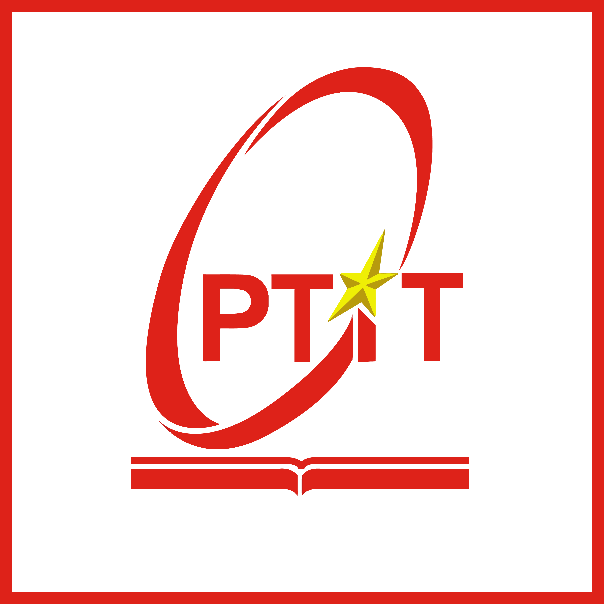
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



Môn học: **THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 12**

**TẤN CÔNG MẬT KHẨU**

|  |
| --- |
| Sinh viên thực hiện: Lê Anh Tuấn |
| Mã sinh viên: B21DCAT205 |
| Giảng viên: Ninh Thị Thu Trang |

~ Hà Nội, tháng 4/2024 ~

**Mục Lục**

[**1** **Mục đích** 2](#_Toc164546124)

[**2** **Nội dung thực hành** 2](#_Toc164546125)

[2.1 Tìm hiểu lý thuyết 2](#_Toc164546126)

[2.1.1 Chương trình Password Cracker 2](#_Toc164546127)

[2.1.2 Các dạng Password attack 2](#_Toc164546128)

[2.1.3 Giới thiệu công cụ John the Ripper 3](#_Toc164546129)

[2.1.4 Mimikatz 3](#_Toc164546130)

[2.2 Nội dung thực hành. 4](#_Toc164546131)

[2.2.1 Chuẩn bị môi trường 4](#_Toc164546132)

[2.2.2 Thực hành 9](#_Toc164546133)

[**3** **Kết luận** 17](#_Toc164546134)

[**4** **Tài liệu tham khảo** 17](#_Toc164546135)

**Bài 12: Tấn công mật khẩu**

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. **Nội dung thực hành**
2. **Tìm hiểu lý thuyết**
3. **Chương trình Password Cracker**

– Password cracker là một công cụ mạnh mẽ trong lĩnh vực thử nghiệm bảo mật và nghiên cứu an ninh mạng. Chức năng chính của nó là phá vỡ mật khẩu, giúp người sử dụng truy cập vào hệ thống, tài khoản, hoặc dữ liệu đã được bảo vệ. Các password cracker thường sử dụng nhiều phương pháp để tìm ra mật khẩu, bao gồm Brute Force (tự động thử tất cả các khả năng có thể), Dictionary Attacks (tấn công từ điển sử dụng danh sách từ khóa thông dụng), và Rainbow Tables (sử dụng bảng băm tiền xử lý).

– Mặc dù password cracker có thể hữu ích trong việc đánh giá sức mạnh của mật khẩu và tìm ra các lỗ hổng bảo mật, nhưng cũng tồn tại nguy cơ lạm dụng chúng để thực hiện các hành động xâm nhập và tấn công. Do đó, việc sử dụng password cracker cần phải tuân thủ các nguyên tắc và quy định etic trong lĩnh vực an toàn thông tin.

– Đối mặt với password cracker, người quản trị hệ thống cần triển khai các biện pháp bảo mật mạnh mẽ, bao gồm sử dụng mật khẩu phức tạp, kích thước mật khẩu đủ lớn, cập nhật đều đặn mật khẩu, và triển khai các biện pháp như Two-Factor Authentication (2FA) để tăng cường bảo mật. Sự hiểu biết vững về password cracker cũng giúp chuyên gia an toàn thông tin ngăn chặn và phản ứng nhanh chóng trước những mối đe dọa liên quan đến việc phá mật khẩu trong môi trường mạng. Trên hệ thống Windows và Linux có hai tài khoản toàn quyền trong hệ thống đó là: root và Administrator, và mục tiêu tấn công là tìm được password của hai tài khoản đó

– Cách các chương trình Password Cracker hoạt động là: Mật khẩu sau khi được tạo ra và lưu vào trong hệ thống sẽ được mã hóa, hệ thống sẽ chứa Key để giải mã mật khẩu. Những phần mềm Password Cracker sẽ tìm cách lấy được các đoạn mật mã đó. Sau khi đã lấy được các đoạn mật mã trên máy của nạn nhân chúng sẽ tiến hành giải mã mật khẩu bằng những phương thức cụ thể cho từng tình huống.

1. **Các dạng Password attack**

– Dictionary Attack: Tìm mật khẩu trong một file từ điển tạo sẵn

– Brute Force Attack: Tìm mật khẩu bằng cách tổ hợp các ký tự

– Hybird Attack: Lai giữa hai phương thức trên

– Smart Table Recovery Attack: Phương thức tấn công tìm mật khẩu thông minh nhất dựa trên các bảng dữ liệu – Khoảng 700MB dữ liệu text.

1. **Giới thiệu công cụ John the Ripper**

John the Ripper là một phần mềm mã nguồn mở được sử dụng để phá mã các mật khẩu, được sử dụng rộng rãi trong lĩnh vực bảo mật và thử thách độ mạnh của mật khẩu. John the Ripper có khả năng phá mật khẩu của nhiều định dạng tập tin khác nhau bao gồm các định dạng thông dụng như ZIP, PDF, RAR, MS Office, và các hệ thống xác thực Unix, Windows, và hơn thế nữa.

Phần mềm John the Ripper có khả năng sử dụng nhiều chiến thuật khác nhau để tìm kiếm mật khẩu và phá mã, bao gồm Brute Force (tấn công mật khẩu bằng việc thử tất cả các khả năng), Dictionary Attack (tấn công bằng cách thử các từ trong từ điển), Hybrid Attack (kết hợp Brute Force và Dictionary Attack), và nhiều phương pháp khác.John theRipper cũng hỗ trợ việc sử dụng các rule-basedattack (tấn công theo quy tắc), cho phép người dùng chỉ định các quy tắc cụ thể để giúp tăng khả năng tìm ra mật khẩu chính xác hơn.

John the Ripper có nhiều chế độ khác nhau để thực hiện các cuộc tấn công tìm kiếm mật khẩu khác nhau. Sau đây là một số chế độ phổ biến của John the Ripper:

- Single mode: Chế độ này sử dụng cho việc tìm kiếm mật khẩu của một tài khoản cụ thể. John the Ripper sẽ sử dụng từ điển mật khẩu hoặc tấn công brute-force để tìm kiếm mật khẩu cho tài khoản đó.

- Wordlist mode: Chế độ này sử dụng một danh sách các từ để tìm kiếm mật khẩu. John the Ripper sẽ kiểm tra các từ trong danh sách để xác định xem chúng có phải là mật khẩu cho tài khoản đó hay không.

- Incremental mode: Chế độ này sử dụng để thực hiện tấn công brute-force trên mật khẩu. John the Ripper sẽ thử tất cả các ký tự có thể trong mật khẩu,bắt đầu từ ký tự đầu tiên đến ký tự cuối cùng. Khi thử hết các ký tự, John the Ripper sẽ tăng độ dài mật khẩu lên một ký tự và bắt đầu lại quá trình tấn công từ đầu.

- Rule-based mode: Chế độ này sử dụng các quy tắc để thay đổi hoặc kết hợp các từ trong từ điển mật khẩu để tạo ra các mật khẩu mới. Quy tắc có thể là thay đổi các ký tự thành các chữ số hoặc các ký tự đặc biệt, hoặc thêm các ký tự đặc biệt vào mật khẩu.

- GPU mode: Chế độ này sử dụng các card đồ họa để tăng tốc độ thực hiện các cuộc tấn công. Các card đồ họa có khả năng tính toán song song nên chế độ này có thể cải thiện tốc độ tấn công rất đáng kể so với sử dụng CPU.

1. **Mimikatz**

Mimikatz là một công cụ đặc biệt quan trọng và đồng thời đầy nhiệm vụ trong lĩnh vực nghiên cứu bảo mật và kiểm thử hệ thống Windows. Được sáng tạo bởi Benjamin Delpy, một nhà nghiên cứu bảo mật hàng đầu, Mimikatz đã trở thành một công cụ không thể phổ qua trong cộng đồng an toàn thông tin. Mục tiêu chính của nó là phân tích và hiểu rõ cơ chế chứng thực trong hệ điều hành Windows, đặc biệt là khả năng khai thác các lỗ hổng bảo mật liên quan đến mật khẩu.

Mimikatz có khả năng đọc mật khẩu trực tiếp từ bộ nhớ của máy tính, bao gồm cả mật khẩu NTLM và các phiên bản đã được mã hóa của chúng. Công cụ này cũng có khả năng thực hiện tấn công Pass-the-Hash, một kỹ thuật tấn công mà không cần biết mật khẩu gốc, chỉ cần thông tin băm (hash) của mật khẩu. Điều này làm cho Mimikatz trở thành một công cụ mạnh mẽ trong tay những người muốn kiểm thử bảo mật hệ thống của mình và hiểu rõ về các mối đe dọa có thể đối mặt từ các kỹ thuật tấn công này. Một số chức năng của Mimikatz bao gồm:

– Lấy mật khẩu đăng nhập của người dùng trên hệ thống Windows.

– Lấy các thông tin chứng chỉ, bảo mật và quản lý thông tin từ bộ nhớ hệ thống.

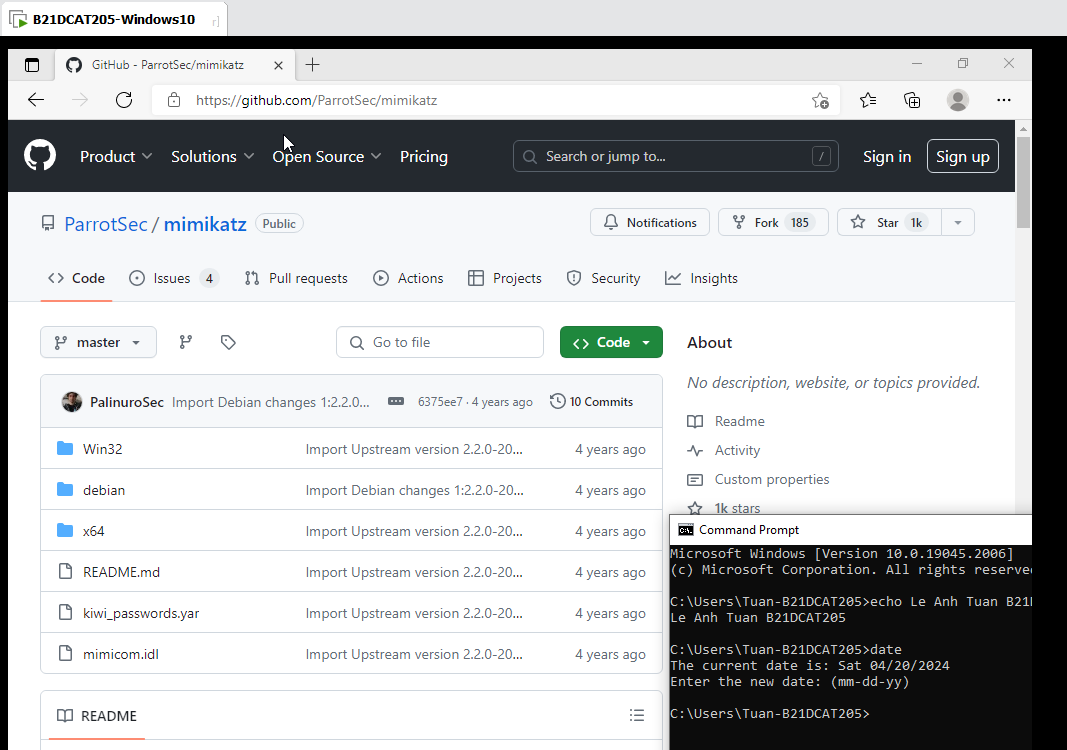
– Thực hiện tấn công Pass-the-Hash để đăng nhập vào hệ thống với tư cách của người dùng đã bị lấy mật khẩu.

– Thực hiện tấn công Golden Ticket để giả mạo giấy phép của người dùng để đăng nhập vào hệ thống.

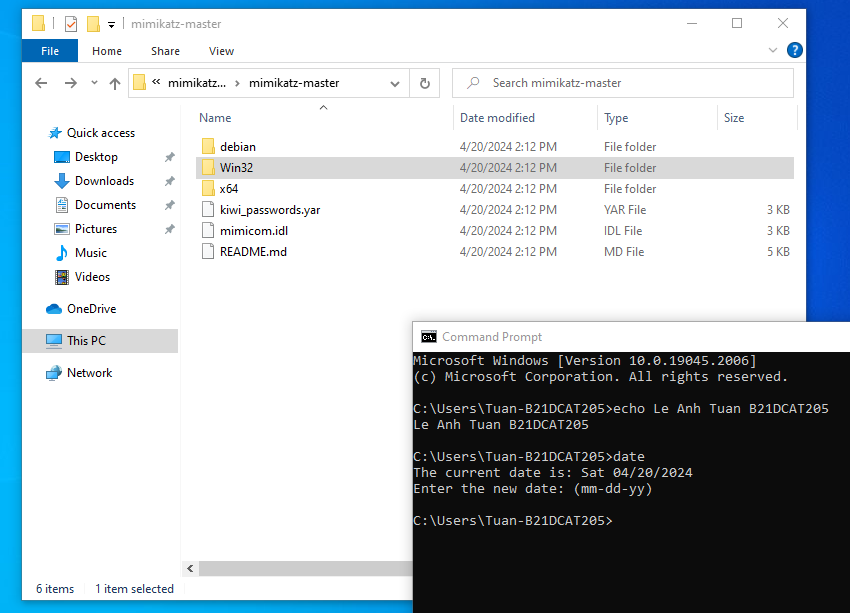
Tuy nhiên, Mimikatz cũng là một công cụ có thể được sử dụng để tấn công và gây tổn hại cho hệ thống của người khác. Vì vậy, việc sử dụng Mimikatz nên được thực hiện một cách cẩn thận và chỉ với mục đích nghiên cứu và kiểm tra tính bảo mật của hệ thống của chính mình hoặc được sự cho phép của chủ sở hữu hệ thống

1. **Nội dung thực hành.**
2. **Chuẩn bị môi trường**

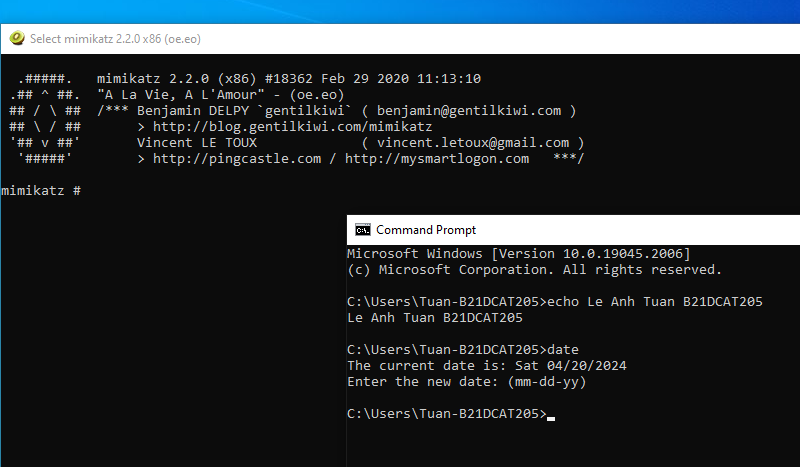
* **Trên Windows, tải công cụ mimikatz và john the ripper**

****

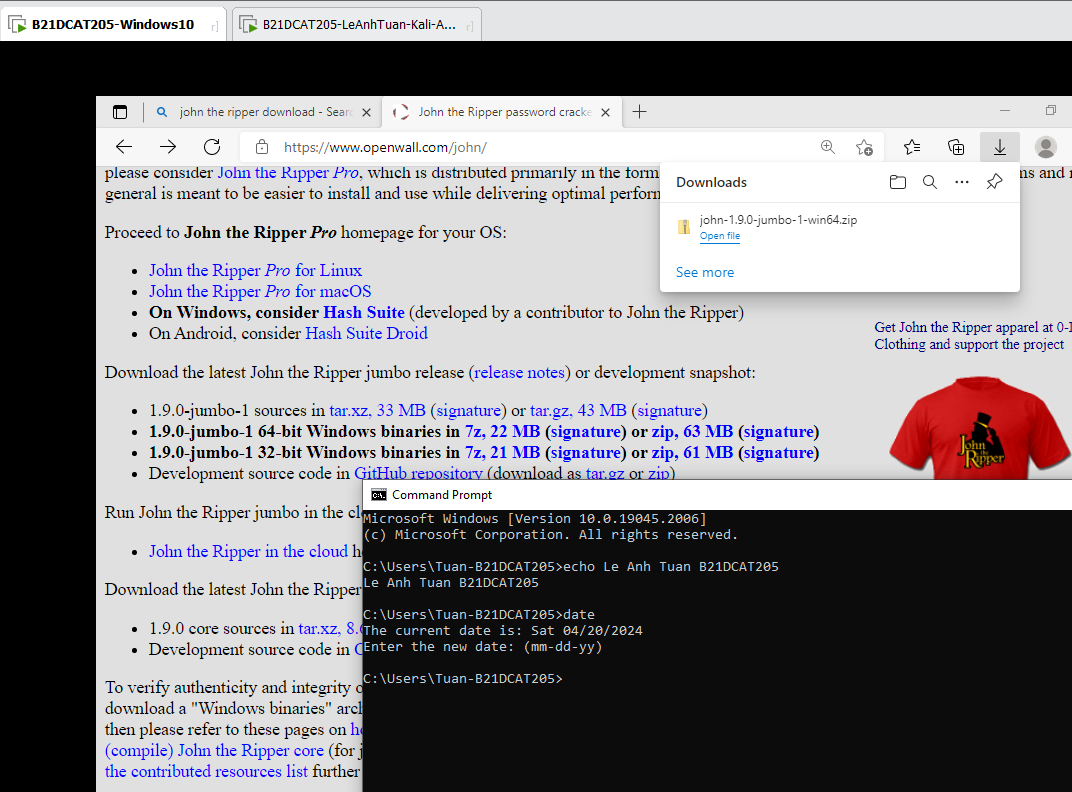
Hình 1: Download mimikatz từ github

****

Hình 2: Download thành công mimikatz

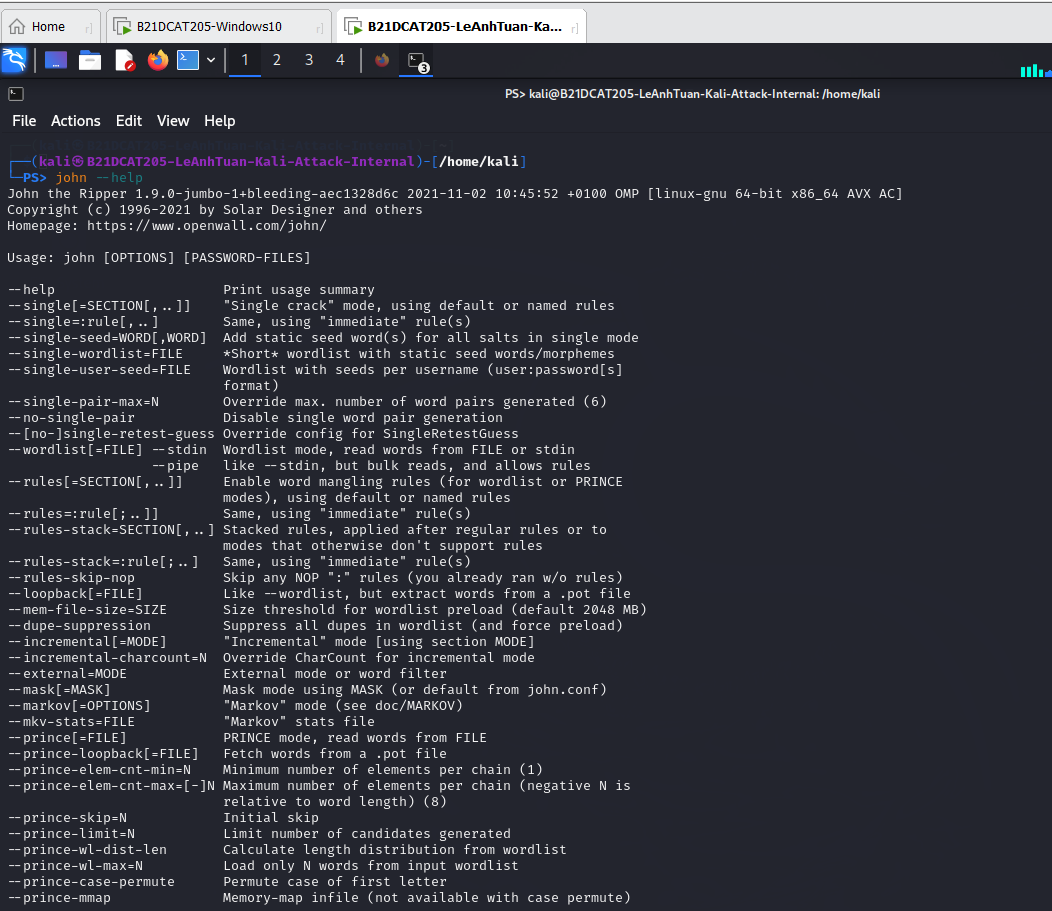
****

Hình 3: Giao diện mimikatz trên cmd

****

Hình 4: Tải John The Ripper trên Windows

* **Trên Kali, john the ripper có sẵn**

****

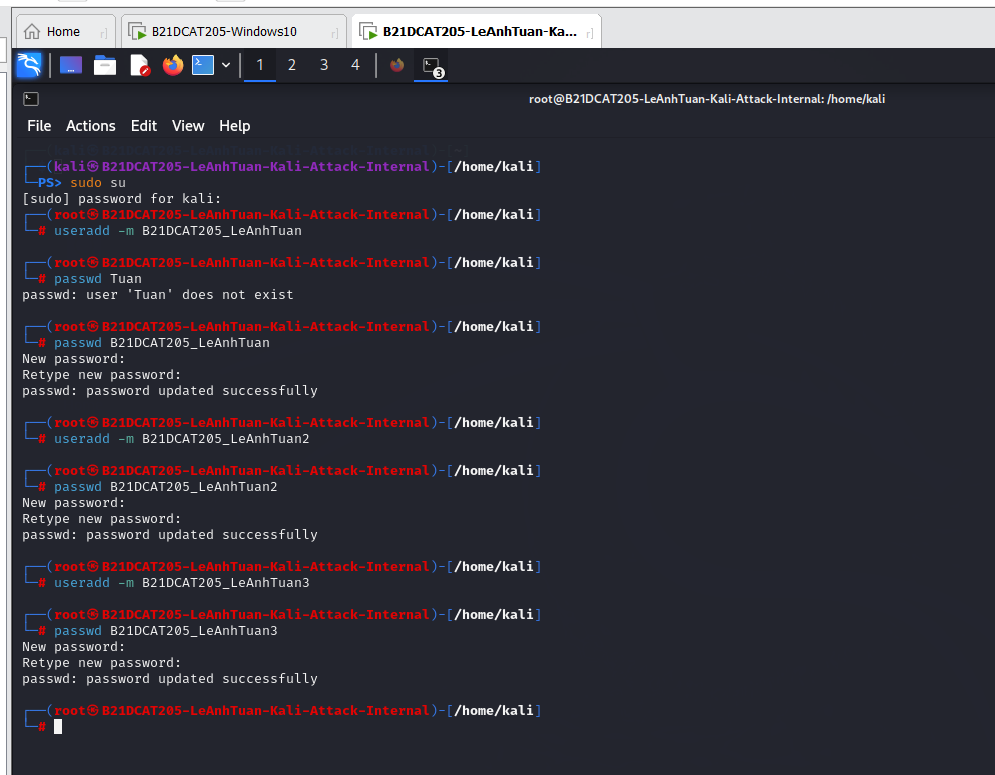
Hình 5: Kiểm tra phiên bản John The Ripper

1. **Thực hành**

* **Trên Kali:**

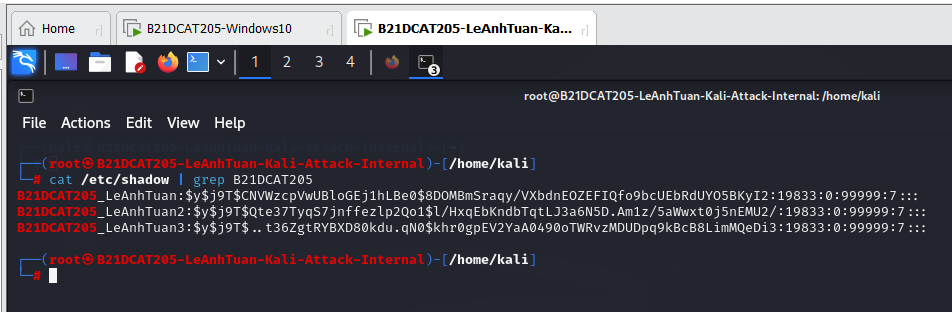
Tạo người dùng với tài khoản và mật khẩu như sau:

|  |  |
| --- | --- |
| Tài khoản | Mật khẩu |
| B21DCAT205\_LeAnhTuan | 1234 |
| B21DCAT205\_LeAnhTuan2 | 123456 |
| B21DCAT205\_LeAnhTuan3 | 12345678 |

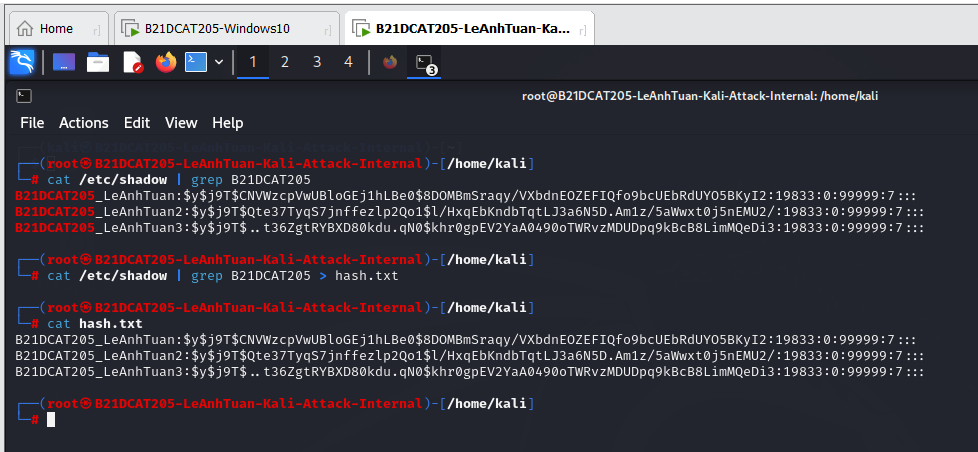
****

Hình 6: Thêm người dùng

Tạo người dùng thành công, mật khẩu được băm và lưu trong **/etc/shadow.**

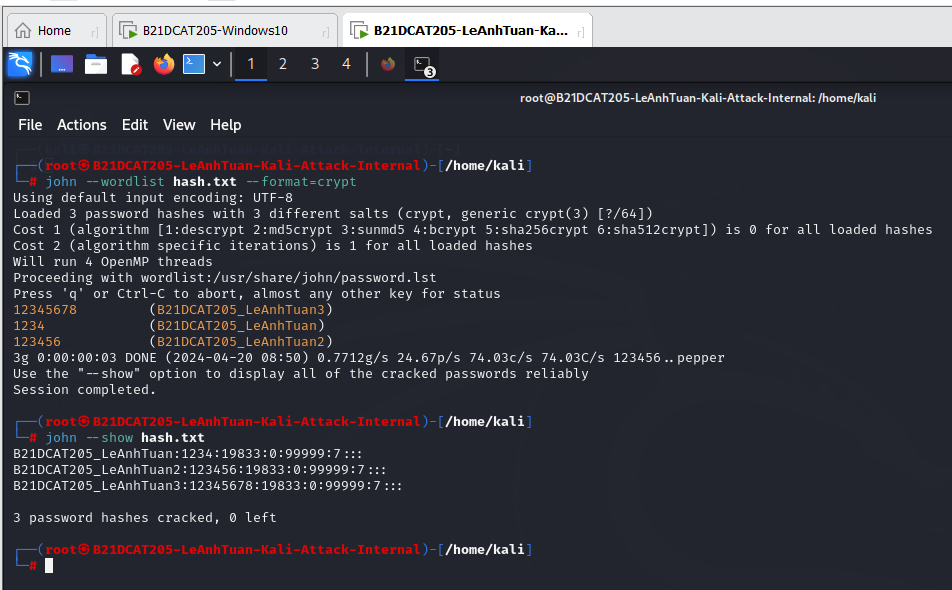
****

Hình 7: Mật khẩu được lưu trong /etc/shadow

****

Hình 8: Lưu thông tin vào file hash.txt

Sử dụng câu lệnh john –wordlist hash.txt –format=crypt

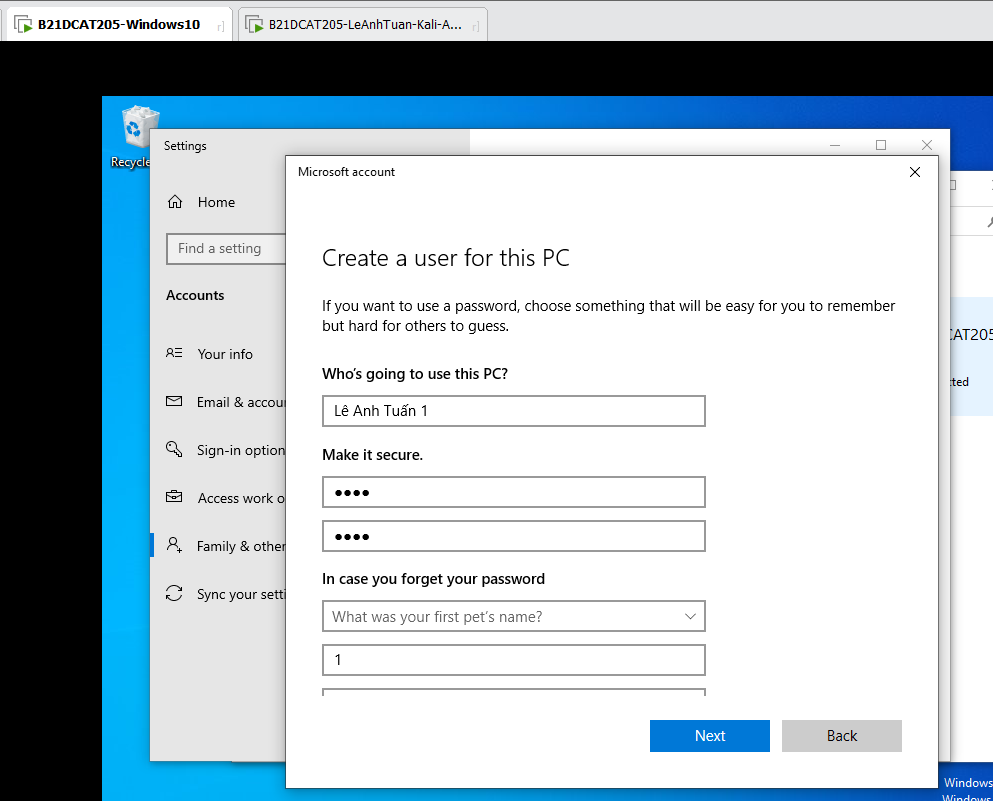
****

Hình 9:Crack mật khẩu thành công

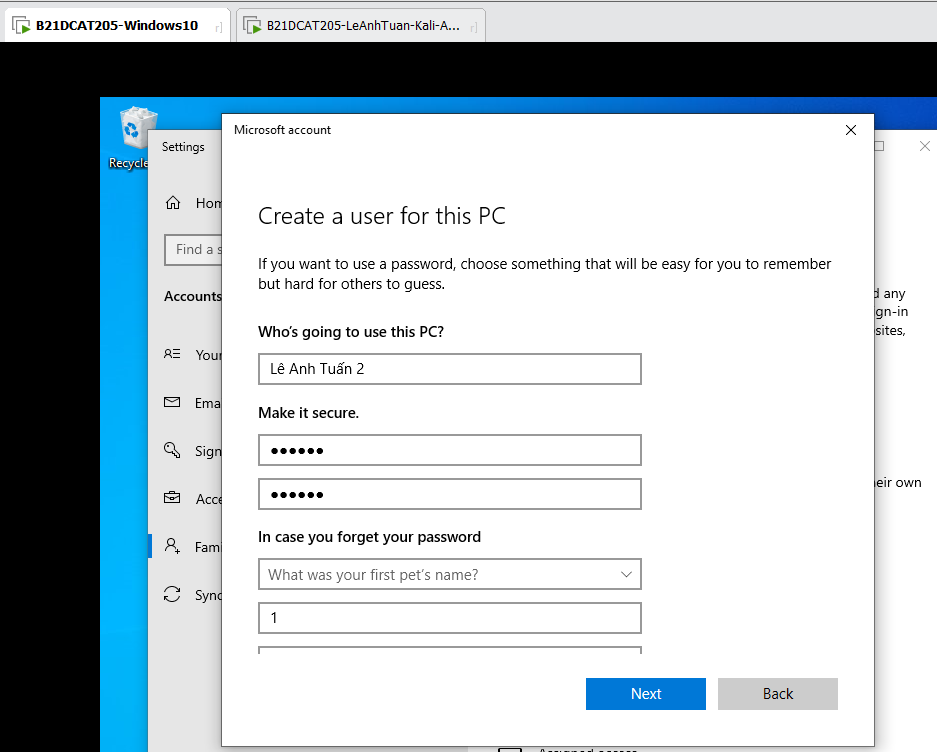
* **Trên Windows:**

Tạo người dùng với tài khoản và mật khẩu như sau:

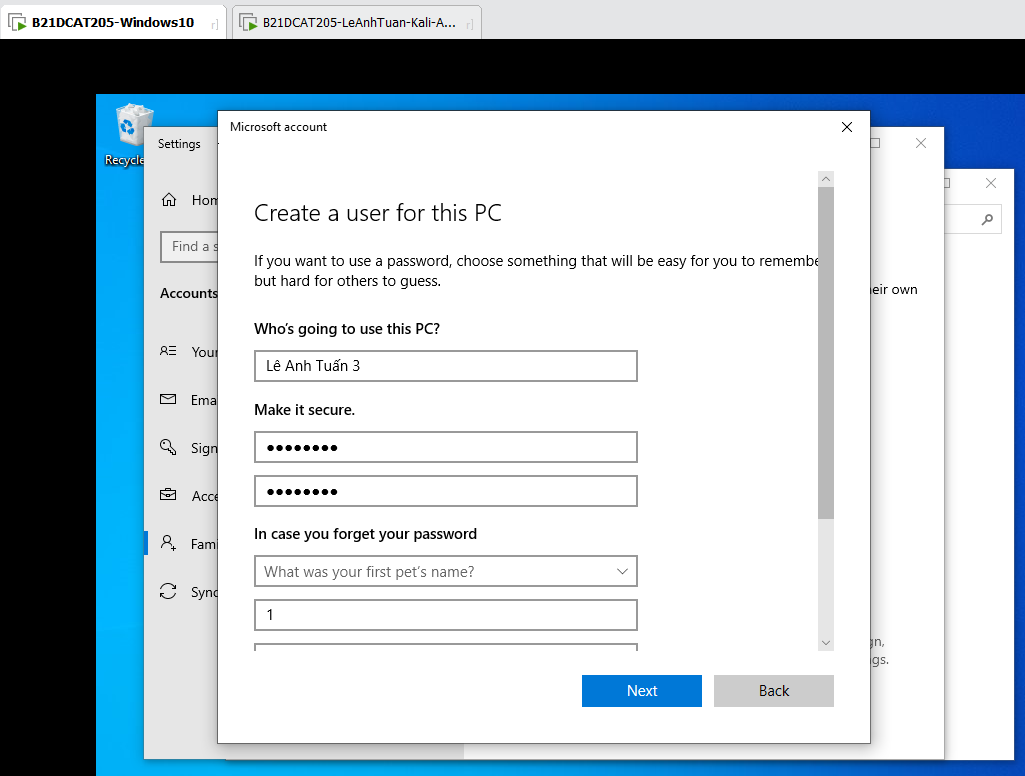
|  |  |
| --- | --- |
| Tài khoản | Mật khẩu |
| Lê Anh Tuấn 1 | 1234 |
| Lê Anh Tuấn 2 | 123456 |
| Lê Anh Tuấn 3 | 12345678 |



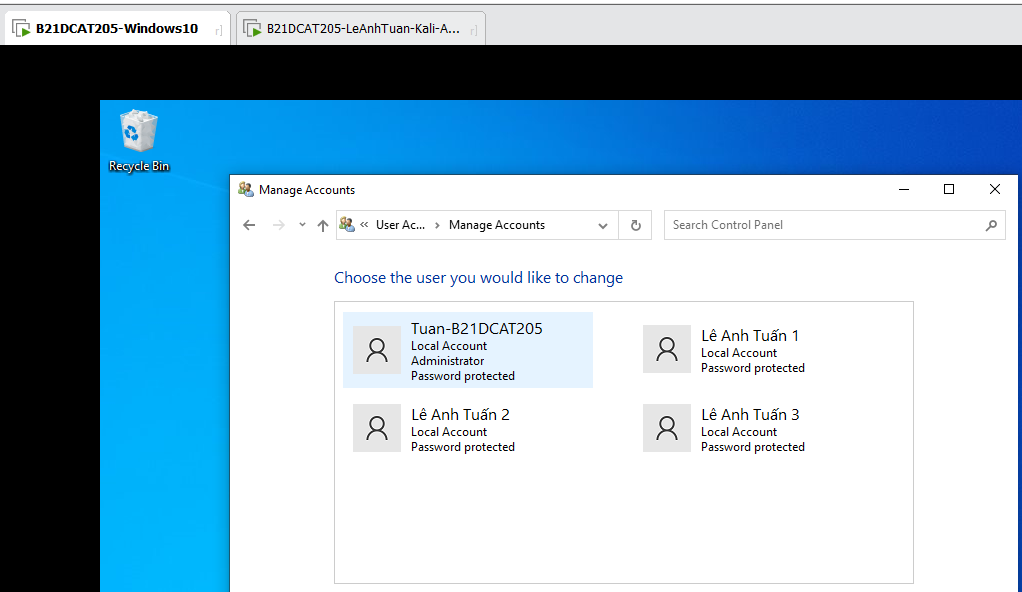
Hình 10: Tạo tài khoản với 4 ký tự số

****

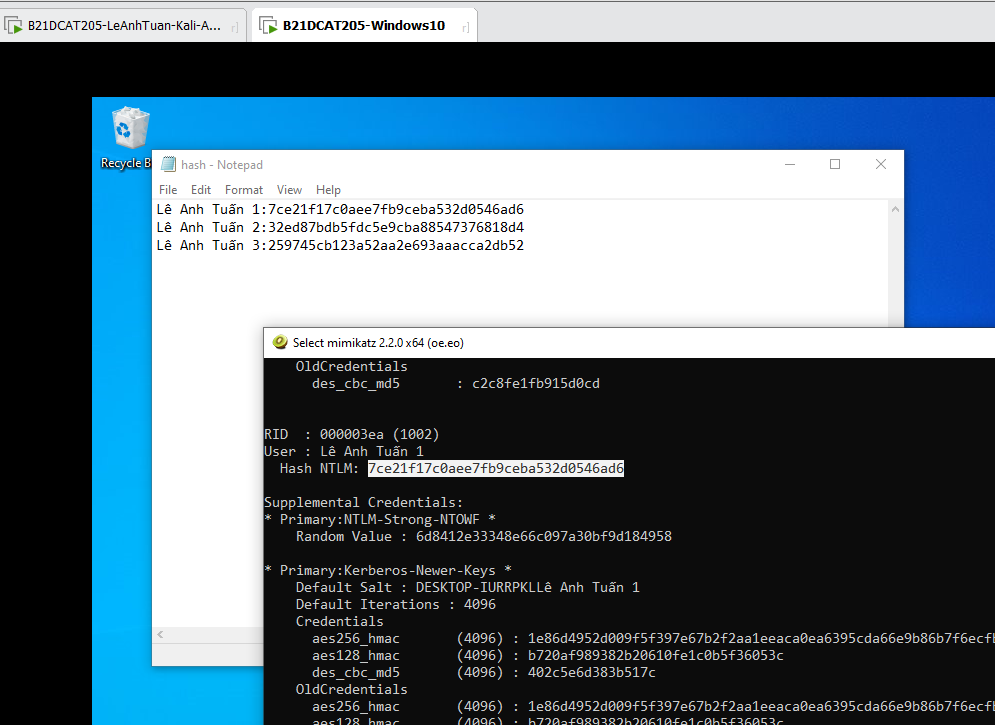
Hình 11: Tạo tài khoản với 6 ký tự số

****

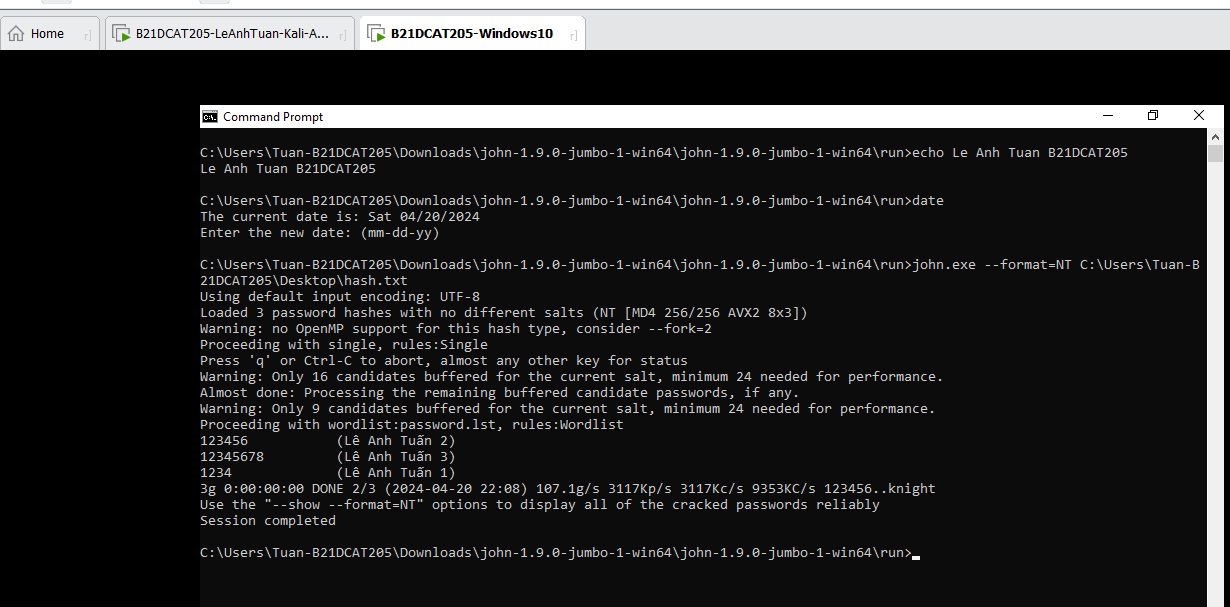
Hình 12: Tạo tài khoản với 8 ký tự số

****

Hình 13: Các người dùng sau khi được thêm

****

Hình 14: Tại dùng Hash NTLM lưu vào 1 file hash.txt

****

Hình 15: Crack mật khẩu thành công

1. **Kết luận**

* Qua bản báo cáo trên, ta đã đi tìm hiểu về mối đe dọa của việc tấn công mật khẩu, cách khai thác tấn công và crack mật khẩu bằng các công cụ. Kết quả ta đã hoàn thành được các mục đích mà bài yêu cầu.

1. **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. Weissm