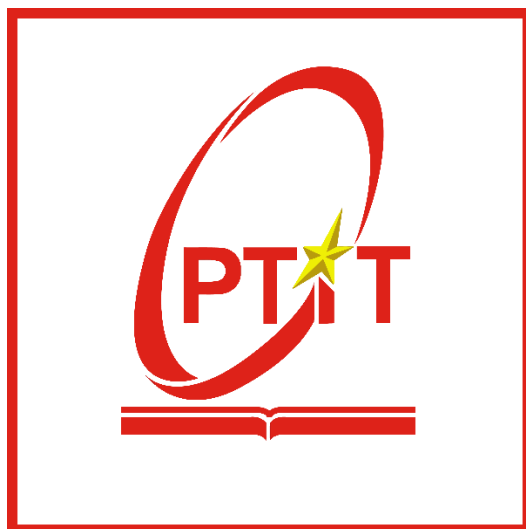


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**



**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

<b>1</b>	<b>Mục đích .....</b>	<b>2</b>
<b>2</b>	<b>Nội dung thực hành.....</b>	<b>2</b>
2.1	Tìm hiểu lý thuyết .....	2
2.1.1	Chương trình Password Cracker.....	2
2.1.2	Các dạng Password attack .....	2
2.1.3	Giới thiệu công cụ John the Ripper .....	3
2.1.4	Mimikatz .....	3
2.2	Nội dung thực hành. ....	4
2.2.1	Chuẩn bị môi trường .....	4
2.2.2	Thực hành.....	9
<b>3</b>	<b>Kết luận .....</b>	<b>17</b>
<b>4</b>	<b>Tài liệu tham khảo .....</b>	<b>17</b>

## 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.

### 2 Nội dung thực hành

#### 2.1 Tìm hiểu lý thuyết

##### 2.1.1 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.

##### 2.1.2 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

- Hybrid 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.

### 2.1.3 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 the Ripper cũng hỗ trợ việc sử dụng các rule-based attack (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.

### 2.1.4 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 phủ 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:

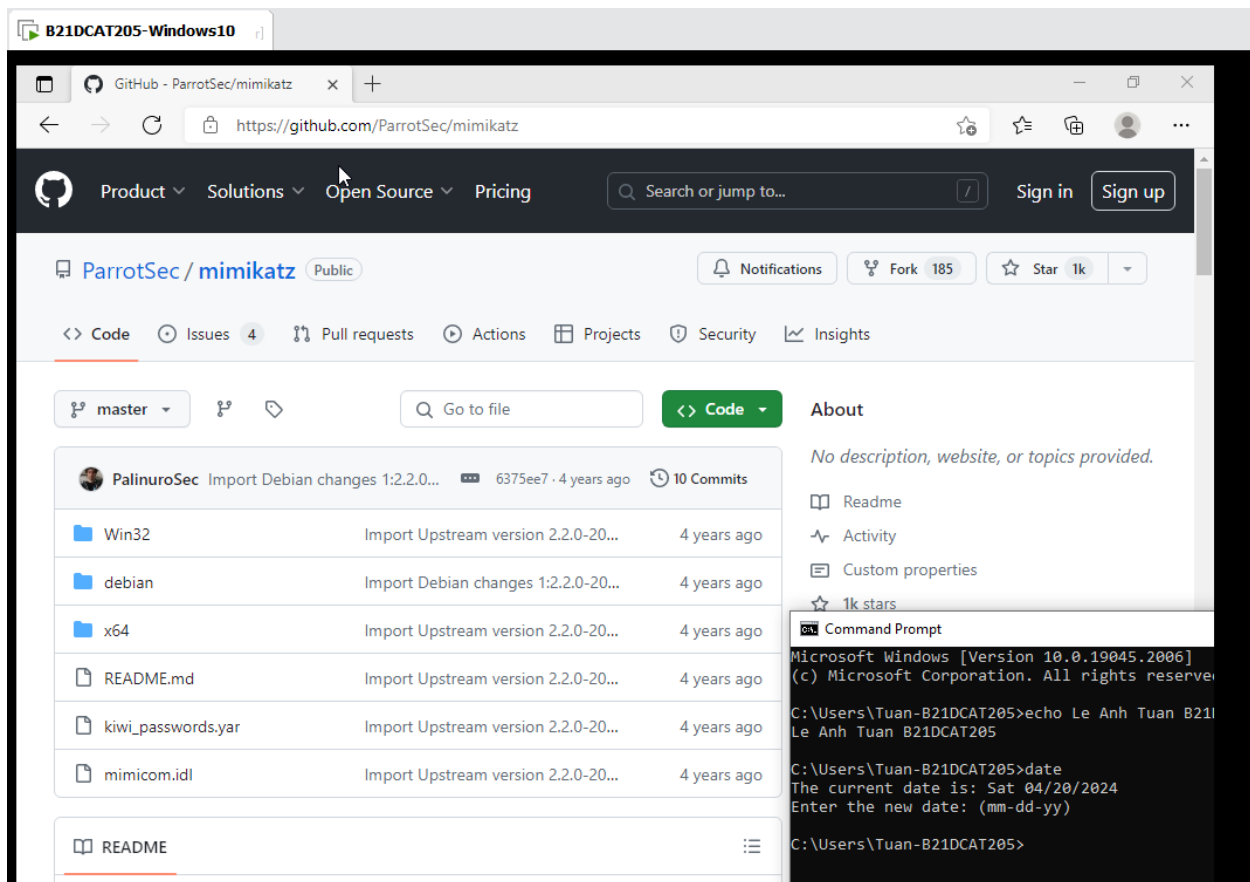
- Lấy mật khẩu đăng nhập của người dùng trên hệ thống Windows.
- Lấy các thông tin chứng chỉ, bảo mật và quản lý thông tin từ bộ nhớ hệ thống.
- Thực hiện tấn công Pass-the-Hash để đăng nhập vào hệ thống với tư cách của người dùng đã bị lấy mật khẩu.
- Thực hiện tấn công Golden Ticket để giả mạo giấy 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

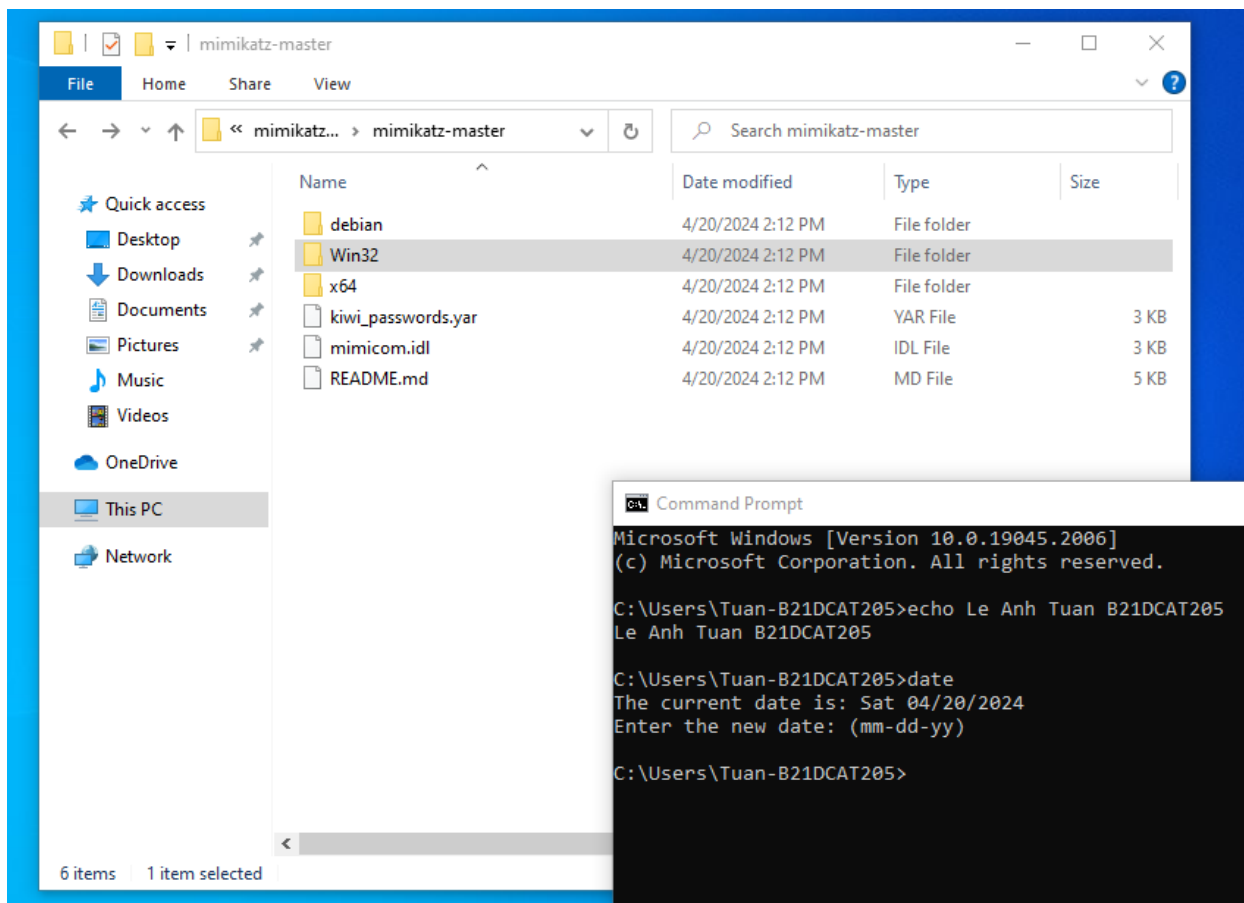
## **2.2 Nội dung thực hành.**

### **2.2.1 Chuẩn bị môi trường**

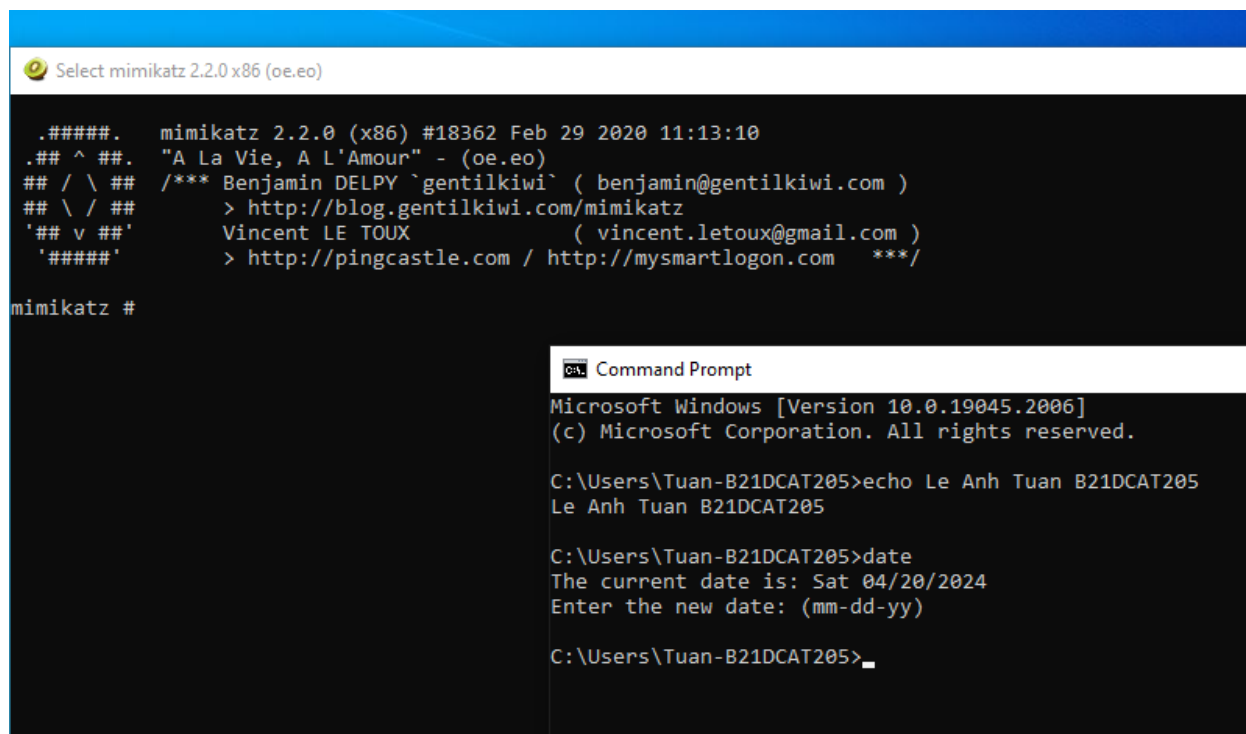
- Trên Windows, tải công cụ mimikatz và john the ripper



*Hình 1: Download mimikatz từ github*



**Hình 2: Download thành công mimikatz**



```
Select mimikatz 2.2.0 x86 (oe.eo)

.#####.  mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##.  "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 #

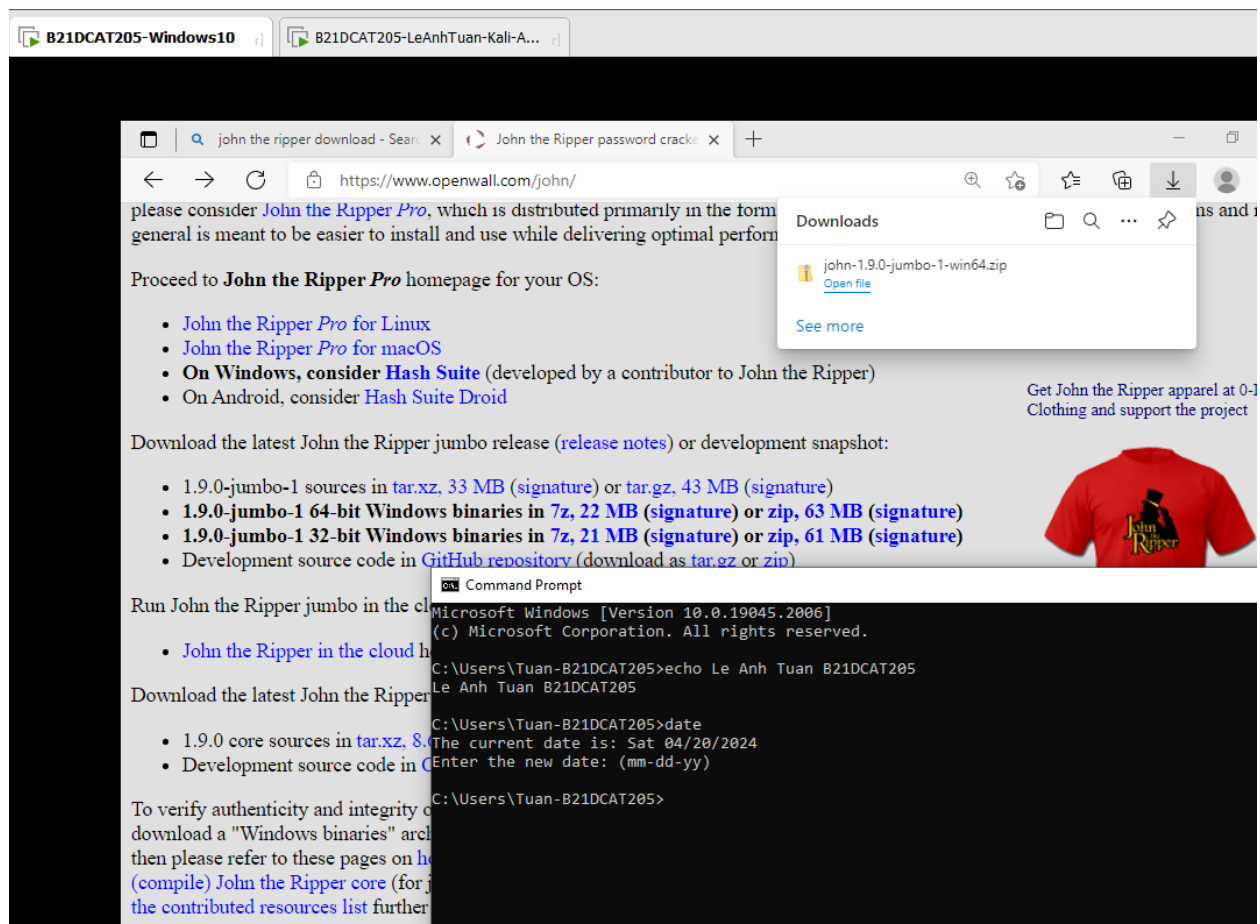
C:\Users\Tuan-B21DCAT205>echo Le Anh Tuan B21DCAT205
Le Anh Tuan B21DCAT205

C:\Users\Tuan-B21DCAT205>date
The current date is: Sat 04/20/2024
Enter the new date: (mm-dd-yy)

C:\Users\Tuan-B21DCAT205>_
```

*Hình 3: Giao diện mimikatz trên cmd*





**Hình 4: Tải John The Ripper trên Windows**

- Trên Kali, john the ripper có sẵn

```

PS> john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                               Print usage summary
--single[=SECTION[,..]]              "Single crack" mode, using default or named rules
--single=rule[,..]                   Same, using "immediate" rule(s)
--single-seed-WORD[,WORD]            Add static seed word(s) for all salts in single mode
--single-wordlist=FILE                *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE               Wordlist with seeds per username (user:password[s]
                                     format)
--single-pair-max=N                  Override max. number of word pairs generated (6)
--no-single-pair                     Disable single word pair generation
--[no-]single-retest-guess            Override config for SingleRetestGuess
--wordlist[=FILE] --stdin             Wordlist mode, read words from FILE or stdin
                                     like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]               Enable word mangling rules (for wordlist or PRINCE
                                     modes), using default or named rules
--rules=rule[,..]                   Same, using "immediate" rule(s)
--rules-stack=SECTION[,..]           Stacked rules, applied after regular rules or to
                                     modes that otherwise don't support rules
--rules-stack=rule[,..]              Same, using "immediate" rule(s)
--rules-skip-nop                     Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]                   Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE                 Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression                   Suppress all dupes in wordlist (and force preload)
--incremental[=MODE]                 "Incremental" mode [using section MODE]
--incremental-charcount=N            Override CharCount for incremental mode
--external-MODE                      External mode or word filter
--mask[=MASK]                        Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]                   "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE                     "Markov" stats file
--prince[=FILE]                      PRINCE mode, read words from FILE
--prince-loopback[=FILE]              Fetch words from a .pot file
--prince-elem-cnt-min=N               Minimum number of elements per chain (1)
--prince-elem-cnt-max=[-]N            Maximum number of elements per chain (negative N is
                                     relative to word length) (8)
--prince-skip=N                      Initial skip
--prince-limit=N                     Limit number of candidates generated
--prince-wl-dist-len                 Calculate length distribution from wordlist
--prince-wl-max=N                    Load only N words from input wordlist
--prince-case-permute                Permute case of first letter
--prince-mmap                        Memory-map infile (not available with case permute)

```

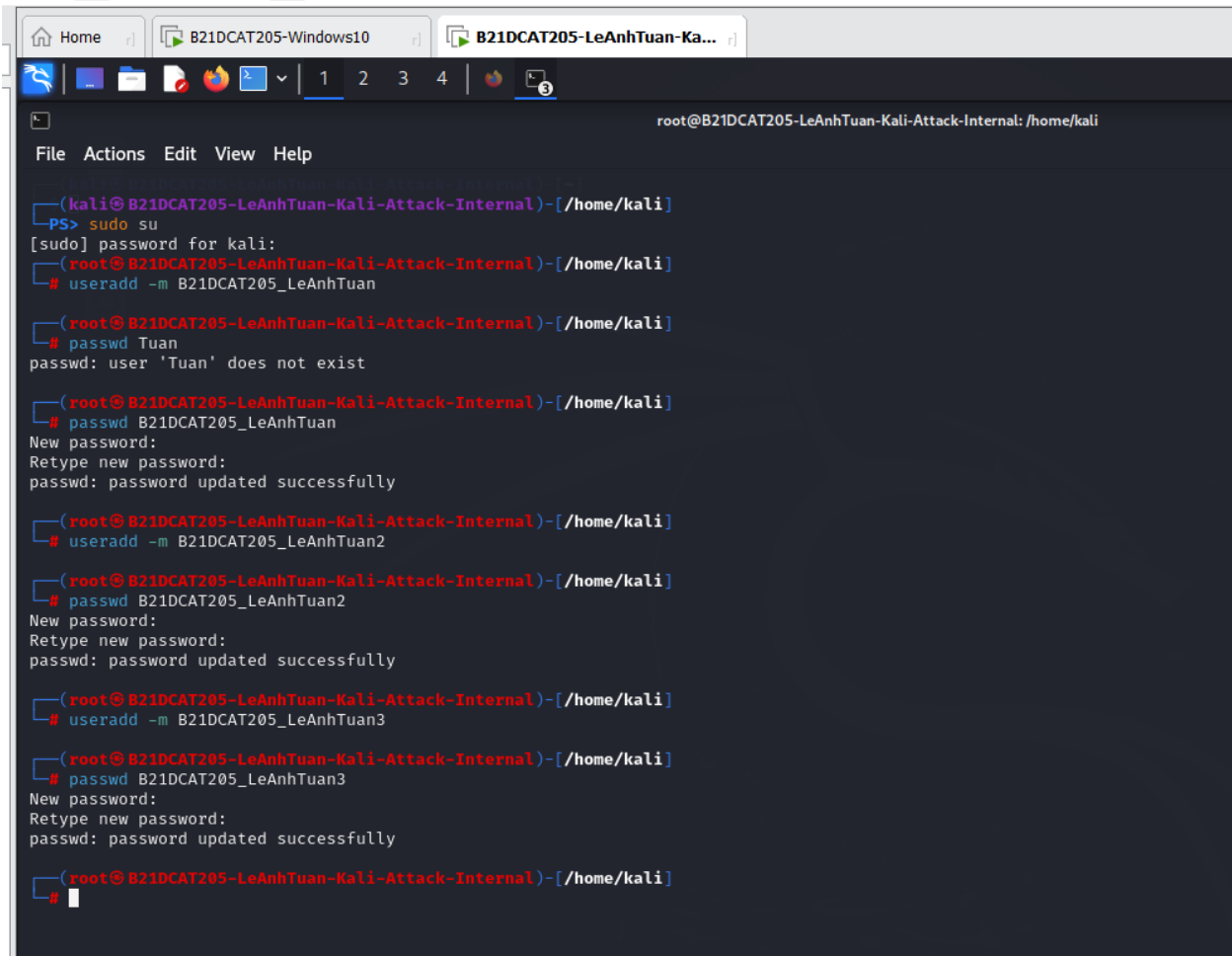
**Hình 5: Kiểm tra phiên bản John The Ripper**

## 2.2.2 Thực hành

### • Trên Kali:

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

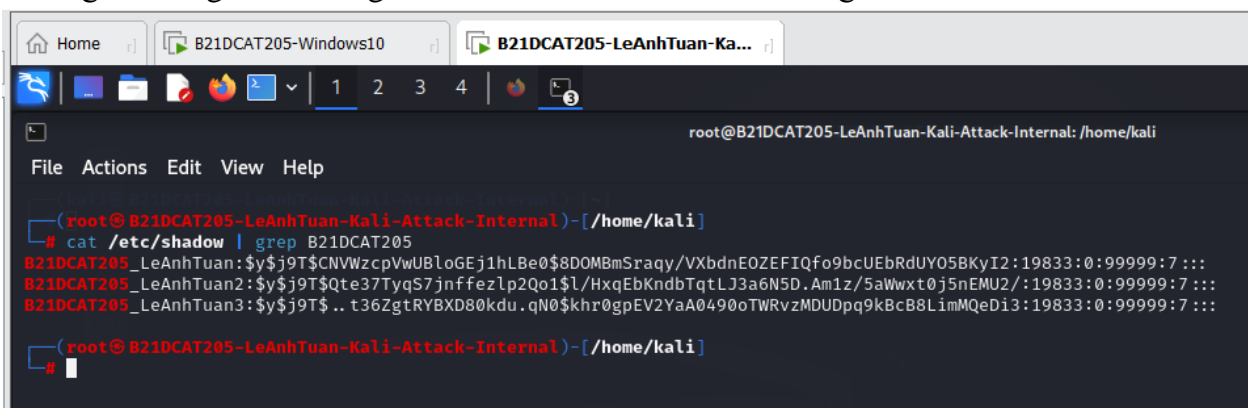
Tài khoản	Mật khẩu
B21DCAT205_LeAnhTuan	1234
B21DCAT205_LeAnhTuan2	123456
B21DCAT205_LeAnhTuan3	12345678



```
(kali@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
PS> sudo su
[sudo] password for kali:
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# useradd -m B21DCAT205_LeAnhTuan
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# passwd Tuan
passwd: user 'Tuan' does not exist
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# passwd B21DCAT205_LeAnhTuan
New password:
Retype new password:
passwd: password updated successfully
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# useradd -m B21DCAT205_LeAnhTuan2
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# passwd B21DCAT205_LeAnhTuan2
New password:
Retype new password:
passwd: password updated successfully
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# useradd -m B21DCAT205_LeAnhTuan3
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# passwd B21DCAT205_LeAnhTuan3
New password:
Retype new password:
passwd: password updated successfully
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
#
```

*Hình 6: Thêm người dùng*

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



```
(root@ B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# cat /etc/shadow | grep B21DCAT205
B21DCAT205_LeAnhTuan:$y$j9T$CNVWzcpVwUBLoGEj1hLBe0$8DOMBmSraqy/VXbdeOZEFIQfo9bcUEbRdUYO58KyI2:19833:0:99999:7:::
B21DCAT205_LeAnhTuan2:$y$j9T$Qte37TyqS7jnffezlp2Qo1$1/HxqEbKndbTqtLJ3a6N5D.Am1z/5aWwxt0j5nEMU2/:19833:0:99999:7:::
B21DCAT205_LeAnhTuan3:$y$j9T$..t36ZgtRYBXD80kdu.qN0$khro0gpEV2YaA0490oTWRvzMDUDpq9kBcB8LimMQeDi3:19833:0:99999:7:::
#
```

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

```
root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali
File Actions Edit View Help

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# cat /etc/shadow | grep B21DCAT205
B21DCAT205_LeAnhTuan:$y$j9T$CNVWzcpVwUBloGEj1hLBe0$8DOMBmSraqy/VXbdnEOZEFIQfo9bcUEbRdUYO5BKyI2:19833:0:99999:7:::
B21DCAT205_LeAnhTuan2:$y$j9T$Qte37TyqS7jnffezlp2Qo1$l/HxqEbKndbTqtLJ3a6N5D.Am1z/5aWwxt0j5nEMU2/:19833:0:99999:7:::
B21DCAT205_LeAnhTuan3:$y$j9T$..t36ZgtRYBXD80kdu.qN0$khR0gpEV2YaA0490oTWRvzMDUDpq9kBcB8LimMQeDi3:19833:0:99999:7:::

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# cat /etc/shadow | grep B21DCAT205 > hash.txt

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# cat hash.txt
B21DCAT205_LeAnhTuan:$y$j9T$CNVWzcpVwUBloGEj1hLBe0$8DOMBmSraqy/VXbdnEOZEFIQfo9bcUEbRdUYO5BKyI2:19833:0:99999:7:::
B21DCAT205_LeAnhTuan2:$y$j9T$Qte37TyqS7jnffezlp2Qo1$l/HxqEbKndbTqtLJ3a6N5D.Am1z/5aWwxt0j5nEMU2/:19833:0:99999:7:::
B21DCAT205_LeAnhTuan3:$y$j9T$..t36ZgtRYBXD80kdu.qN0$khR0gpEV2YaA0490oTWRvzMDUDpq9kBcB8LimMQeDi3:19833:0:99999:7:::

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
#
```

*Hình 8: Lưu thông tin vào file hash.txt*

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

```
root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali
File Actions Edit View Help

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# john --wordlist hash.txt --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 wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
12345678      (B21DCAT205_LeAnhTuan3)
1234         (B21DCAT205_LeAnhTuan)
123456       (B21DCAT205_LeAnhTuan2)
3g 0:00:00:03 DONE (2024-04-20 08:50) 0.7712g/s 24.67p/s 74.03c/s 74.03C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
# john --show hash.txt
B21DCAT205_LeAnhTuan:1234:19833:0:99999:7:::
B21DCAT205_LeAnhTuan2:123456:19833:0:99999:7:::
B21DCAT205_LeAnhTuan3:12345678:19833:0:99999:7:::

3 password hashes cracked, 0 left

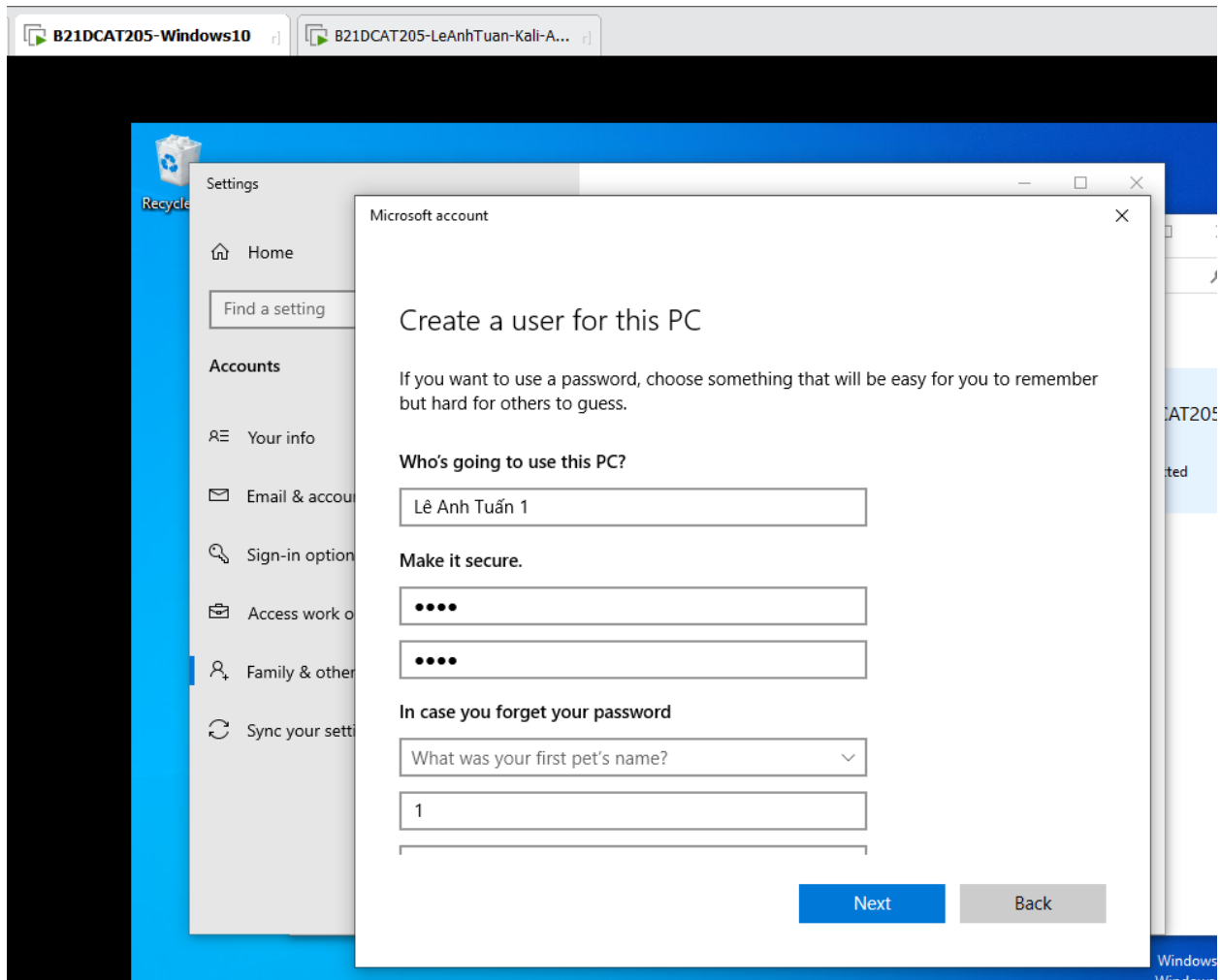
(root@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali]
#
```

*Hình 9: Crack mật khẩu thành công*

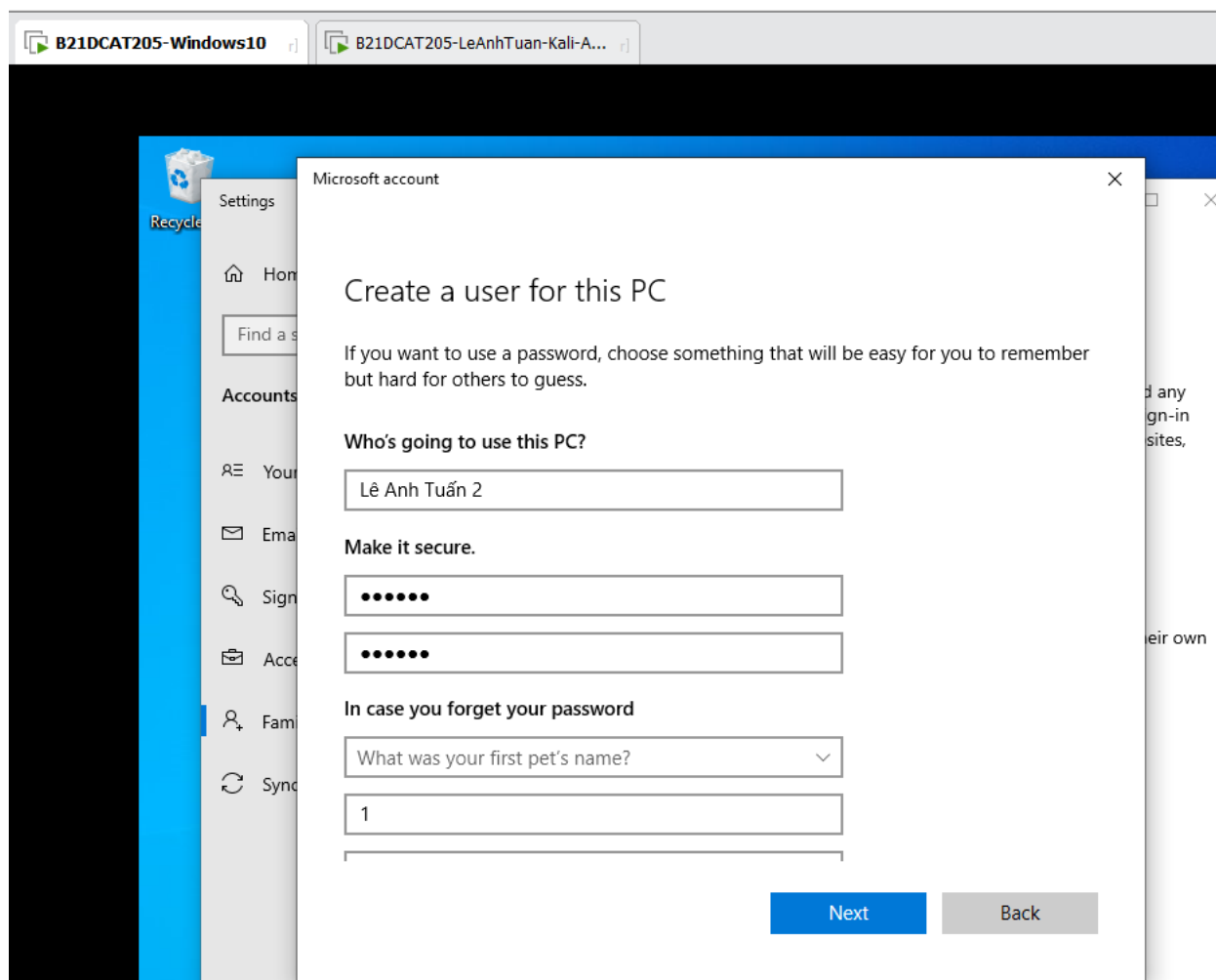
•Trên Windows:

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

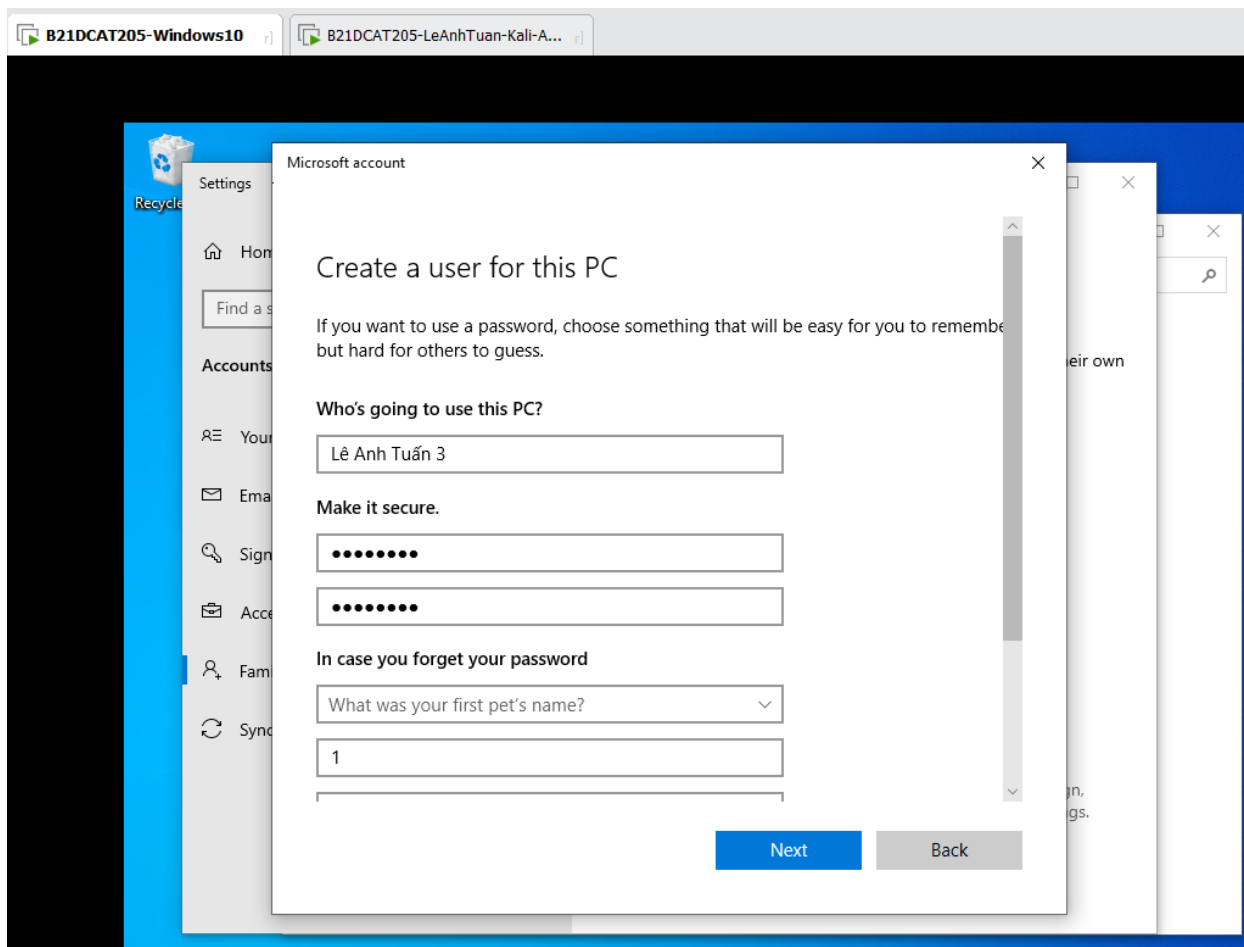
Tài khoản	Mật khẩu
Lê Anh Tuấn 1	1234
Lê Anh Tuấn 2	123456
Lê Anh Tuấn 3	12345678



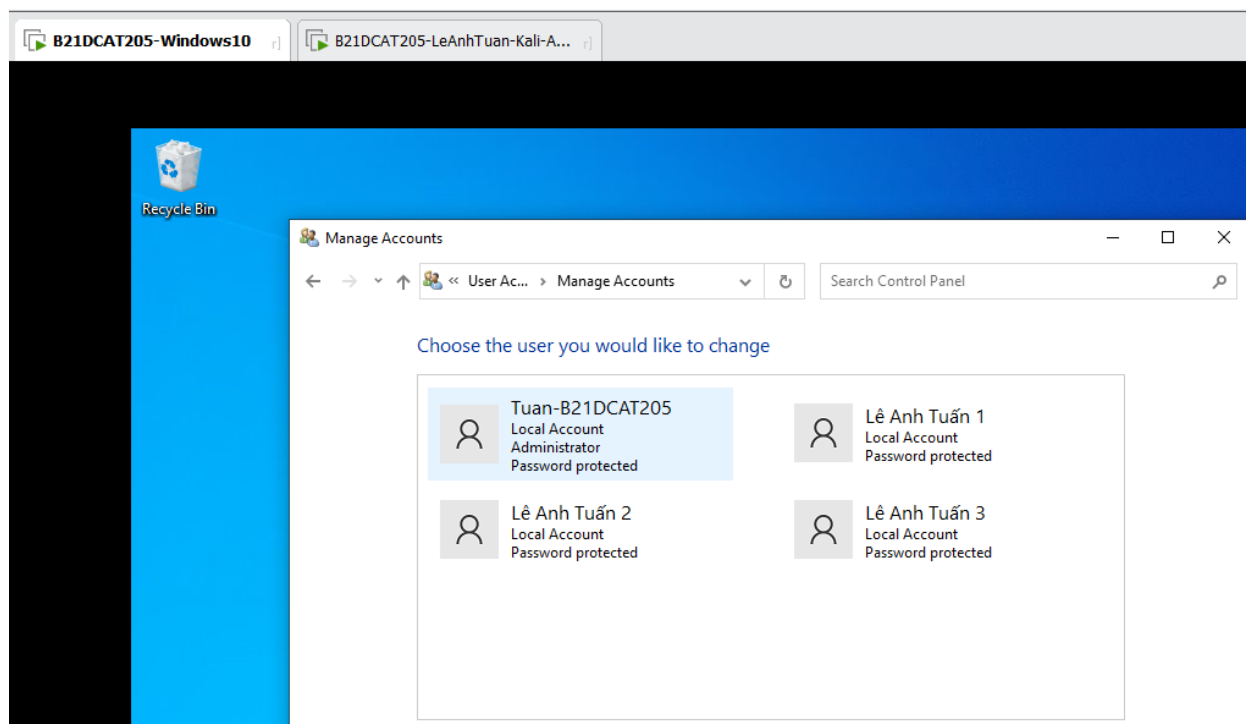
**Hình 10: Tạo tài khoản với 4 ký tự số**



***Hình 11: Tạo tài khoản với 6 ký tự số***

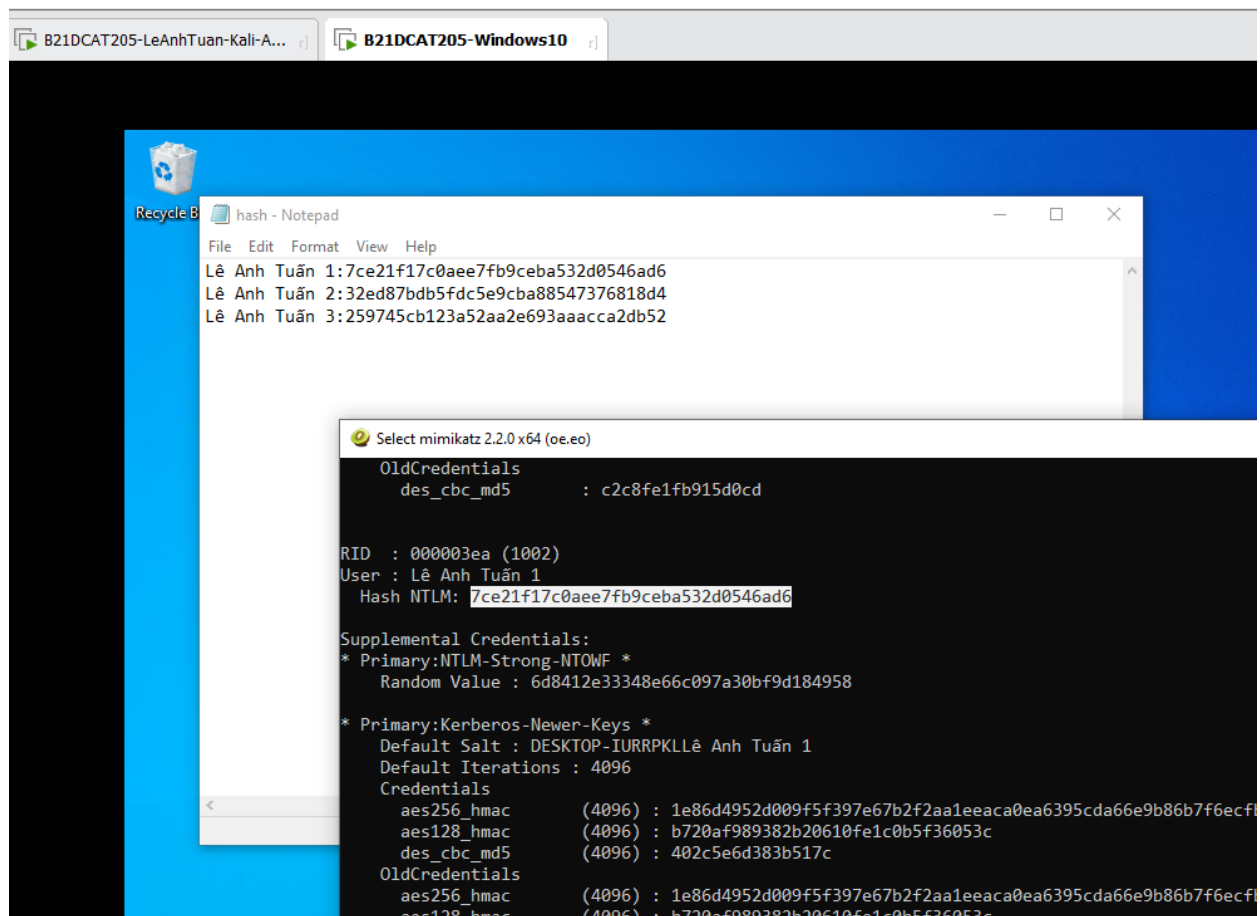


***Hình 12: Tạo tài khoản với 8 ký tự số***

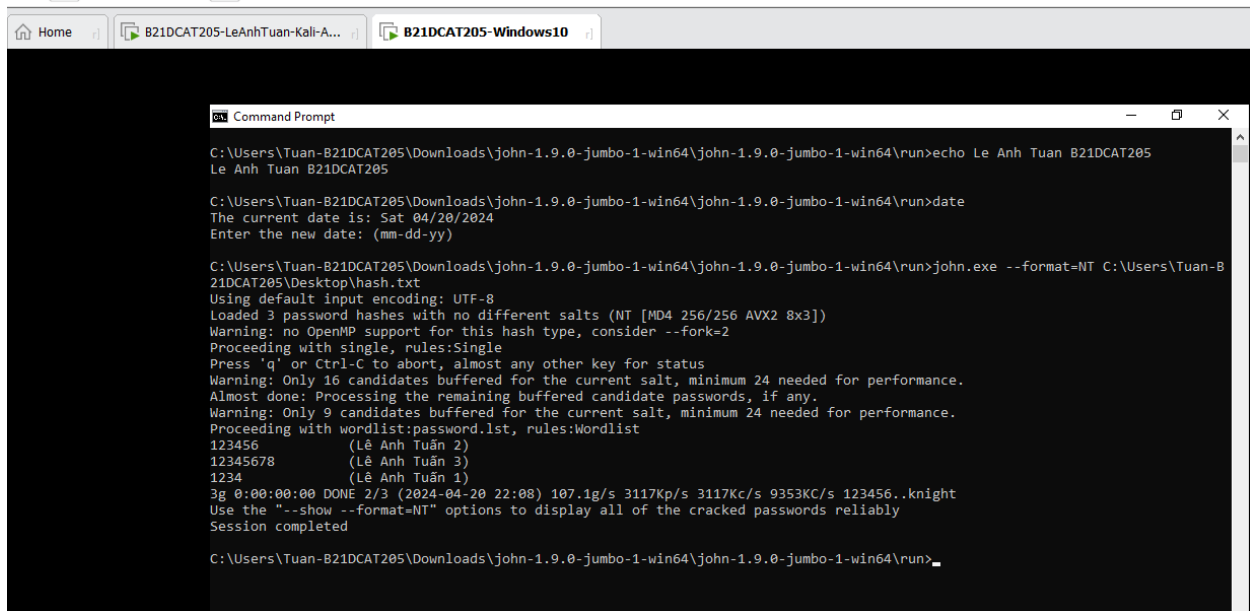


***Hình 13: Các người dùng sau khi được thêm***





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



```
C:\Users\Tuan-B21DCAT205\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>echo Le Anh Tuan B21DCAT205
Le Anh Tuan B21DCAT205

C:\Users\Tuan-B21DCAT205\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>date
The current date is: Sat 04/20/2024
Enter the new date: (mm-dd-yy)

C:\Users\Tuan-B21DCAT205\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>john.exe --format=NT C:\Users\Tuan-B21DCAT205\Desktop\hash.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 16 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 9 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:password.lst, rules:Wordlist
123456 (Lê Anh Tuấn 2)
12345678 (Lê Anh Tuấn 3)
1234 (Lê Anh Tuấn 1)
3g 0:00:00:00 DONE 2/3 (2024-04-20 22:08) 107.1g/s 3117Kp/s 3117Kc/s 9353Kc/s 123456..knight
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed

C:\Users\Tuan-B21DCAT205\Downloads\john-1.9.0-jumbo-1-win64\john-1.9.0-jumbo-1-win64\run>
```

*Hình 15: Crack mật khẩu thành công*

### 3 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.

### 4 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