

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



BÀI BÁO CÁO THỰC HÀNH SỐ 12

MÔN THỰC TẬP CƠ SỞ

CRACK MẬT KHẨU

Tên sinh viên: Ninh Chí Hương

Mã sinh viên: B20DCAT094

Số điện thoại: 0353770347

Giảng viên hướng dẫn : Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 5/2023

Table of Contents

I.Tìm hiểu lý thuyết.....	3
1. Tìm hiểu về John the Ripper.....	3
2. Tìm hiểu về phần mềm Cain	3
II Nội dung thực hành:	4
2.1. Chuẩn bị môi trường:	4
2.2 Nội dung thực hành	4
2.2.1 Crack mật khẩu trên hệ điều hành Linux sử dụng John the Ripper	4
2.2.3 crack mật khẩu trên windown bằng phần mềm Cain and abel	6
Tài liệu tham khảo :.....	9

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.
- 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 độm.
- 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 hiện 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:

2.1. Chuẩn bị môi trường:

Một máy ubuntu

Một máy win7

Phần mềm VMware

2.2 Nội dung thực hành

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

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

B20AT094-NinhChiHuong1 – pass 1234

B20AT094-NinhChiHuong2 – pass 123456

B20AT094-NinhChiHuong3 – pass 12345678

```

(root@B20AT094-Huong-Kali)-[~]
# useradd B20AT094-NinhChiHuong1

(root@B20AT094-Huong-Kali)-[~]
# useradd B20AT094-NinhChiHuong2

(root@B20AT094-Huong-Kali)-[~]
# useradd B20AT094-NinhChiHuong3

(root@B20AT094-Huong-Kali)-[~]
# passwd B20AT094-NinhChiHuong1
New password:
Retype new password:
passwd: password updated successfully

(root@B20AT094-Huong-Kali)-[~]
# passwd B20AT094-NinhChiHuong2
New password:
Retype new password:
passwd: password updated successfully

(root@B20AT094-Huong-Kali)-[~]
# passwd B20AT094-NinhChiHuong3
New password:
Retype new password:
passwd: password updated successfully

```

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

```

root@B20AT094-Huong-Kali: ~
File Actions Edit View Help
GNU nano 6.2 password
B20AT094-NinhChiHuong1:$y$j9T$vtP9cDhWPk/kwy9bQSwQk.$v8cfNgNuF/1njvw3rrSwMJW.OdTu8S4414uoJlubR03:19480:0:99999:7:::
B20AT094-NinhChiHuong2:$y$j9T$WTjo4ptFJEXHEK/F40SPx0$UNvedvHaD8WCRAFzkK4tPhIIHYIYLbqgcfwtkGjqFL3:19480:0:99999:7:::
B20AT094-NinhChiHuong3:$y$j9T$gGWJw0.Vf3lXr.OXinqMW1$SXQ.CdLZ5NDgN1zM7dkFzL5xMjC..cyVZafDxP25SV9:19480:0:99999:7:::

```

Chạy lệnh john password –format=crypt để tiến hành crack mật khẩu :

```

(root@B20AT094-Huong-Kali)-[~]
# john password --format=crypt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 1.75% 1/3 (ETA: 08:23:26) 0g/s 76.03p/s 76.03c/s 76.03C/s bat-ninhchihuongbat..BAT-NinhChiHuong4
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
123456 (B20AT094-NinhChiHuong2)
12345678 (B20AT094-NinhChiHuong3)
1234 (B20AT094-NinhChiHuong1)
3g 0:00:12:18 DONE 2/3 (2023-05-03 08:31) 0.004060g/s 73.81p/s 74.08c/s 74.08C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Mật khẩu của 3 tài khoản đã được crack thành công

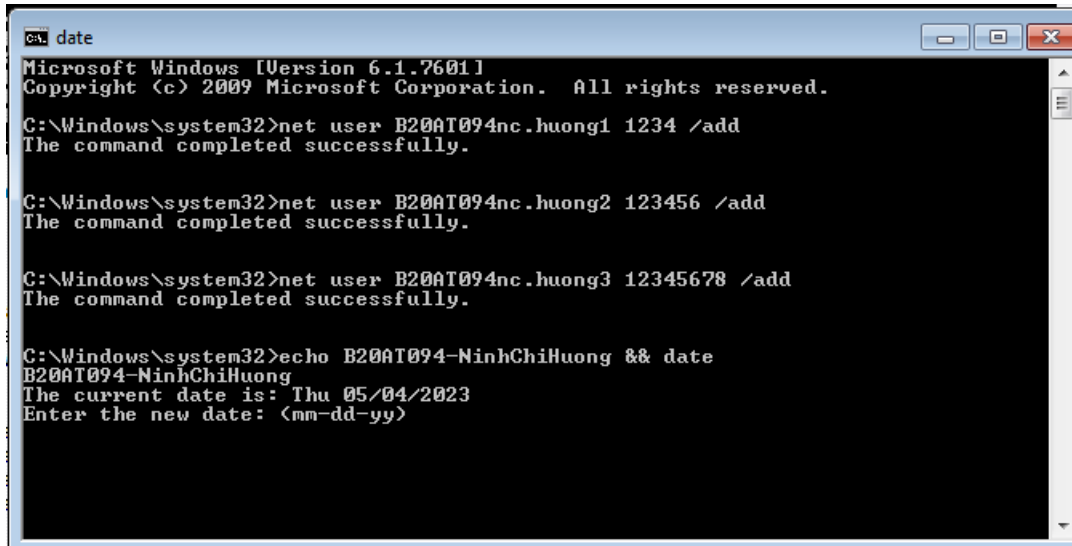
2.2.3 crack mật khẩu trên windown bằng phần mềm Cain and abel

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

B20AT094nc.huong1 – 1234

B20AT094nc.huong2 – 123456

B20AT094nc.huong3 – 12345678



```
Ca date
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

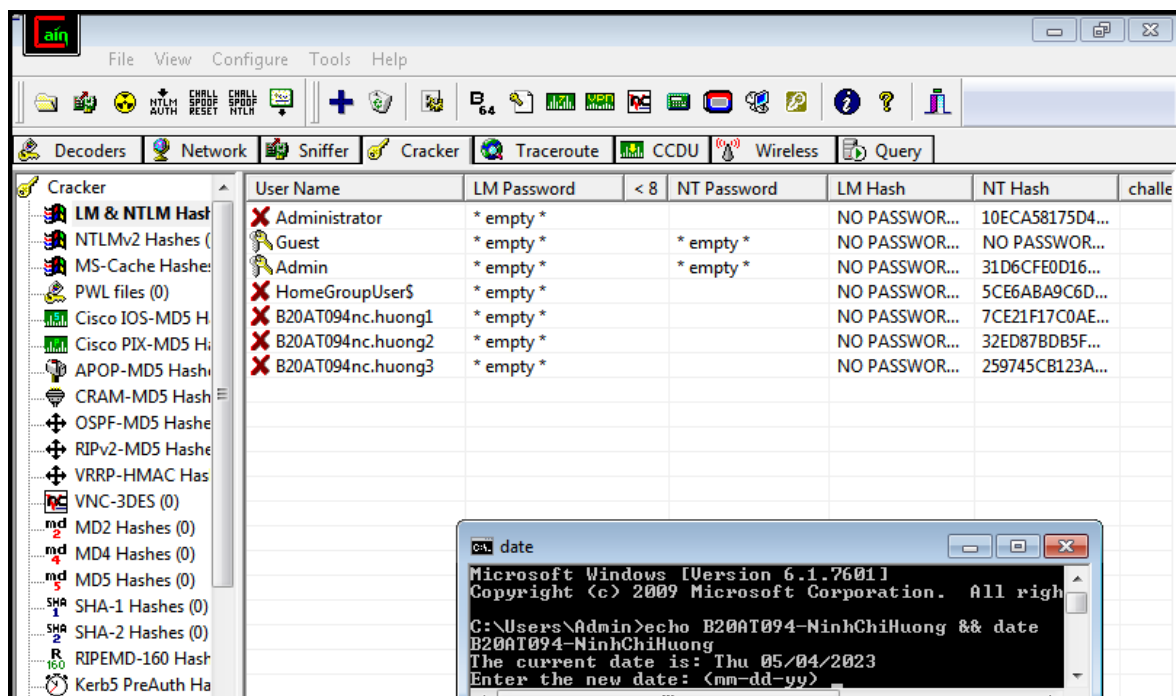
C:\Windows\system32>net user B20AT094nc.huong1 1234 /add
The command completed successfully.

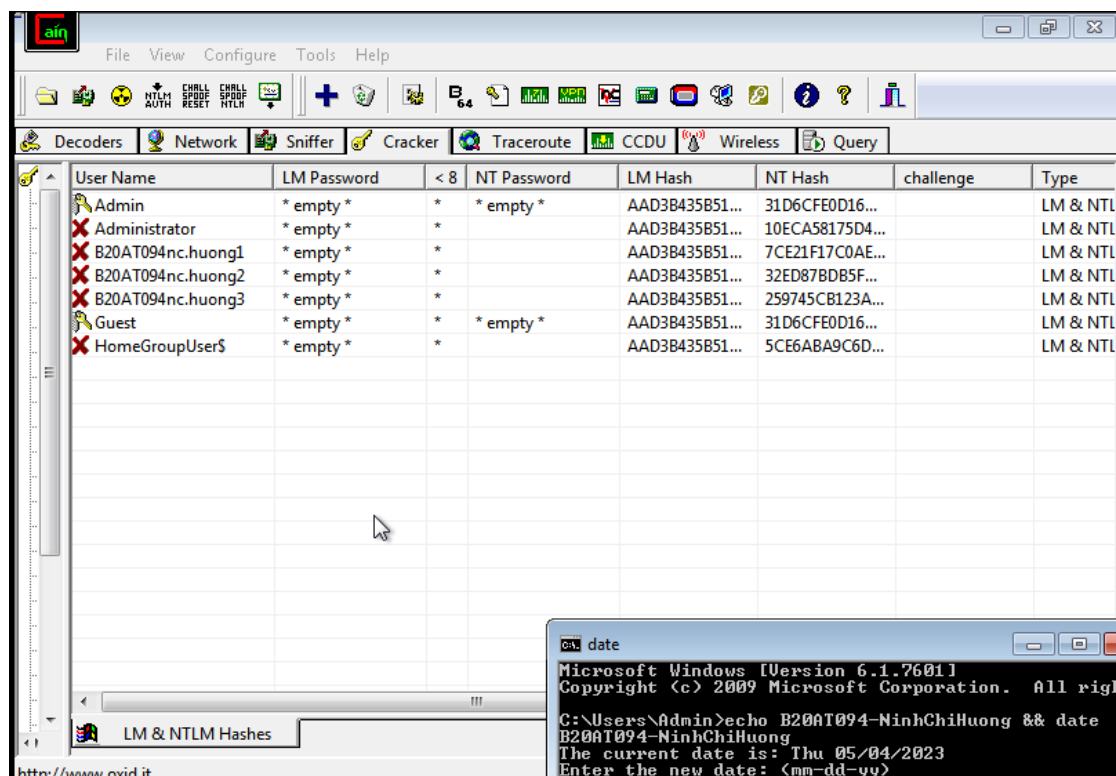
C:\Windows\system32>net user B20AT094nc.huong2 123456 /add
The command completed successfully.

C:\Windows\system32>net user B20AT094nc.huong3 12345678 /add
The command completed successfully.

C:\Windows\system32>echo B20AT094-NinhChiHuong && date
B20AT094-NinhChiHuong
The current date is: Thu 05/04/2023
Enter the new date: <mm-dd-yy>
```

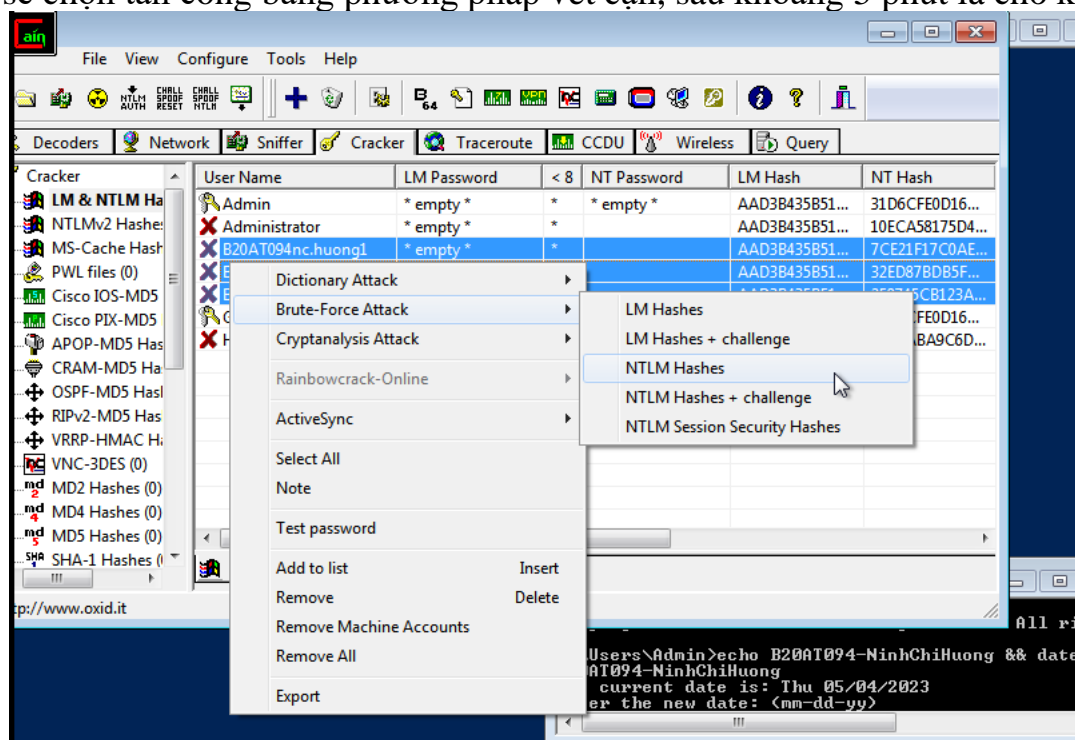
Khởi chạy Cain , sau đó chọn CRACK,chuột phải, chọn Add to list ,chọn Next:

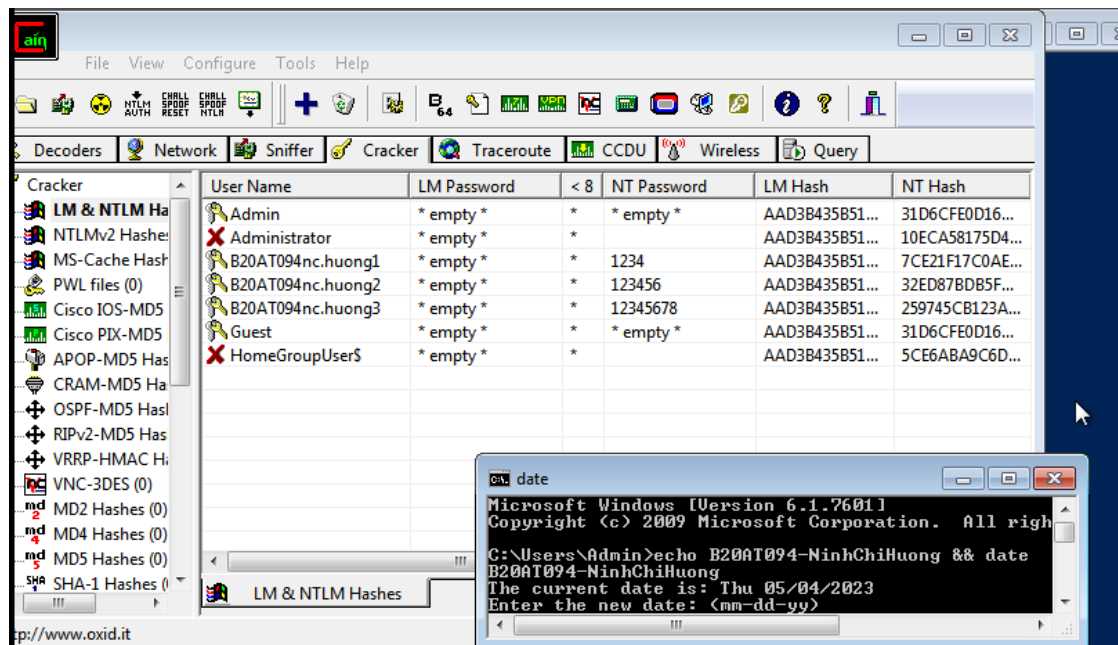




Bôi đen 3 tài khoản cần crack sau đó chuột phải sẽ hiện ra 3 tùy chọn lần lượt là : Tấn công bằng từ điển, tấn công vét cạn, tấn công bằng cách phân tích thuật toán.

Ta sẽ chọn tấn công bằng phương pháp vét cạn, sau khoảng 5 phút là cho kết quả :





Crack mật khẩu của 3 user thành công

Tài liệu tham khảo :

- 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.
- Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman