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

**KHOA AN TOÀN THÔNG TIN**

****

**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 13**

**Kiểm thử thông qua tấn công mật khẩu**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 2/2023

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 ađược 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.

-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.

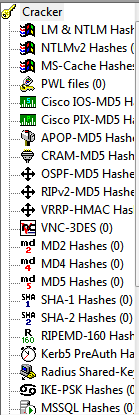
+Ghi lại cuộc đàm thoại VoIP: hỗ trợ việc ghi âm lại cuộc đàm thoại thông qua VoIP và lưu dưới dạng mp3.

+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:**

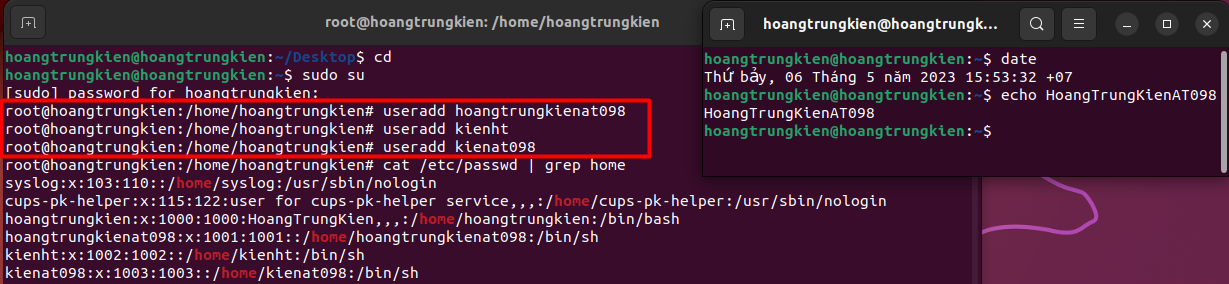
Một máy ubuntu

Một máy win7

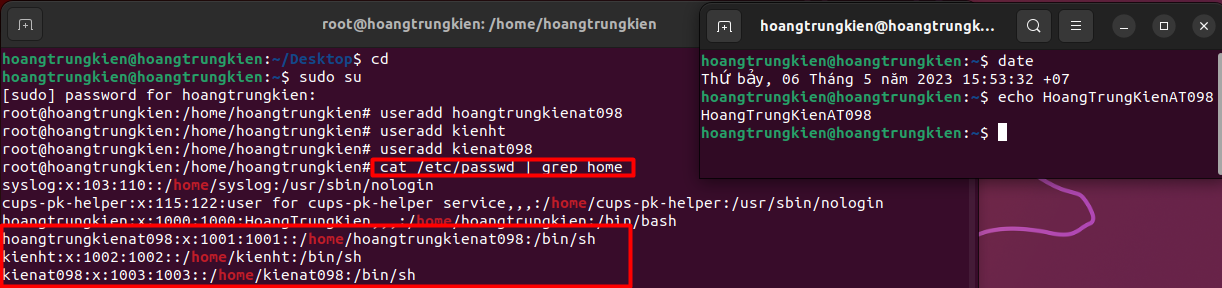
Phần mềm VMware

**2. Nội dung thực hành**

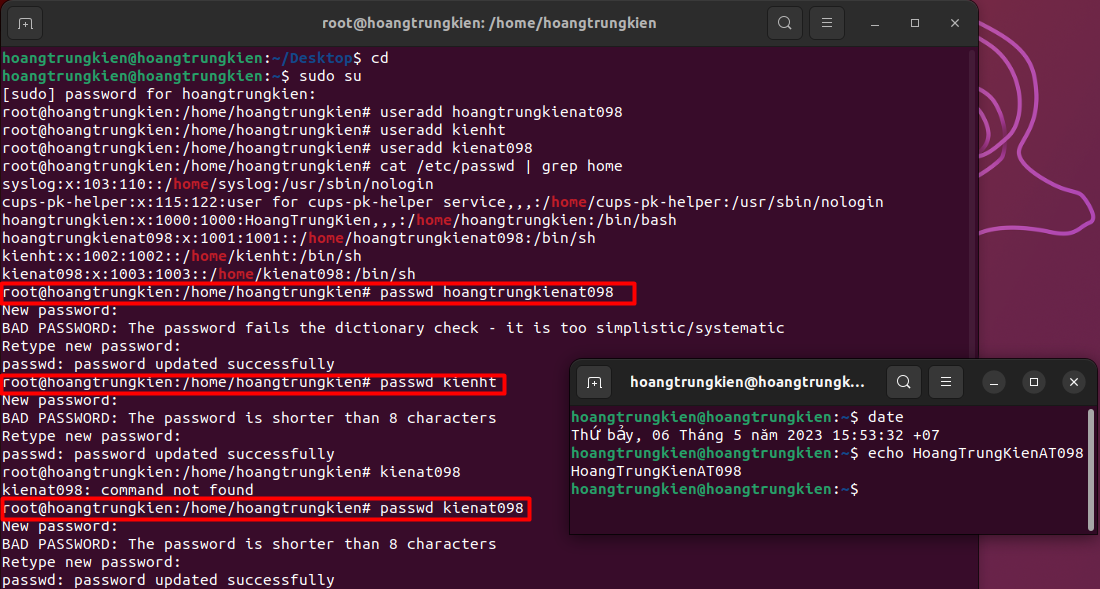
**2.1 Crack mật khẩu trên hệ điều hành Linux sử dụng John the Ripper**

Mở terminal, tạo 3 user với tên lần lượt là: hoangtrungkienat098, kienht, kienat098 

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

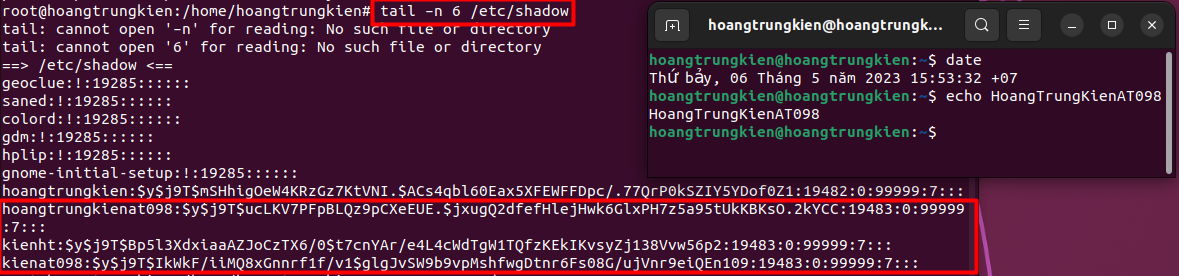


-Đặt mật khẩu cho các tài khoản vừa tạo: hoangtrungkienat098 (12345678), kienht (123456), kienat098 (1234)

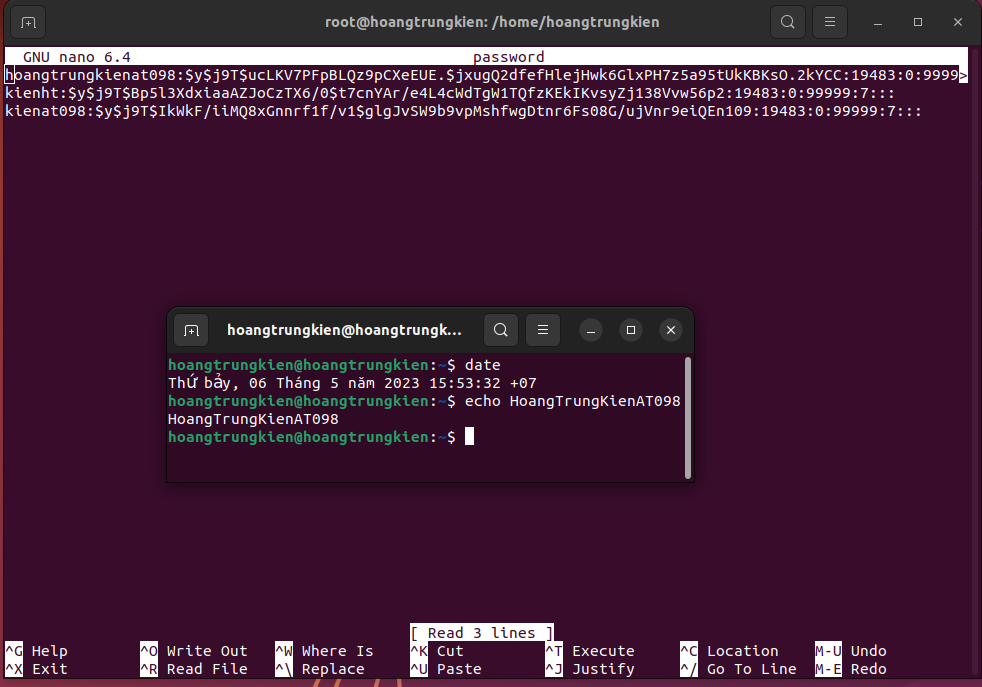


-Lấy mã băm mật khẩu của các tài khoản vừa tạo và copy vào clipbroad:

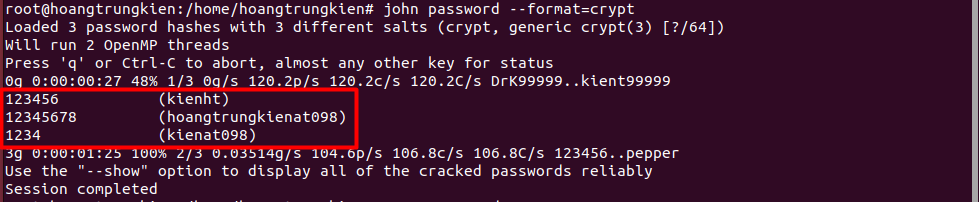
*tail –n 6 /etc/shadow*



Copy những mã băm trên vào file password: *nano password*

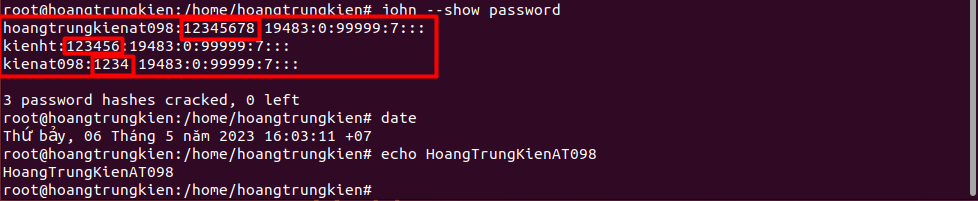


Sử dụng John the Ripper để tiến hành crack mật khẩu: *john password --format=crypt*



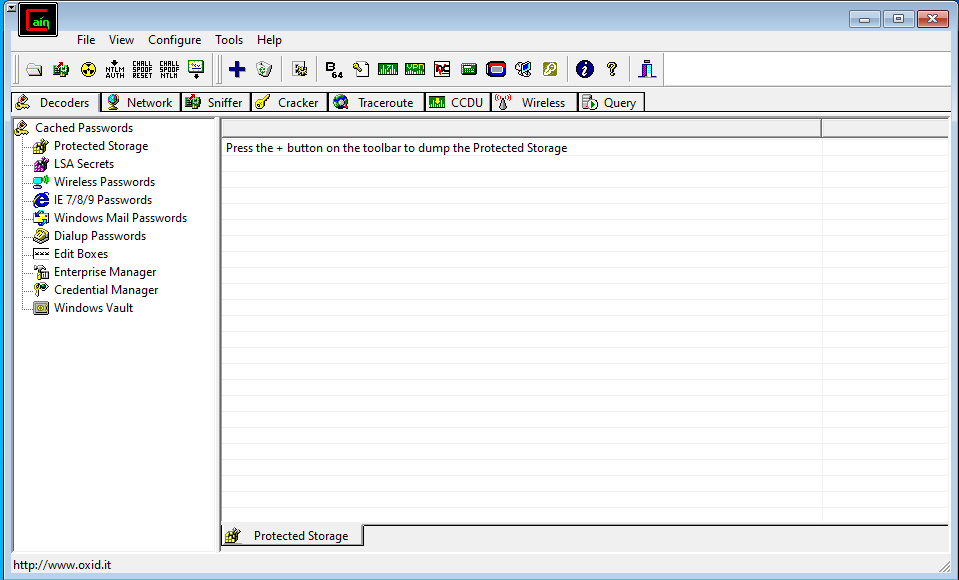
Đã crack thành công mật khẩu của 3 tài khoản

Gõ lệnh: *john --show password* để xem

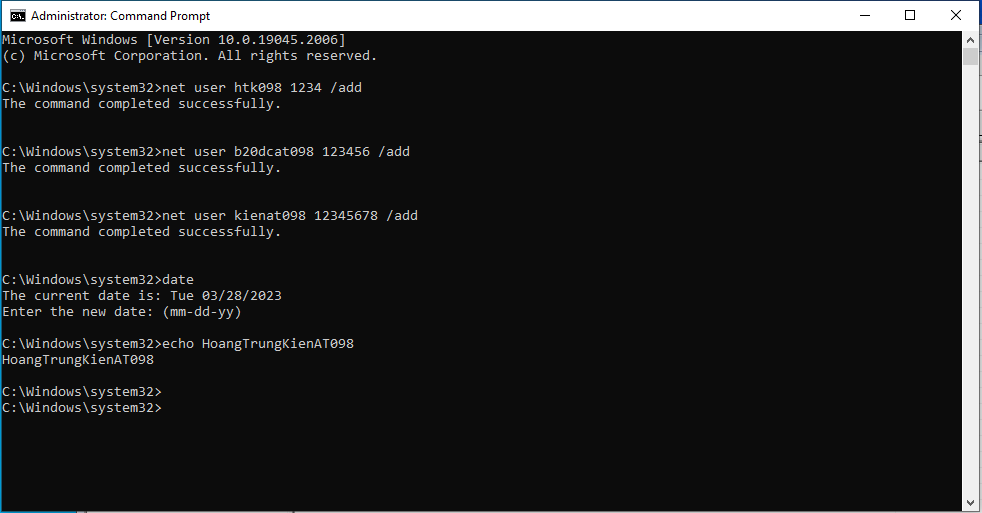


**2.2 Crack mật khẩu trên hệ điều hành Windows sử dụng Cain**

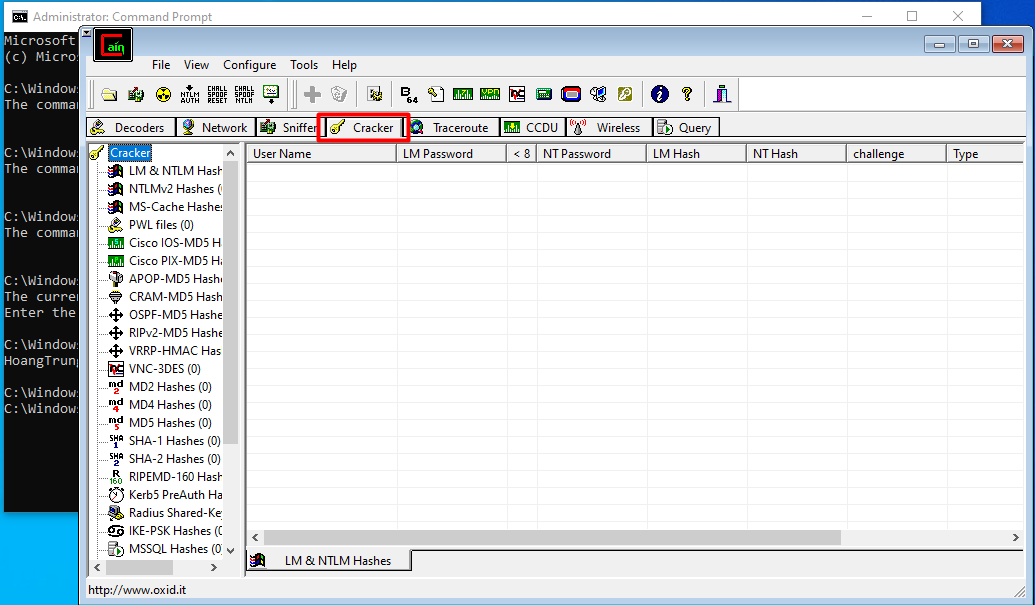
-Giao diện của Cain sau khi được cài đặt thành công

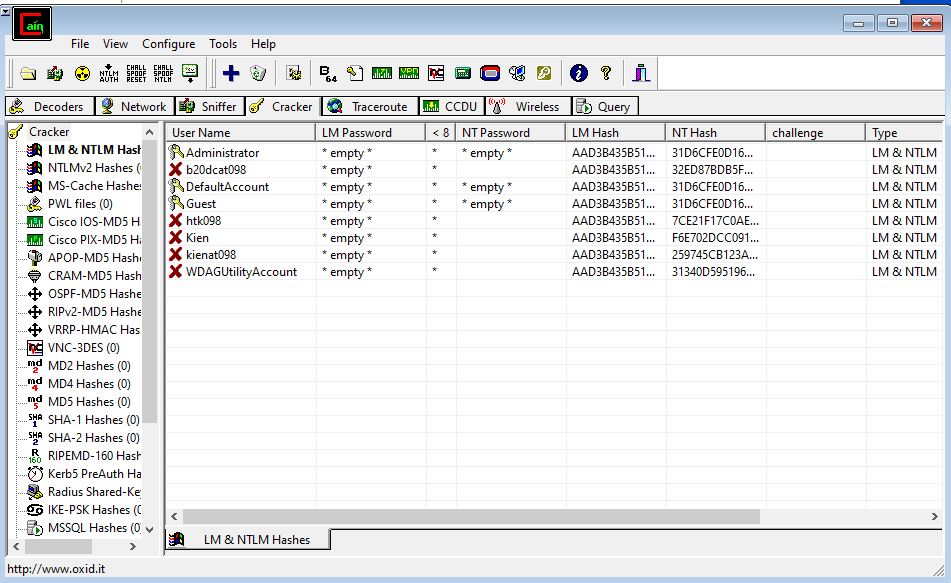


-Mở cmd, tiến hàng tạo 3 user và password lần lượt như sau: htk098 (1234), b20dcat098 (123456), kienat098(12345678)

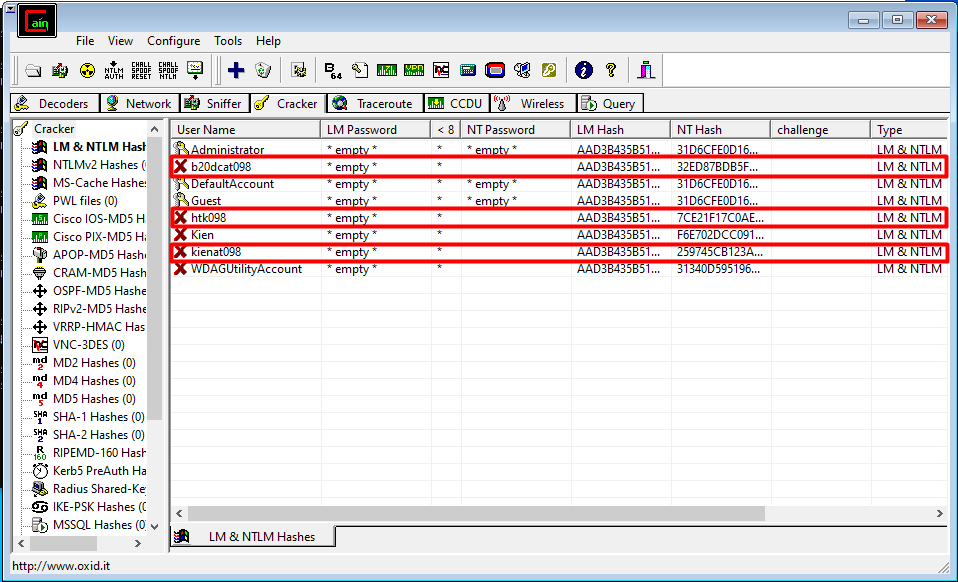


-Mở ứng dụng Cain, chọn tab Cracker, chuột phải chọn Add to list

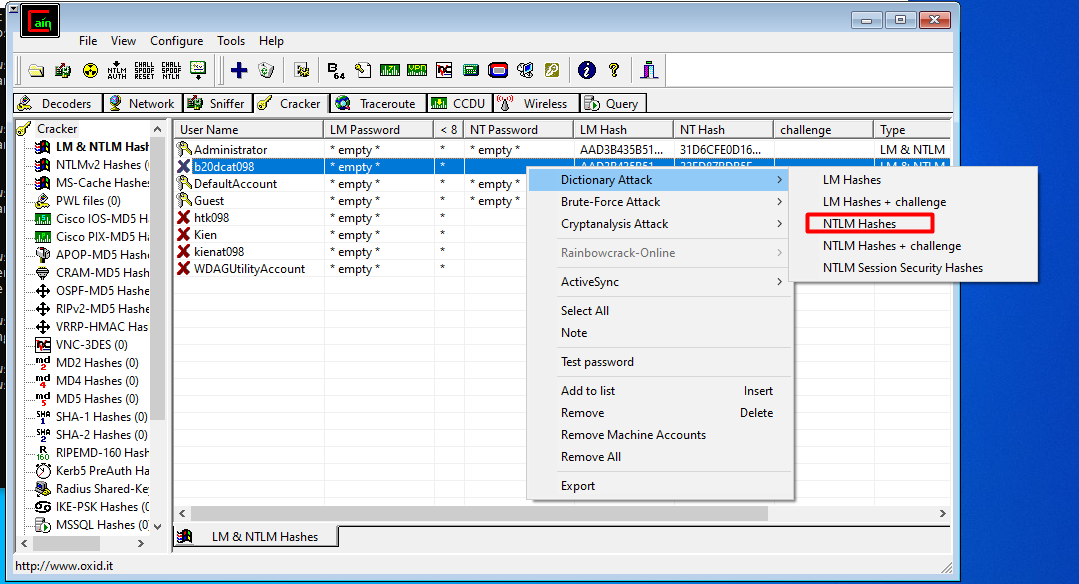


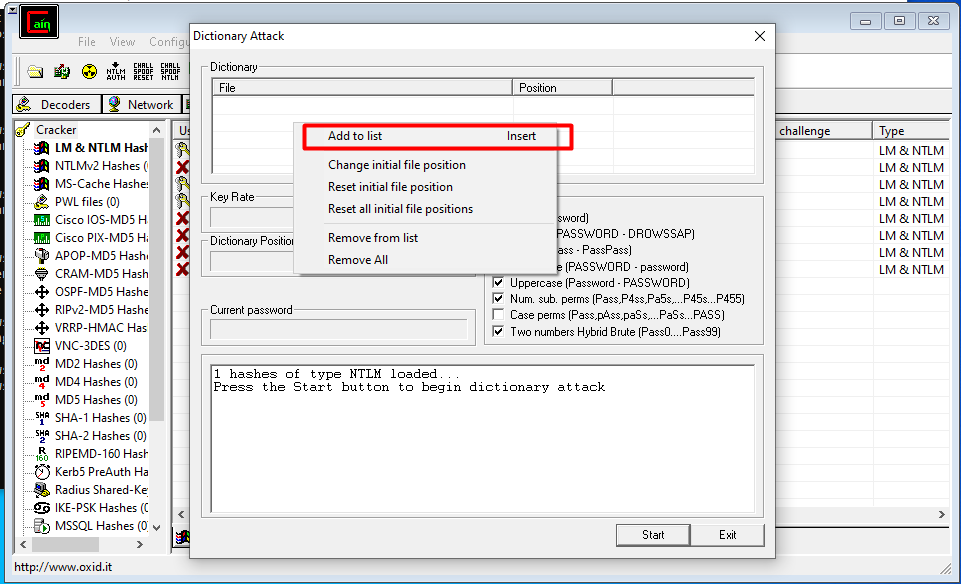


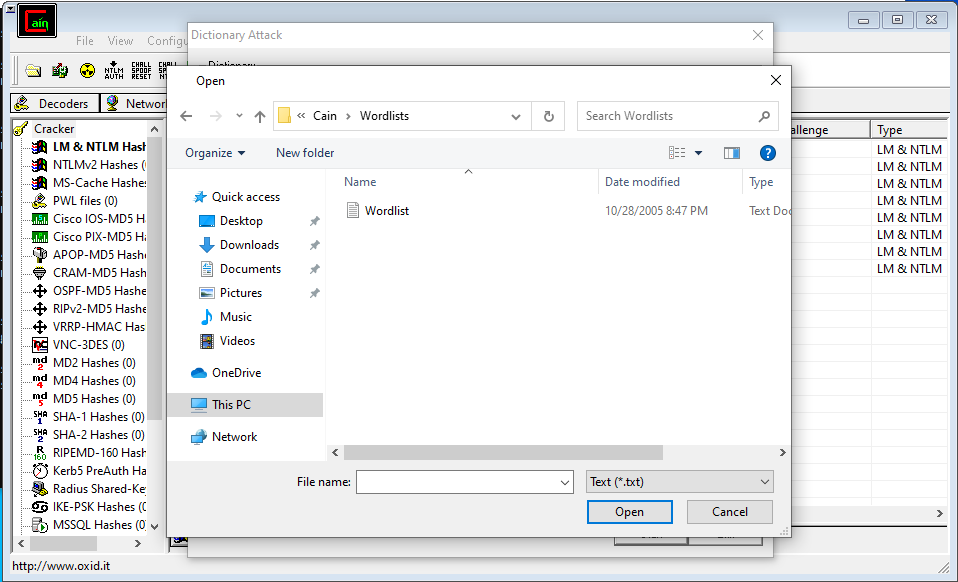
-Sau khi hiển thị ra các user trên hệ thống, click chọn 3 user vừa tạo để tiến hành crack mật khẩu



-Chuột phải chọn Dictionary Attack -> Chọn NTLM Hashes

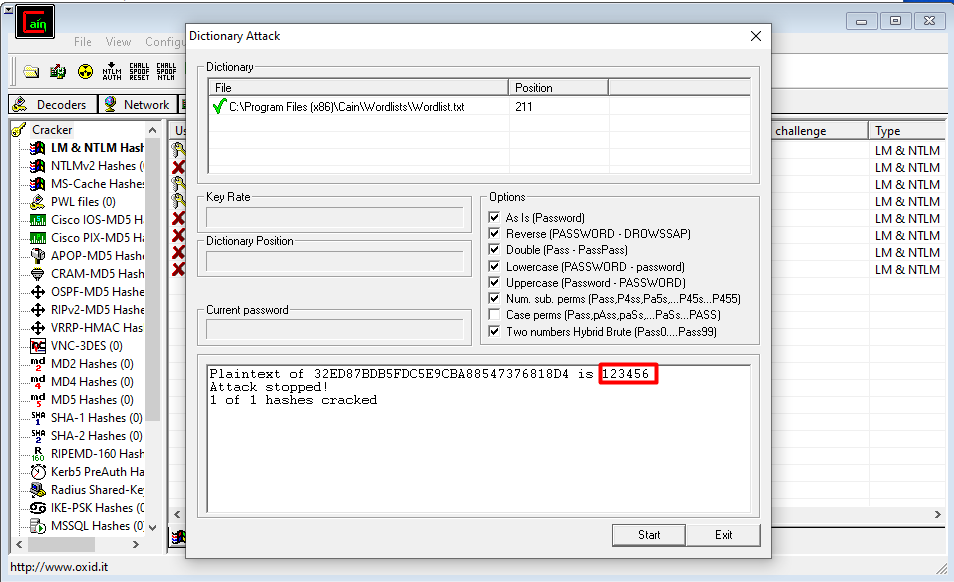




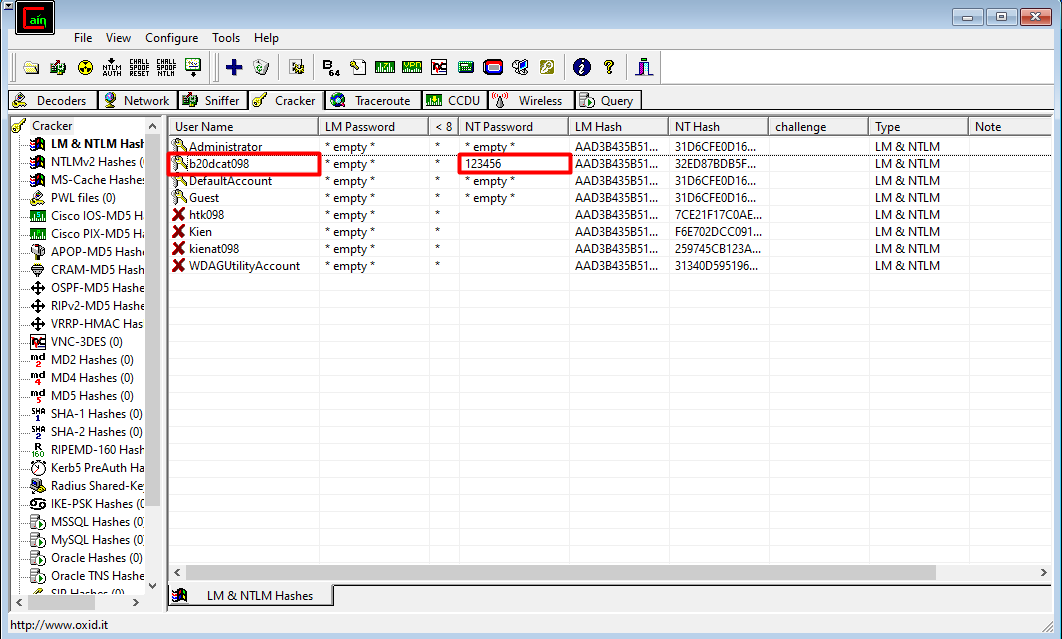


-Chọn start để bắt đầu crack

-Màn hình hiển thị mật khẩu đã crack

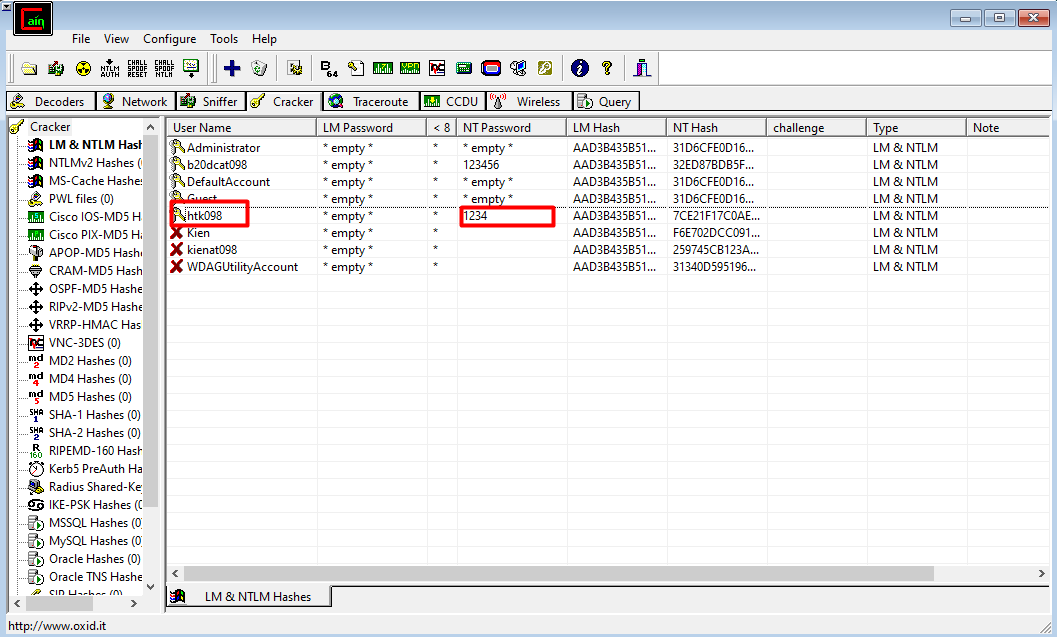


Mật khẩu của người dùng b20dcat098 là 123456

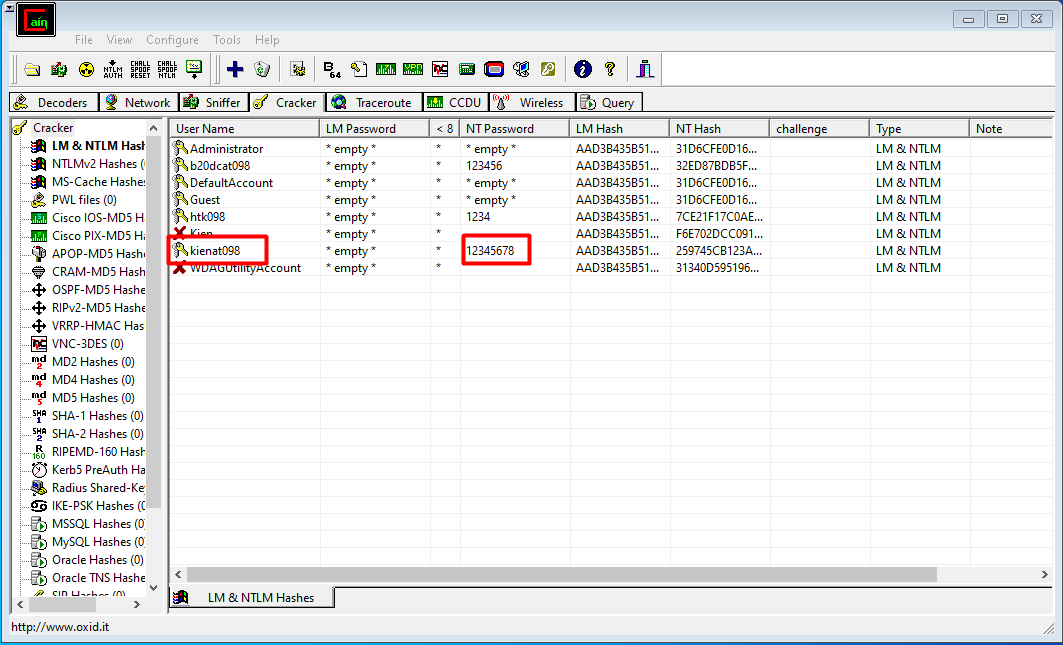


Ta làm tương tự với 2 người dùng htk098 và kienat098

Mật khẩu của người dùng htk098 là 1234



Mật khẩu của người dùng kienat098 là 12345678



Kiểm tra lại là tất cả mật khẩu đều đúng

