

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
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

Giảng viên hướng dẫn : PGS.TS Hoàng Xuân Dậu
Sinh viên thực hiện : Nguyễn Nhật Minh
Mã sinh viên : B21DCAT132

Hà Nội, tháng 3 năm 2024

Môn học: Thực tập cơ sở

Bài 12: Crack 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. Tìm hiểu lý thuyết

2.1. Các loại tấn công mật khẩu

Rất hiếm tình huống tấn công hệ thống bắt đầu bằng việc phá mật khẩu vì đây là một trong những thông tin quan trọng nhất để truy cập vào hệ thống. Có nhiều dạng mật khẩu khác nhau nhưng thông thường khi người dùng muốn truy cập vào hệ thống của mình thì anh ta cần phải cung cấp thông tin gồm tài khoản cùng với mật khẩu liên quan. Vì nhiều lý do cá nhân mà người dùng thường đặt mật khẩu khá dễ nhớ và liên quan đến các thông tin đặc biệt của bản thân. Do đó mà việc tấn công mật khẩu thường có tỉ lệ thành công cao. Đặc biệt, các mật khẩu lại thường được dùng chung cho nhiều dịch vụ khác nhau cho nên khi một mật khẩu bị phá vỡ thì các hệ thống khác cũng chịu chung số phận. Một khi việc bẻ khóa thành công thì hacker sẽ tiến hành các thao tác leo thang đặc quyền, chạy những chương trình nguy hiểm trên hệ thống bị tấn công và sau đó là tiến hành che dấu tập tin, xóa dấu vết để phòng chống bị điều tra

Một cách tổng quan, có 4 dạng tấn công mật khẩu là:

1. Passive Online: Nghe trộm sự thay đổi mật khẩu trên mạng. Cuộc tấn công thụ động trực tuyến bao gồm: sniffing, man-in-the-middle, replay attacks(tấn công dựa vào phản hồi)
2. Active Online: Đoán trước mật khẩu người quản trị. Các cuộc tấn công trực tuyến bao gồm việc đoán password tự động.
3. Offline: Các kiểu tấn công như Dictionary, hybrid, brute-force.
4. Non-electronic: Các cuộc tấn công dựa vào yếu tố con người như Social engineering, Phising...

Passive Online Attack

Một cuộc tấn công thụ động trực tuyến là đánh hơi(sniffing) để tìm kiếm các dấu vết, các mật khẩu trên một mạng. Mật khẩu là bị bắt (capture) trong quá trình xác thực và sau đó có thể được so sánh với một từ điển (dictionary) hoặc là danh sách từ (wordlist). Tài khoản người dùng có mật khẩu thường được băm (hashed) hoặc mã hóa (encrypted) trước khi gửi lên mạng để ngăn chặn truy cập trái phép và sử dụng. Nếu mật khẩu được bảo vệ bằng cách trên, một số công cụ đặc biệt giúp hacker có thể phá vỡ các thuật toán mã hóa mật khẩu.

Active Online Attack

Cách dễ nhất để đạt được cấp độ truy cập của 1 quản trị viên hệ thống là phải đoán từ

đơn giản thông qua giả định là các quản trị viên sử dụng 1 mật khẩu đơn giản. Mật khẩu đoán là để tấn công. Active online attack dựa trên yếu tố con người tham gia vào việc tạo ra mật khẩu và cách tấn công này chỉ hữu dụng với những mật khẩu yếu. Hầu hết các hệ thống ngăn chặn kiểu tấn công này bằng cách thiết lập một số lượng tối đa của các nỗ lực đăng nhập vào 1 hệ thống trước khi tài khoản bị khóa. Ví dụ bạn có thể đăng nhập vào 1 trang web mà bạn nhập sai 3 lần thì tài khoản sẽ tự động bị khóa 1 ngày.

Offline Attack

Các cuộc tấn công Offline được thực hiện tại một vị trí khác hơn là hành động tại máy tính mục tiêu. Cuộc tấn công Offline yêu cầu phần cứng để truy cập vật lý vào máy tính và sao chép các tập tin mật khẩu từ hệ thống lên phương tiện di động. Hacker sau đó có file đó và tiếp tục khai thác lỗ hổng bảo mật. Một vài kiểu tấn công Offline phổ biến:

1. Brute-Force-Attacks

Kẻ tấn công thử tất cả các khả năng mật khẩu có thể có bằng cách liên tục thử từng ký tự, từng từ, hoặc thậm chí thử tất cả các kết hợp có thể của các ký tự để kiểm tra xem mật khẩu nào là chính xác.

Có thể sử dụng một số tool như Hashcat, John the Ripper.

2. Dictionary Attack

Đây là cách tấn công đơn giản và nhanh nhất trong các loại hình tấn công. Kẻ tấn công sử dụng một "từ điển" chứa các từ phổ biến, mật khẩu thông dụng, và các kết hợp ký tự thường được người dùng sử dụng. Đối với mỗi mật khẩu có thể, hacker thử tất cả các từ trong từ điển để xem có trùng khớp không.

Có thể sử dụng một số tool như Hashcat, John the Ripper.

3. Hybrid Attack

Đây là cấp độ tiếp theo của hacker, một nỗ lực nếu mật khẩu không thể được tìm thấy bằng cách sử dụng Dictionary Attack. Các cuộc tấn công Hybrid bắt đầu với một tập tin từ điển và thay thế các con số và các ký hiệu cho các ký tự trong mật khẩu. Ví dụ, nhiều người sử dụng thêm số 1 vào cuối mật khẩu của họ để đáp ứng yêu cầu mật khẩu mạnh. Hybrid được thiết kế để tìm những loại bất thường trong mật khẩu.

4. Pass the Hash Attacks

Kẻ tấn công sử dụng giá trị băm (hash) của mật khẩu đã được đánh cắp để đăng nhập vào hệ thống mà không cần biết mật khẩu thực tế. Điều này làm tăng khả năng thành công nếu hệ thống không sử dụng các biện pháp bảo mật như salt hoặc các phương thức băm mạnh mẽ.

Có thể sử dụng một số tool như Mimikatz, PTH-Winexe.

5. Credential Stuffing

Kẻ tấn công sử dụng tên người dùng và mật khẩu đã bị đánh cắp từ một trang web hoặc

dịch vụ khác để thử đăng nhập vào các tài khoản khác của người dùng (vì nhiều người tái sử dụng mật khẩu)

Non-Electronic Attack

Các cuộc tấn công non-electronic là dạng tấn công mà không sử dụng bất kỳ kiến thức kỹ thuật nào. Loại tấn công có thể bao gồm các kỹ thuật như:

1. Social engineering: sử dụng tâm lý, mẹo khéo và lừa dối để lôi kéo thông tin quan trọng từ mục tiêu.
2. Shoulder surfing: hacker quan sát màn hình hoặc bàn làm việc của người dùng mục tiêu để thu thập thông tin nhạy cảm
3. Keyboard Sniffing: sử dụng thiết bị đặc biệt để nghe hoặc ghi lại âm thanh khi các phím được nhấn trên bàn phím
4. Dumpster Diving: thu thập thông tin từ rác thải hoặc các vật liệu vứt đi như tài liệu, ổ cứng ...
5. Tailgating: hacker bắt chước một người có quyền truy cập để vào khu vực hạn chế mà không được phép
6. Impersonation: hacker giả mạo thành một cá nhân hoặc đối tượng khác để đánh lừa người khác.

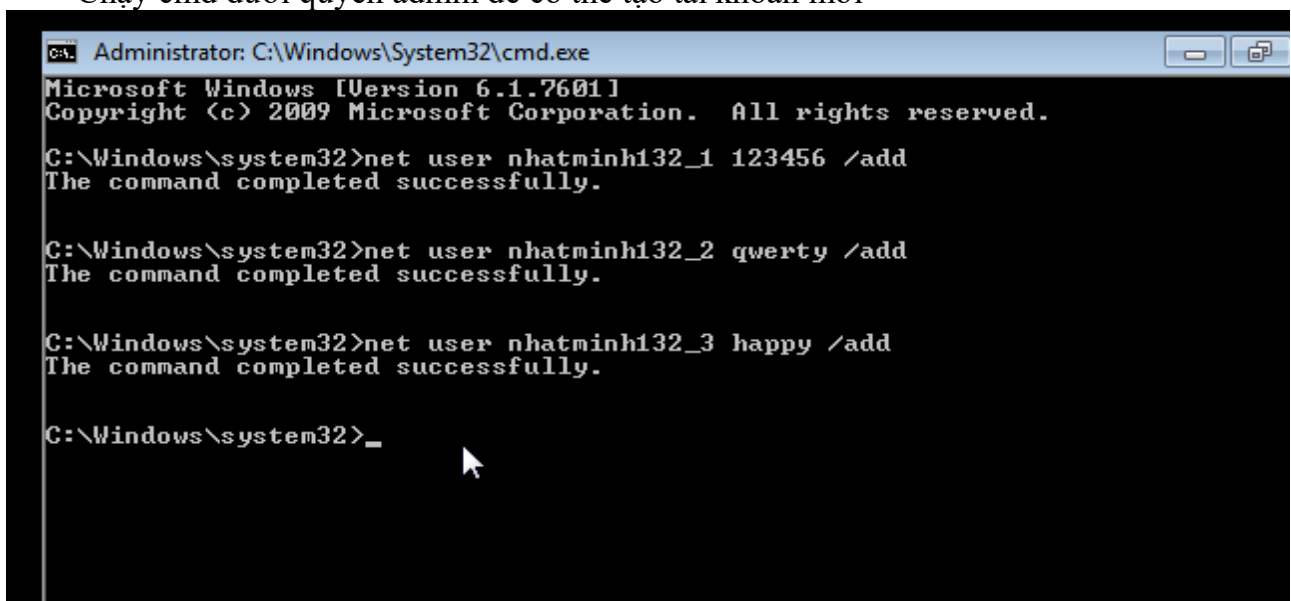
3. Chuẩn bị môi trường

- 1 máy windows 7 để thực hành crack password trên hệ điều hành windows
- 1 máy linux để thực hành crack password trên hệ điều hành linux

4. Thực hành

4.1. Crack password trên windows 7 bằng pwdump7 và hash suite

- Ở đây chúng ta sẽ dùng pwdump7 để trích xuất các hash mật khẩu từ SAM và hiển thị chúng sang dạng văn bản, sau đó sử dụng hash suite để crack mật khẩu
- Chạy cmd dưới quyền admin để có thể tạo tài khoản mới



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

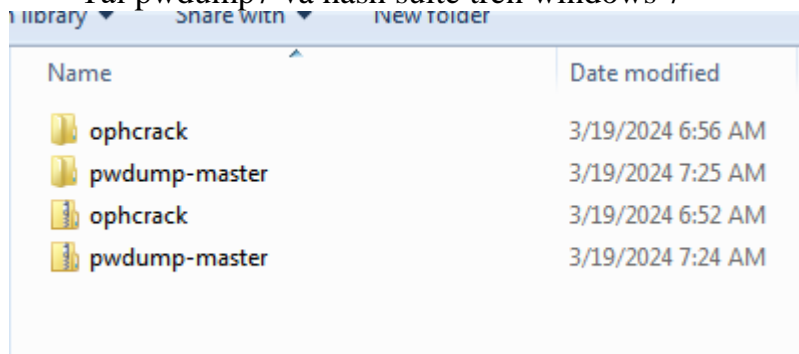
C:\Windows\system32>net user nhatminh132_1 123456 /add
The command completed successfully.

C:\Windows\system32>net user nhatminh132_2 qwerty /add
The command completed successfully.

C:\Windows\system32>net user nhatminh132_3 happy /add
The command completed successfully.

C:\Windows\system32>_
```

- Tải pwdump7 và hash suite trên windows 7

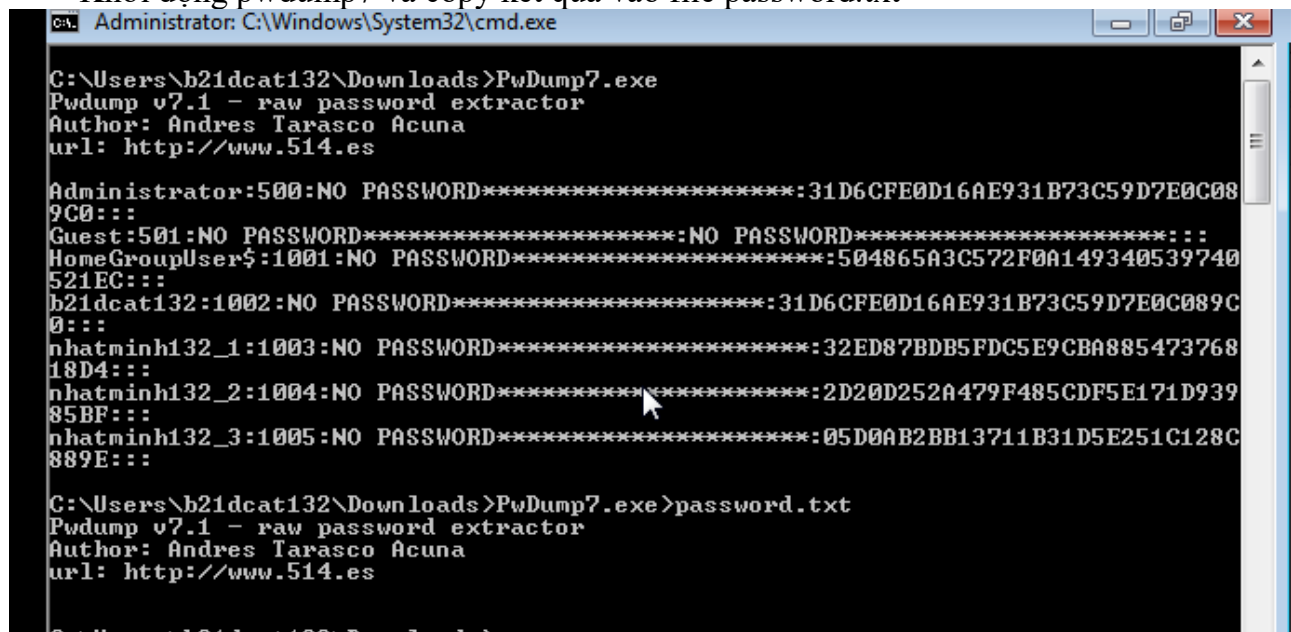


- Sử dụng lệnh wmic useraccount get name, sid để xem thông tin tài khoản và mật khẩu

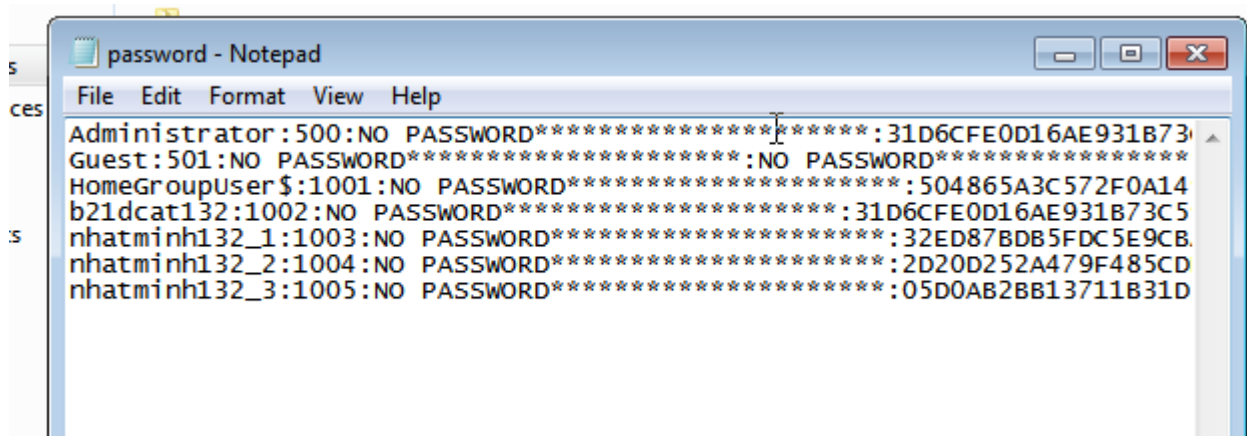
```
C:\Windows\system32>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-4054232014-4107577376-2269026556-500
b21dcat132 S-1-5-21-4054232014-4107577376-2269026556-1002
Guest S-1-5-21-4054232014-4107577376-2269026556-501
HomeGroupUser$ S-1-5-21-4054232014-4107577376-2269026556-1001
nhatminh132_1 S-1-5-21-4054232014-4107577376-2269026556-1003
nhatminh132_2 S-1-5-21-4054232014-4107577376-2269026556-1004
nhatminh132_3 S-1-5-21-4054232014-4107577376-2269026556-1005

C:\Windows\system32>wmic useraccount get name,sid > minh.txt
C:\Windows\system32>_
```

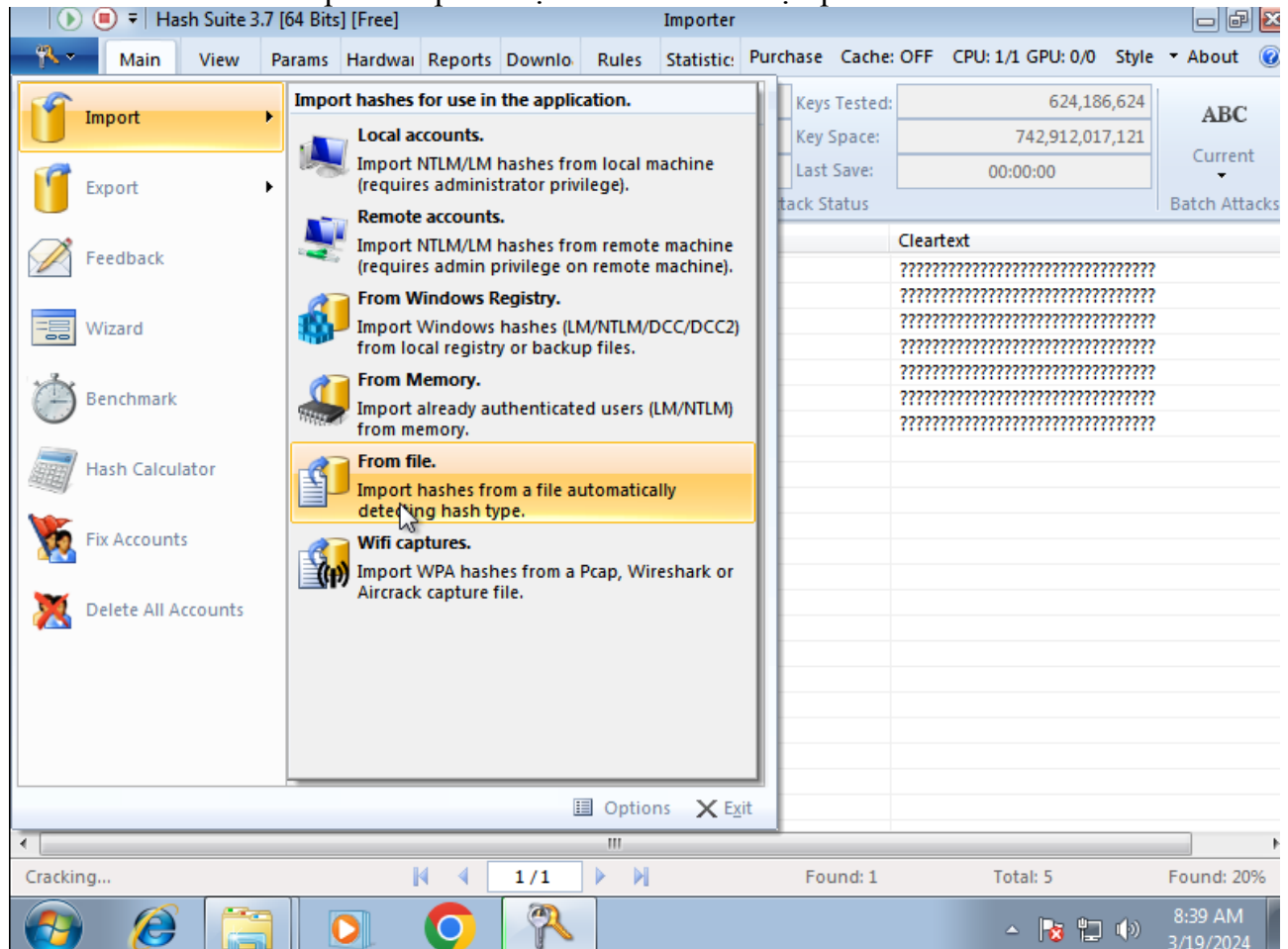
- Khởi động pwdump7 và copy kết quả vào file password.txt



- Kiểm tra để chắc chắn file đã lưu



- Trên hash suite ở phần import chọn from file và chọn password.txt



- Sau khi start thì tool đã tìm ra mật khẩu của 3 user

Username	Hash	Cleartext
Administrator	31D6CFE0D16AE931B73C59D7E0C089C0	
Guest	31D6CFE0D16AE931B73C59D7E0C089C0	
b21dcat132	31D6CFE0D16AE931B73C59D7E0C089C0	
HomeGroupUser\$	504865A3C572F0A149340539740521EC	????????????????????????????????
nhatminh132_1	32ED87BDB5FDC5E9CBA88547376818D4	123456
nhatminh132_2	2D20D252A479F485CDF5E171D93985BF	qwerty
nhatminh132_3	05D0AB2BB13711B31D5E251C128C889E	happy

4.2. Crack mật khẩu bằng john the ripper trên linux

- Tạo 3 tài khoản và mật khẩu trên linux

```

root@minhnn132: /home/b21dcat132

root@minhnn132:/home/b21dcat132# useradd -m minh132_1
root@minhnn132:/home/b21dcat132# useradd -m minh132_2
root@minhnn132:/home/b21dcat132# useradd -m minh132_3
root@minhnn132:/home/b21dcat132# passwd minh132_1
New password:
Retype new password:
passwd: password updated successfully
root@minhnn132:/home/b21dcat132# passwd minh132_2
New password:
Retype new password:
passwd: password updated successfully
root@minhnn132:/home/b21dcat132# passwd minh132_3
New password:
Retype new password:
passwd: password updated successfully

```

- Tài khoản và mật khẩu sẽ được lưu ở mục /etc/shadow
- Sử dụng lệnh grep để lọc kết quả
- Copy tài khoản và mật khẩu hash vào file password.txt

```

root@minhnn132: /home/b21dcat132

root@minhnn132:/home/b21dcat132# cat /etc/shadow | grep minh132
minh132_1:$6$LjEc6bcB3146eNSX$RUU09MP1F04LJOI1NTdF9o.X8npMkzUTVjsdbkDuV.5z0JfT
MnMqMJynB60wHR5//qNwnXx4eJVHZ6s0m9JfW0:19801:0:99999:7:::
minh132_2:$6$FvPUwJAYBT8yLaoQ$oiMJUr3oFR9tzrnQCWahvPgNpNENbE07e5Qhi3AaGPPaBtue
yugvZrWVxVBrpEQyNVQD0egUCMqslZ2Mi2U06.:19801:0:99999:7:::
minh132_3:$6$AHeweJDKAZFC7fWN$XWD3DfCSPPFGLdqWzZ3stwIb08GTYZU4CxtmqMwtJAns4db
AfkQuAfdiEsEXrHLUb15EFEBa03bLVUaSWJUS/:19801:0:99999:7:::
root@minhnn132:/home/b21dcat132# echo > password.txt
root@minhnn132:/home/b21dcat132# chmod 777 password.txt

```

- Cài đặt john the ripper bằng lệnh `sudo apt install john`
- Sử dụng lệnh `john password.txt` để thực hiện tìm mật khẩu


```
0g 0:00:00:03 7% 1/3 0g/s 261.0p/s 261.0c/s 261.0C/s 38..mminhat132_3d
Session aborted
root@minhnn132:/home/b21dcat132# john --format=crypt /home/b21dcat132/password.txt
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 8% 1/3 0g/s 266.1p/s 266.1c/s 266.1C/s minhat13299999d..minhat132k
password      (minhat132_3)
1234          (minhat132_1)
qwerty        (minhat132_2)
3g 0:00:02:16 100% 2/3 0.02192g/s 237.2p/s 238.7c/s 238.7C/s 123456..pepper
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@minhnn132:/home/b21dcat132#
```

- Kết quả đã crack thành công

5. Kết luận

- Bài thực hành hoàn thành vào ngày 19/03/2024

```
Session completed
root@minhnn132:/home/b21dcat132# date
Thứ ba, 19 Tháng 3 năm 2024 22:58:31 +07
root@minhnn132:/home/b21dcat132# nguyen nhat minh b21dcat132
nguyen: command not found
root@minhnn132:/home/b21dcat132#
```