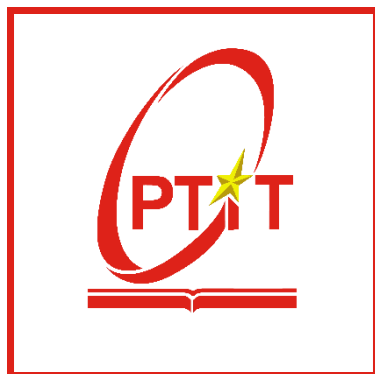


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

---



**THỰC TẬP CƠ SỞ**  
**Bài 12: Crack mật khẩu**

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

**Hà Nội – 2024**

# Môn học Thực tập cơ sở

## Bài 12: Crack mật khẩu

### I. Lý thuyết

#### 1. Các loại tấn công mật khẩu

Rất hiệu 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 dung 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 dung 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 dung 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.

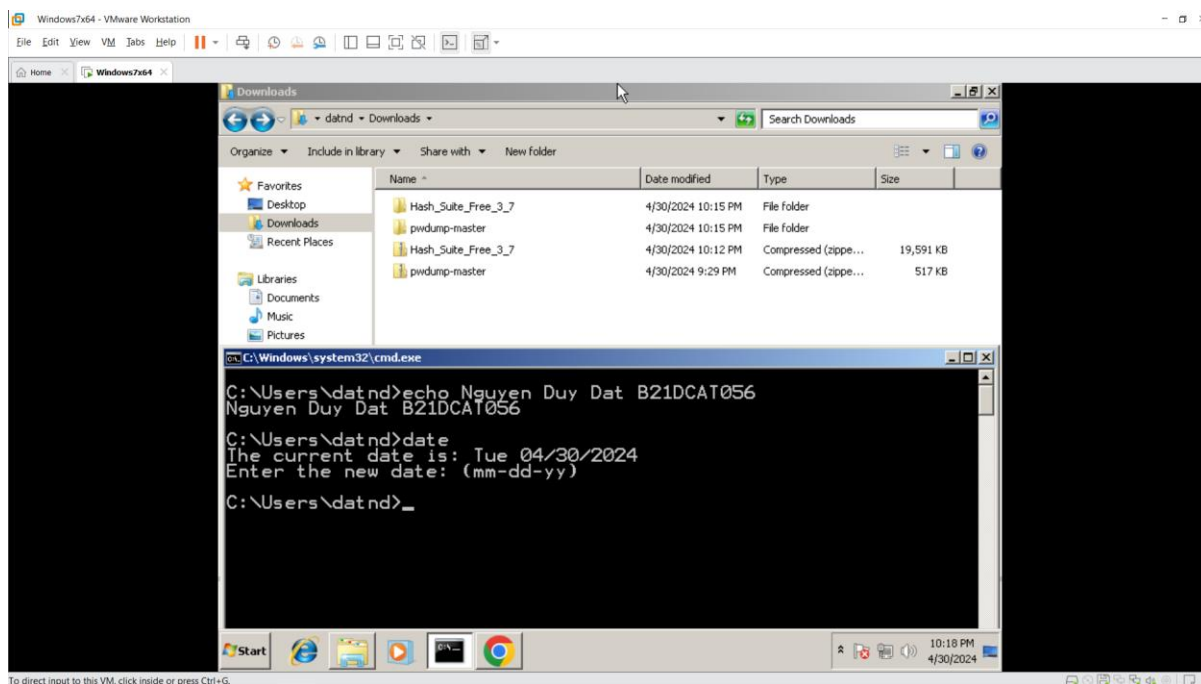
Một cách tổng quan, có 4 dạng tấn công mật khẩu là:

- ✓ 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)
- ✓ Active Online: Đoán trước mật khẩu người quản trị. Các cuộc tấn công trực tuyến bao gồm việc đoán password tự động.
- ✓ Offline: Các kiểu tấn công như Dictionary, hybrid, brute-force.
- ✓ Non-electronic: Các cuộc tấn công dựa vào yếu tố con người như Social engineering, Phising...

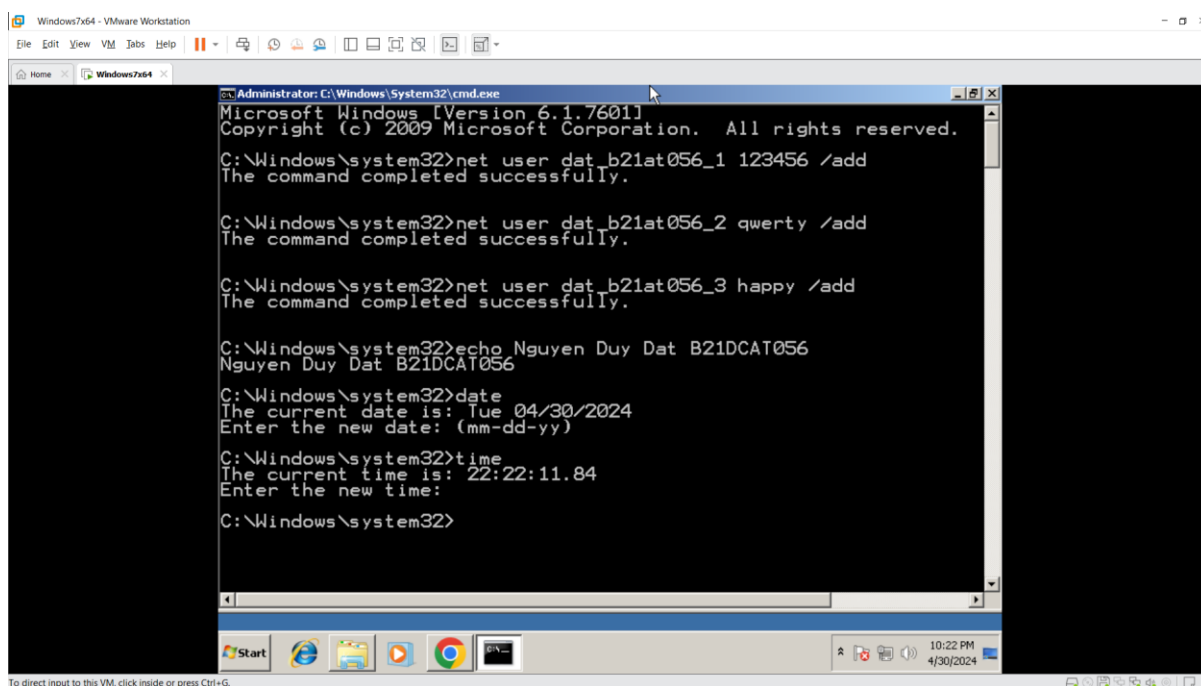
## II. Thực hành

### 1. Crack password trên Windows 7 bằng pwdump7 và hash suite

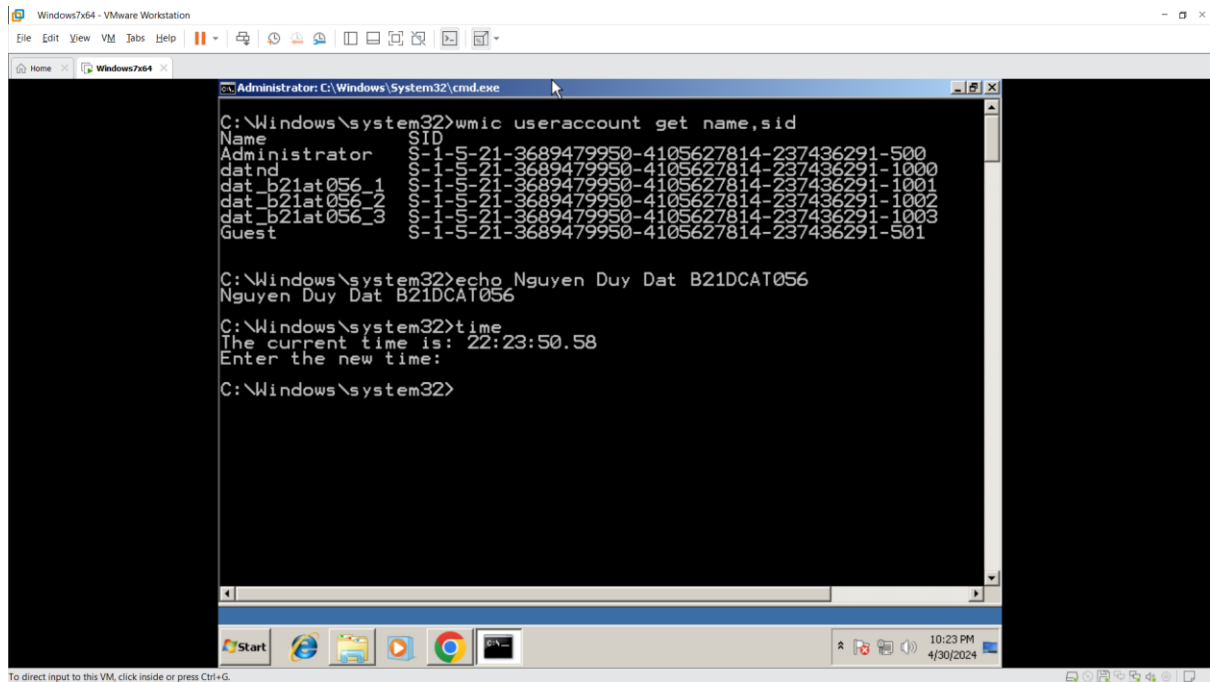
- Ở đây chúng ta sẽ dùng pwdump7 để trích xuất các hash mật khẩu từ SAM và hiển thị chúng sang dạng văn bản, sau đó sử dụng hash suite để crack mật khẩu
- Tải pwdump7 và hash suite trên Windows 7



- Chạy cmd dưới quyền admin để có thể tạo tài khoản mới



- 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-1-5-21-3689479950-4105627814-237436291-500
datnd S-1-5-21-3689479950-4105627814-237436291-1000
dat_b21at056_1 S-1-5-21-3689479950-4105627814-237436291-1001
dat_b21at056_2 S-1-5-21-3689479950-4105627814-237436291-1002
dat_b21at056_3 S-1-5-21-3689479950-4105627814-237436291-1003
Guest S-1-5-21-3689479950-4105627814-237436291-501

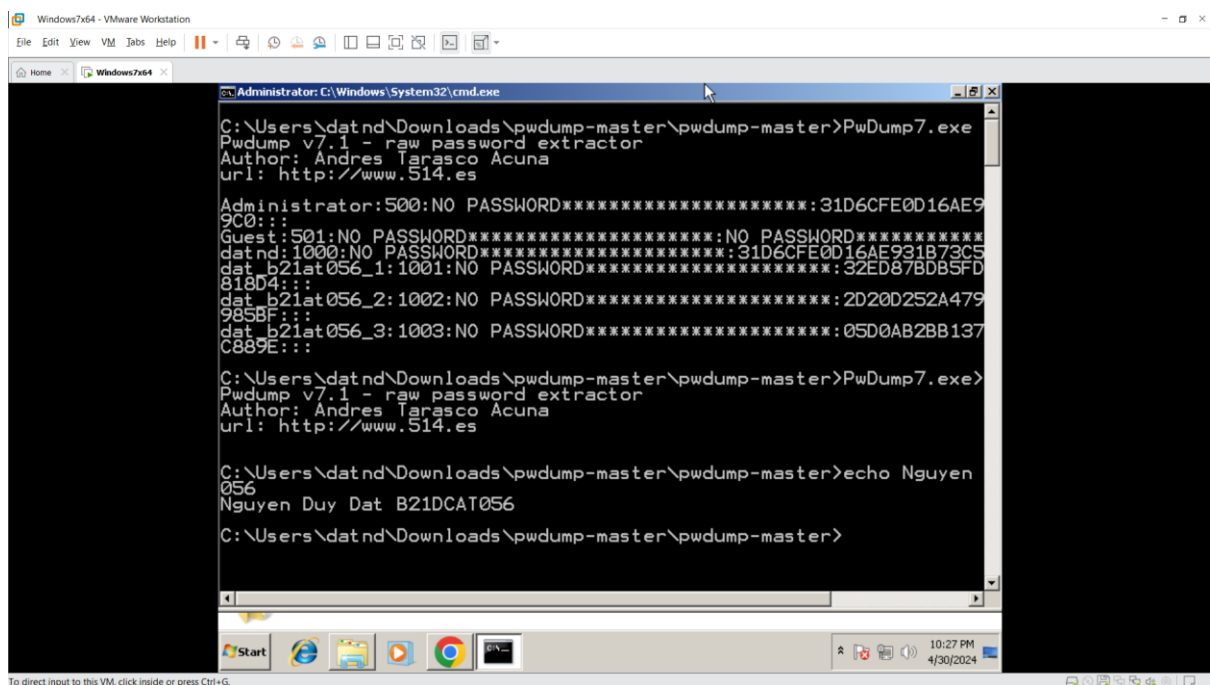
C:\Windows\system32>echo Nguyen Duy Dat B21DCAT056
Nguyen Duy Dat B21DCAT056

C:\Windows\system32>time
The current time is: 22:23:50.58
Enter the new time:

C:\Windows\system32>

```

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



```

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

Administrator:500:NO PASSWORD*****:31D6CFE0D16AE9
9C0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****
datnd:1000:NO PASSWORD*****:31D6CFE0D16AE931B73C5
dat_b21at056_1:1001:NO PASSWORD*****:32ED87BDB5FD
818D4:::
dat_b21at056_2:1002:NO PASSWORD*****:2D20D252A479
985BF:::
dat_b21at056_3:1003:NO PASSWORD*****:05D0AB2BB137
C889E:::

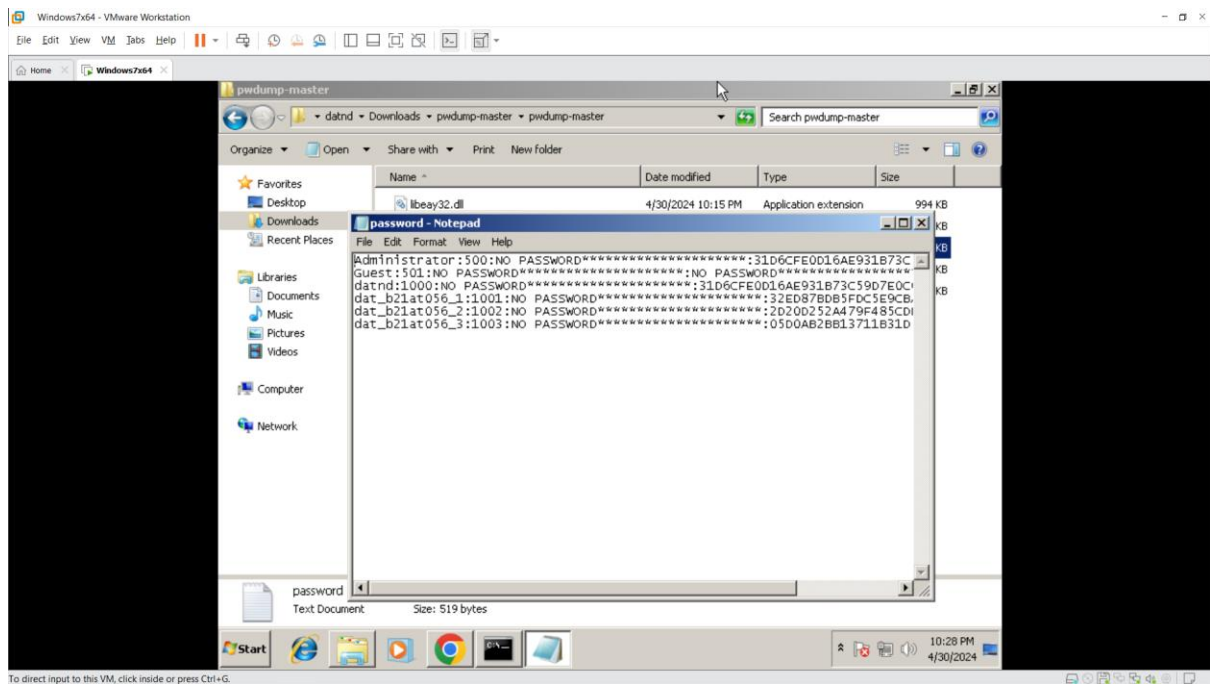
C:\Users\datnd\Downloads\pwdump-master\pwdump-master>PwDump7.exe>
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\datnd\Downloads\pwdump-master\pwdump-master>echo Nguyen
056
Nguyen Duy Dat B21DCAT056

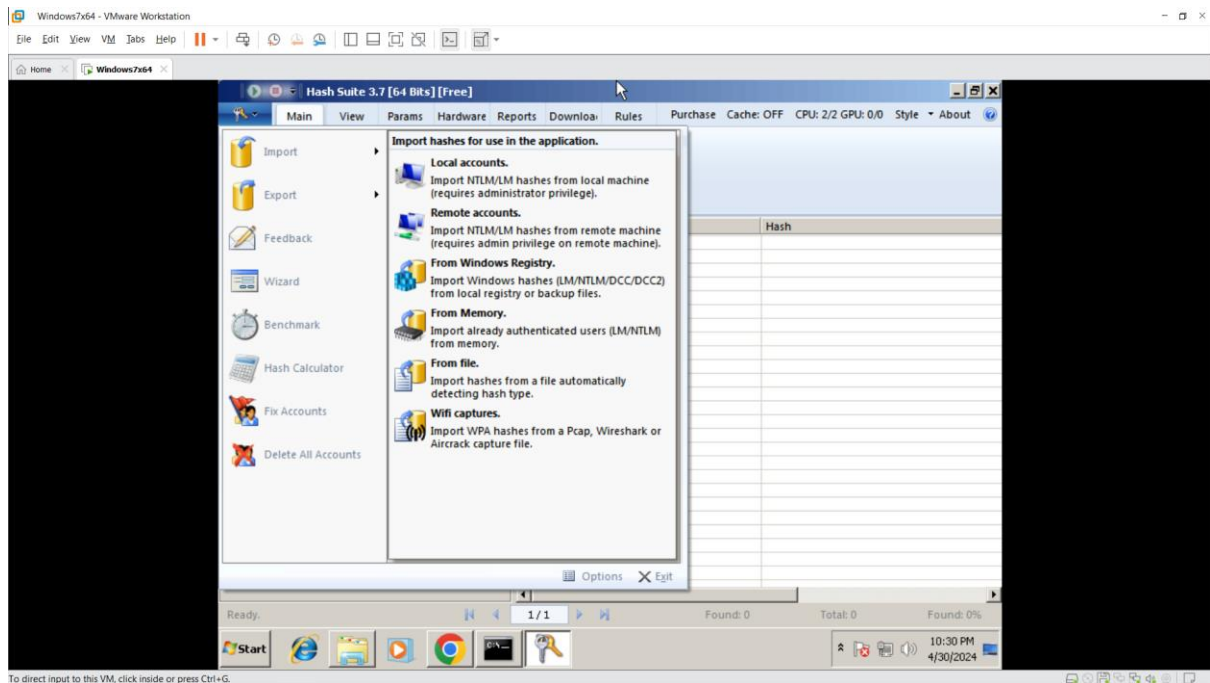
C:\Users\datnd\Downloads\pwdump-master\pwdump-master>

```

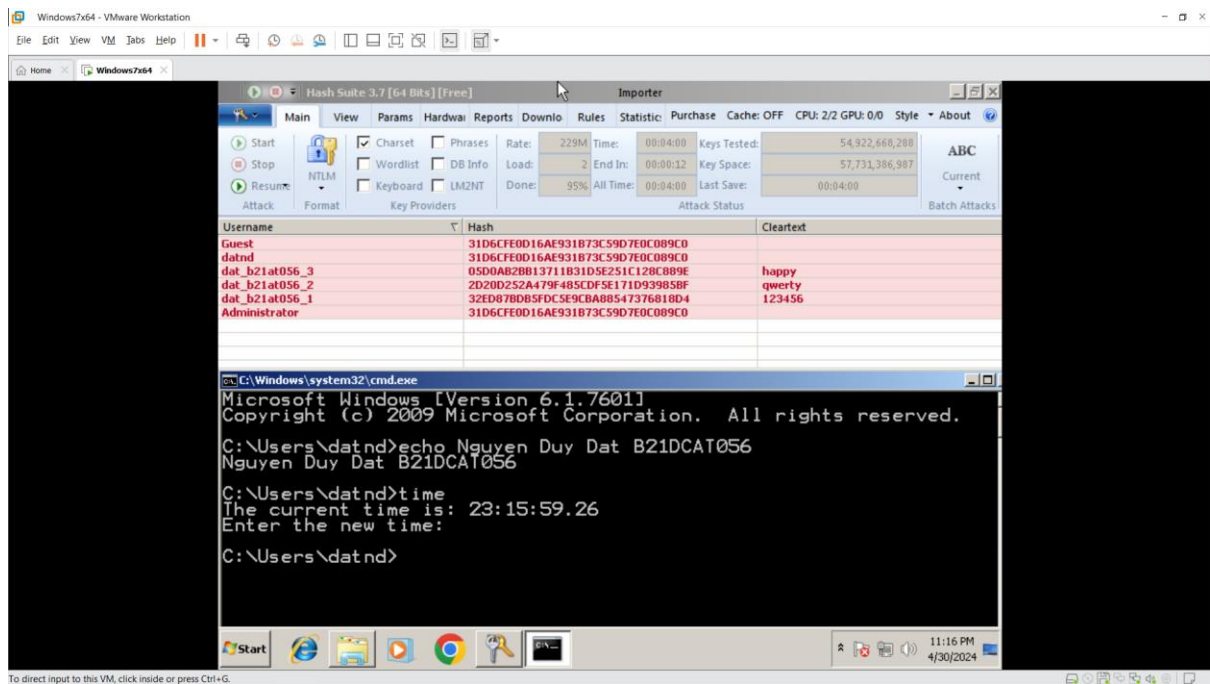
- Kiểm tra để chắc chắn file đã lưu



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

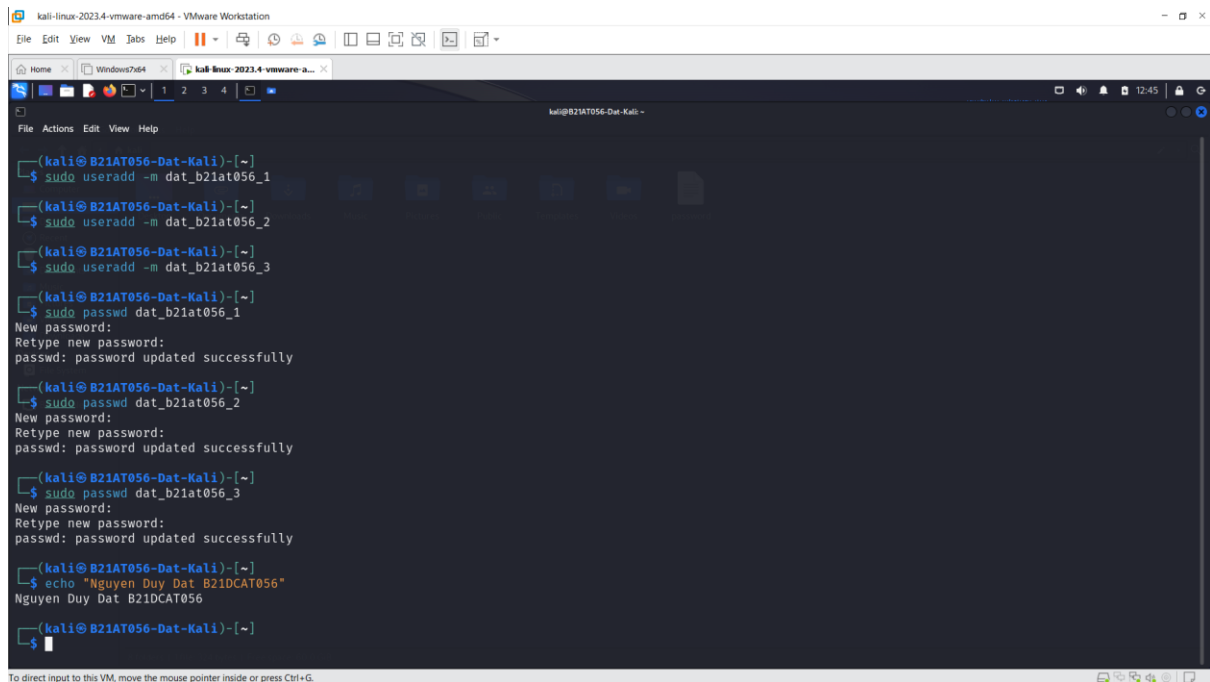


- Sau khi start thì tool đã tìm ra mật khẩu của 3 user



## 2. Crack mật khẩu bằng john the ripper trên Linux

- Tạo 3 tài khoản và mật khẩu trên linux



- 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 passwords.txt

```

kali@kali:~$ sudo cat /etc/shadow | grep dat_b21at056
dat_b21at056_1:5$5j9T$0f4*0eES.LXhLqNVtEJPv/$fke2WTeihzYfuV3tCoj0CetZsL70PVTvpGi.i10tux3:19843:0:99999:7:::
dat_b21at056_2:5$5j9T$dpzyHfaCLhpNiiYfAMyn0$hPF67rHoC.Oq/BtyRjUHAzDhM6DLfTbsMgEWHnYid5/:19843:0:99999:7:::
dat_b21at056_3:5$5j9T$NZ0eSNGUWC/mXHCN24N/00$zXRg3TTkdW0Wu0w6lrdkZCL5H7F/WZcqFg.krkoLS8:19843:0:99999:7:::

kali@kali:~$ sudo cat /etc/shadow | grep dat_b21at056 > passwords.txt

kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@kali:~$ date
Tue Apr 30 12:46:15 PM EDT 2024

kali@kali:~$

```

- Cài đặt john the ripper bằng lệnh sudo apt install john
- Sử dụng lệnh john cùng với từ điển mật khẩu wordlist để thực hiện tìm mật khẩu

```

kali@kali:~$ sudo john --wordlist=/home/kali/wordlist --format=crypt passwords.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [??/64])
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 8 candidates left, minimum 96 needed for performance.
happy      (dat_b21at056_3)
123456     (dat_b21at056_1)
qwerty    (dat_b21at056_2)
3g 0:00:00:00 DONE (2024-05-01 06:44) 18.75g/s 50.00p/s 150.0c/s 150.0c/s abcdef..password
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@kali:~$ date
Wed May 1 06:44:30 AM EDT 2024

kali@kali:~$

```