HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ

BÀI 12:
TẤN CÔNG MẬT KHẨU

Giảng viên : Nguyễn Ngọc Điệp
Sinh viên : Nguyễn Đức Anh
Mã sinh viên : B21DCAT031
Hệ : Đại học chính quy

Hà Nội, 3/2024

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.

2. *Nội dung thực hành*

2.1 Tìm hiểu lý thuyết

a. 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 lĩnh vực 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.

b. Tìm hiểu về Cain and Abel

- 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.
- 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.

2.2 Tài liệu tham khảo

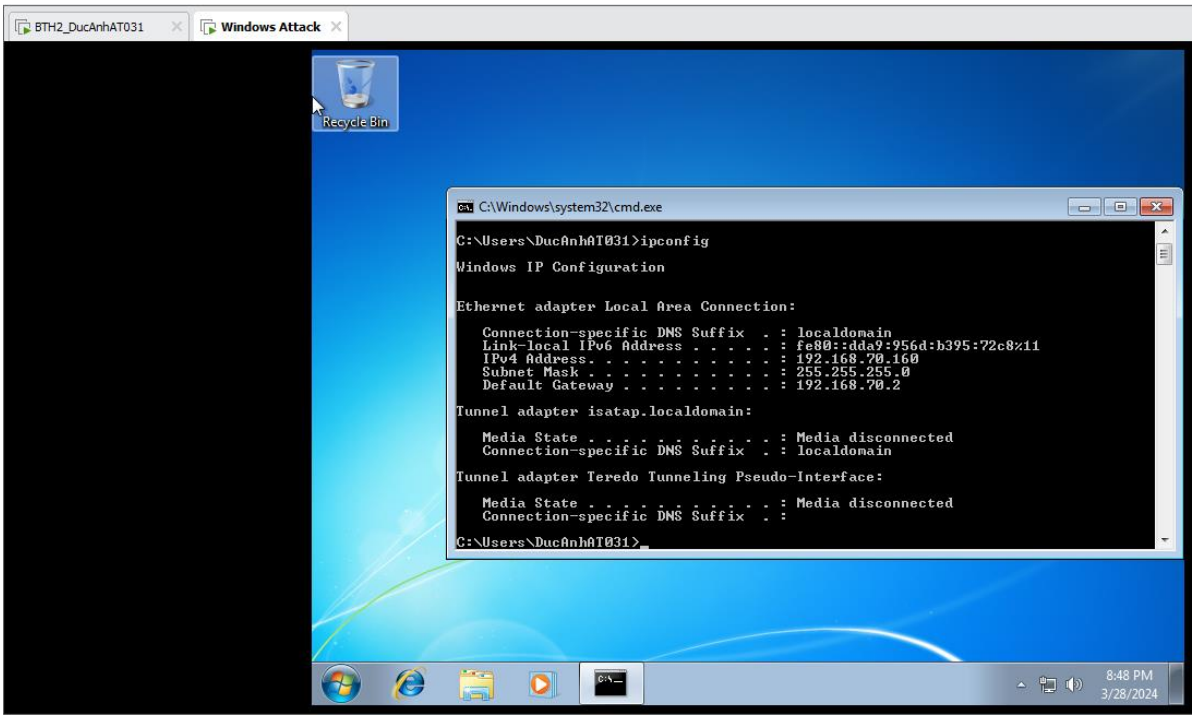
- Đỗ Xuân Chợ, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.

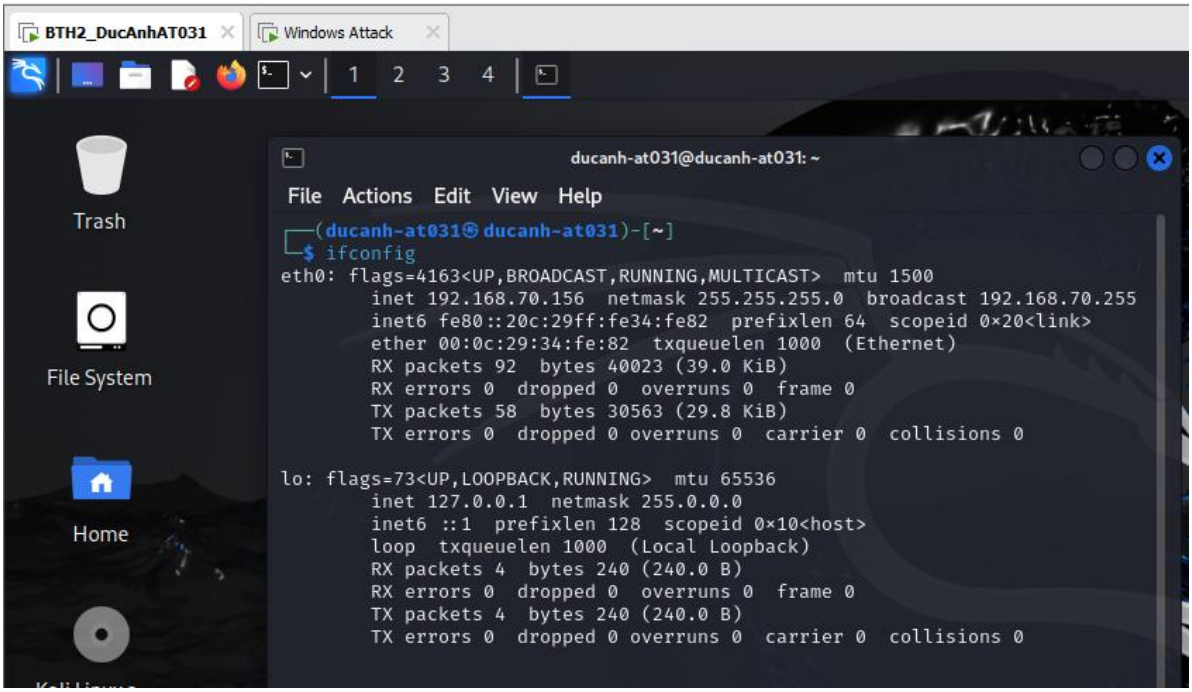
2.3 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.
- Máy ảo Kali Linux
- Máy ảo Windows 7

2.4 Các bước thực hiện

Bước 1: Chuẩn bị các máy ảo





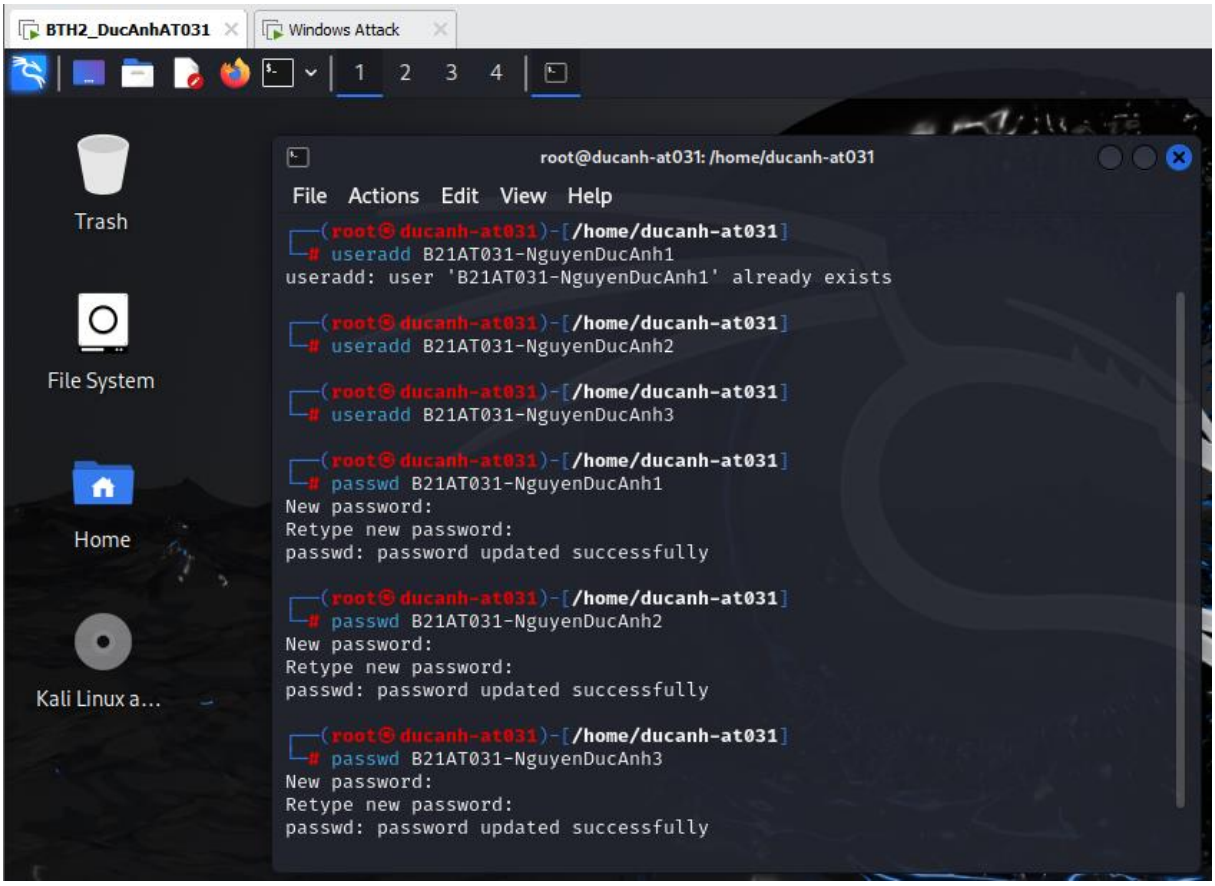
Bước 2: Crack mật khẩu trên máy Kali sử dụng John the Ripper

Ta tiến hành tạo 3 user như sau:

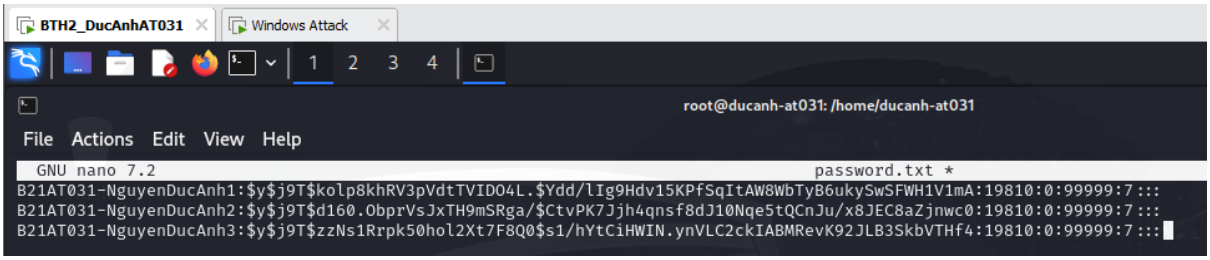
B21AT031-NguyenDucAnh1 – pass 1234

B21AT031-NguyenDucAnh2 – pass 123456

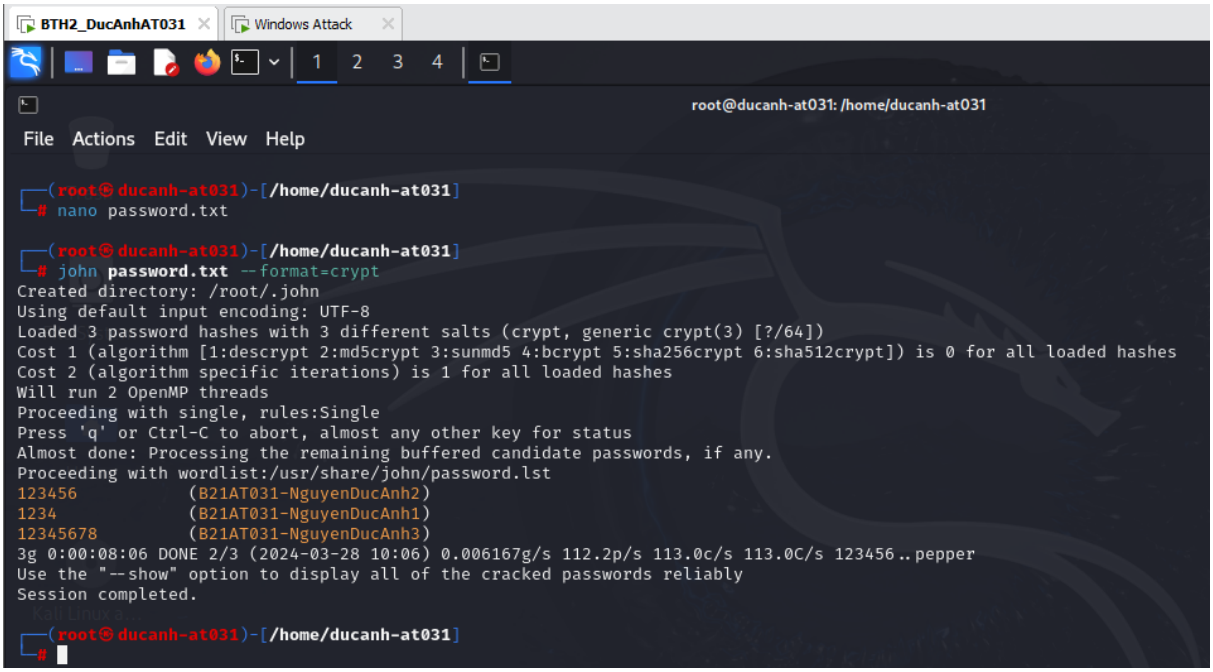
B21AT031-NguyenDucAnh3 – pass 12345678



Vào file etc/shadow sau đó copy chuỗi kí tự hash mật khẩu của 3 tài khoản vừa tạo, sau đó paste vào file password.txt



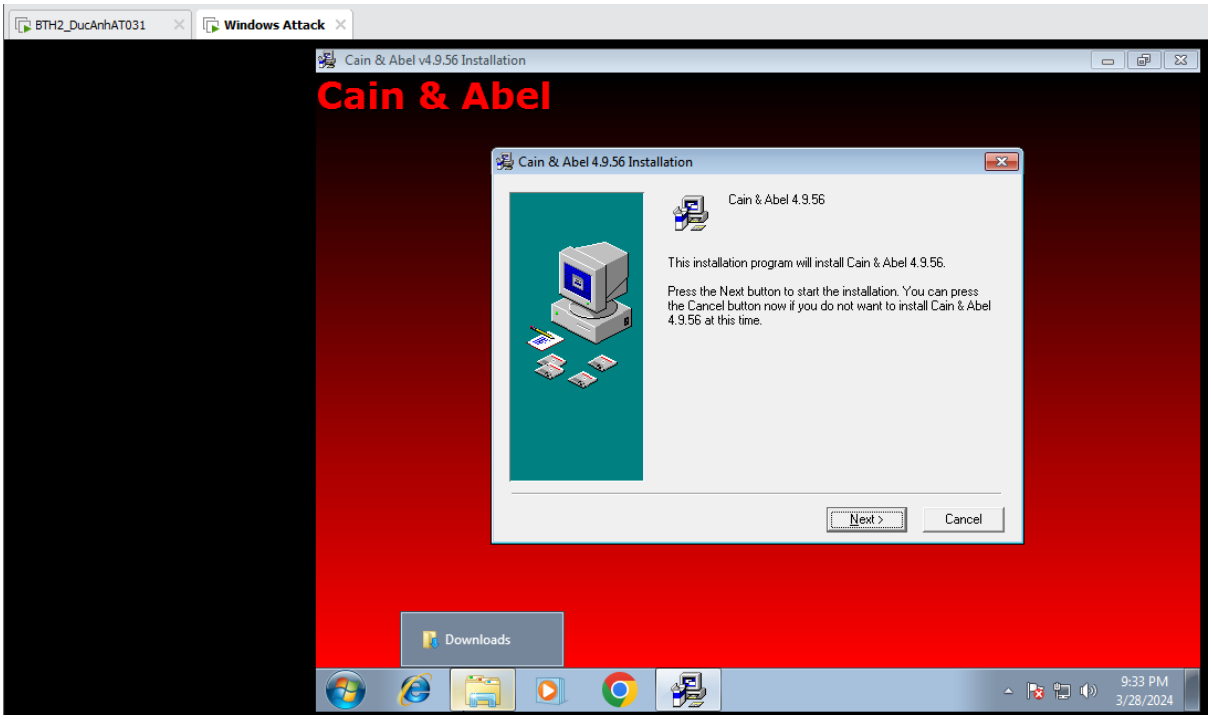
Chạy lệnh john password.txt --format=crypt để tiến hành crack mật khẩu

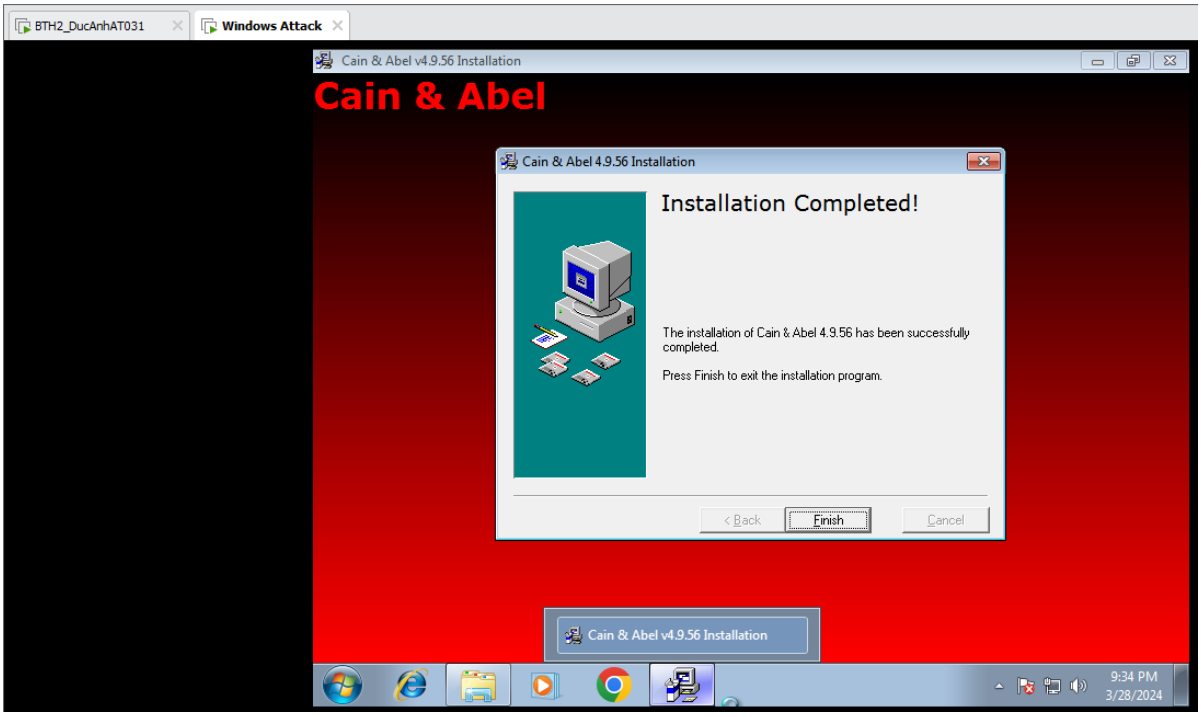


Đã crack thành công.

Bước 3: Sử dụng Cain and Abel để crack mật khẩu ở máy Windows 7

Đầu tiên ta cài đặt phần mềm Cain and Abel ở máy Windows 7



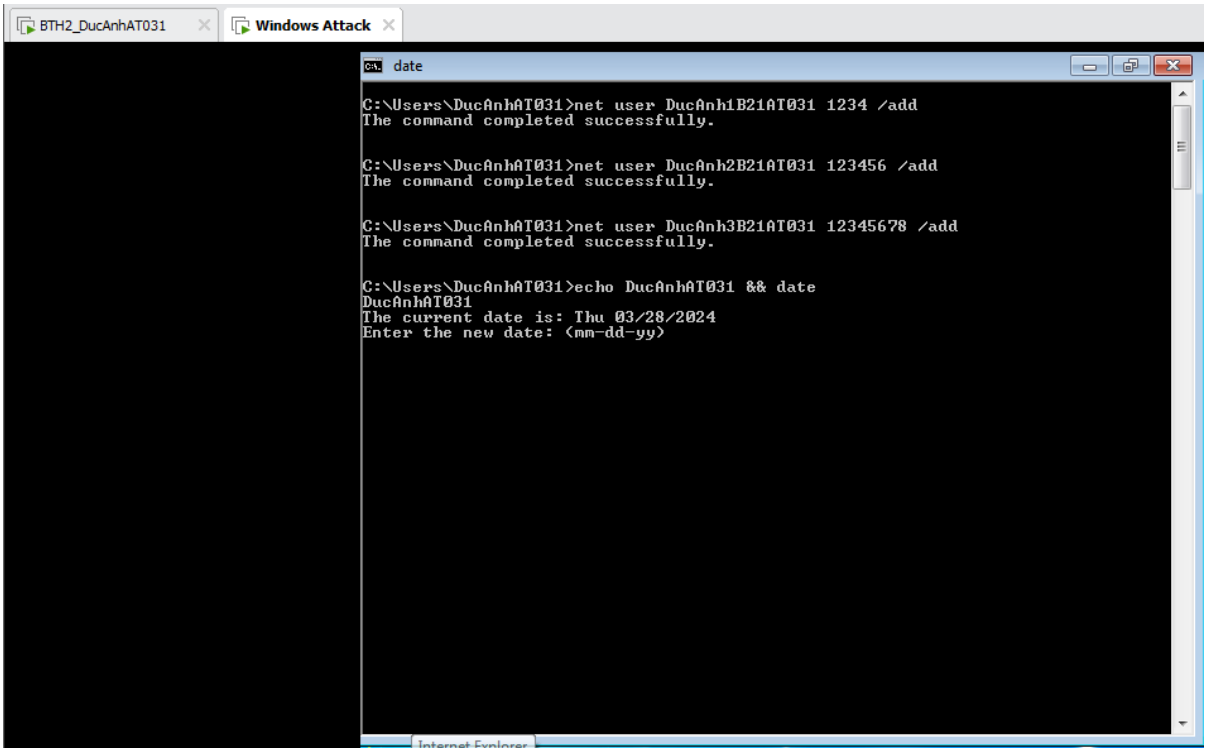


Tạo 3 tài khoản ở máy có tên và mật khẩu lần lượt là:

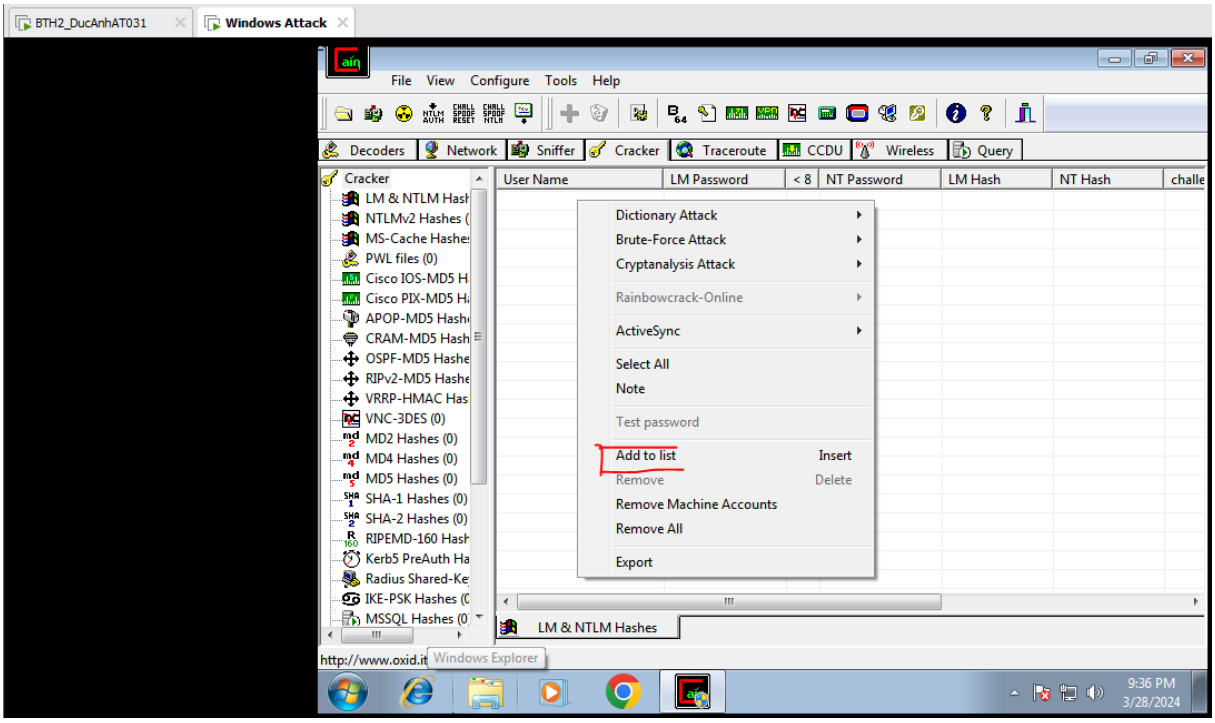
DucAnh1B21AT031 – 1234

DucAnh2B21AT031 – 123456

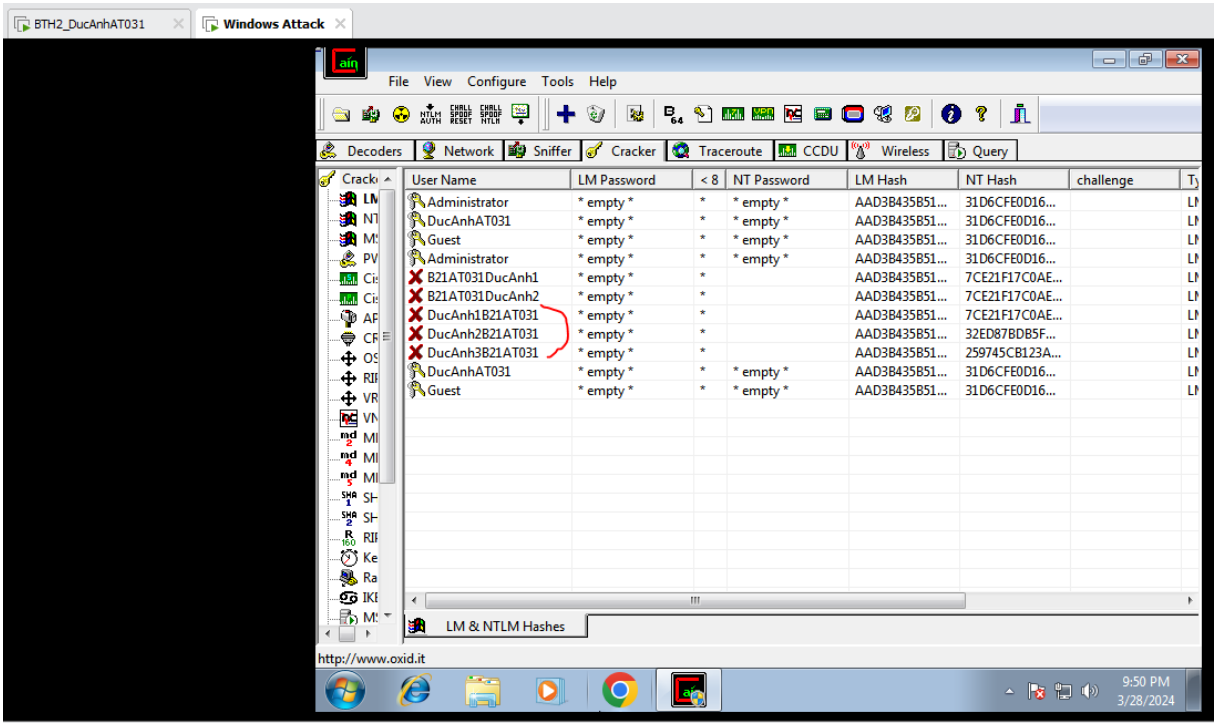
DucAnh3B21AT031 – 12345678



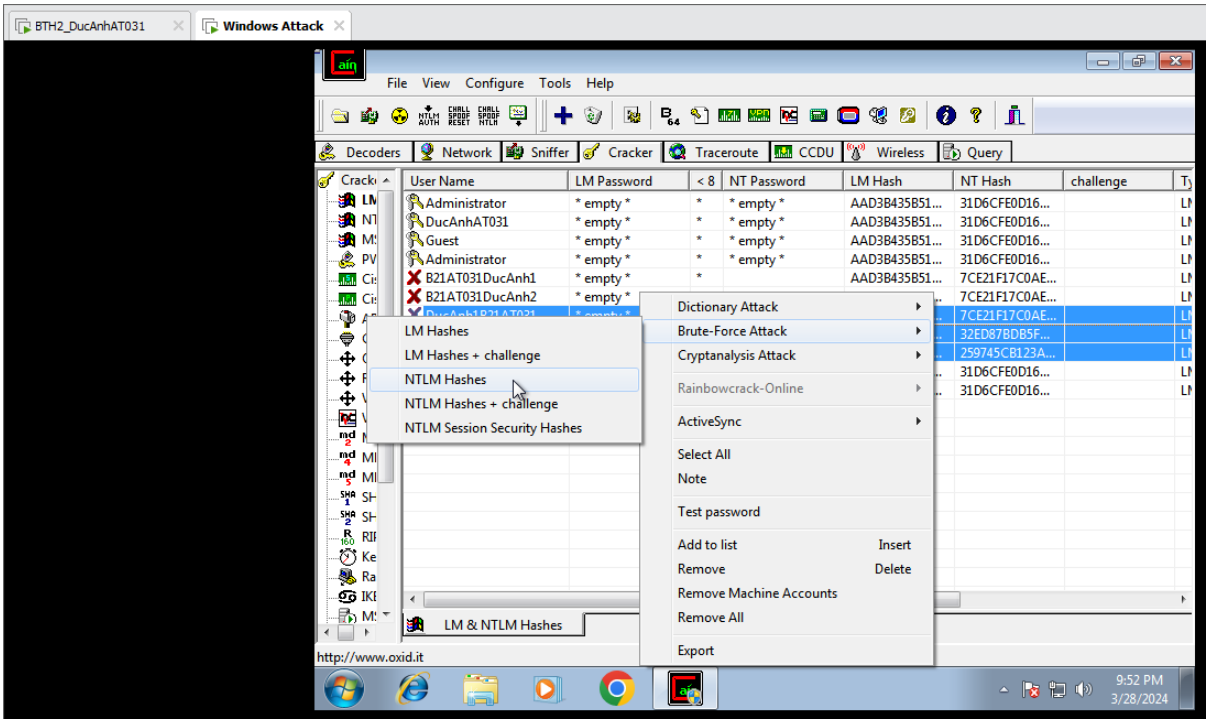
Mở phần mềm Cain, chọn thẻ Cracker, nhấn chuột phải rồi chọn Add to list.



Chọn Next.

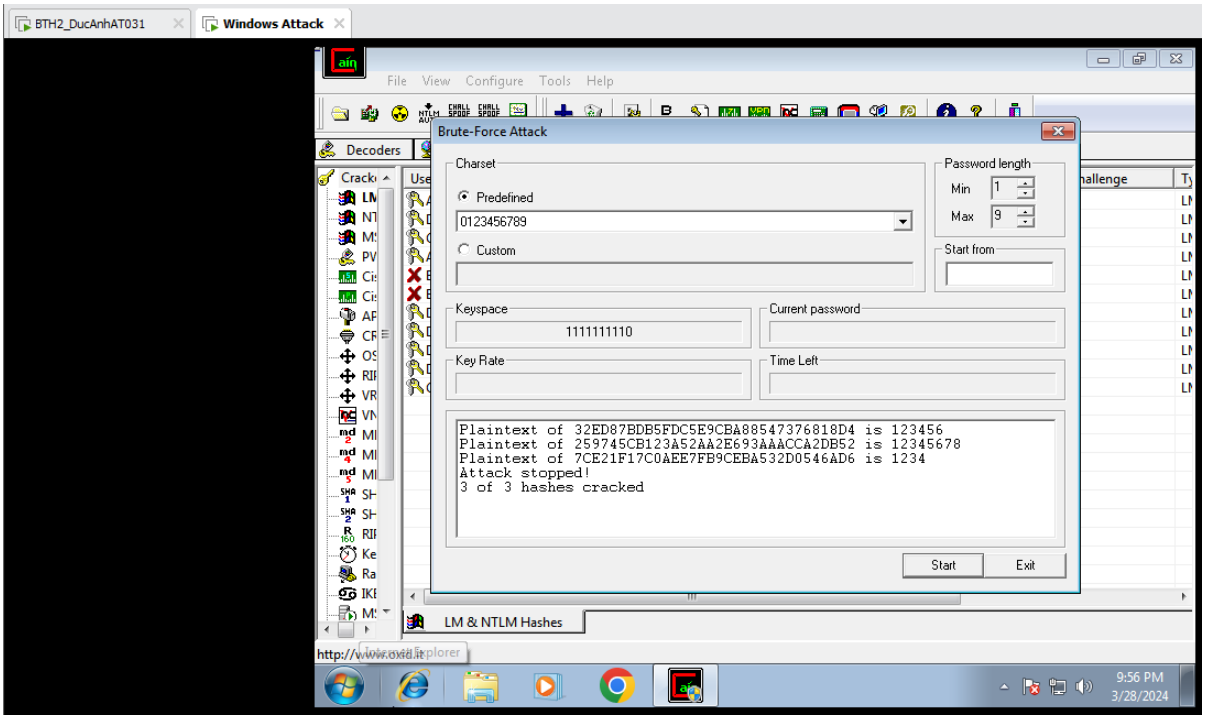


Bôi đen 3 tài khoản cần crack sau đó chuột phải sẽ hiện ra 3 tùy chọn lần lượt là : Tấn tông bằng từ điển, tấn công vét cạn, tấn công bằng cách phân tích thuật toán. Ta sẽ chọn tấn công bằng phương pháp vét cạn.



Chọn Start để bắt đầu vét cạn.

Lưu ý ở đây để tiết kiệm thời gian vét cạn ta có thể điều chỉnh các thông số như bộ ký tự, chiều dài tối thiểu/tối đa của mật khẩu



Đã crack mật khẩu thành công.

3. Kết quả đạt được

- Sử dụng John the Ripper để bẻ khóa mật khẩu trên máy Kali Linux
- Sử dụng được Cain and Abel để bẻ khóa mật khẩu trên máy Windows 7