

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: THỰC TẬP CƠ SỞ  
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.2  
TẤN CÔNG VÀO MẬT KHẨU**

Sinh viên thực hiện:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
<b>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</b> .....	5
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết .....	5
<b>1.2.1</b> Các công cụ crack mật khẩu.....	5
<b>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</b> .....	9
2.1 Chuẩn bị môi trường .....	9
2.2 Các bước thực hiện.....	9
<b>2.2.1</b> Crack mật khẩu trên hệ điều hành Window .....	9
<b>2.2.2</b> Crack mật khẩu trên hệ điều hành Linux .....	15
TÀI LIỆU THAM KHẢO.....	20

## DANH MỤC CÁC HÌNH VẼ

Hình 1 Sử dụng công cụ John the Ripper.....	7
Hình 2 Công cụ pwdump .....	9
Hình 3 Công cụ ophcrack.....	10
Hình 4 Rainbow tables của công cụ ophcrack .....	11
Hình 5 Tạo 3 user có mật khẩu .....	12
Hình 6 Sử dụng công cụ pwdump .....	12
Hình 7 Kết quả thu được sau khi sử dụng pwdump .....	13
Hình 8 Lựa chọn table .....	13
Hình 9 Thêm file pwdump .....	14
Hình 10 Bỏ khóa thành công mật khẩu .....	15
Hình 11 Tạo 3 user .....	16
Hình 12 Kiểm tra file /etc/shadow .....	17
Hình 13 Kết hợp 2 file chứa thông tin mật khẩu .....	18
Hình 14 Kiểm tra file vừa tạo.....	18
Hình 15 Crack thành công mật khẩu 2 user .....	19
Hình 16 Crack thành công user còn lại .....	19

## DANH MỤC CÁC TỪ VIẾT TẮT

<b>Từ viết tắt</b>	<b>Thuật ngữ tiếng Anh/Giải thích</b>	<b>Thuật ngữ tiếng Việt/Giải thích</b>
SAM	Security Account Manager	Trình quản lý tài khoản bảo mật của Windows
GUI	Graphical User Interface	Giao diện đồ họa người dùng
JtR	John the Ripper	Công cụ bẻ khóa mật khẩu mã nguồn mở
MD5	Message-Digest Algorithm 5	Thuật toán băm mật khẩu MD5
SHA512	Secure Hash Algorithm 512	Thuật toán băm an toàn SHA-512

# CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

## 1.1 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.

## 1.2 Tìm hiểu lý thuyết

### 1.2.1 Các công cụ crack mật khẩu

#### 1.2.1.1 Pwdump

pwdump là một công cụ được sử dụng để trích xuất mật khẩu đã băm (hashed passwords) từ cơ sở dữ liệu SAM (Security Account Manager) trên hệ điều hành Windows. Công cụ này thường được dùng trong kiểm thử bảo mật, khôi phục mật khẩu, hoặc nghiên cứu về bảo mật hệ thống.

pwdump lấy thông tin mật khẩu từ SAM database, nơi Windows lưu trữ thông tin đăng nhập. Tuy nhiên, mật khẩu không được lưu ở dạng văn bản thuần túy mà được băm bằng thuật toán NTLM hoặc LM (LAN Manager). Công cụ này có thể trích xuất và hiển thị các giá trị băm này để phân tích hoặc tấn công bằng cách bẻ khóa.

#### 1.2.1.2 Ophcrack

Ophcrack là một công cụ bẻ khóa mật khẩu cực kỳ nhanh vì nó sử dụng một thuật toán đặc biệt gọi là bảng cầu vồng (rainbow table). Các công cụ bẻ khóa bằng cách thử hàng nghìn tổ hợp chữ cái, số và ký tự đặc biệt mỗi giây, nhưng việc bẻ khóa mật khẩu bằng cách thử mọi tổ hợp có thể tương đương được có thể mất hàng giờ hoặc nhiều ngày. Bảng cầu vồng tính toán trước các hàm băm được mật khẩu sử dụng, cho phép tra cứu mật khẩu nhanh chóng bằng cách so sánh các hàm băm mà mật khẩu có, thay vì tính toán chúng từ đầu.

Ophcrack hoạt động trên các băm LAN Manager (LM) và NT LAN Manager (NTLM) và có các bảng cầu vồng để bẻ khóa mật khẩu Windows XP và Windows Vista. Nó đi kèm với GUI bóng bẩy và chạy trên Windows, Linux/Unix, Mac OS X hoặc từ LiveCD có thể khởi động. Ophcrack có khả năng lấy băm mật khẩu từ Security Accounts Manager (SAM), cơ sở dữ liệu sổ đăng ký mà Windows sử dụng để lưu trữ mật khẩu người dùng được bảo vệ.

#### 1.2.1.3 John The Ripper

John the Ripper (JtR) là một chương trình mã nguồn mở được thiết kế để bẻ khóa mật khẩu. Được phát triển lần đầu tiên vào năm 1996, nó đã trở thành một trong những công cụ phổ biến nhất cho những người làm công tác bảo mật, chuyên gia an ninh mạng và cả những kẻ tấn công. Với khả năng xử lý nhiều mật khẩu băm thuật toán khác nhau, JtR có thể hỗ trợ bẻ khóa mật khẩu cho nhiều hệ điều hành và ứng dụng.

## Nguyên lý hoạt động

John the Ripper hoạt động bằng cách sử dụng các công cụ tấn công phương pháp khác nhau để bẻ khóa mật khẩu. Các phương pháp này bao gồm:

- Tấn công Brute Force : JtR thử nghiệm tất cả các khả năng mật khẩu có thể. Đây là phương pháp đơn giản nhưng rất tốn kém thời gian.
- Tấn công từ điển : Sử dụng một phổ biến mật khẩu danh sách, JtR sẽ thử từng mật khẩu trong danh sách để tìm ra mật khẩu đúng.
- Tấn công thông tin : JtR có khả năng tự động tối ưu hóa chiến lược dựa trên các mật khẩu mẫu mà không có nhận dạng.

## Truy cập và Cài đặt

John the Ripper có sẵn nhiều hệ điều hành, bao gồm Windows, Linux và macOS. Quá trình cài đặt rất đơn giản, chỉ cần tải nguồn mã hóa từ trang GitHub chính thức và biên dịch.

## Cú pháp sử dụng:

- Không chỉ định thuật toán crack: sẽ rất tốn thời gian  
*john path/to/password-file*
- Chỉ định thuật toán crack:  
*john --format=<Format> path/to/password-file -*
- Crack mật khẩu sử dụng 1 danh sách từ điển:  
*john --format=FORMAT --wordlist=mywordlist.txt path/to/password-file*

Trong đó, --format=FORMAT là định dạng của mật khẩu bạn muốn crack (ví dụ: --format=md5, --format=sha512,...), và path/to/password-file là đường dẫn đến tệp chứa mật khẩu.

```

kali@kali:~$ echo -n test2 | md5sum
ad0234829205b9033196ba818f7a872b -
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}'
ad0234829205b9033196ba818f7a872b
kali@kali:~$ echo -n test2 | md5sum | awk '{print $1}' > hash
kali@kali:~$
kali@kali:~$ for x in $(seq 0 9); do echo test$x >> wordlists; done
kali@kali:~$ grep test2 wordlists
test2
kali@kali:~$ wc -l wordlists
10 wordlists
kali@kali:~$
kali@kali:~$ john --list=formats | grep -i 'md5'
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
mschapv2-naive, krb5pa-md5, mssql, mssql05, mssql12, multibit, mysqlna,
mysql-sha1, mysql, net-ah, nethalflm, netlm, netlmv2, net-md5, netntlmv2,
netntlm, netntlm-naive, net-sha1, nk, notes, md5ns, nsec3, NT, o10glogon,
PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA256,
PHPS2, pix-md5, PKZIP, po, postgres, PST, PuTTY, pwsafe, qnx, RACF,
Raw-Keccak, Raw-Keccak-256, Raw-MD4, Raw-MD5, Raw-MD5u, Raw-SHA1,
Stribog-256, Stribog-512, STRIP, SunMD5, SybaseASE, Sybase-PROP, tacacs-plus,
tcp-md5, telegram, tezos, Tiger, tc_aes_xts, tc_ripemd160, tc_ripemd160boot,
ZipMonster, plaintext, has-160, HMAC-MD5, HMAC-SHA1, HMAC-SHA224,
kali@kali:~$
kali@kali:~$ john --format=raw-md5 --wordlist=wordlists hash
Created directory: /home/g0tmilk/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 10 candidates left, minimum 12 needed for performance.
test2 (?)
1g 0:00:00:00 DONE (2021-11-04 10:30) 100.0g/s 1000p/s 1000c/s 1000C/s test0..test9
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
kali@kali:~$

```

*Hình 1 Sử dụng công cụ John the Ripper*

## Ứng dụng thực tế của John the Ripper

### *Kiểm tra tính bảo mật*

Một trong những ứng dụng chính của JtR là kiểm tra tính bảo mật của các mật khẩu trong hệ thống. Bằng cách xác định xem mật khẩu nào dễ bị bẻ khóa, tổ chức có thể thay đổi để tăng cường tính bảo mật.

### *Đào tạo và giáo dục*

John the Ripper cũng được sử dụng trong các khóa học về an ninh mạng để giúp sinh viên hiểu về cách mà mật khẩu có thể bị bẻ khóa và cách phòng chống.

### *Phân tích an ninh*

Bảo mật lớn sử dụng JtR trong quá trình phân tích và sau các cuộc tấn công để hiểu rõ hơn về lỗi trong hệ thống và cải thiện các biện pháp phòng vệ tốt hơn.

### *Những điều cần lưu ý*

Mặc dù John the Ripper là một công cụ hữu ích, nhưng việc sử dụng nó cần có dưỡng thủ đạo đức và pháp luật. Sử dụng JtR để tấn công các hệ thống không được phép là hành vi vi phạm pháp luật và có thể dẫn đến hậu quả nghiêm trọng.



## CHƯƠNG 2. NỘI DUNG THỰC HÀNH

### 2.1 Chuẩn bị môi trường

Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.

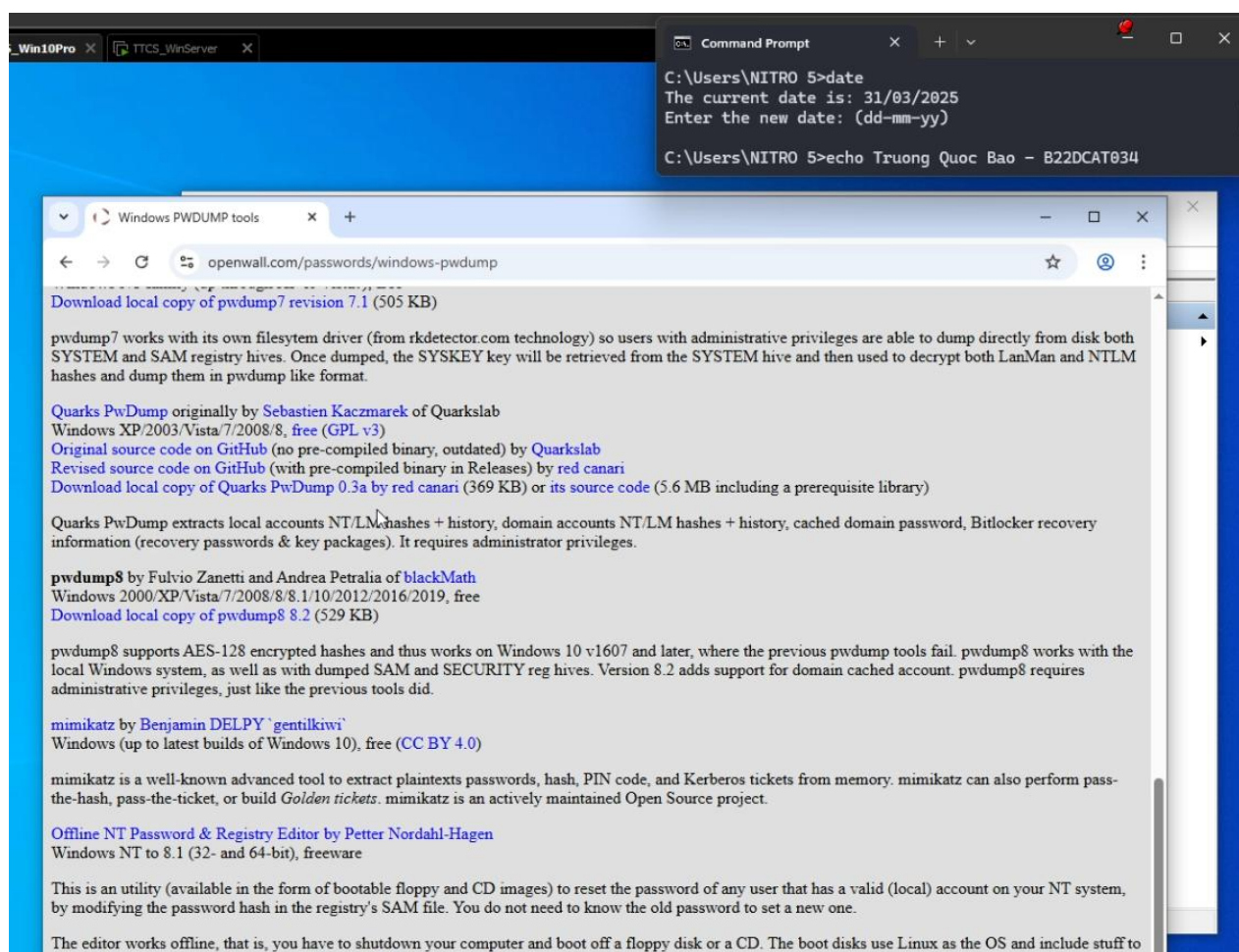
Phần mềm hệ điều hành Linux và Windows

### 2.2 Các bước thực hiện

#### 2.2.1 Crack mật khẩu trên hệ điều hành Window

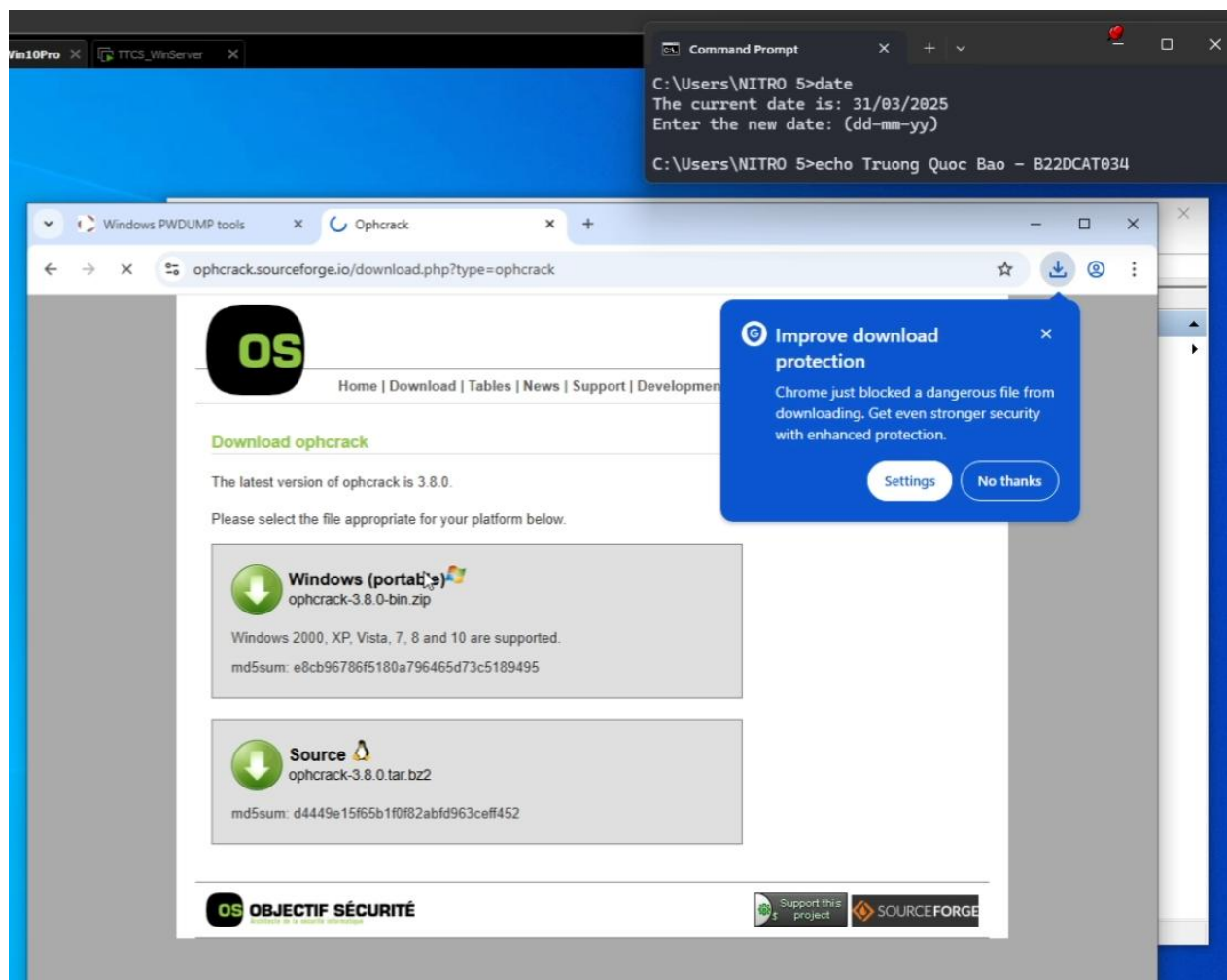
Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Tải công cụ Pwdump trên trang chủ.



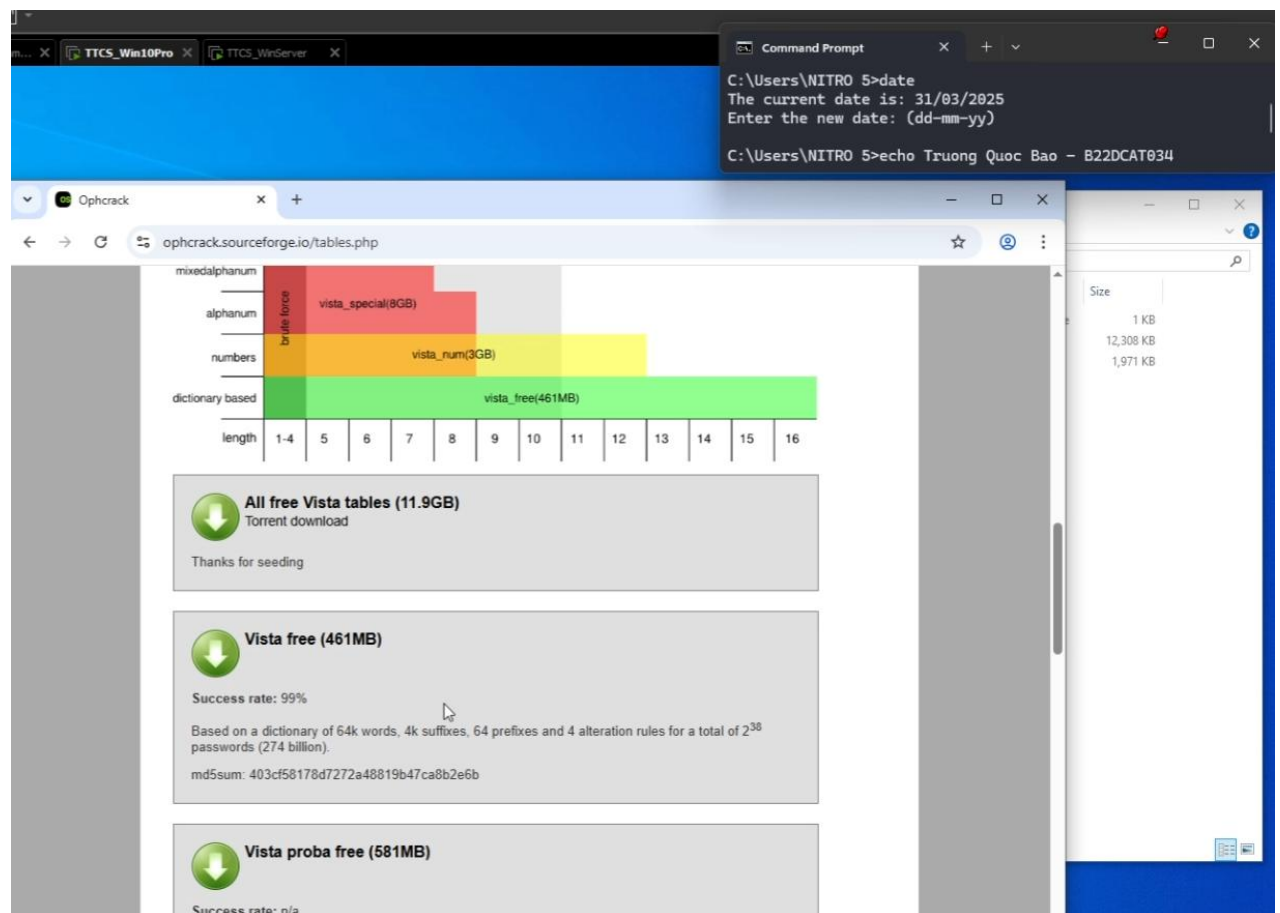
Hình 2 Công cụ pwdump

Tải công cụ Ophcrack trên trang chủ.



Hình 3 Công cụ ophcrack

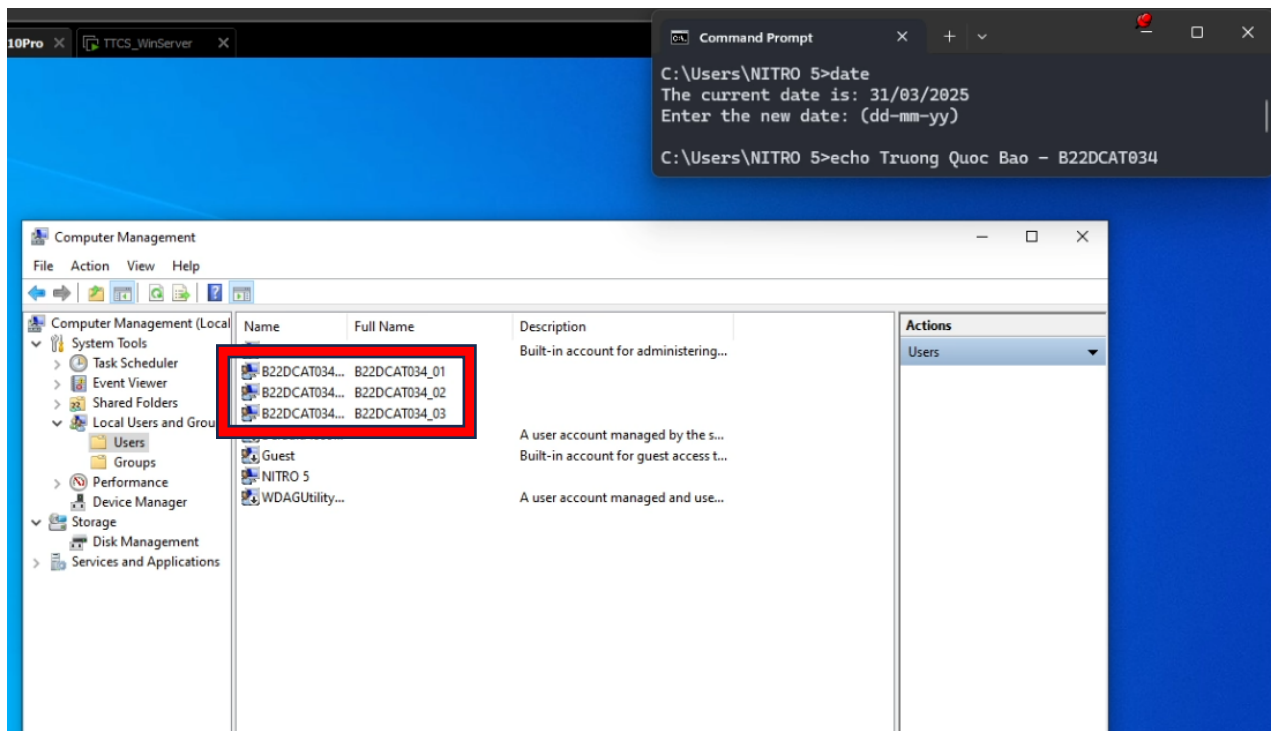
Tải Rainbow tables của công cụ ophcrack trên trang chủ.



Hình 4 Rainbow tables của công cụ ophcrack

Để tạo các User mới và mật khẩu ta làm theo các bước sau:

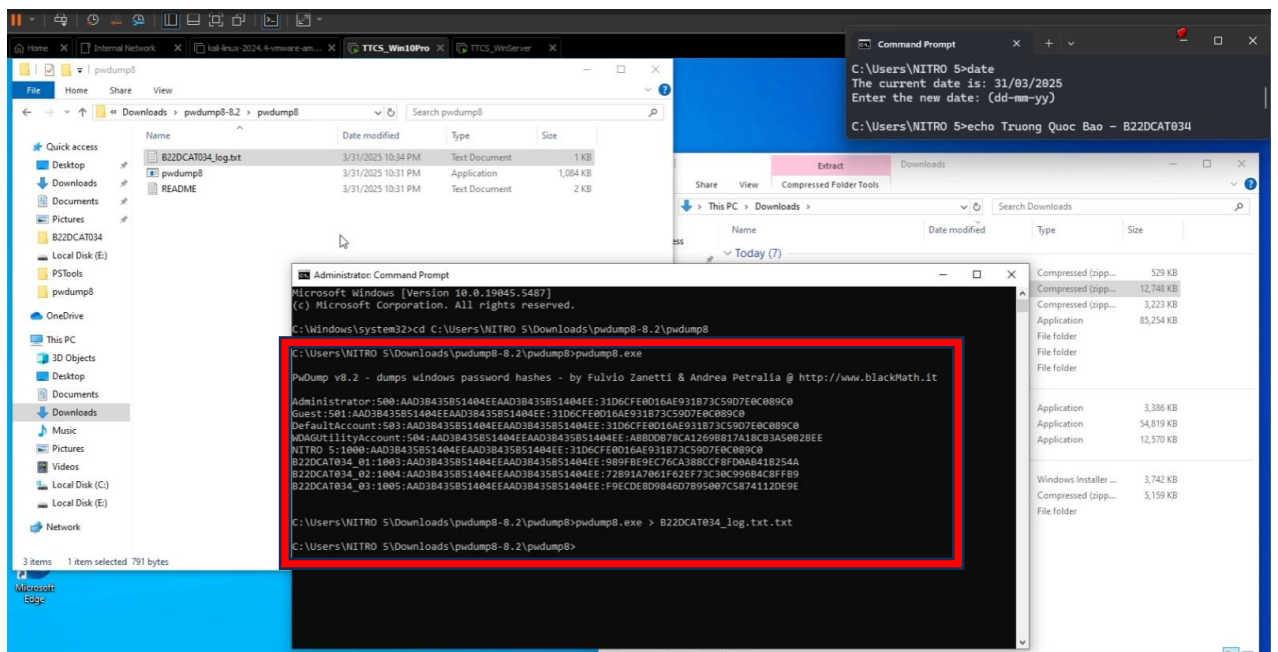
- Computer Management -> Local Users and Groups -> User -> New User
- Nhập tên và mật khẩu muốn đặt
- Do chính sách của Windows nên ta chỉ có thể đặt các mật khẩu dài hơn 7 kí tự và đủ mạnh. Việc này sẽ tăng thời gian cho việc crack mật khẩu.
- Nhấn OK để hoàn thành
- Các User với tên tương ứng sẽ hiện ngay sau đó



Hình 5 Tạo 3 user có mật khẩu

Chạy công cụ pwdump trên terminal

Sau đó lưu lại dữ liệu dump của mật khẩu vào 1 file bất kì để sử dụng sau này.



Hình 6 Sử dụng công cụ pwdump

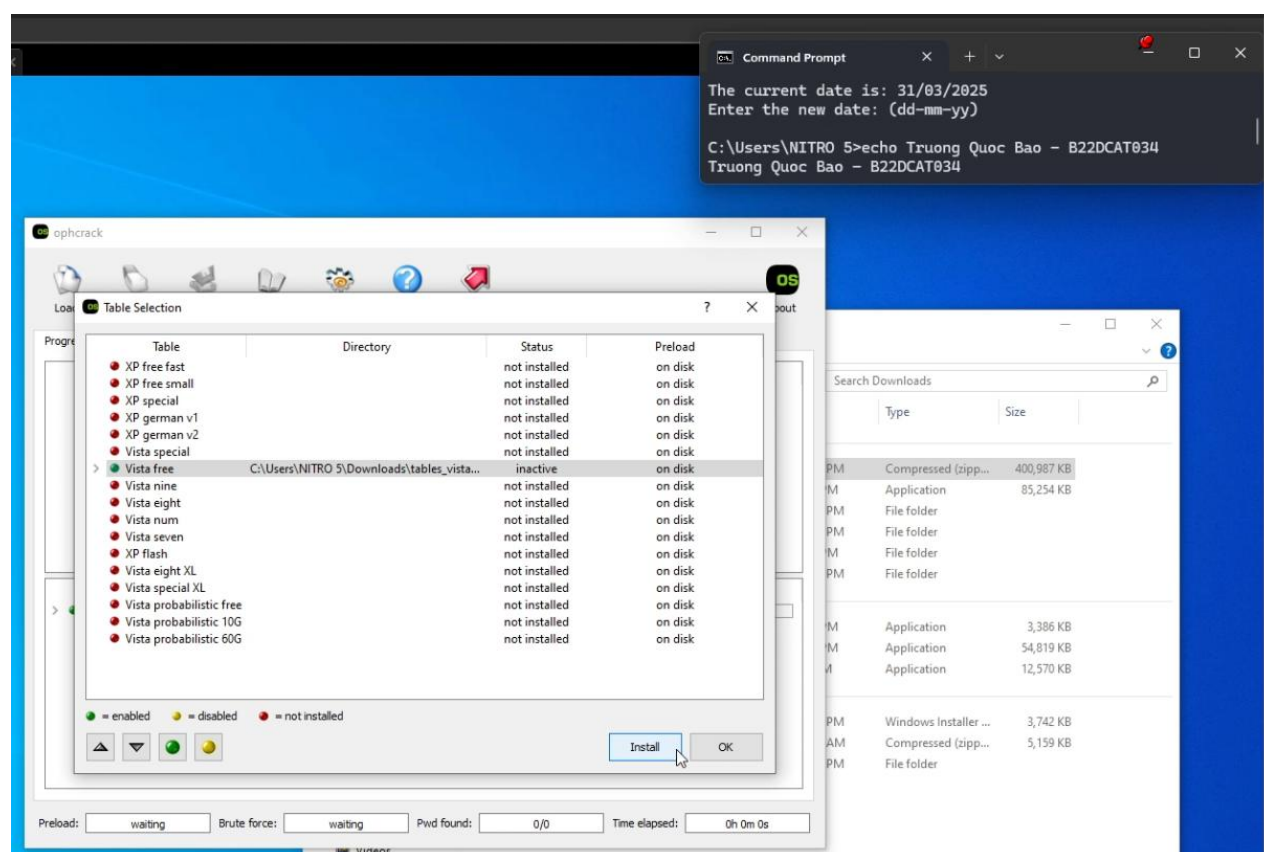
Đảm bảo thông tin lưu được có dạng như dưới đây.



Hình 7 Kết quả thu được sau khi sử dụng pwdump

Khởi động công cụ Ophcrack

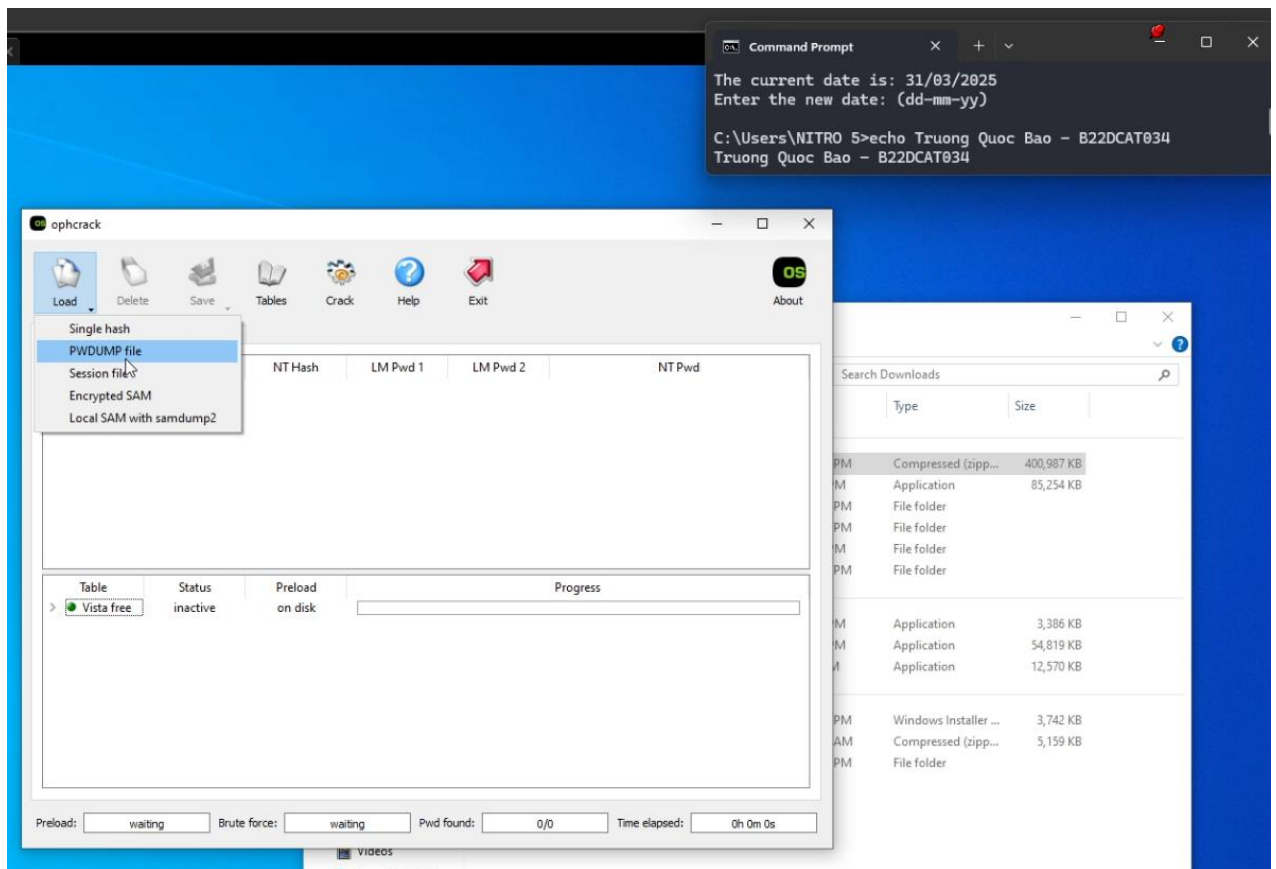
Chọn Tables -> Install -> File Rainbow vừa tải. Nếu table tương ứng hiện màu xanh (enable) là đã thành công.



Hình 8 Lựa chọn table



Chọn Load -> PWDUMP file để tải lên file dữ liệu dump trước đó.

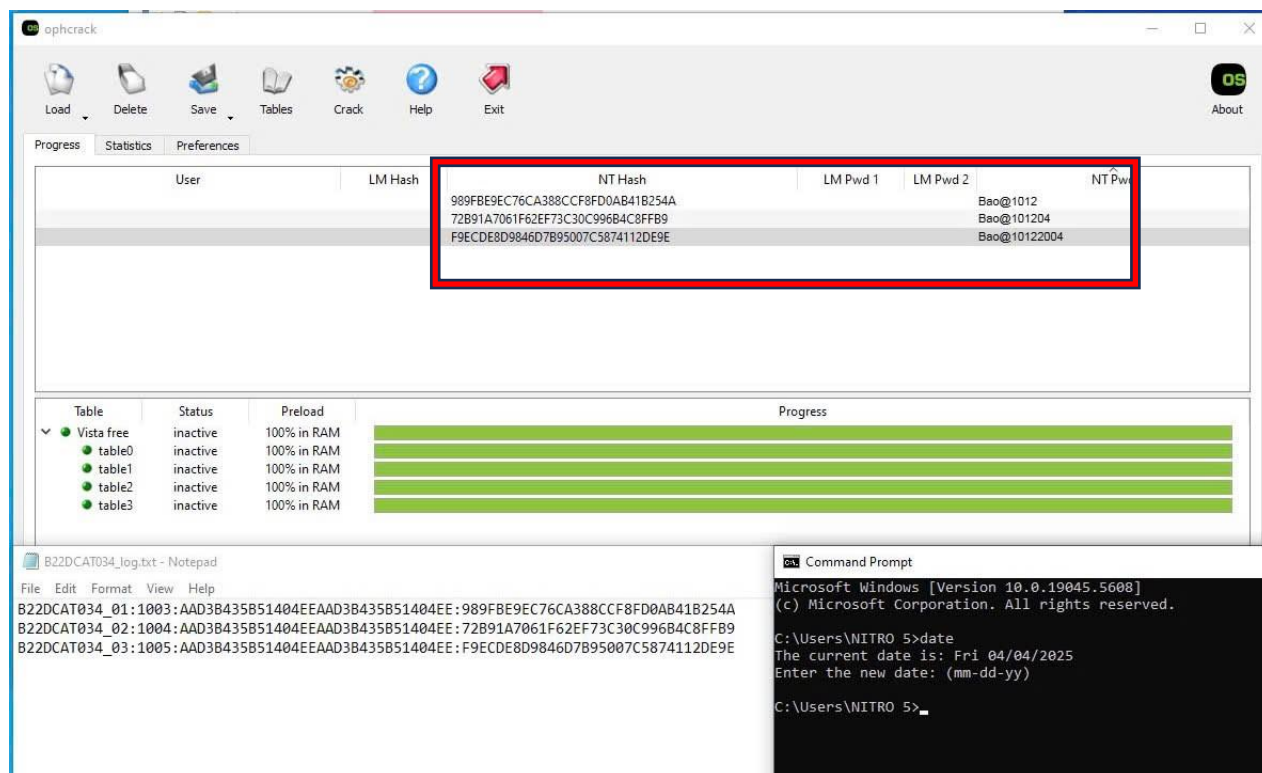


Hình 9 Thêm file pwdump

Chờ đợi file LOAD và chọn nút Crack để tiến hành bẻ khóa.

Có thể chọn “Single hash” để lựa chọn từng mật khẩu. Yêu cầu phải đúng định dạng như đã hướng dẫn.

Thời gian bẻ khóa phụ thuộc vào độ khó của mật khẩu.



Hình 10 Bẻ khóa thành công mật khẩu

### 2.2.2 Crack mật khẩu trên hệ điều hành Linux

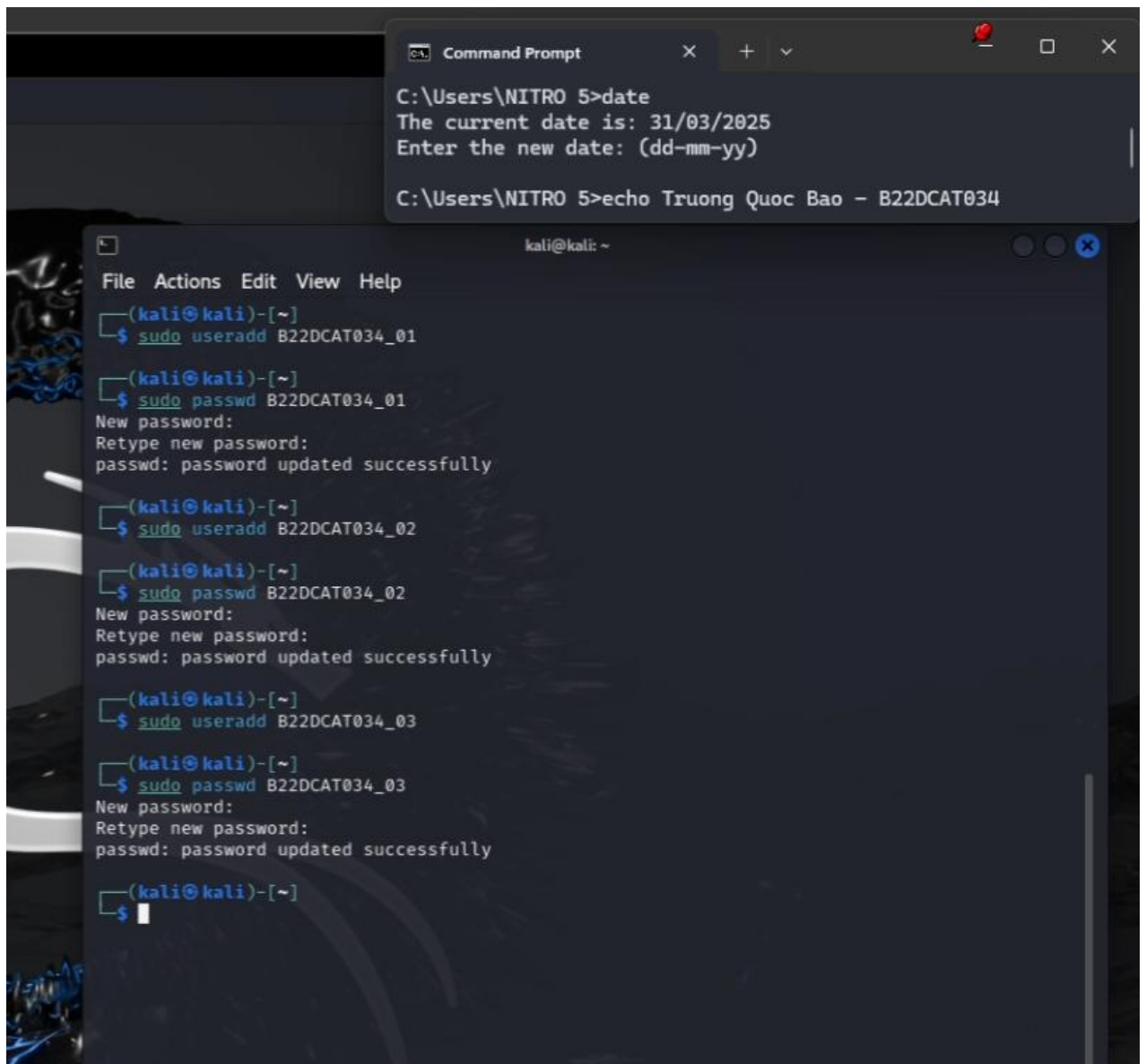
Thử nghiệm crack mật khẩu trên hệ điều hành Linux với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,.... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Mở terminal làm việc

Tạo các user và mật khẩu bằng lệnh

`sudo useradd <tên user>`

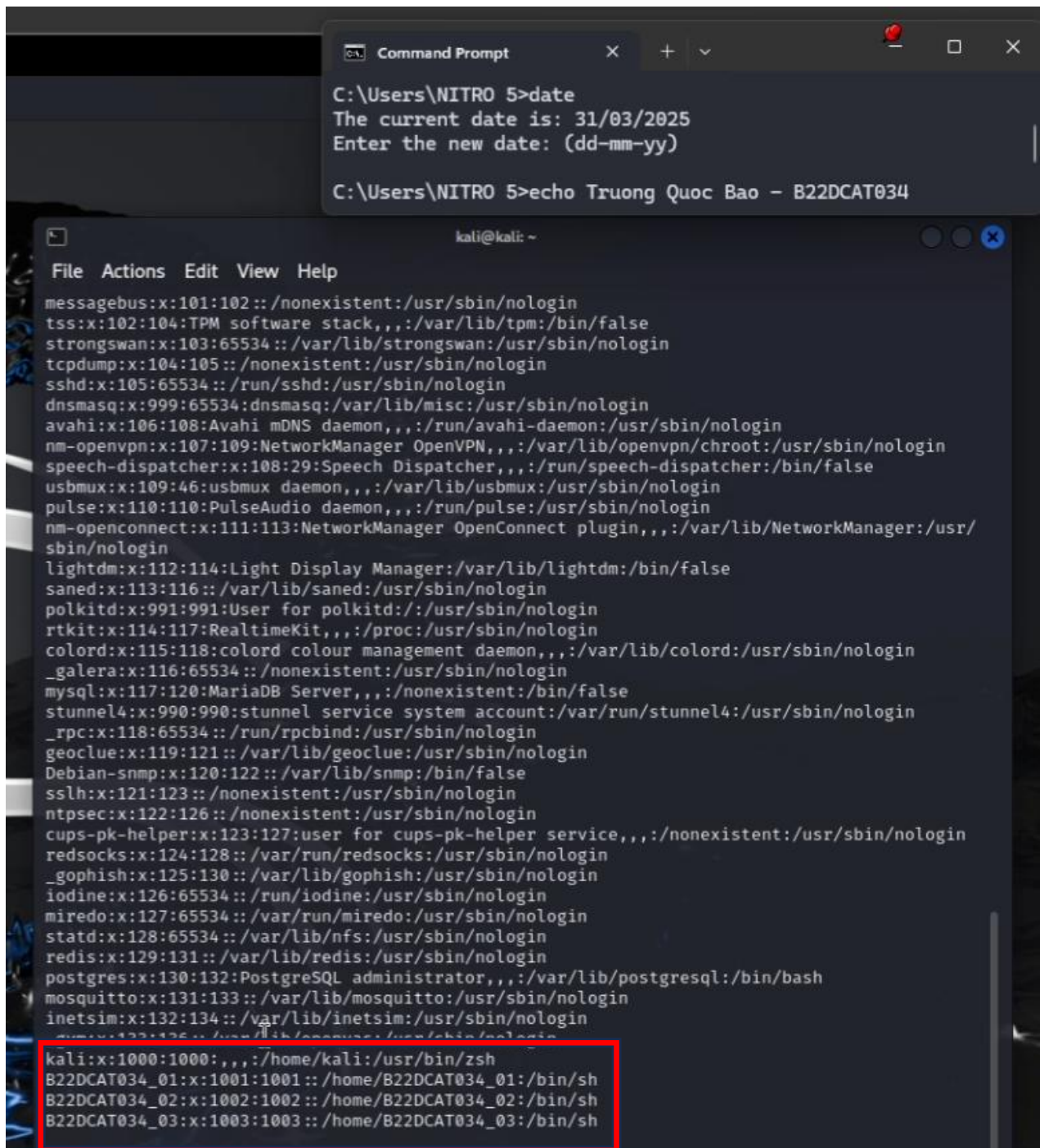
`sudo passwd <tên user>`



*Hình 11 Tạo 3 user*

Ta có thể kiểm tra 2 file /etc/shadow và /etc/passwd để đảm bảo các user đều tạo thành công và có mật khẩu.

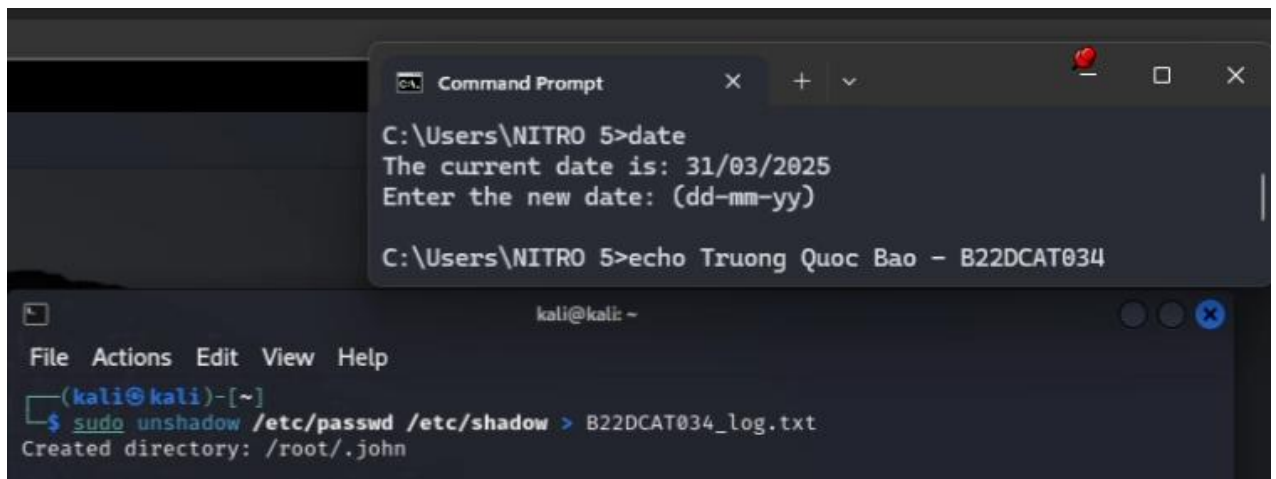




Hình 12 Kiểm tra file /etc/shadow

Ta sẽ tạo một file dump nhằm phục vụ việc crack mật khẩu bằng cách kết hợp 2 file /etc/shadow và /etc/passwd để mã hóa bằng lệnh

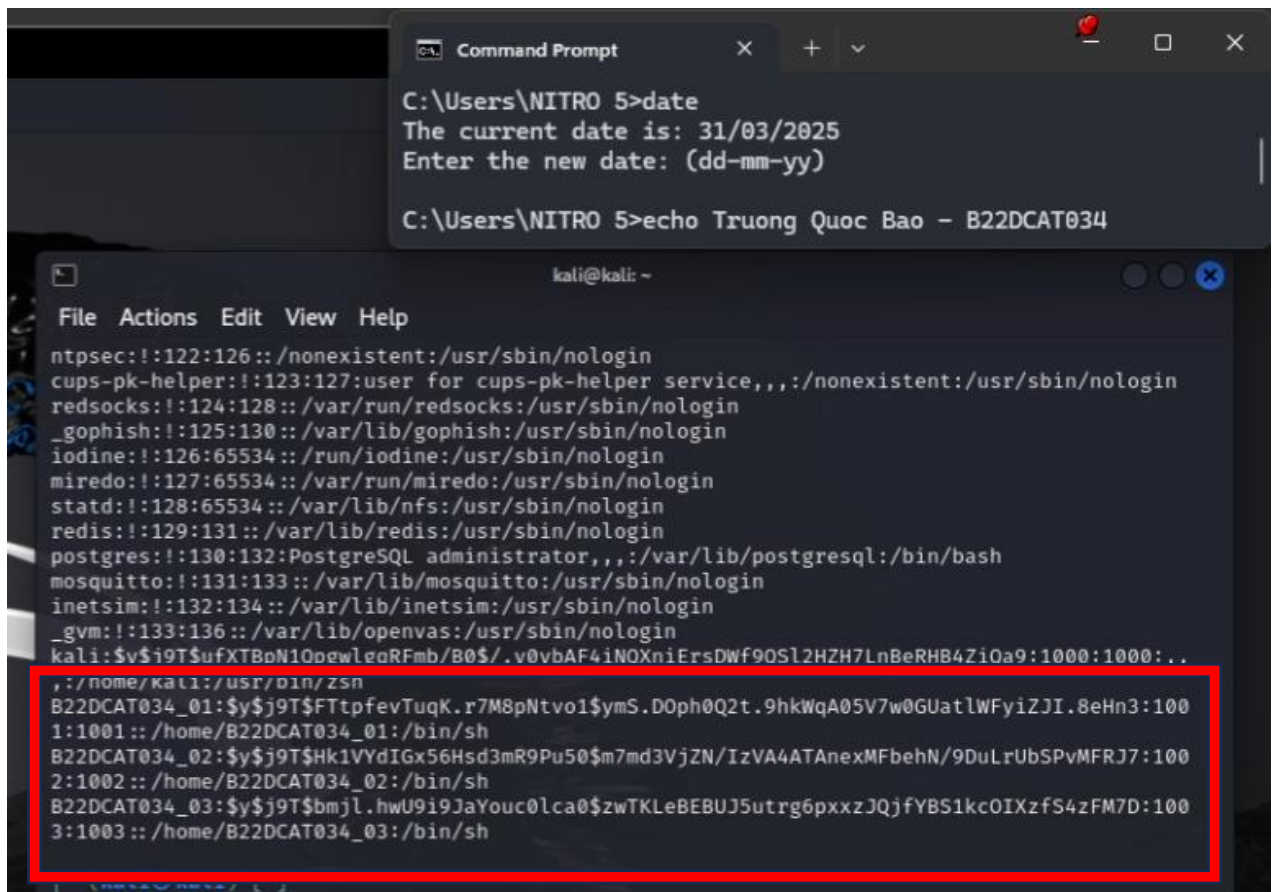
*sudo unshadow /etc/shadow /etc/passwd > <tên file>*



Hình 13 Kết hợp 2 file chứa thông tin mật khẩu

Kiểm tra file vừa tạo bằng lệnh cat

Ta thấy file này chứa thông tin về mật khẩu đã được mã hóa.



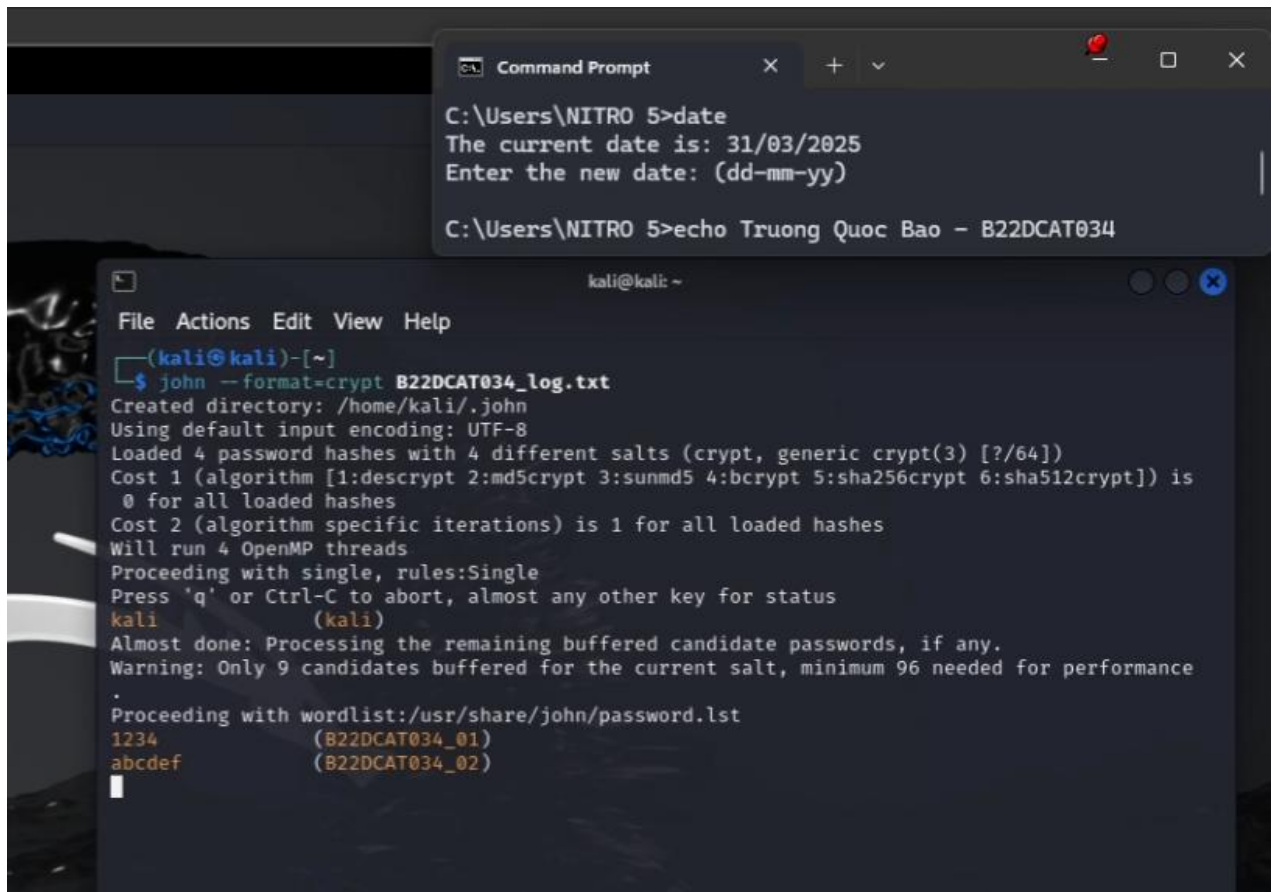
Hình 14 Kiểm tra file vừa tạo

Ta sử dụng công cụ John The Ripper ( đã được cài đặt sẵn trên Kali) để tiến hành crack mật khẩu bằng lệnh

*john --format=crypt <tên file>*

Thời gian chờ có thể khá lâu và tiêu tốn nhiều tài nguyên bộ nhớ

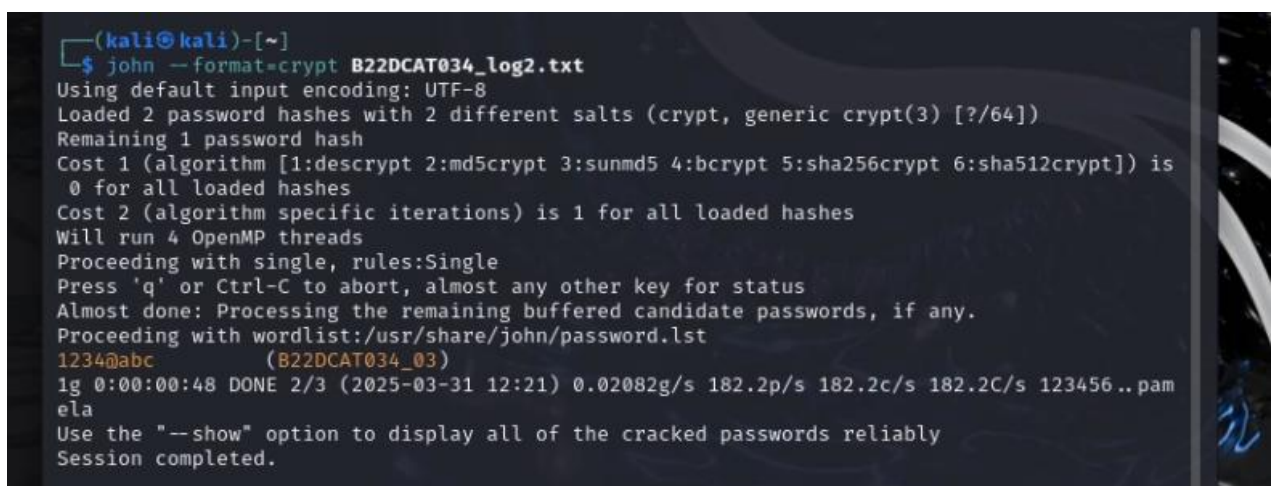
Kết quả thu được sẽ như 2 hình bên dưới.



The image shows two overlapping windows. The top window is a Windows Command Prompt titled 'Command Prompt' with the following text:  
C:\Users\NITRO S>date  
The current date is: 31/03/2025  
Enter the new date: (dd-mm-yy)  
C:\Users\NITRO S>echo Truong Quoc Bao - B22DCAT034

The bottom window is a Kali Linux terminal titled 'kali@kali: ~'. It shows the execution of the command `john --format=crypt B22DCAT034_log.txt`. The output includes:  
Created directory: /home/kali/.john  
Using default input encoding: UTF-8  
Loaded 4 password hashes with 4 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  
kali (kali)  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Warning: Only 9 candidates buffered for the current salt, minimum 96 needed for performance  
Proceeding with wordlist:/usr/share/john/password.lst  
1234 (B22DCAT034\_01)  
abcdef (B22DCAT034\_02)

Hình 15 Crack thành công mật khẩu 2 user



The image shows a Kali Linux terminal window titled 'kali@kali: ~'. It displays the output of the command `john --format=crypt B22DCAT034_log2.txt`. The output includes:  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])  
Remaining 1 password hash  
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  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
1234@abc (B22DCAT034\_03)  
1g 0:00:00:48 DONE 2/3 (2025-03-31 12:21) 0.02082g/s 182.2p/s 182.2c/s 182.2C/s 123456..pam  
ela  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.

Hình 16 Crack thành công user còn lại

## **TÀI LIỆU THAM KHẢO**

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] 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.
- [4] Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman