

**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 13: Kiểm thử thông qua tấn công mật khẩu**

**Họ và tên giảng viên:** PGS.TS.Đỗ Xuân Chợt  
**Họ và tên:** Phạm Thanh Tùng  
**Mã sinh viên:** B20DCAT171  
**Lớp:** D20CQAT03-B  
**Số điện thoại:** 0856915668

Hà Nội 2023

## 1. 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 bẻ 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 bẻ 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 bẻ 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, bẻ 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 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 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 bẻ khóa hầu hết các mật khẩu trong vòng vài phút
- Một bảng cầu vồng 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 vồng xen kẽ giữa các hàm băm và hàm giảm để tạo chuỗi băm xen kẽ và bản rõ.

## 2. Nội dung thực hành

### 2.1. 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@B20DCAT171-Tung-Kali)-[~]
$ sudo useradd B20DCAT171-PhamThanhTung
sudo: unable to resolve host B20DCAT171-Tung-Kali: Temporary failure in name resolution
n /etc/passwd:/var/run/utmp:/usr/sbin/nologin
n /etc/passwd:/var/spool/cvsroot:/usr/sbin/nologin
(kali@B20DCAT171-Tung-Kali)-[~]
$ sudo passwd B20DCAT171-PhamThanhTung
sudo: unable to resolve host B20DCAT171-Tung-Kali: Temporary failure in name resolution
n
New password:
Retype new password:
passwd: password updated successfully
(kali@B20DCAT171-Tung-Kali)-[~]
$ sudo unshadow /etc/passwd /etc/shadow >password
sudo: unable to resolve host B20DCAT171-Tung-Kali: Temporary failure in name resolution
n
```

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

### Crack mật khẩu 4 ký tự:

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
$ john --format=crypt password
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
0g 0:00:00:24 24.98% 1/3 (ETA: 02:13:26) 0g/s 125.3p/s 125.3c/s b20dcat171-pha
mthanhtungphamthanhtung!! ..b20dcat171-phamthanhtungged
0g 0:00:00:43 41.37% 1/3 (ETA: 02:13:32) 0g/s 111.5p/s 111.5c/s \phamthanhtung
..jb20dcat171b20dcat171-phamthanhtung
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234 (B20DCAT171-PhamThanhTung)
1g 0:00:02:41 DONE 2/3 (2023-03-04 02:14) 0.006190g/s 83.03p/s 83.03c/s 123456
..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B20DCAT171-Tung-Kali)-[~]
$

File Actions Edit View Help
$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Sat Mar 4 02:10:06 AM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

### Crack mật khẩu 6 ký tự:

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
$ john --format=crypt password
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
0g 0:00:00:27 35.93% 1/3 (ETA: 02:09:12) 0g/s 143.8p/s 143.8c/s 143.8C/s Mpb20dcat171..
Tphamthanhtungb20dcat171-phamthanhtung
0g 0:00:00:59 68.10% 1/3 (ETA: 02:09:23) 0g/s 138.6p/s 138.6c/s 138.6C/s B20dcat171-pha
mthanhtungphamthanhtungE..B20dcat171-phamthanhtungL
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456 (B20DCAT171-PhamThanhTung)
1g 0:00:01:39 DONE 2/3 (2023-03-04 02:09) 0.01005g/s 134.8p/s 134.8c/s 134.8C/s 123456.
..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@B20DCAT171-Tung-Kali)-[~]
$

File Actions Edit View Help
$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171


(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Sat Mar 4 02:10:06 AM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

## Crack mật khẩu 8 ký tự:

```
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ john --format=crypt password  
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: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  
0g 0:00:00:52 24.98% 1/3 (ETA: 02:19:09) 0g/s 58.98p/s 58.98c/s 58.98C/s b20dcat171-pha  
mthanhtungphamthanhtung!! ..b20dcat171-phamthanhtungged  
0g 0:00:01:45 59.68% 1/3 (ETA: 02:18:36) 0g/s 65.62p/s 65.62c/s 65.62C/s B20dcat171-pha  
mthanhtungphamthanhtung04..b20dcat171-phamthanhtung71  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
12345678 (B20DCAT171-PhamThanhTung)  
1g 0:00:03:20 DONE 2/3 (2023-03-04 02:19) 0.004983g/s 66.84p/s 66.84c/s 66.84C/s 123456  
..pepper  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo Pham Thanh Tung B20DCAT171  
Pham Thanh Tung B20DCAT171  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ date  
Sat Mar 4 02:10:06 AM EST 2023  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$
```


## 2.2. Crack mật khẩu trên hệ điều hành Windows: Tải công cụ mimikatz

 Product Team Enterprise Explore Marketplace Pricing Search

ic / mimikatz Public

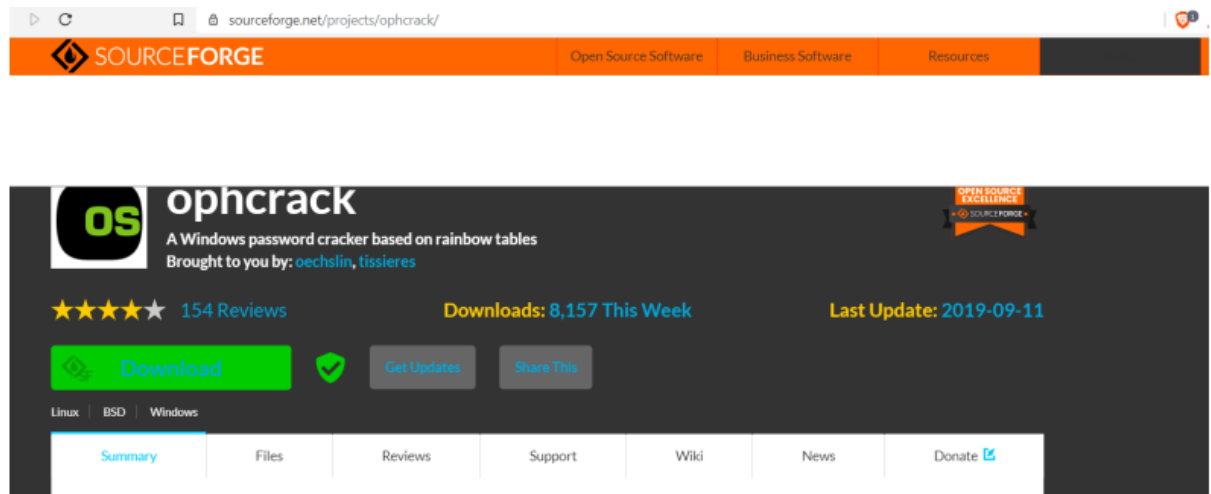
Issues Pull requests Actions Projects Wiki Security Insights

master 2 branches 6 tags Go to file Code

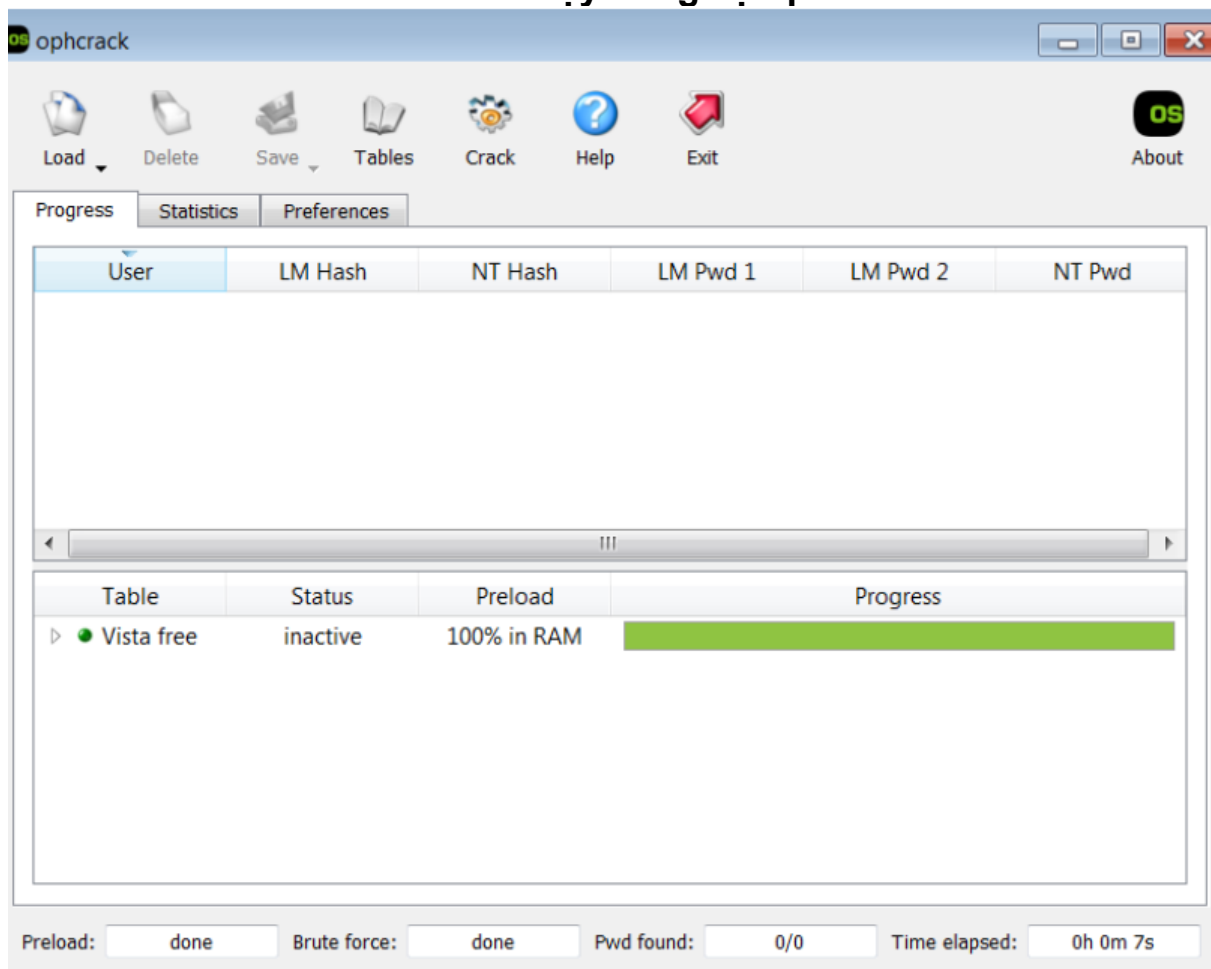
 PalinuroSec Import Debian changes 1:2.2.0-20200229-1parrot2 6375ee7 on Mar 2, 2020 10 commits

Win32	Import Upstream version 2.2.0-20200229	2 years ago
debian	Import Debian changes 1:2.2.0-20200229-1parrot2	2 years ago
x64	Import Upstream version 2.2.0-20200229	2 years ago
README.md	Import Upstream version 2.2.0-20200229	2 years ago
kiwi_passwords.yar	Import Upstream version 2.2.0-20200229	2 years ago
mimicom.idl	Import Upstream version 2.2.0-20200229	2 years ago

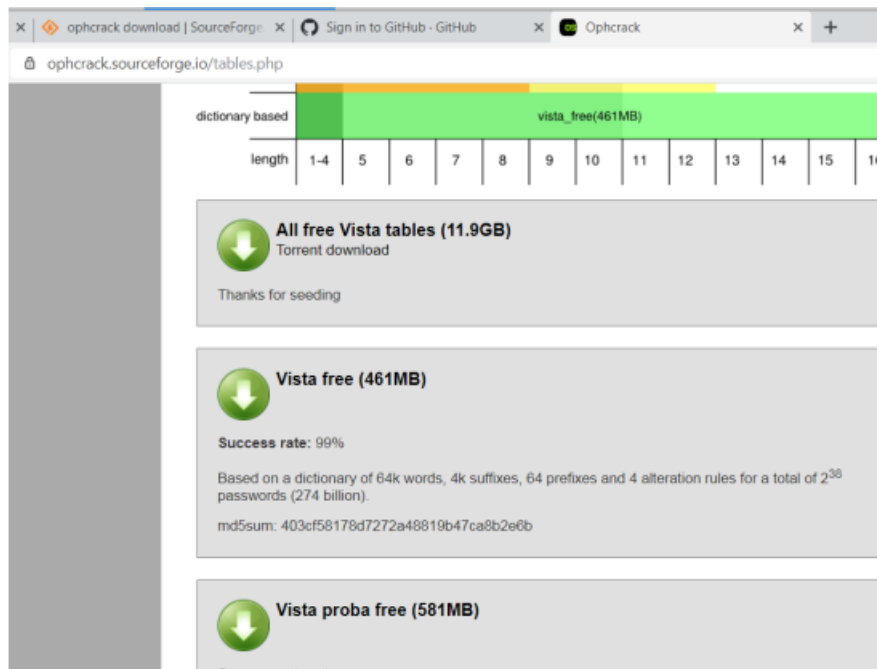
## Tải công cụ ophcrack



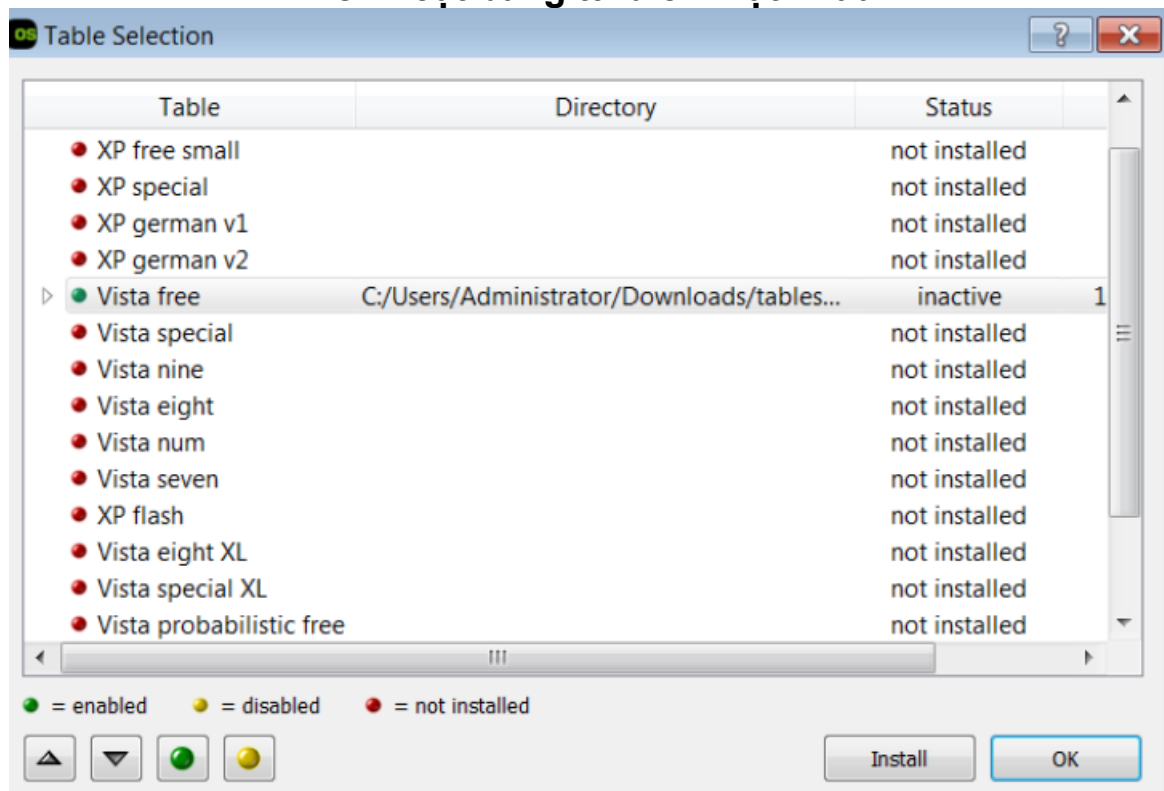
## Giải nén file và chạy công cụ ophcrack



## 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>ref save hklm\SAM sam.hiv
'ref' is not recognized as an internal or external command,
operable program or batch file.

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>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>

Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tùng>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Tùng>date
The current date is: Sat 03/04/2023
Enter the new date: (mm-dd-yy)
```

```
mimikatz 2.2.0 x64 (oe.eo)
RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: f02a5a544df11441fffc55c5cd563cbd

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : e4bd51eb63559d034be37397f38bc384

* Primary:Kerberos-Newer-Keys *
  Default Salt : WDAGUtilityAccount
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : ace9d59ca92894df34352fa1202eaaa19022f5fa720c1c62bdeac87f2aa09fc8
    aes128_hmac (4096) : b7cb60e0d6614cf5fe5f794bc6dd9e2f
    des_cbc_md5 (4096) : dfdafb455db33802

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : WDAGUtilityAccount
  Credentials
    des_cbc_md5 : dfdafb455db33802

RID : 000003e8 (1000)
User : Tùng
Hash NTLM: 7ce21f17c0aee7fb9ceba532d0546ad6

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 3ba7dcb15c9ccd8c497a58ed4c553735

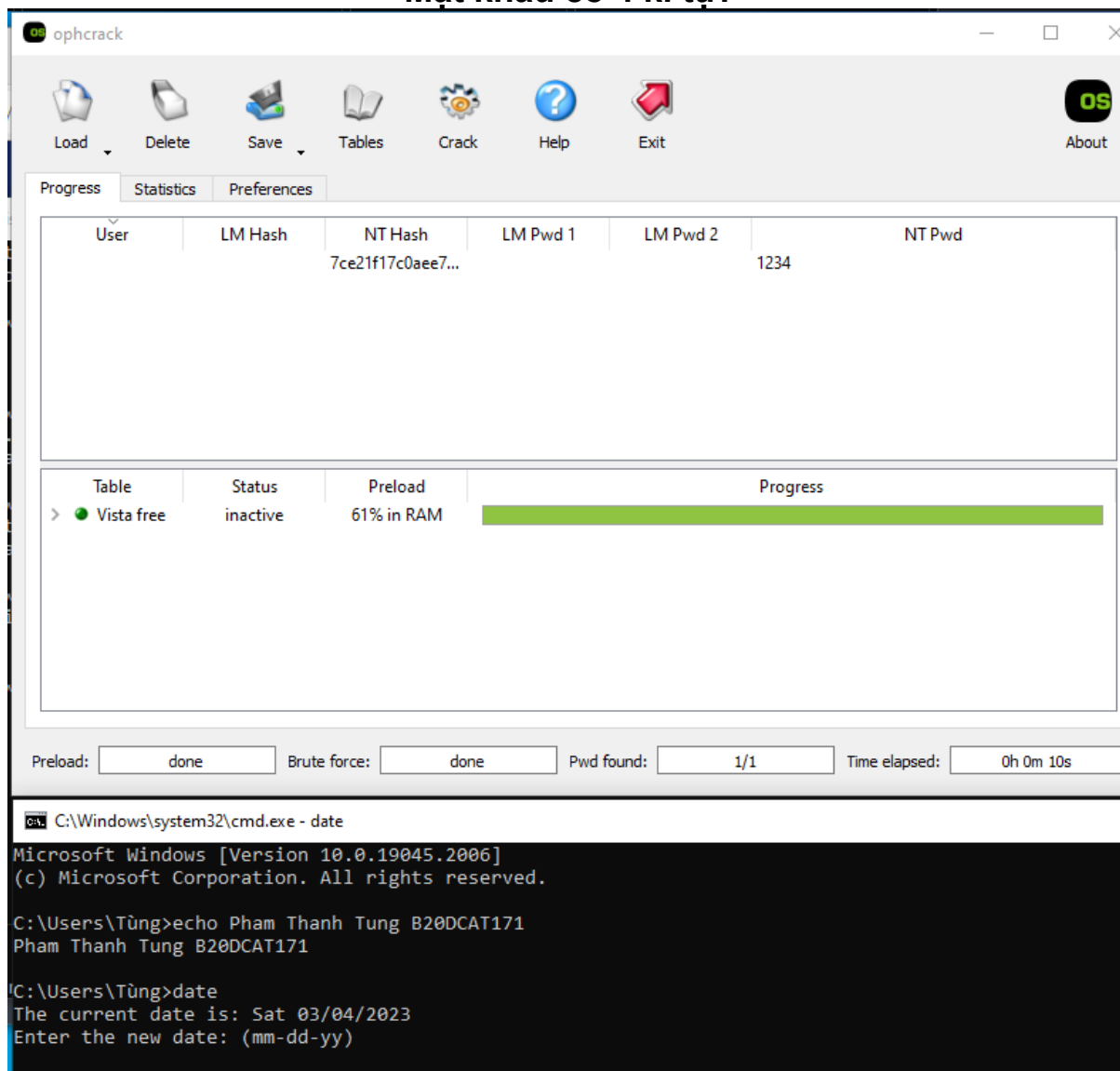
* Primary:Kerberos-Newer-Keys *
  Default Salt : DESKTOP-F10LA1STùng
  Default Iterations : 4096

C:\Users\Tùng>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Tùng>date
The current date is: Sat 03/04/2023
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 kí tự:



The screenshot displays the Ophcrack application window. The top menu bar includes icons for Load, Delete, Save, Tables, Crack, Help, and Exit, along with an 'About' button. Below the menu is a tabbed interface with 'Progress', 'Statistics', and 'Preferences' tabs. The 'Progress' tab shows a table with columns: User, LM Hash, NT Hash, LM Pwd 1, LM Pwd 2, and NT Pwd. The data row shows 'User' as 'Vista free', 'LM Hash' as '7ce21f17c0aee7...', 'NT Hash' as '1234', and 'LM Pwd 1' as '1234'. Below the table is a progress bar labeled 'Progress' showing 61% completion. At the bottom of the application window, there are status fields: 'Preload: done', 'Brute force: done', 'Pwd found: 1/1', and 'Time elapsed: 0h 0m 10s'. Below the application window is a command prompt window showing the following text:

```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tùng>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Tùng>date
The current date is: Sat 03/04/2023
Enter the new date: (mm-dd-yy)
```

## Mật khẩu có 6 kí tự:

ophcrack

Load Delete Save Tables Crack Help Exit About

Progress Statistics Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
		7ce21f17c0aee7...			1234
		32ed87bdb5fdc...			123456

Table	Status	Preload	Progress
> Vista free	inactive	100% in RAM	<div></div>

Preload: done Brute force: done Pwd found: 2/2 Time elapsed: 0h 0m 12s

C:\Windows\system32\cmd.exe - date

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tùng>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Tùng>date
The current date is: Sat 03/04/2023
Enter the new date: (mm-dd-yy)
```

## Mật khẩu có 8 kí tự:

ophcrack

Load Delete Save Tables Crack Help Exit About

Progress Statistics Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
		7ce21f17c0aee7...			1234
		32ed87bdb5fdc...			123456
		259745cb123a5...			12345678

Table	Status	Preload	Progress
> Vista free	inactive	100% in RAM	<div></div>

Preload: done Brute force: done Pwd found: 3/3 Time elapsed: 0h 0m 14s

C:\Windows\system32\cmd.exe - date

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tùng>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Tùng>date
The current date is: Sat 03/04/2023
Enter the new date: (mm-dd-yy)
```