

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



Môn học: Thực Tập Cơ Sở
Báo Cáo Bài Thực Hành 12
Tấn công mật khẩu

Họ và tên: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Nhóm môn học: 04

Giảng viên: Đinh Trường Duy

Hà Nội, 4/2024

Mục lục

1. Mục đích	3
2. Nội dung thực hành	3
2.1. Cơ sở lý thuyết: công cụ tấn công mật khẩu	3
a. OphCrack.....	3
b. PWDUMP.....	3
c. Hashcat:	4
d. John The Ripper.....	5
2.2. Các bước thực hiện	6
2.2.1 Chuẩn bị môi trường	6
2.2.2 Crack mật khẩu trên Windows.....	6
2.2.3 Crack mật khẩu trên Linux.....	10
3. Kết luận	13
4. Tài liệu tham khảo.....	13

Danh mục hình ảnh

Tạo các Account	7
Kết quả.....	7
Các gói cần cài đặt.....	8
Giao diện OphCrack sau khi tải.....	8
Trích xuất mật khẩu	9
Kích hoạt Rainbow	9
Kết quả.....	10
Tạo các User	11
Kiểm tra lại trên file /etc/passwd.....	11
Kết hợp 2 file /etc/passwd và file /etc/shadow	12
Crack thành công mật khẩu 4 kí tự, 6 kí tự	12
Crack thành công mật khẩu 8 kí tự.....	13

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 nghệ Crack mật khẩu trên các hệ điều hành Linux và Windows

2. Nội dung thực hành

2.1. Cơ sở lý thuyết: công cụ tấn công mật khẩu

a. OphCrack

OphCrack là một 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 mật khẩu. 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 bố công khai và có thể được sửa đổi, phát triển 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 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

b. PWDUMP

PWDUMP là một công cụ phần mềm dùng để thu thập thông tin về mật khẩu từ hệ thống Windows. Cụ thể, nó thường được sử dụng để thu thập và trích xuất mật khẩu đã được mã hóa từ cơ sở dữ liệu của hệ thống Windows. Thông qua việc sử dụng

PWDUMP, người dùng có thể thu thập các mật khẩu này để phục vụ cho các mục đích kiểm tra bảo mật, phân tích hoặc khôi phục mật khẩu.

c. Hashcat:

Hashcat là phần mềm crack hash/khôi phục mật khẩu từ hash nhanh nhất và tiên tiến nhất hiện nay trên giao diện dòng lệnh. Hashcat cung cấp cho người sử dụng 5 chế độ tấn công/khôi phục mật khẩu khác nhau áp dụng cho hơn 300 thuật toán hash khác nhau. Hashcat là một phần mềm mã nguồn mở và hoàn toàn miễn phí. Hashcat có thể được sử dụng trên nhiều nền tảng khác nhau như Linux, Windows và MacOS.

Ở thời điểm hiện tại, Hashcat có thể sử dụng GPU, CPU và các phần cứng tăng tốc độ tính toán khác trên hệ thống máy tính để tăng tốc độ phá password hash. Tuy nhiên, vì phần lớn chúng ta sử dụng máy ảo Kali Linux trên Virtual Box, nên chúng ta sẽ mất đi sự hỗ trợ đặc lực của GPU (card đồ họa).

Trước khi sử dụng Hashcat, chúng ta phải xác định thuật toán mã hóa, có thể sử dụng công cụ: Hash Identifier (ở ngay trên Kali), Hash Analyzer của TunnelsUP.com (online), Password hash identification (online)

Hash cat hỗ trợ 4 hình thức crack hash:

- **Dictionary (-a 0):** Bạn sẽ cung cấp cho Hashcat một danh sách (có thể là tập hợp những passwords hay được dùng nhất). Hashcat sẽ sử dụng lần lượt từng giá trị trong danh sách này để hash nó với thuật toán đã chỉ định và so sánh với hash đầu vào, nếu kết quả sai, Hashcat sẽ thử giá trị tiếp theo trong danh sách được cung cấp, nếu đúng thì Hashcat trả lại kết quả đã tạo nên giá trị hash trùng khớp với giá trị hash đầu vào.
- **Combination (-a 1):** Tương tự như Dictionary attack ở trên, tuy nhiên khi dùng Combination các bạn sẽ phải cung cấp 2 danh sách chứ không phải chỉ 1 danh sách như Dictionary attack. Hình thức tấn công này được sử dụng khi bạn muốn tìm username và password của người dùng. Lúc này bạn sẽ cần 1 danh sách những usernames hay được dùng nhất và 1 danh sách những passwords hay được dùng nhất. Hashcat sẽ lần lượt tạo ra các cặp kết hợp giữa danh sách username và danh sách password và lần lượt thử đăng nhập bằng các cặp kết hợp này cho đến khi tìm ra được username và password chính xác hoặc cho đến khi tất cả các cặp kết hợp đều đã được thử và không có cặp nào chính xác.
- **Mask (-a 3):** Mask attack tương tự như Bruteforce attack, bạn sẽ cung cấp một loạt các ký tự ví dụ a, b, c, d, e, f, 1, 2, 3, v.v. và từ các ký tự được cung cấp này, Hashcat sẽ tự kết hợp các ký tự lại với nhau và tạo ra các chuỗi ký tự ngẫu nhiên ví dụ như abc123, và các chuỗi này sẽ được dùng để tấn công giống như Dictionary attack. Cách tấn công này sẽ phù hợp để tìm những username và password không

nằm trong danh sách được cung cấp khi tấn công Dictionary attack, tuy nhiên sẽ rất mất thời gian.

- **Hybrid (-a 6 và -a 7):** Kết hợp cả Dictionary attack và Mask attack.

Cú pháp cơ bản:

hashcat -a <tấn-công> -m <thuật-toán-hash> <file-chứa-hash-đầu-vào> <danh-sách hoặc chuỗi-ký-tự>

Theo đó ta có các thành phần bắt buộc phải có như sau:

- **-a:** Số của hình thức tấn công:
 - **-a 0:** Dictionary
 - **-a 1:** Combination
 - **-a 3:** Mask
 - **-a 6 và -a 7:** Dictionary + Mask
- **-m:** Số của thuật toán hash (bất cứ khi nào quên, bạn đều có thể tra cứu lại bằng lệnh **hashcat -help**). Trong ví dụ mình dùng -m 0 để chỉ thuật toán hash MD5.
- **File chứa hash đầu vào**
- **File chứa danh sách nếu tấn công Dictionary hoặc chuỗi ký tự nếu tấn công Mask**

VD: hashcat -a 0 -m 0 file-chứa-hash file-danh-sách

Chú ý: trên Kali cũng có 1 danh sách mật khẩu: /usr/share/wordlists/rockyou.txt

d. John The Ripper

John the Ripper là một công cụ phần mềm bẻ khóa mật khẩu miễn phí. Đây cũng là một công cụ trên giao diện dòng lệnh và cũng có thể được cài trên nhiều hệ điều hành khác nhau như MacOS, Windows và Linux.

John The Ripper được thiết kế rất dễ sử dụng và có tích hợp cả tính năng tự động nhận diện thuật toán hash, thế nên chúng ta không cần phải xác định thuật toán rồi mới crack giống như Hashcat. Nó cũng hỗ trợ rất nhiều thuật toán mã hóa:

```
(tranhthuphuong@tranhthuphuong151)-[~]
$ john --list=formats
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS, tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssh1, aix-ssh256, aix-ssh512, andOTP, ansible, argon2, as400-des, as400-ssh1, asa-md5, AxCrypt, AzureAD, BestCrypt, BestCryptVE4, bfegg, Bitcoin, BitLocker, bitshares, Bitwarden, BKS, BlackBerry-ES10, WoWSRP, Blockchain, chap, Clipperz, cloudkeychain, dynamic_n, cq, CRC32, cryptoSafe, sha1crypt, sha256crypt, sha512crypt, Citrix_NS10, dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec, dominosec8, DPAPImk, dragonfly3-32, dragonfly3-64, dragonfly4-32, dragonfly4-64, Drupal7, eCryptfs, eigrp, electrum, EncFS, enpass, EPI, EPiServer, ethereum, fde, Fortigate256, Fortigate, FormSpring, FVDE, geli, gost, gpg, HAVAL-128-4, HAVAL-256-3, hdaa, hMailServer, hsrp, IKE, ipb2, itunes-backup, iwork, KeePass, keychain, keyring, keystore, known_hosts, krb4, krb5, krb5asrep, krb5pa-sha1, krb5tgs,
```

John the Ripper có các chế độ:

- Tấn công từ điển: Nó lấy các mẫu chuỗi văn bản (trong danh sách từ điển), mã hóa nó theo cùng định dạng với mật khẩu đang được kiểm tra, rồi so sánh đầu ra với chuỗi mật khẩu được mã hóa.
- John cũng có chế độ vét cạn: nó sẽ thử tất cả các tổ hợp có thể của các ký tự, đem đi mã hóa rồi so sánh mật khẩu đã mã khóa cho đến khi tìm ra mật khẩu chính xác. Cách này rất tốn thời gian.

Cú pháp sử dụng:

- Không chỉ định thuật toán crack: sẽ rất tốn thời gian

John path/to/password-file

- Chỉ định thuật toán crack:

john --format=<Format> path/to/password-file

- Crack mật khẩu sử dụng 1 danh sách từ điển:

john --format=FORMAT --wordlist=mywordlist.txt path/to/password-file

Trong đó, **--format=FORMAT** là định dạng của mật khẩu bạn muốn crack (ví dụ: **--format=md5**, **--format=sha512**,...), và **path/to/password-file** là đường dẫn đến tệp chứa mật khẩu.

2.2. Các bước thực hiện

2.2.1 Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa.
- Phần mềm hệ điều hành Linux và Windows.
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Linux
- Cài đặt các công cụ Crack mật khẩu trên hệ điều hành Windows

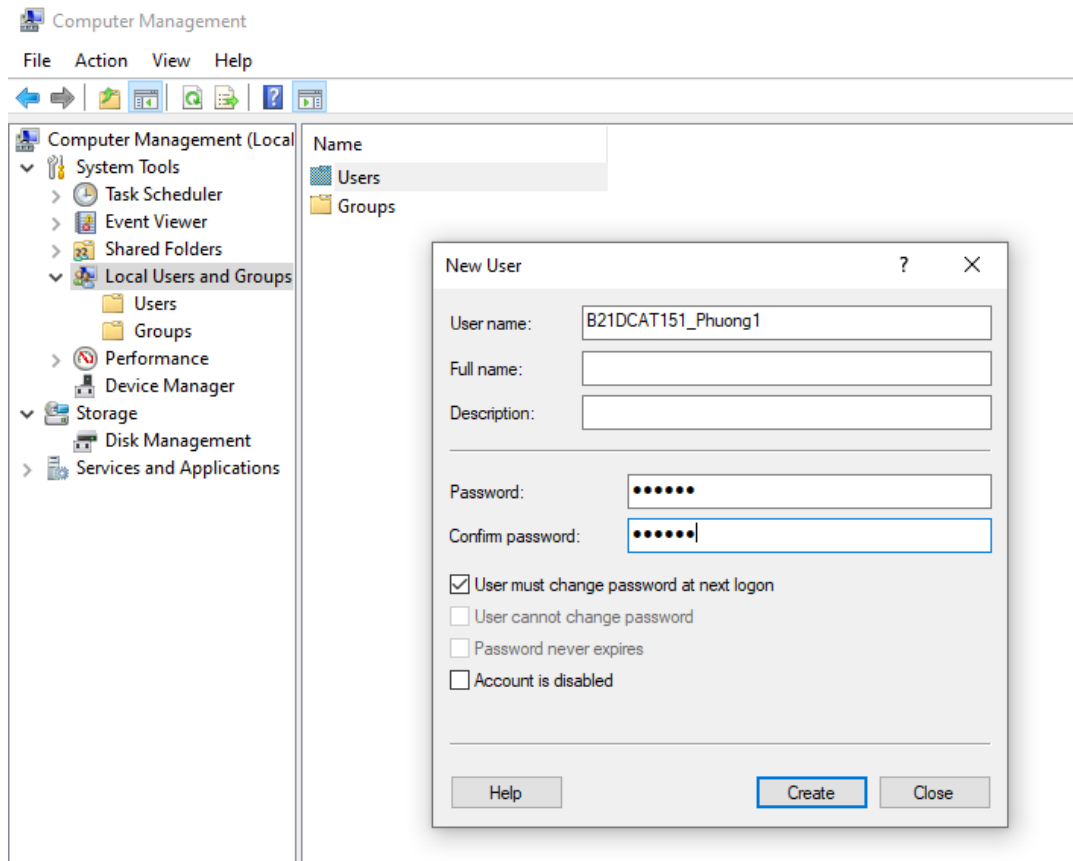
2.2.2 Crack mật khẩu trên Windows

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.

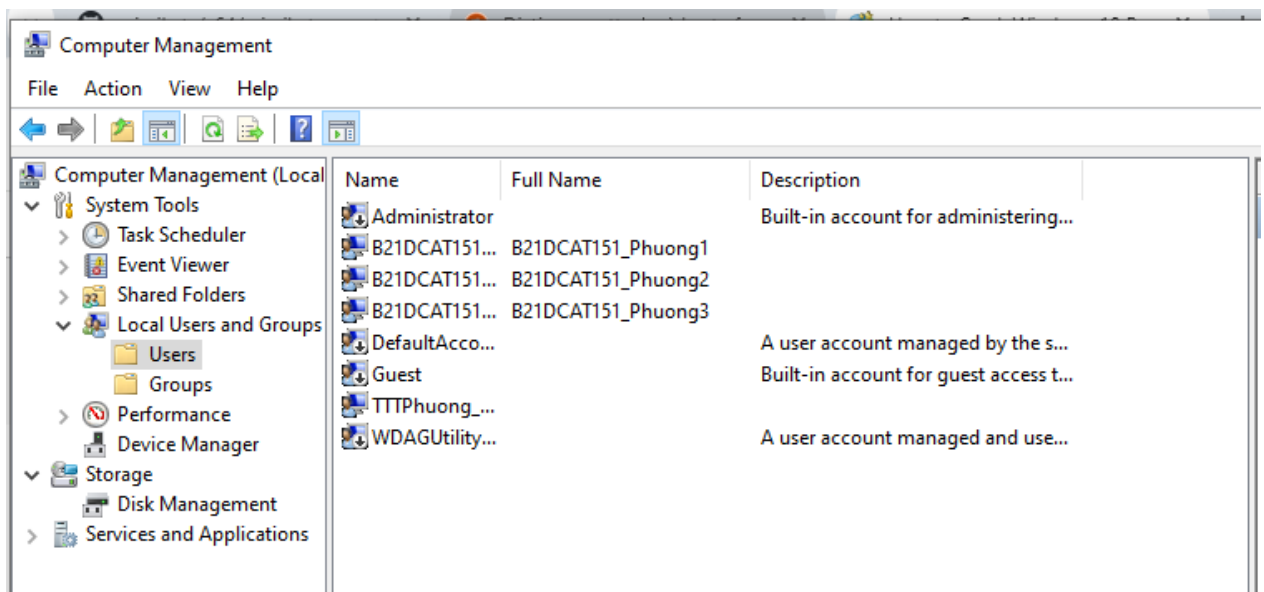
Bài 12: Tấn công mật khẩu

- Tạo thêm 3 tài khoản trên Windows có mật khẩu thỏa mãn 4 ký tự, 6 ký tự, 8 ký tự:

Computer Management → Local Users and Group → chuột phải vào Users → Add User.



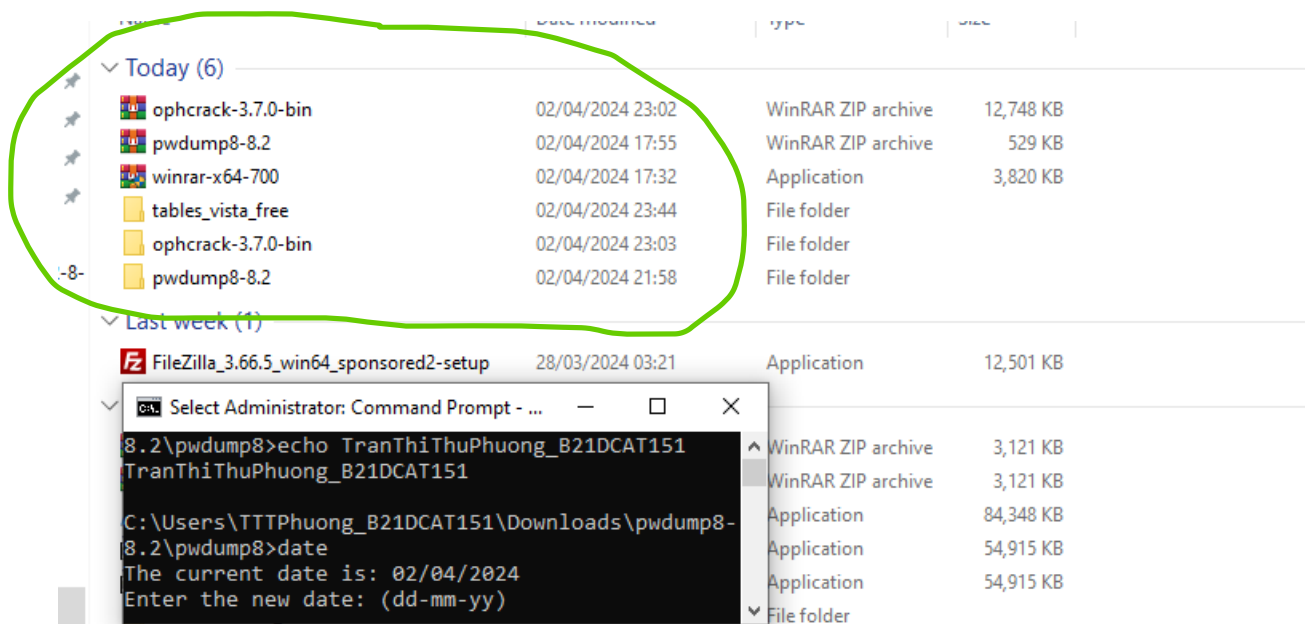
Tạo các Account



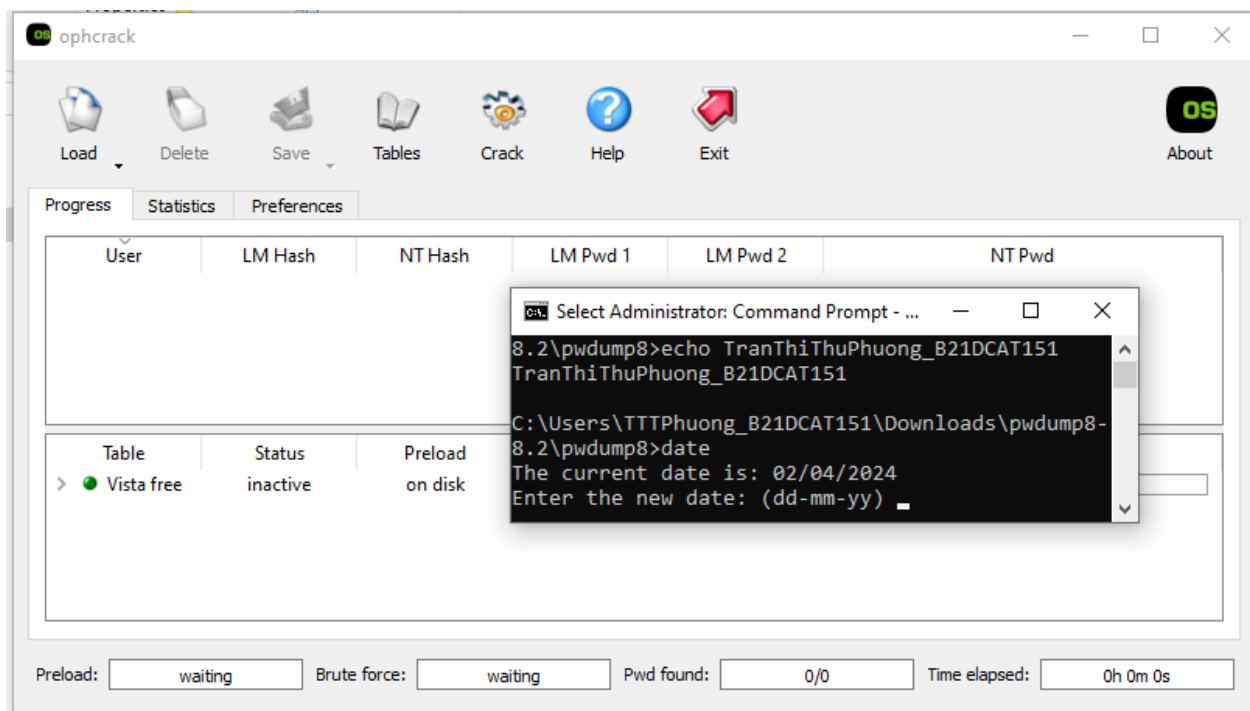
Kết quả

Bài 12: Tấn công mật khẩu

- Tải công cụ PwDump8, Ophcrack (phải tải cả các Rainbow của Ophcrack). Giải nén các tập tin đã tải và tiến hành cài đặt.



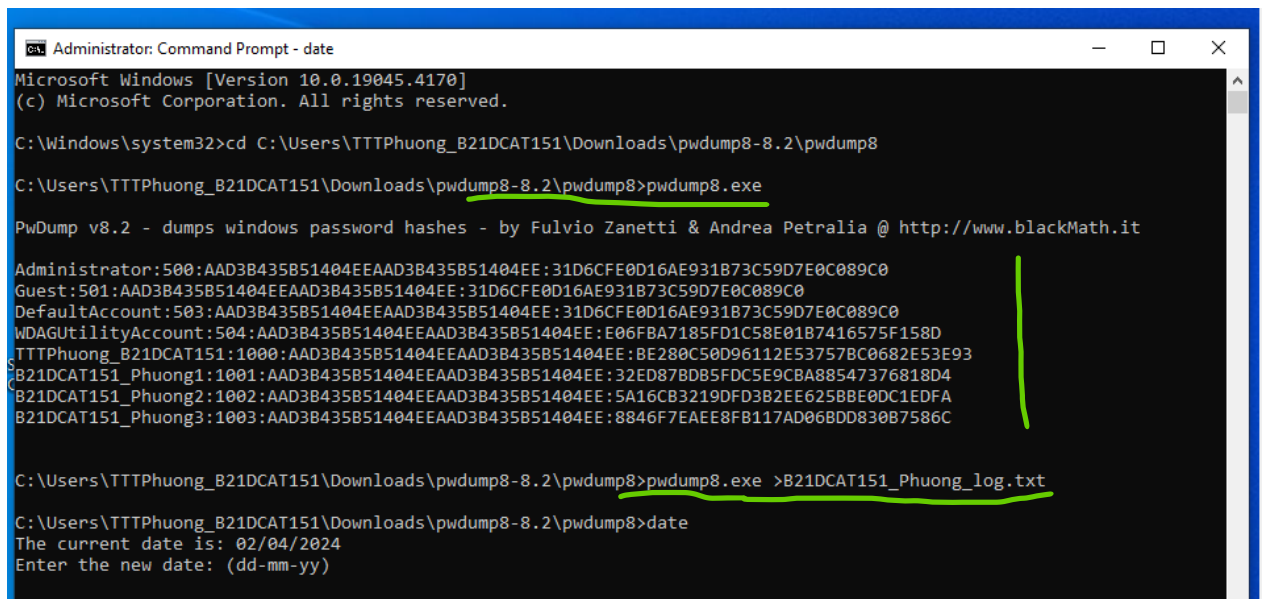
Các gói cần cài đặt



Giao diện OphCrack sau khi tải

Bài 12: Tấn công mật khẩu

- Chạy PwDump với quyền Administrator để trích xuất mật khẩu đăng nhập, đưa nó vào file B21DCAT151_Phuong_log.txt



```
Administrator: Command Prompt - date
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\TTTPhuong_B21DCAT151\Downloads\pwdump8-8.2\pwdump8

C:\Users\TTTPhuong_B21DCAT151\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe

PwDump v8.2 - dumps windows password hashes - by Fulvio Zanetti & Andrea Petralia @ http://www.blackMath.it

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
DefaultAccount:503:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
WDAGUtilityAccount:504:AAD3B435B51404EEAAD3B435B51404EE:E06FBA7185FD1C58E01B7416575F158D
TTTPhuong_B21DCAT151:1000:AAD3B435B51404EEAAD3B435B51404EE:BE280C50D96112E53757BC0682E53E93
B21DCAT151_Phuong1:1001:AAD3B435B51404EEAAD3B435B51404EE:32ED87BDB5FDC5E9CBA88547376818D4
B21DCAT151_Phuong2:1002:AAD3B435B51404EEAAD3B435B51404EE:5A16CB3219DFD3B2EE625B8E0DC1EDFA
B21DCAT151_Phuong3:1003:AAD3B435B51404EEAAD3B435B51404EE:8846F7EAE8FB117AD06BDD830B7586C

C:\Users\TTTPhuong_B21DCAT151\Downloads\pwdump8-8.2\pwdump8>pwdump8.exe >B21DCAT151_Phuong_log.txt

C:\Users\TTTPhuong_B21DCAT151\Downloads\pwdump8-8.2\pwdump8>date
The current date is: 02/04/2024
Enter the new date: (dd-mm-yy)
```

Trích xuất mật khẩu

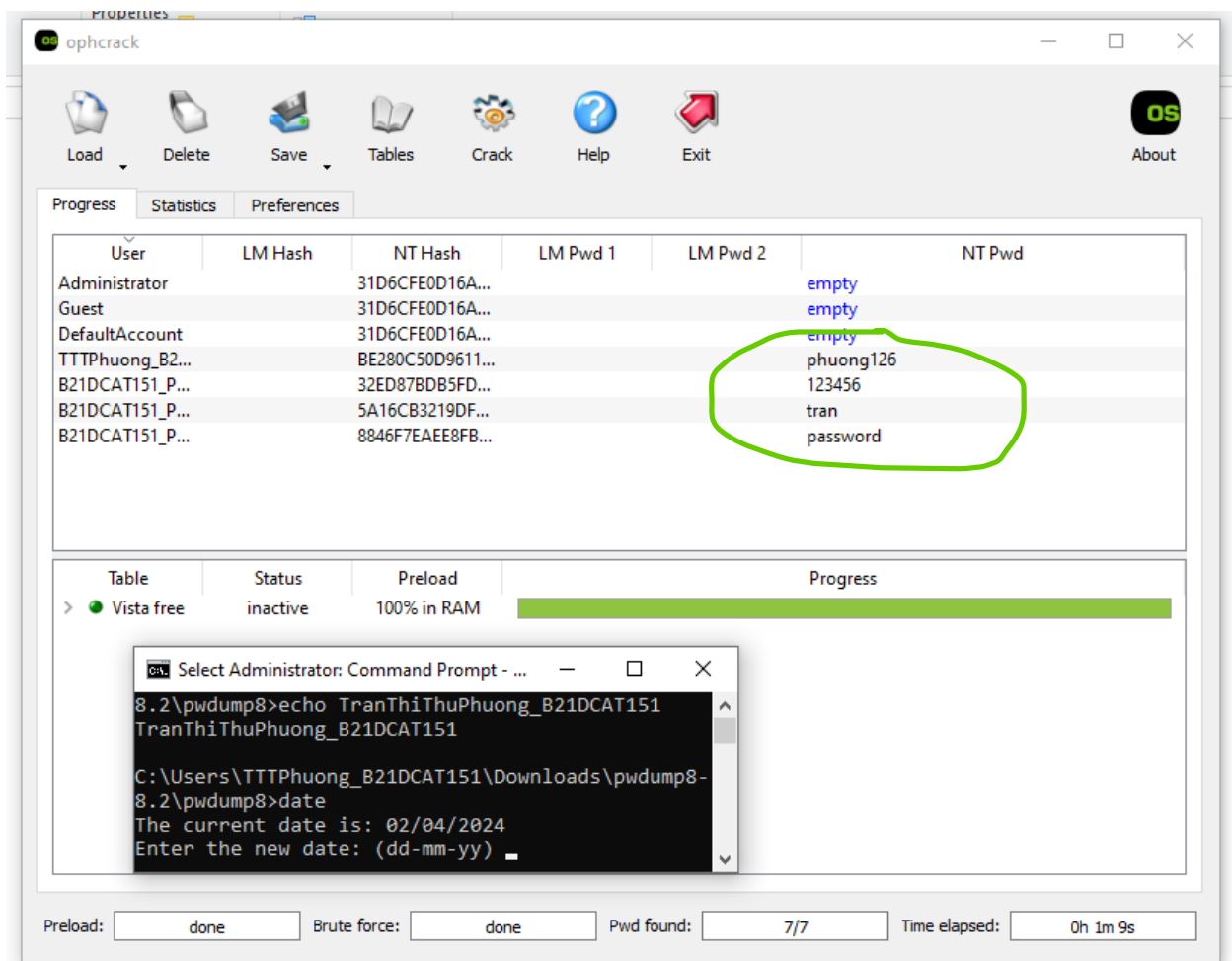
- Lưu ý, mỗi dòng trong file B21DCAT151_Phuong_log.txt cần phải đảm bảo đúng định dạng như sau:
B21DCAT151_Phuong3:1003:AAD3B435B51404EEAAD3B435B51404EE:8846F7EAE8FB117AD06BDD830B7586C:::
- Sử dụng OphCrack để crack mật khẩu:
 - + Đầu tiên phải kích hoạt các Rainbow đã tải: Tables → chọn thư mục đã lưu Rainbow

XP german v2	not installed	on disk
Vista special	not installed	on disk
> Vista free	C:\Users\TTTPhuong_B21DCAT151\Downl...	inactive on disk
Vista nine	not installed	on disk
Vista eight	not installed	on disk

Kích hoạt Rainbow

- Crack các mật khẩu đã lưu trên file B21DCAT151_Phuong_log.txt: Load → PWDUMP File → chọn File đã lưu. Đợi file tải hết và chọn Crack để tiến hành bẻ khóa mật khẩu. Kết quả đã bẻ khóa thành công mật khẩu 4 kí tự, 6 kí tự, 8 kí tự, 9 kí tự (cả số cả chữ) (rất nhanh).

Bài 12: Tấn công mật khẩu



Kết quả

2.2.3 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 đầu là mã sinh viên.

- Tạo user và đặt mật khẩu theo yêu cầu

```
tranphuong@tranthithuphuong151: ~  
  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo passwd B21DCAT151_TTTPhuong1  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo useradd B21DCAT151_TTTPhuong2  
  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo passwd B21DCAT151_TTTPhuong2  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo useradd B21DCAT151_TTTPhuong3  
  
(tranphuong@tranthithuphuong151)-[~]  
$ sudo passwd B21DCAT151_TTTPhuong3  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(tranphuong@tranthithuphuong151)-[~]  
$ date  
Tue Apr 2 00:08:03 EDT 2024
```

Tạo các User

```
nm-openconnect:x:132:139:NetworkManager OpenConnect plugin,,:/var/lib/NetworkMan  
ager:/usr/sbin/nologin  
tranphuong:x:1000:1000:tranphuong,,:/home/tranphuong:/usr/bin/zsh  
B21DCAT151_TTTPhuong1:x:1001:1001:/:home/B21DCAT151_TTTPhuong1:/bin/sh  
B21DCAT151_TTTPhuong2:x:1002:1002:/:home/B21DCAT151_TTTPhuong2:/bin/sh  
B21DCAT151_TTTPhuong3:x:1003:1003:/:home/B21DCAT151_TTTPhuong3:/bin/sh  
  
(tranphuong@tranthithuphuong151)-[~]  
$
```

Kiểm tra lại trên file /etc/passwd

- Kết hợp 2 file /etc/passwd và file /etc/shadow để phục vụ cho quá trình crack mật khẩu sử dụng John The Ripper (đây là công cụ có sẵn trên Kali)

Bài 12: Tấn công mật khẩu

```
(tranhuphuong@tranhuphuong151)-[~]
$ sudo unshadow /etc/passwd /etc/shadow > Account_Phuong151.txt
Created directory: /root/.john

(tranhuphuong@tranhuphuong151)-[~]
$ date
Tue Apr 2 00:12:20 EDT 2024

(tranhuphuong@tranhuphuong151)-[~]
$
```

Kết hợp 2 file /etc/passwd và file /etc/shadow

- Kết quả: crack thành công mật khẩu 4 ký tự, 6 ký tự, 8 ký tự

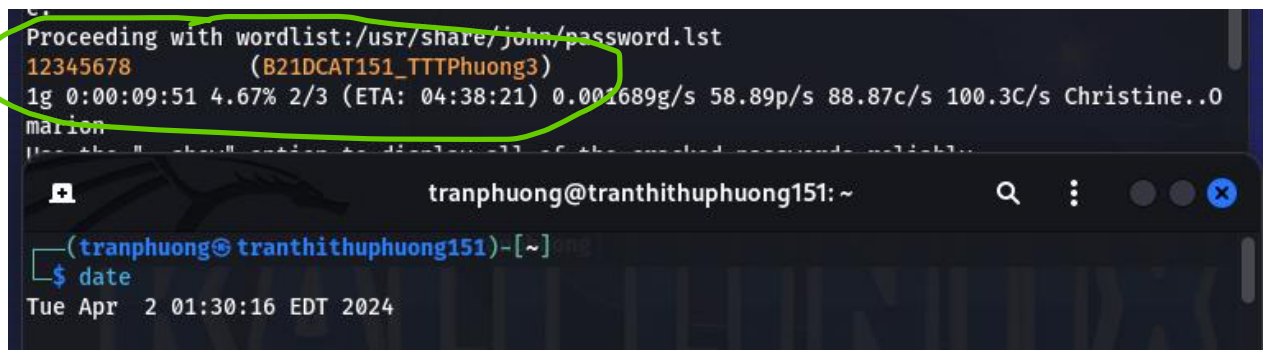
```
root@tranhuphuong151: ~tranhuphuong

(tranhuphuong@tranhuphuong151)-[/home/tranhuphuong]
# john --format=crypt Account_Phuong151.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 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 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
phuong (B21DCAT151_TTTPhuong2)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 68 candidates buffered for the current salt, minimum 96 needed for performanc
e.
Proceeding with wordlist:/usr/share/john/password.lst
1234 (B21DCAT151_TTTPhuong1)
2g 0:00:37:03 34.70% 2/3 (ETA: 02:14:49) 0.000899g/s 39.04p/s 91.03c/s 91.03C/s hoops0..max
0

tranhuphuong@tranhuphuong151: ~
(tranhuphuong@tranhuphuong151)-[~]
$ date
Tue Apr 2 01:30:16 EDT 2024

(tranhuphuong@tranhuphuong151)-[~]
$
```

Crack thành công mật khẩu 4 ký tự, 6 ký tự



```
Proceeding with wordlist:/usr/share/john/password.lst
12345678 (B21DCAT151_TTTPhuong3)
1g 0:00:09:51 4.67% 2/3 (ETA: 04:38:21) 0.001689g/s 58.89p/s 88.87c/s 100.3C/s Christine..0
marion
```

tranphuong@tranthithuphuong151: ~

(tranphuong@tranthithuphuong151)-[~]

\$ date

Tue Apr 2 01:30:16 EDT 2024

Crack thành công mật khẩu 8 kí tự

3. Kết luận

- Lý thuyết về các công cụ crack mật khẩu trên Windows, Kali Linux
- Crack mật khẩu thành công trên Windows
- Crack mật khẩu thành công trên Kali Linux

4. Tài liệu tham khảo

- [1]. Crack mật khẩu trên Windows: [xem tại đây](#)
- [2]. Crack mật khẩu trên Kali: [Xem tại đây](#)
- [3]. 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.
- [4]. Chapter 11 Authentication and Remote Access, sách Principles of Computer Security CompTIA Security+ and Beyond Lab Manual (Exam SY0-601) by Jonathan S. Weissman