

**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: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

<i>MỤC LỤC</i>	2
<i>DANH MỤC CÁC HÌNH ẢNH</i>	3
<i>DANH MỤC CÁC TỪ VIẾT TẮT</i>	3
<i>CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH</i>	5
I. Mục đích	5
II. Tìm hiểu lý thuyết.....	5
1. Mô tả ngắn gọn lý thuyết về các công cụ crack mật khẩu trên Windows	5
2. Mô tả cách thức hoặc phương pháp công cụ áp dụng crack trên Windows và Linux	5
2.1 John The Ripper	5
2.2 Mimikatz	6
2.3 OphCrack	7
<i>CHƯƠNG 2. NỘI DUNG THỰC HÀNH</i>	9
I. Chuẩn bị môi trường	9
II. Các bước thực hiện	9
1. Crack mật khẩu trên Windows	9
2. Crack mật khẩu trên Linux.....	14
TÀI LIỆU THAM KHẢO	17

DANH MỤC HÌNH ẢNH

<i>Hình ảnh 1: Cách thức hoạt động của John the Ripper.....</i>	<i>6</i>
<i>Hình ảnh 2: Cách thức hoạt động của Mimikatz</i>	<i>6</i>
<i>Hình ảnh 3: Cách hoạt động của OphCrack.....</i>	<i>8</i>
<i>Hình ảnh 4: Tạo 3 tài khoản trên Windows.</i>	<i>9</i>
<i>Hình ảnh 5: Kết quả sau khi tạo người dùng.</i>	<i>9</i>
<i>Hình ảnh 6: Tải phần mềm PwDump8.....</i>	<i>10</i>
<i>Hình ảnh 7: Cài đặt OrpCrack và rainbow của nó.....</i>	<i>11</i>
<i>Hình ảnh 8: Giải nén các tập tin đã tải về.</i>	<i>11</i>
<i>Hình ảnh 9: Khởi động phần mềm OphCrack.</i>	<i>12</i>
<i>Hình ảnh 10: Chạy PwDump với quyền Administrator.</i>	<i>12</i>
<i>Hình ảnh 11: Kiểm tra lại file B22DCAT176_Linh_log.txt</i>	<i>13</i>
<i>Hình ảnh 12: Kích hoạt Rainbow</i>	<i>12</i>
<i>Hình ảnh 13: Kết quả sau khi crack mật khẩu.</i>	<i>14</i>
<i>Hình ảnh 14: Tạo user và đặt mật khẩu cho các user.....</i>	<i>15</i>
<i>Hình ảnh 15: Kiểm tra lại file trên /etc/password.</i>	<i>15</i>
<i>Hình ảnh 16: Kết hợp 2 file.....</i>	<i>16</i>
<i>Hình ảnh 17: Crack thành công mật khẩu 8 ký tự.</i>	<i>16</i>
<i>TÀI LIỆU THAM KHẢO</i>	<i>17</i>

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SIEM	Security Information and Event Management	Giải pháp giám sát, phát hiện và phản ứng nhanh với mối đe dọa.
DNS	Domain Name System	Giao thức tên miền
DHCP	Dynamic Host Configuration Protocol	Giao thức cấp phát địa chỉ IP tự động
IIS	Internet Information Services	Dịch vụ Web Server chính của Microsoft
WAS	Windows Process Activation Service	Dịch vụ hỗ trợ cho IIS

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. 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.

II. Tìm hiểu lý thuyết

1. Mô tả ngắn gọn lý thuyết về các công cụ crack mật khẩu trên hệ điều hành Windows và Linux.

Các công cụ crack mật khẩu trên hệ điều hành Windows bao gồm:

- *Ophcrack*: Sử dụng chiến lược phân tích mật khẩu đã mã hóa để khôi phục mật khẩu.
- *Offline NT Password & Registry Editor*: Đọc và thay đổi Registry để đặt lại mật khẩu.
- *Cain & Abel*: Tìm kiếm thông tin tài khoản mật khẩu được lưu trữ trên hệ thống mạng.
- *John the Ripper*: Sử dụng công nghệ brute-force để tìm ra mật khẩu bằng cách thử từng ký tự một.

Các công cụ crack mật khẩu trên Linux bao gồm những phần mềm phân tích và tấn công các chuỗi mật khẩu như John the Ripper, Rainbow Crack, Hydra, Medusa. Những công cụ này thường được sử dụng để kiểm tra tính bảo mật của hệ thống và giúp người quản trị đánh giá mức độ an toàn của mật khẩu sử dụng trên máy tính và hệ thống mạng từ đó đưa ra biện pháp bảo vệ thích hợp.

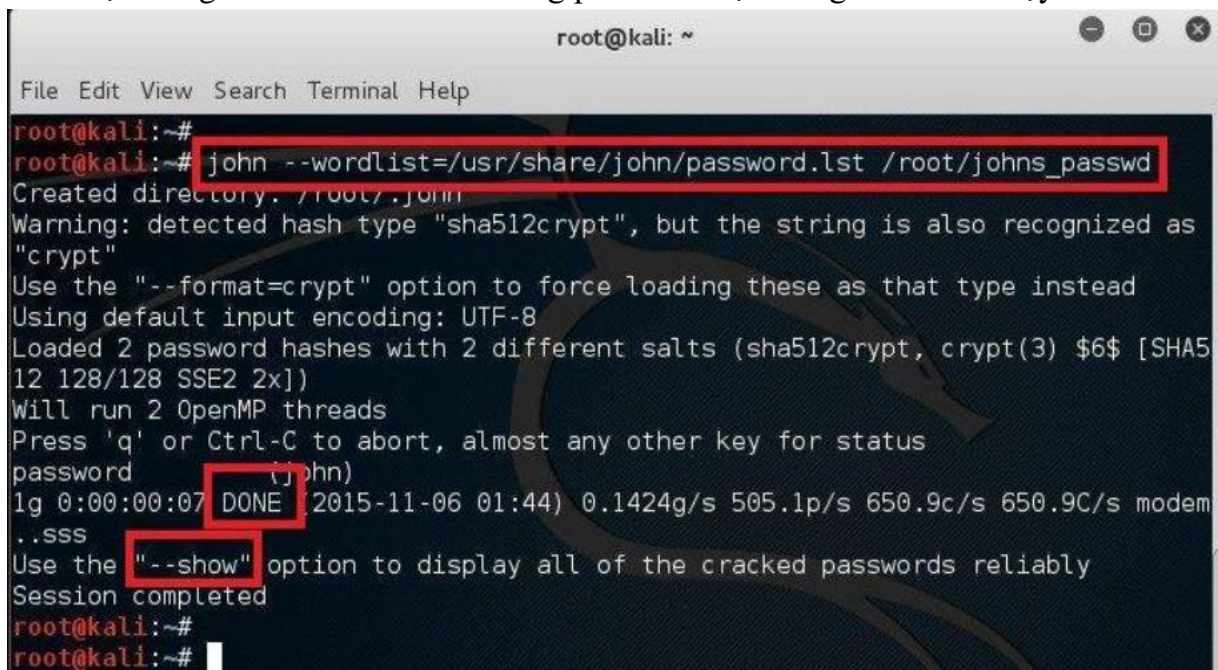
2. Mô tả cách thức hoặc phương pháp các công cụ áp dụng để crack mật khẩu trên hệ điều hành Windows và Linux.

2.1 John the Ripper

John the Ripper là công cụ phần mềm bẻ khóa mật khẩu miễn phí. Được phát triển ban đầu cho hệ điều hành Unix, nó có thể chạy trên 15 nền tảng khác nhau (11 trong số đó là các phiên bản cụ thể của kiến trúc Unix, DOS, Win32, BeOS và OpenVMS). Đây là một trong những chương trình kiểm tra và phá vỡ mật khẩu được sử dụng thường xuyên nhất vì nó kết hợp nhiều dạng tấn công crack mật khẩu vào một gói chương trình, tự động hóa các loại băm mật khẩu và tấn công tùy chỉnh. Nó có thể được chạy đối với các loại định dạng mật khẩu được mã hóa khác nhau bao gồm một số loại băm mật khẩu thường thấy nhất trên các phiên bản UNIX khác nhau (DES, MD5 hoặc Blowfish), Kerberos Á và Windows NT/2000/XP/2003 LM Hash. Các module bổ sung đã mở rộng khả năng bao gồm các băm mật khẩu và mật khẩu dựa trên MD4 được lưu trữ trong LDAP, MySQL và các loại khác.

Một trong những chế độ John có thể sử dụng là cuộc tấn công từ điển. Nó lấy các mẫu chuỗi văn bản (Chứa các từ được tìm thấy trong một từ điển hoặc mật khẩu đã bị bẻ

khóa trước đó), mã hóa nó theo cùng định dạng với mật khẩu đang được kiểm tra rồi so sánh đầu ra với chuỗi đã được mã hóa. John cũng có chế độ vét cạn. Trong loại tấn công này, chương trình trải qua tất cả các bản rõ có thể, băm từng cái và sau đó so sánh nó với hàm băm đầu vào. John sử dụng các bảng tần số kỹ tự để thử khai chứa các ký tự được sử dụng thường xuyên hơn trước. Phương pháp này hữu ích để bẻ khóa mật khẩu không xuất hiện trong danh sách từ điển nhưng phải mất một thời gian dài để chạy.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~#  
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd  
Created directory: /root/.john  
Warning: detected hash type "sha512crypt", but the string is also recognized as  
"crypt"  
Use the "--format=crypt" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5  
12 128/128 SSE2 2x])  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (john)  
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem  
..sss  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed  
root@kali:~#  
root@kali:~#
```

Hình ảnh 1: Cách thức hoạt động của John the Ripper.

2.2 Mimikatz

Mimikatz là một ứng dụng nguồn mở cho phép người dùng xem và lưu thông tin xác thực như vé Kerberos. Bộ công cụ hoạt động với bản phát hành Windows hiện tại và bao gồm các chế độ tấn công mới nhất, Những kẻ tấn công thường sử dụng Mimikatz để đánh cắp thông tin xác thực và đặc quyền leo thang: Trong hầu hết các trường hợp, phần mềm bảo vệ điểm cuối và các hệ thống chống virus sẽ phát hiện và xóa nó. Ngược lại, người kiểm thử xâm nhập sử dụng Mimikatz để phát hiện và khai thác các lỗ hổng trong magnj của bạn để bạn có thể sửa chúng. Mimikatz có thể thực hiện nhiều kỹ thuật thu thập thông tin đăng nhập như:

- **Pass-the-hash:** Windows được sử dụng để lưu trữ dữ liệu mật khẩu trong băm NTLM. Những kẻ tấn công sử dụng Mimikatz để truyền chuỗi băm đó vào máy tính đích để đăng nhập. Những kẻ tấn công không cần phải bẻ khóa mật khẩu, họ chỉ cần sử dụng chuỗi băm.
- **Pass-the-Ticket:** Các phiên bản mới hơn của dữ liệu mật khẩu Windows Store trong một cấu trúc được gọi là vé. Mimikatz cung cấp chức năng cho người chuyển vé Kerberos cho một máy tính khác và đăng nhập bằng vé người dùng đó.
- **Pass-the-Key:** Giống với Pass-the-Hash nhưng kỹ thuật này vượt qua một chìa khóa duy nhất để mạo danh người dùng từ Domain Controller.

```
.#####. mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 176409 (00000000:0002b119)
Session : Interactive from 1
User Name : sphil
Domain : SPHIL2AB1
Logon Server : SPHIL2AB1
Logon Time : 11/4/2019 2:45:19 PM
SID : S-1-5-21-3123691167-3462951650-3668972122-1000

msv :
[00000003] Primary
* Username : sphil
* Domain : SPHIL2AB1
* NTLM : d3b4230029c4a099823fd08451c14194
* SHA1 : 6d99a0126dd45d142f92d81d8bac7eb4ed458af9
tspkg :
wdigest :
* Username : sphil
* Domain : SPHIL2AB1
```

Hình ảnh 2: Cách thức hoạt động của Mimikatz.

2.3. OphCrack

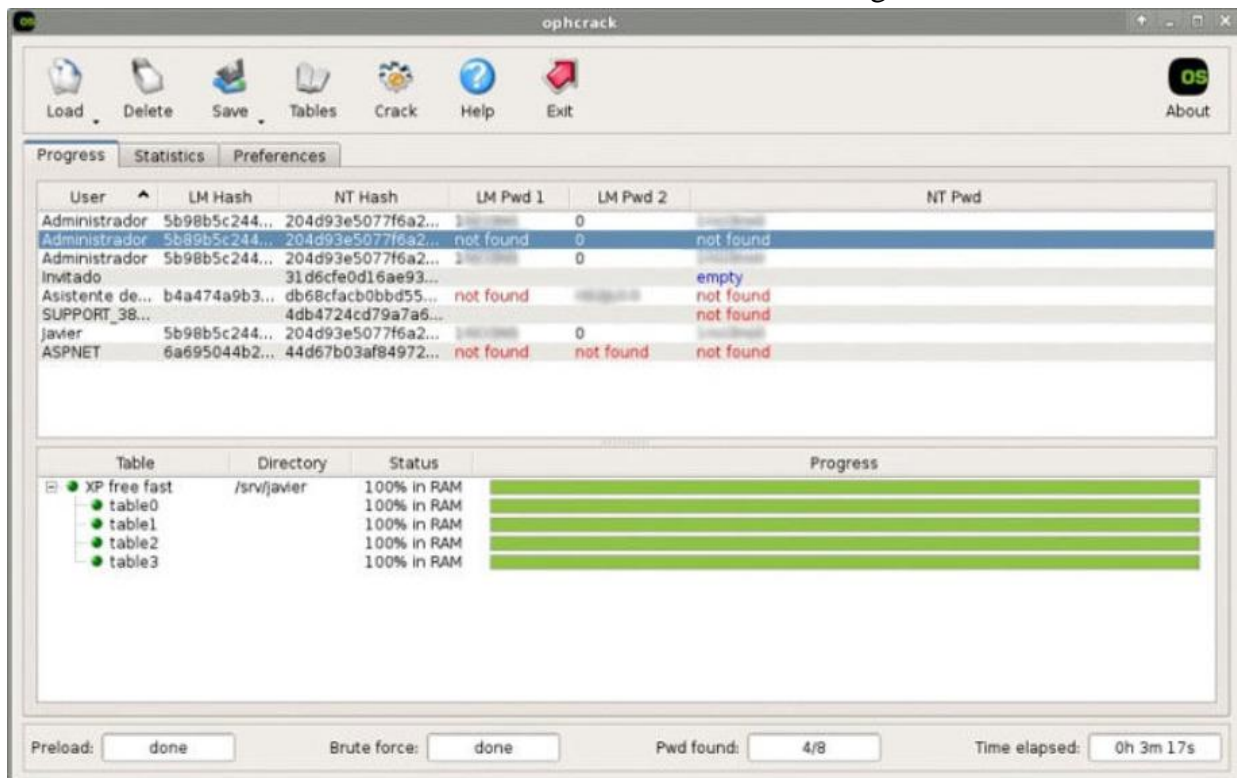
OphCrack là một bộ công cụ mã nguồn mở dùng để khôi phục mật khẩu trong hệ thống Windows. Đặc biệt, nó được sử dụng để phá mật khẩu của người dùng trên các phiên bản của hệ điều hành Windows bằng cách sử dụng kỹ thuật khai thác lỗ hổng bảo mật. OphCrack sử dụng một phương pháp gọi là “bảng màu” hoặc “rainbow table” để tìm kiếm và phục hồi mật khẩu đã mã hóa bằng cách sử dụng thuật toán băm.

OphCrack có giao diện đồ họa và rất dễ sử dụng, crack mật khẩu rất nhanh tuy nhiên các rainbow của nó khá tốn dung lượng.

OphCrack có một số đặc điểm đáng chú ý sau:

- **Mã nguồn mở:** OphCrack là một phần mềm mã nguồn mở, điều này có nghĩa là mã nguồn của nó được công khai và có thể được sửa đổi, phát hiện bởi cộng đồng người dùng. Điều này tạo điều kiện cho sự minh bạch và kiểm soát mã nguồn.
- **Hỗ trợ đa nền tảng:** OphCrack có sẵn cho nhiều nền tảng hệ điều hành, bao gồm Windows, Linux và macOS. Điều này cho phép người dùng sử dụng nó trên các hệ thống khác nhau.
- **Tích hợp tấn công từ điển và bảng mã rainbow:** Ophcrack thực hiện việc khôi phục mật khẩu bằng cách sử dụng cả tấn công từ điển và tấn công bảng mã rainbow. Điều này làm tăng cơ hội khôi phục mật khẩu thành công.
- **Giao diện đồ họa dễ sử dụng:** OphCrack cung cấp một giao diện người dùng đồ họa (GUI) thân thiện và dễ sử dụng, không yêu cầu người dùng phải có kiến thức kỹ thuật sâu.
- **Hiệu suất và thời gian khôi phục:** Thời gian để khôi phục mật khẩu có thể biến đổi tùy thuộc vào độ phức tạp của mật khẩu và khả năng của máy tính. Tuy nhiên, Ophcrack thường có hiệu suất khá tốt trong việc khôi phục mật khẩu.

- Cập nhật định kỳ: Ophcrack thường được cập nhật để hỗ trợ các phiên bản mới của hệ điều hành Windows và để cải thiện hiệu suất cũng như bảo mật.



Hình ảnh 3: Cách hoạt động của OphCrack.

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

I. Chuẩn bị môi trường

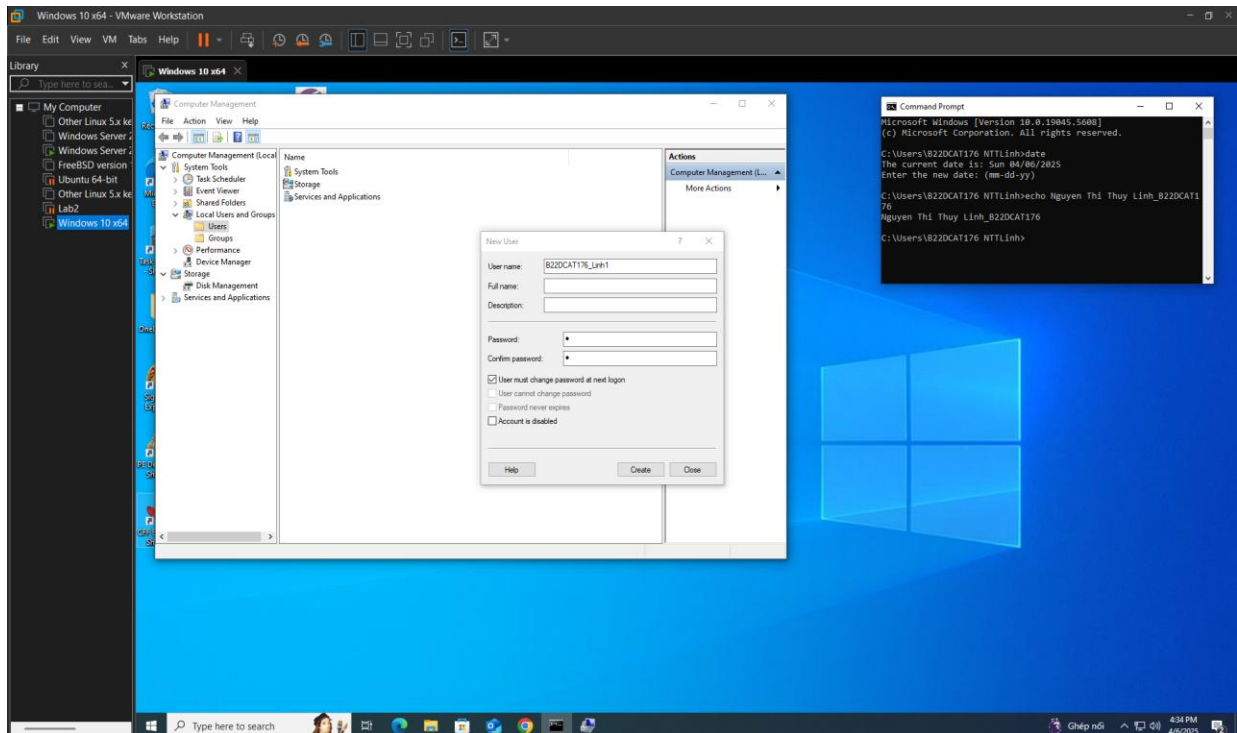
- Cài đặt công cụ ảo hóa VMWare Workstation hoặc VirtualBox hoặc phần mềm ảo hóa khác.
- Phần mềm hệ điều hành Linux và Windows.
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Linux và Windows

II. Các bước thực hiện

1. Crack mật khẩu trên Windows

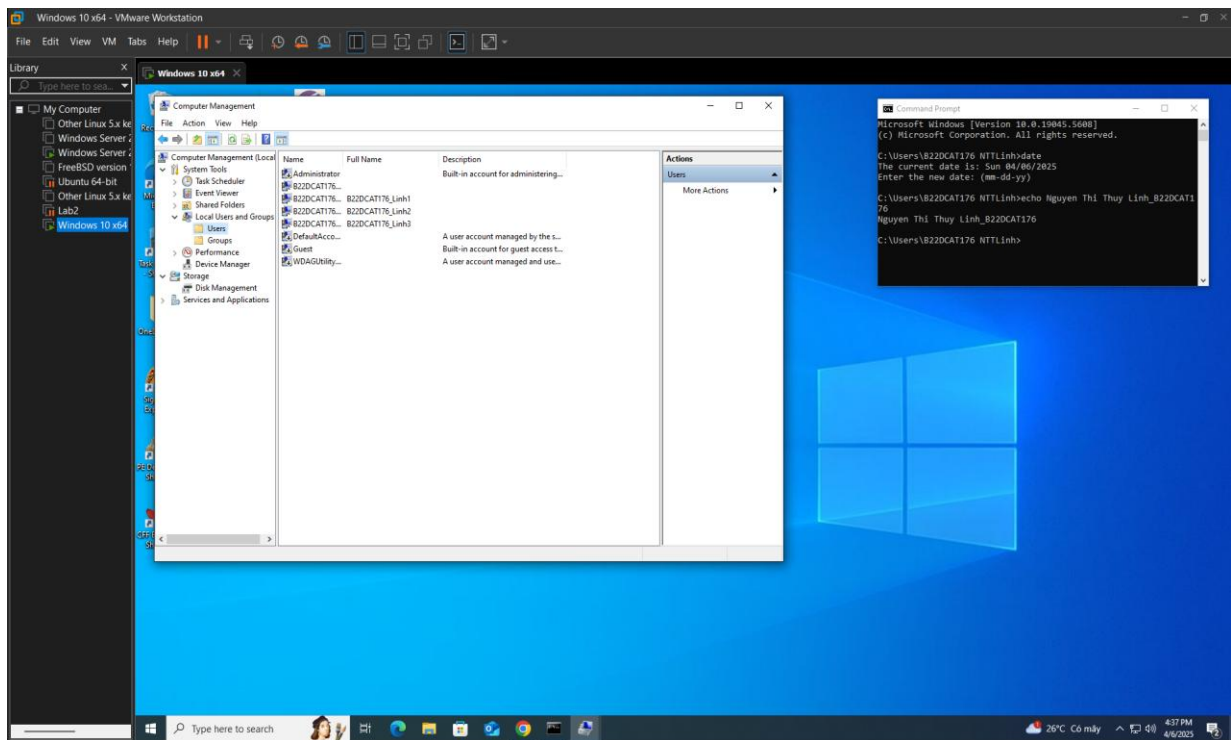
Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,... Các tên tài khoản này đều có phần đầu là mã sinh viên.

Tạo thêm 3 tài khoản trên Windows có mật khẩu thỏa mãn 4 ký tự, 6 ký tự, 8 ký tự:
Computer Management -> Local User and Group -> Chuột phải vào Users -> New User



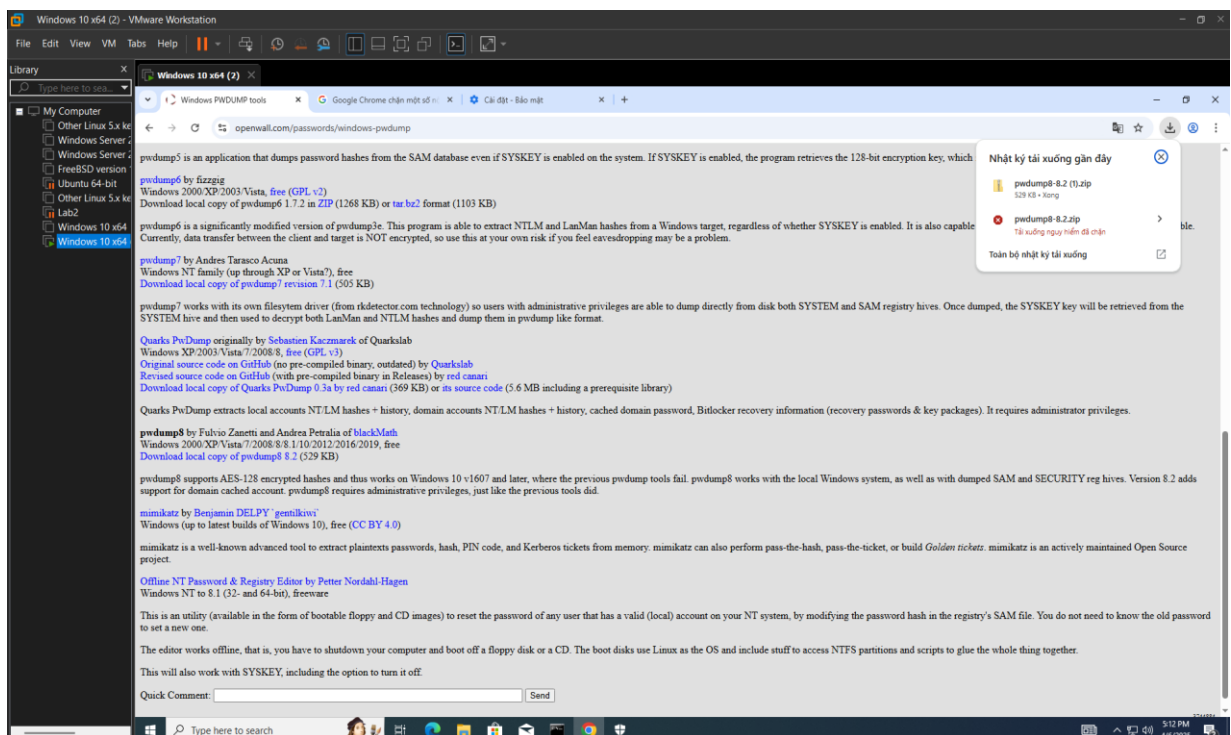
Hình ảnh 4: Tạo 3 tài khoản trên Windows.

- Kiểm tra kết quả sau khi tạo người dùng.



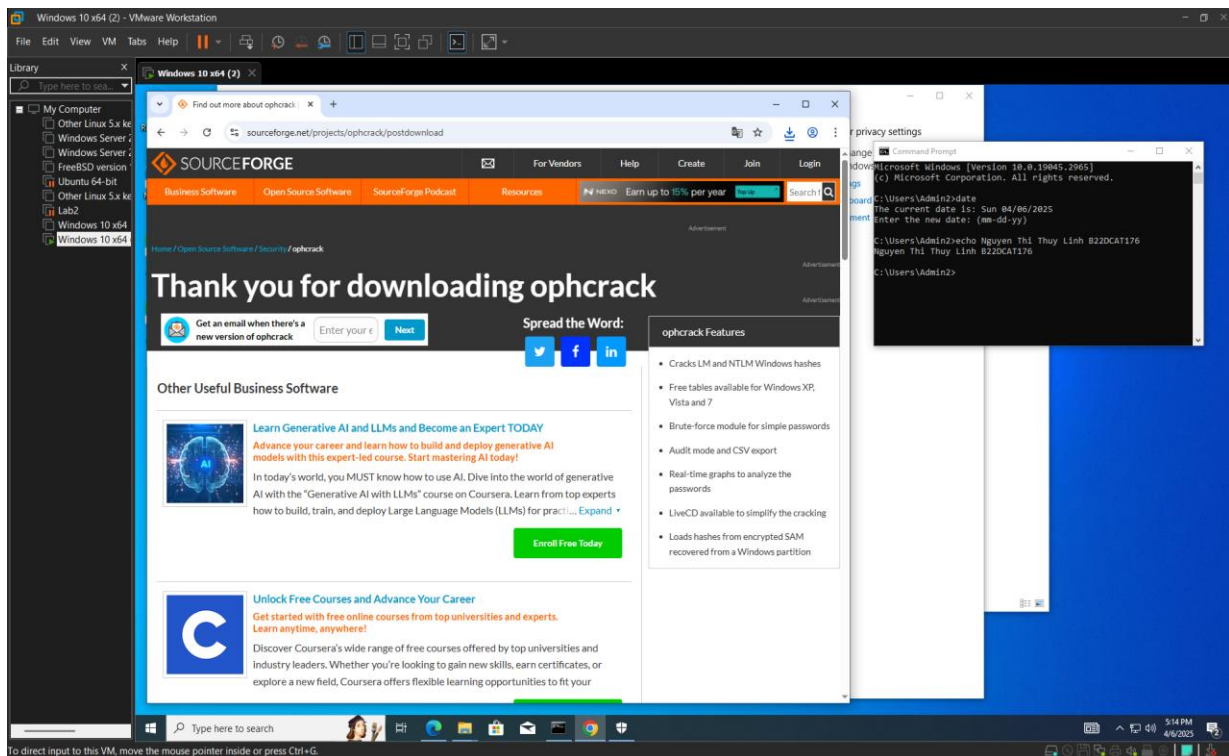
Hình ảnh 5: Kết quả sau khi tạo người dùng.

Tải công cụ PwDump8, Ophcrack (phải tải cả các Rainbow của Ophcrack)



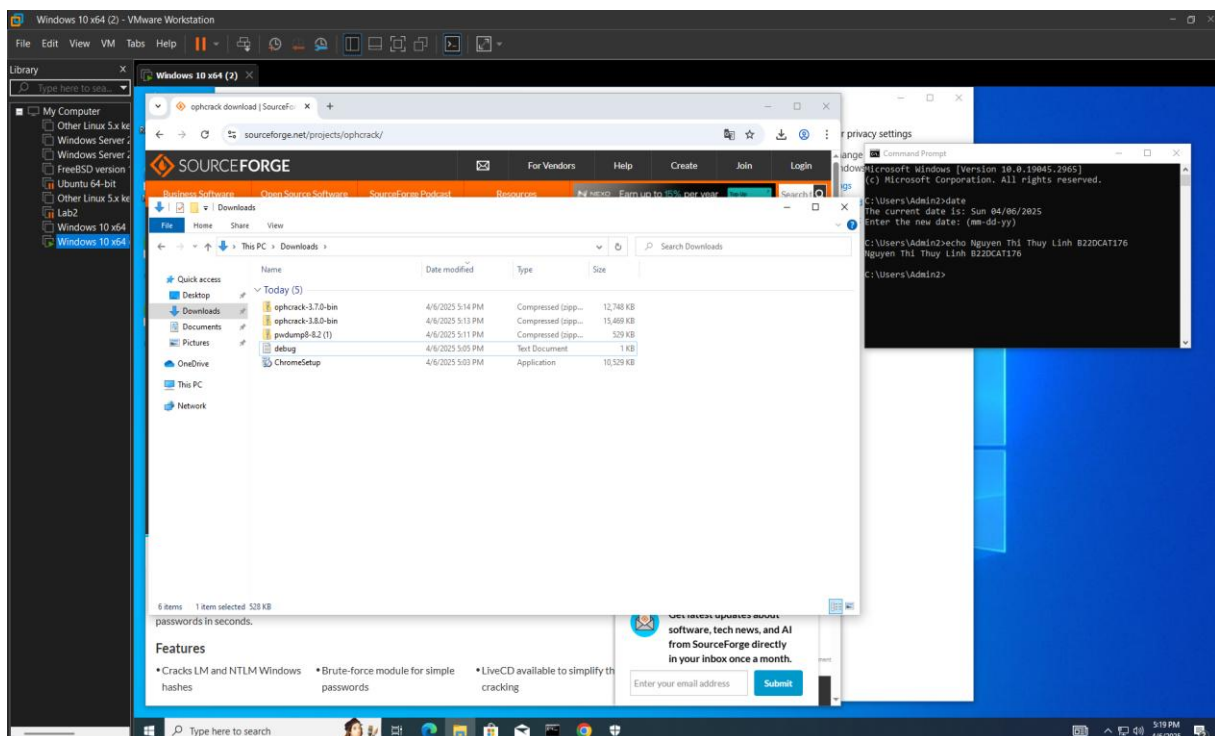
Hình ảnh 6: Tải phần mềm PwDump8.

- Tải phần mềm OphCrack và các rainbow của OphCrack.



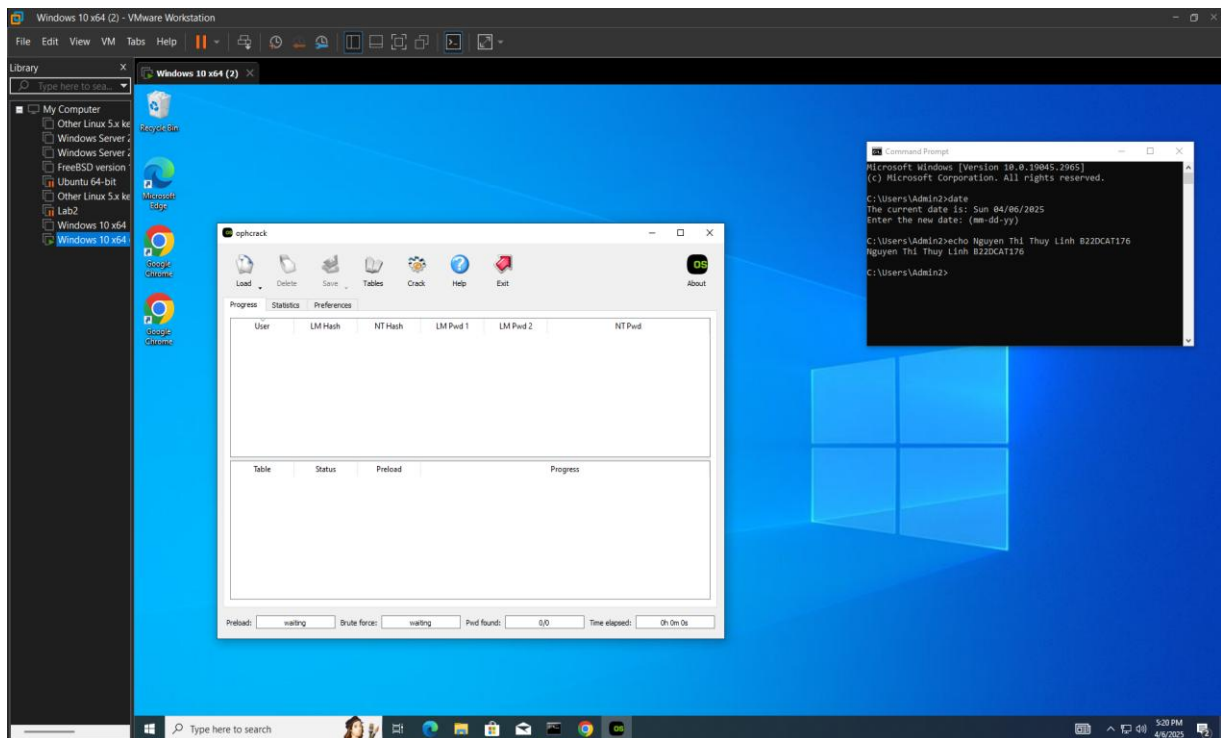
Hình ảnh 7: Cài đặt OrpCrack và rainbow của nó.

Giải nén các tập tin đã tải về và tiến hành cài đặt.



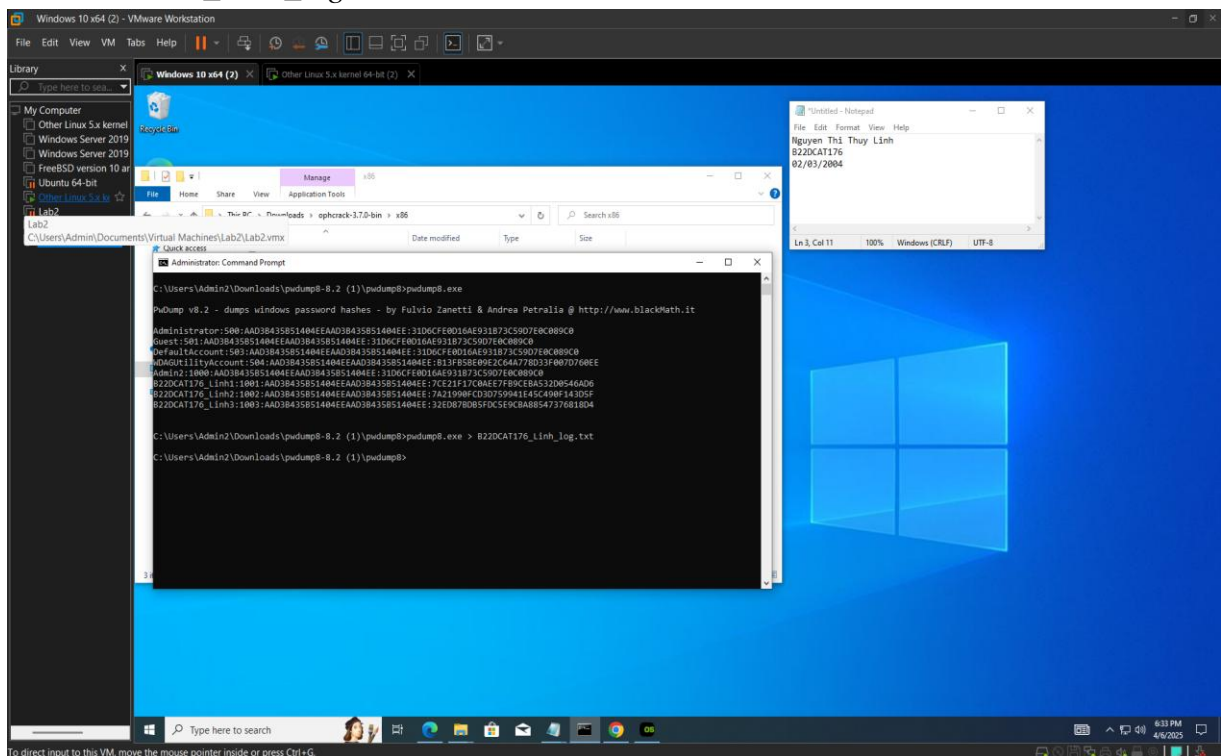
Hình ảnh 8: Giải nén các tập tin đã tải về.

-Khởi động phần mềm OphCrack.



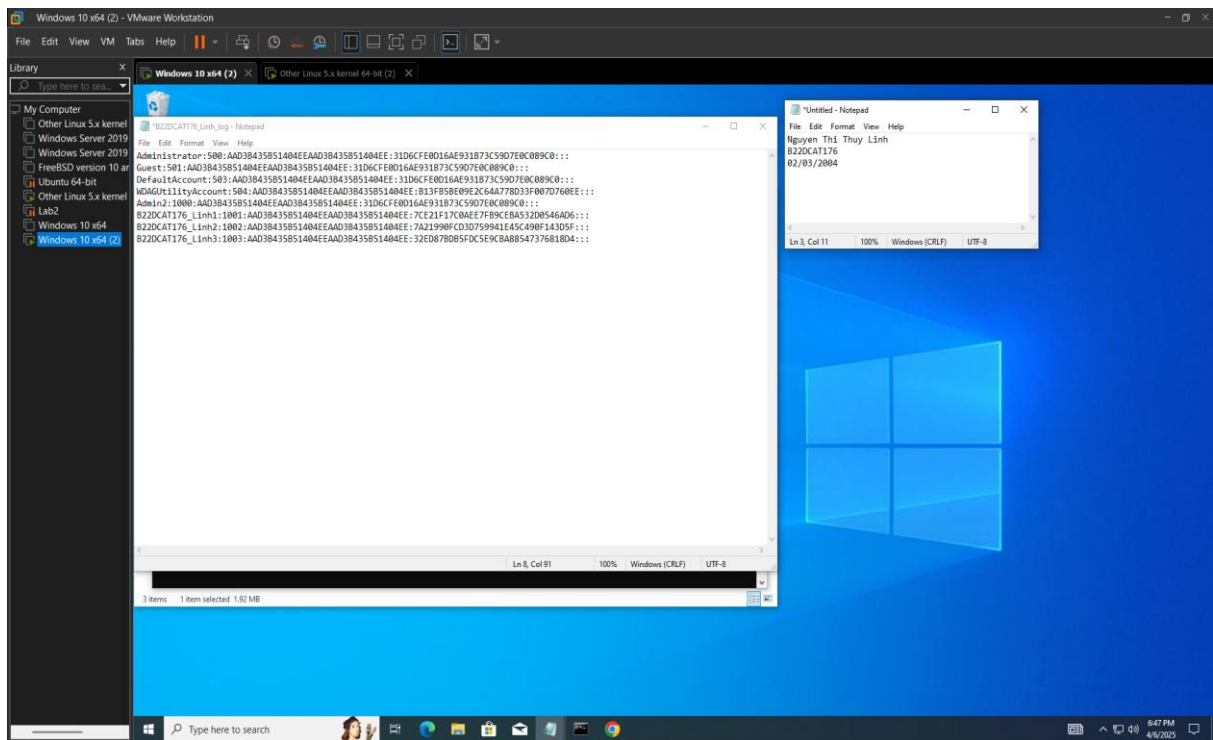
Hình ảnh 9: Khởi động phần mềm OphCrack.

Chạy Pwdump với quyền Administrator để trích xuất mật khẩu đăng nhập, đưa vào file *B22DCAT176_Linh_log.txt*



Hình ảnh 10: Chạy PwDump với quyền Administrator.

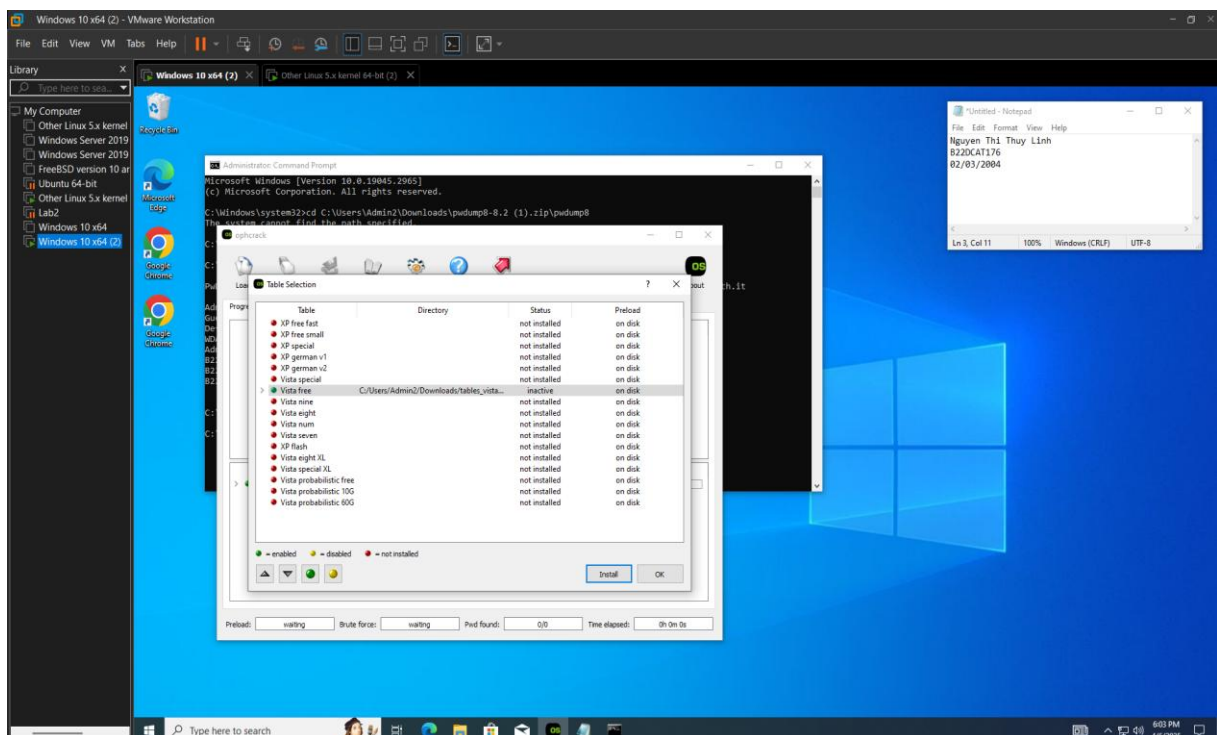
Kiểm tra lại file *B22DCAT176_Linh_log.txt*



Hình ảnh 11: Kiểm tra lại file B22DCAT176_Linh_log.txt

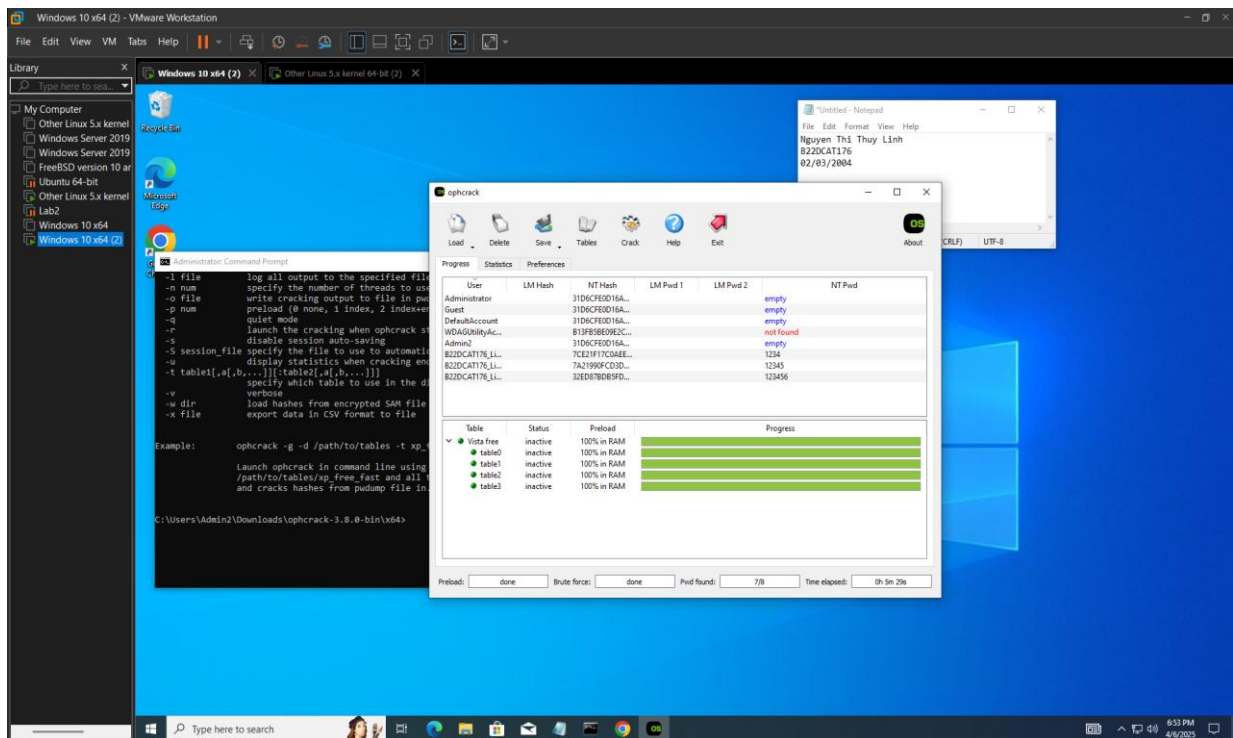
Sử dụng OphCrack để crack mật khẩu.

Đầu tiên phải kích hoạt các Rainbow đã tải: Tables -> chọn thư mục đã lưu Rainbow.



Hình ảnh 12: Kích hoạt Rainbow.

- Crack mật khẩu đã lưu trong file B22DCAT176_Linh_log.txt: Load -> PWDUMP File -> chọn File đã lưu . Đợi file tải hết.



Hình ảnh 13: Kết quả sau khi crack mật khẩu.

2. Crack mật khẩu trên Linux

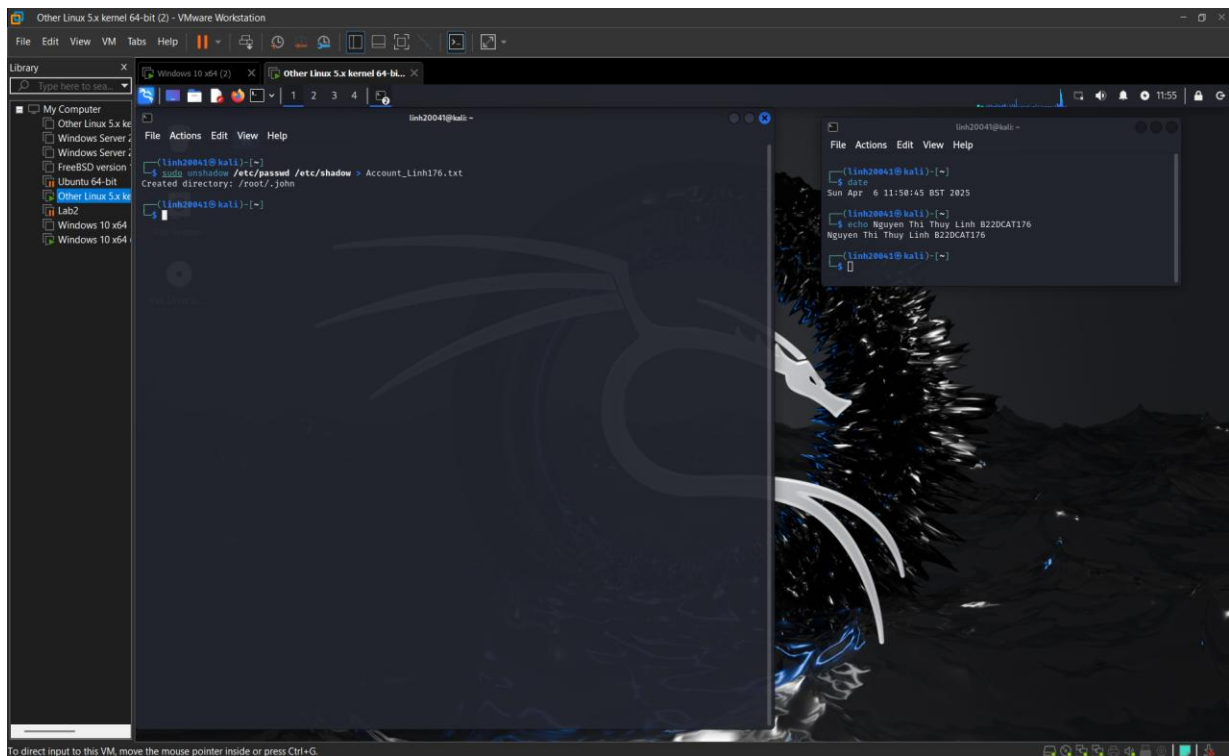
Thử nghiệm crack mật khẩu trên hệ điều hành Linux với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự... Các tên tài khoản này đều có phần mở đầu là mã sinh viên:

B22DCAT176_NguyenThiThuyLinh1

B22DCAT176_NguyenThiThuyLinh2

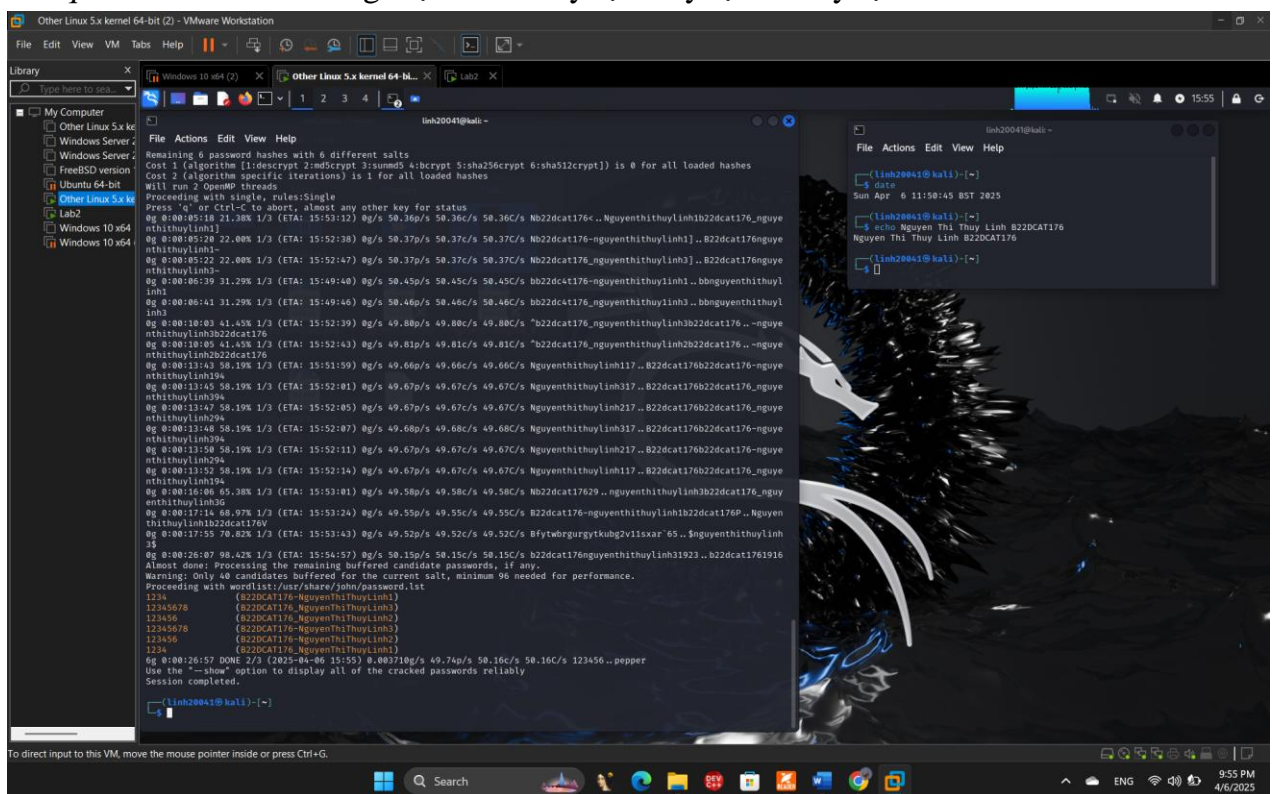
B22DCAT176_NguyenThiThuyLinh3

Sau khi tạo user thì đặt mật khẩu.



Hình ảnh 16: Kết hợp 2 file

Kết quả: Crack thành công mật khẩu 4 ký tự, 6 ký tự và 8 ký tự.



Hình ảnh 17: Crack thành công mật khẩu 8 ký tự.

TÀI LIỆU THAM KHẢO

- [1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.