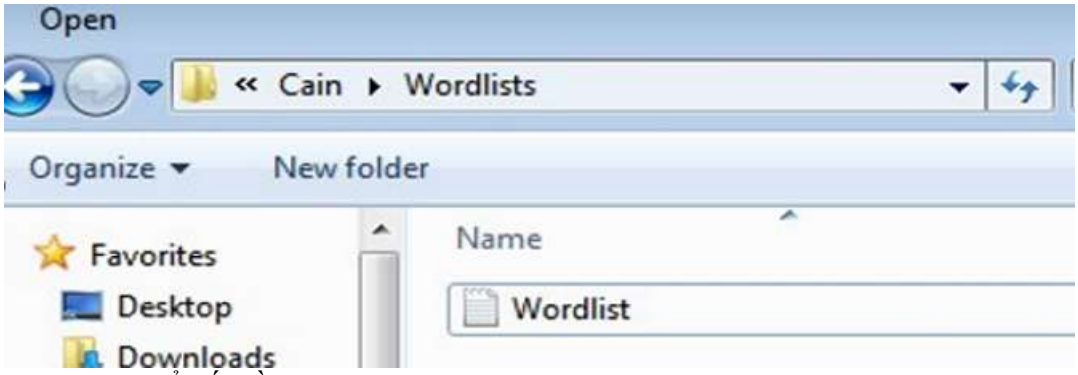
- Giao diện Dictionary Attack hiển thị lên



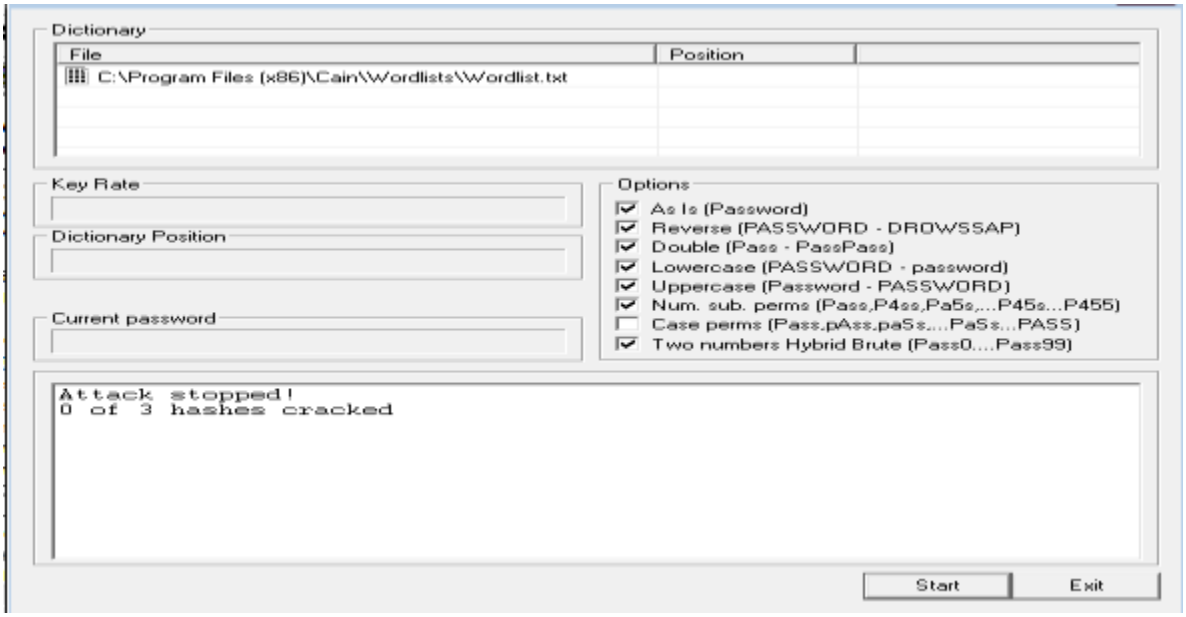
- Tại cửa sổ Dictionary, chọn Add to list
- Chọn thư mục Wordlists



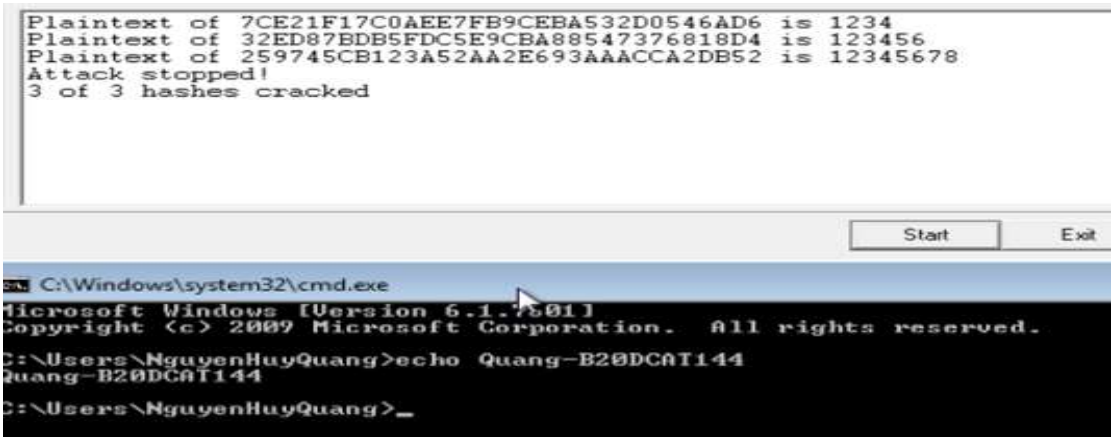
- Chọn file Wordlist



- Chọn start để bắt đầu crack



- Các mật khẩu đã được crack



III. Tài liệu tham khảo

1. Lab 13: Mitigation and Deterrent Techniques - Password Cracking (laspositascollege.edu)
2. John the Ripper - Wikipedia
3. Nguyen minhthanh cain & abel (slideshare.net)