Báo cáo bài thực hành số 9

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

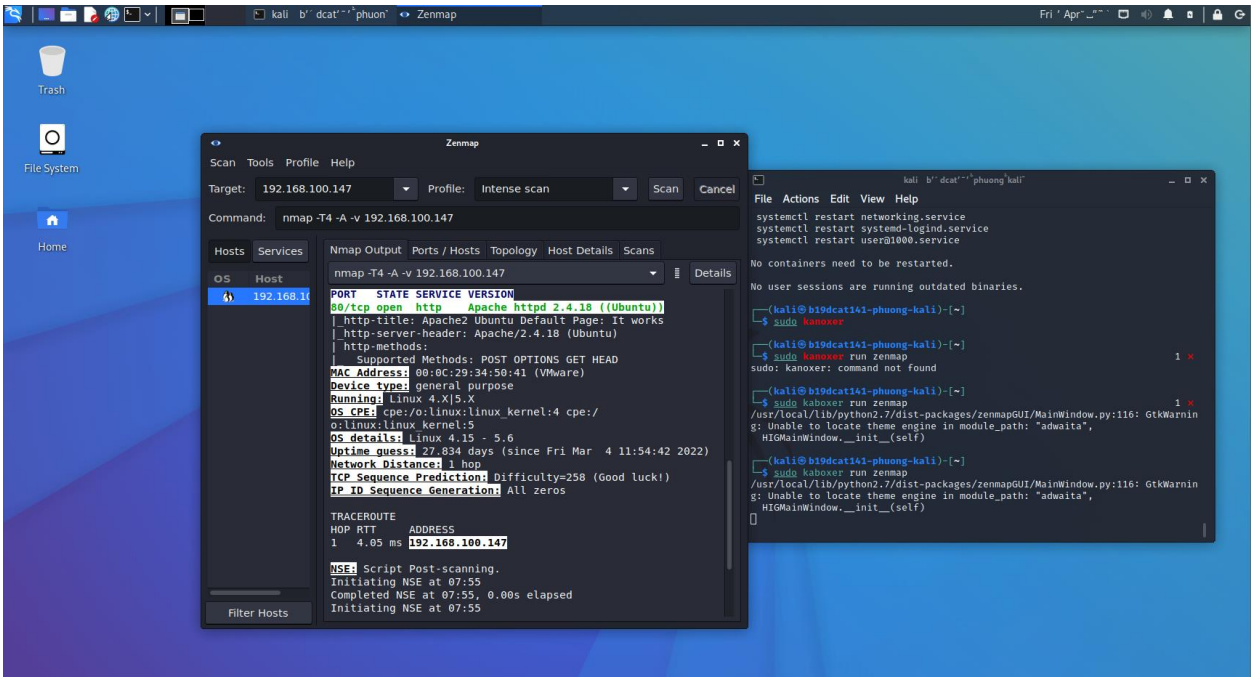
Mã SV: B19DCAT141

I. Lý thuyết

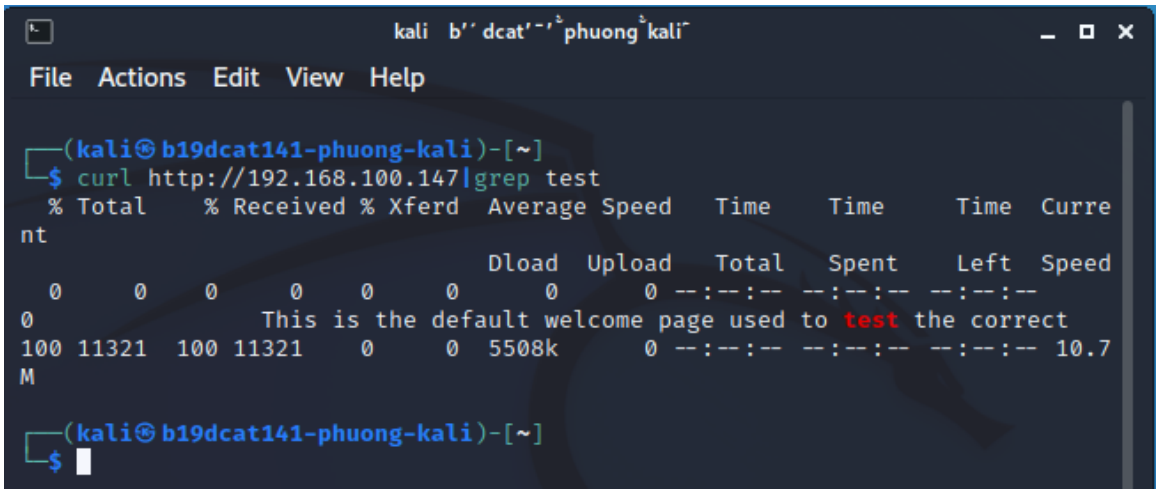
- Grep: Là command hiển thị dòng chứa chuỗi ký tự trong file. Có thể chỉ định nhiều file hoặc nhiều đường dẫn của đối tượng search. Có thể thay file hoặc đường dẫn bằng kết quả output từ command khác.
- Gawk: là một ngôn ngữ lập trình hỗ trợ thao tác dễ dàng đối với kiểu dữ liệu có cấu trúc, thường được sử dụng cho việc tìm kiếm và xử lý text. Gawk là bản phát hành mới nhất của GNU awk.
- Find được sử dụng để tìm kiếm một chuỗi văn bản trong một tệp hoặc các tệp và hiển thị các dòng văn bản chứa chuỗi đã chỉ định trong cmd Windows.
- Access_log:
  + Có chức năng ghi lại những lần sử dụng, truy cập, yêu cầu đến apache server.
  + Được lưu trữ tại /var/log/httpd/access_log (hoặc /var/log/apache2/access.log).
- xHydra:
  + xHydra là giao diện người dùng GUI cho trình bẻ khóa mật khẩu Hydra.
  + Hydra có thể được sử dụng để bẻ khóa mật khẩu, có thể được sử dụng cho nhiều loại tấn công trực tuyến, bao gồm cả các cuộc tấn công MySQL, SMB, FTP, MSSQL và HTTP / HTTPS.

II. Thực hành

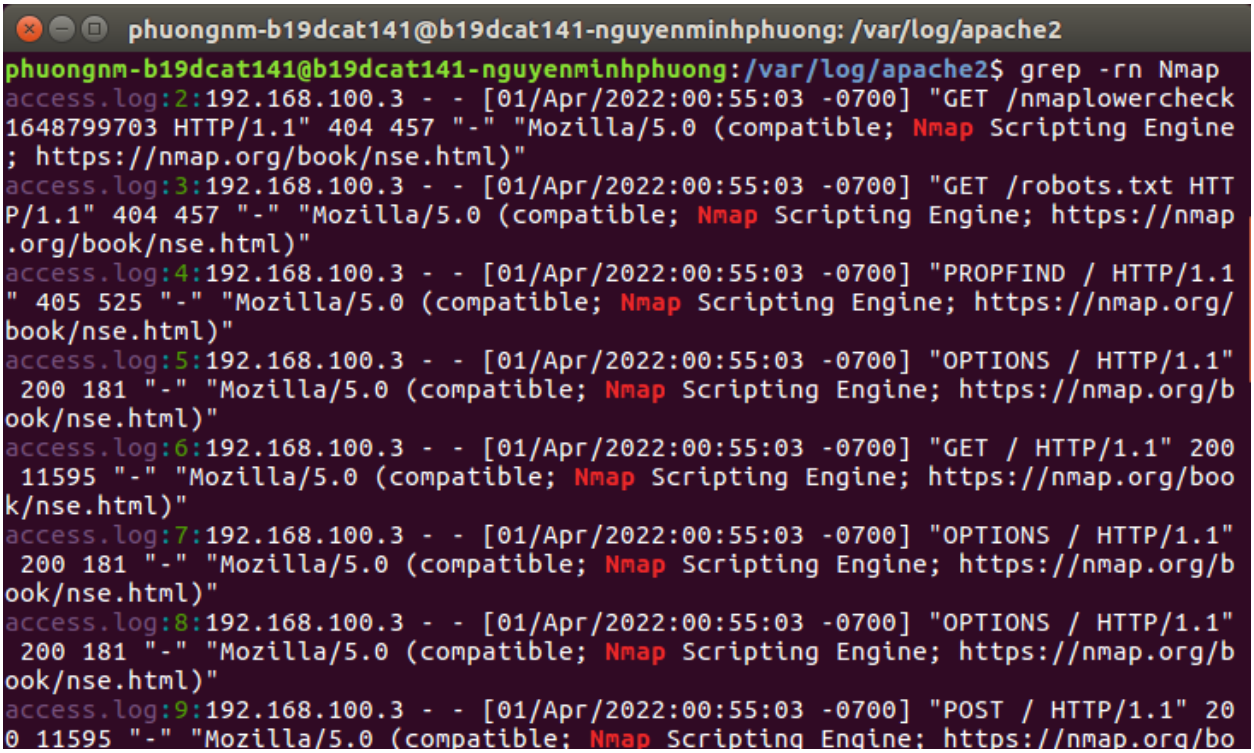
- **Phân tích log sử dụng grep trong Linux**
  + Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.2.3



+ Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web http://192.168.100.147. Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”(root@bt:~#curl http://192.168.100.147| grep test)



+ Trên máy Linux Internal Victim, để xem thư mục chứa access_log dùng lệnh: [root@rhel ~]# cd /var/log/httpd



- **Phân tích log sử dụng gawk trong Linux**
  + Trên máy Kali attack tiến hành remote vào máy Linux Internal Victim. Tạo một account mới với tên sinh viên và mật khẩu tùy chọn. Sau đó tiến hành thay đổi mật khẩu cho tài khoản vừa tạo.

```
┌──(root💀b19dcat141-phuong-kali)-[~]
└─# ssh 192.168.100.147
root@192.168.100.147's password:
Permission denied, please try again.
root@192.168.100.147's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

14 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
Last login: Tue Mar 22 23:23:13 2022 from 10.10.19.148
root@b19dcat141-nguyenminhphuong:~#
```

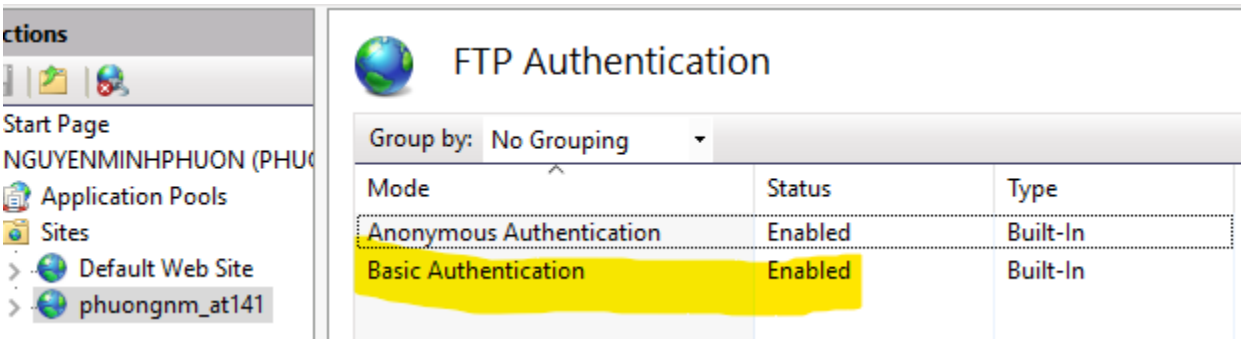
```
kali@b19dcat141-phuong-kali: ~
File  Actions  Edit  View  Help
*** System restart required ***
Last login: Tue Mar 22 23:23:13 2022 from 10.10.19.148
root@b19dcat141-nguyenminhphuong:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.147  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 00:0c:29:f7:d4:d3  txqueuelen 1000  (Ethernet)
        RX packets 3291  bytes 516613 (516.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1393  bytes 376119 (376.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 714  bytes 64128 (64.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 714  bytes 64128 (64.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@b19dcat141-nguyenminhphuong:~# useradd PhuongNM-B19DCAT141
root@b19dcat141-nguyenminhphuong:~# passwd PhuongNM-B19DCAT141
New password:
Retype new password:
passwd: password updated successfully
root@b19dcat141-nguyenminhphuong:~#
```

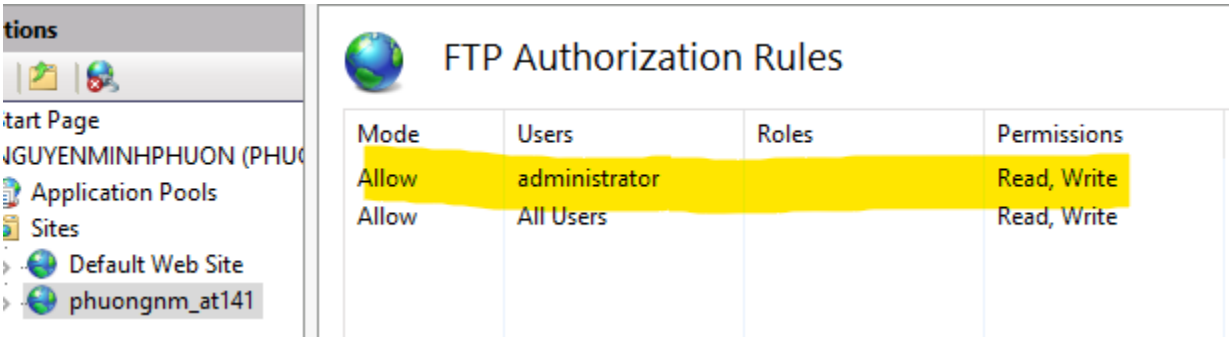
+ Trên máy Linux Internal Victim, tiến hành xem file log

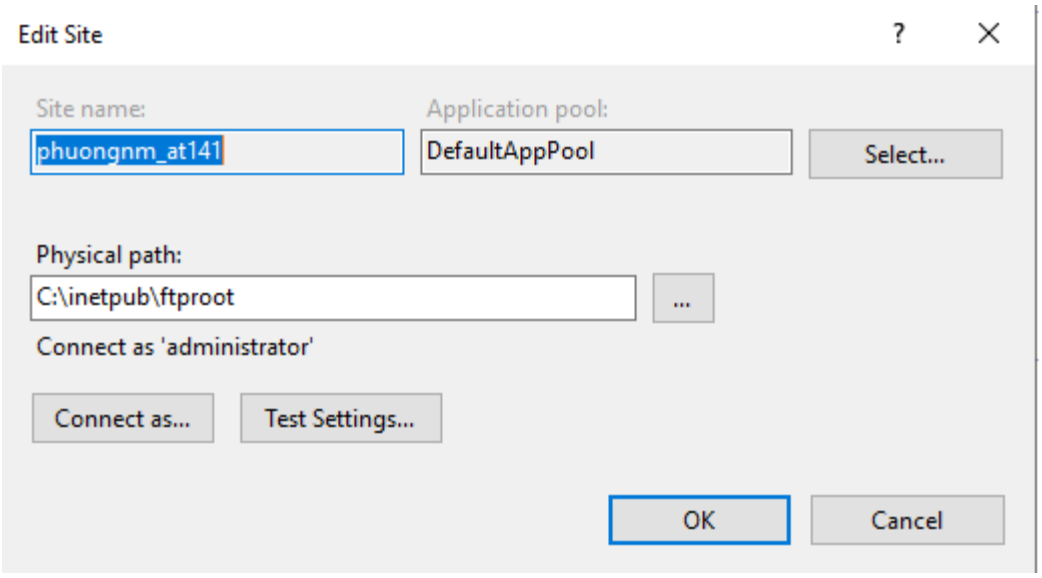
```
65 Mar 28 10:49:28 b19dcat141-nguyenminhphuong sshd[31528]: Failed password for root from 192.168.100.3 port 49710 ssh2
66 Mar 28 10:49:39 b19dcat141-nguyenminhphuong sshd[31528]: Accepted password for root from 192.168.100.3 port 49710 ssh2
67 Mar 28 10:49:39 b19dcat141-nguyenminhphuong sshd[31528]: pam_unix(sshd:session): session opened for user root by (uid=0)
68 Mar 28 10:49:39 b19dcat141-nguyenminhphuong systemd-logind[810]: New session 10 of user root.
69 Mar 28 10:49:39 b19dcat141-nguyenminhphuong systemd: pam_unix(systemd-user:session): session opened for user root by (uid=0)
70 Mar 28 10:56:55 b19dcat141-nguyenminhphuong useradd[31646]: new group: name=PhuongNM-B19DCAT141, GID=1002
71 Mar 28 10:56:55 b19dcat141-nguyenminhphuong useradd[31646]: new user: name=PhuongNM-B19DCAT141, UID=1001, GID=1002, home=/home/-
   PhuongNM-B19DCAT141, shell=/bin/sh, from=/dev/pts/2
72 Mar 28 10:57:18 b19dcat141-nguyenminhphuong passwd[31654]: pam-unix(passwd: maruminie): password changed for PhuongNM-B19DCAT141
73 Mar 28 10:57:18 b19dcat141-nguyenminhphuong passwd[31654]: gkr-pam: couldn't update the login keying password: no old password
   was entered
74 Mar 28 11:07:11 b19dcat141-nguyenminhphuong gdm-password: gkr-pam: unlocked login keyring
75 Mar 28 11:09:01 b19dcat141-nguyenminhphuong CRON[31776]: pam_unix(cron:session): session opened for user root by (uid=0)
```

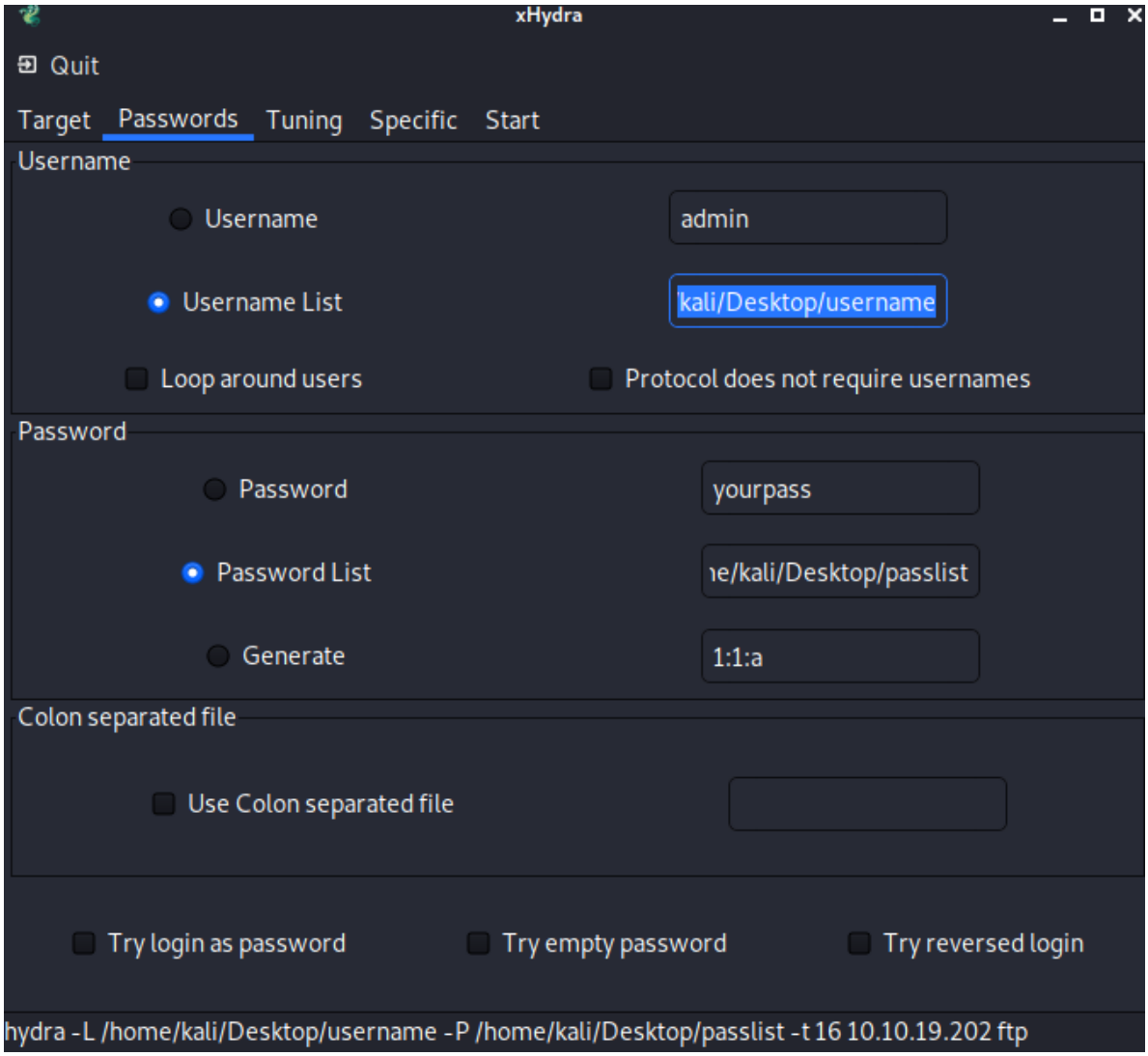
+ Trên máy Kali attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep, và dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được.

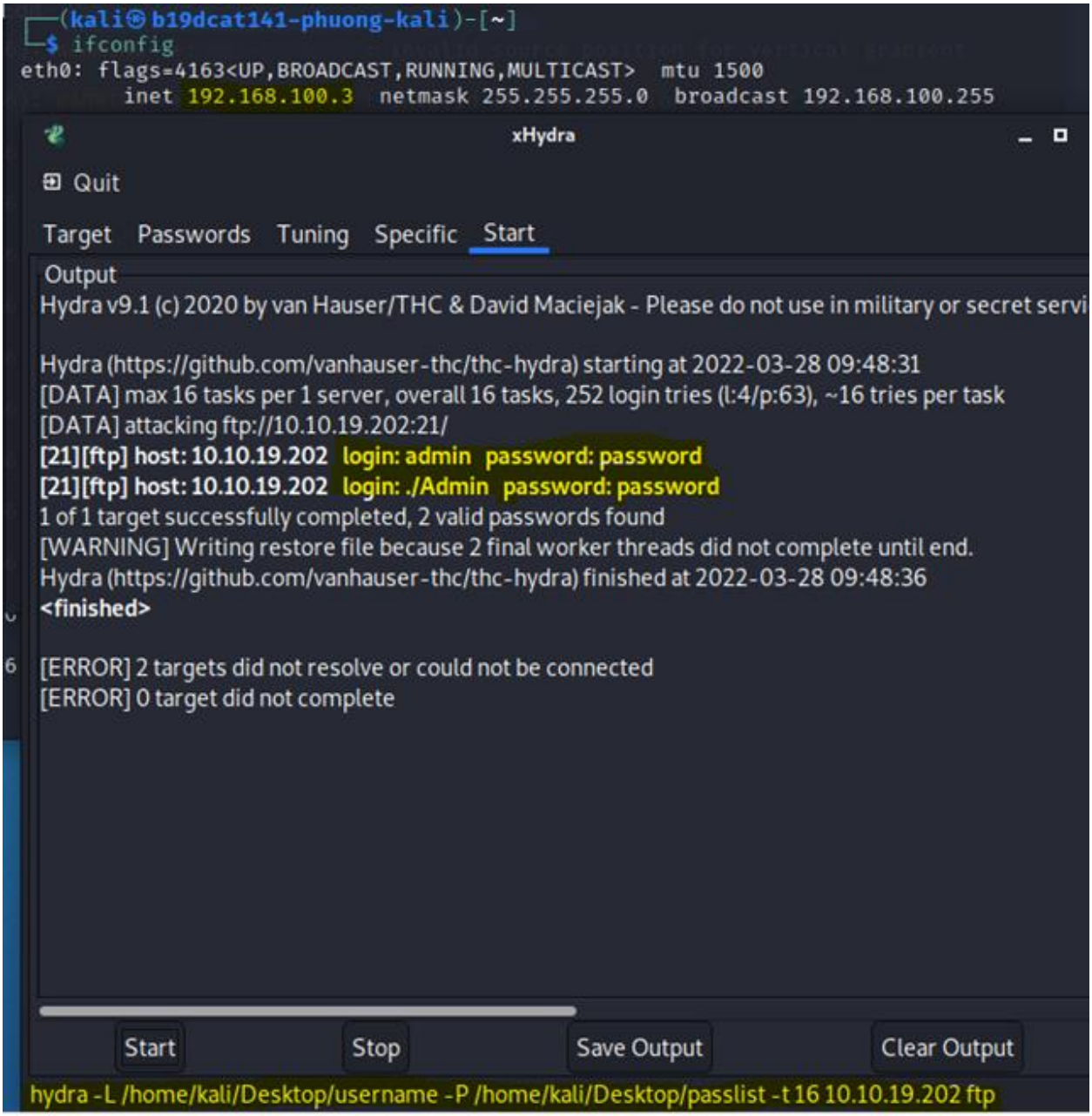
- **Phân tích log sử dụng find trong Windows**
  + Trên máy Kali External Attack khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu



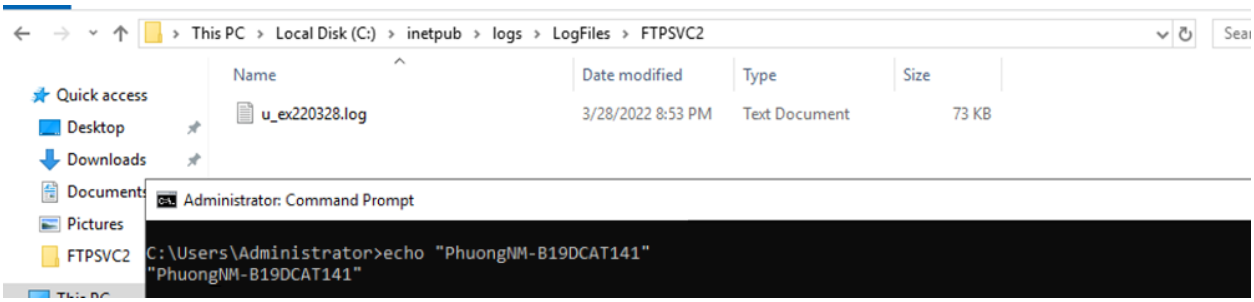



Edit Site
Site name:
phuongnm_at141
Application pool:
DefaultAppPool
Select...
Physical path:
C:\inetpub\ftproot
...
Connect as 'administrator'
Connect as...
Test Settings...
OK
Cancel


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
admin
Username List
kali/Desktop/username
Loop around users
Protocol does not require usernames
Password
Password
yourpass
Password List
ıe/kali/Desktop/passlist
Generate
1:1:a
Colon separated file
Use Colon separated file
Try login as password
Try empty password
Try reversed login
hydra -L /home/kali/Desktop/username -P /home/kali/Desktop/passlist -t 16 10.10.19.202 ftp



+ Trên máy Windows 2003 Server External Victim, thực hiện điều hướng đến FTP Logfile(C:\cd c:\Windows\System32\Logfiles\msftpsvc1). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd). Gõ lệnh để tìm kiếm kết quả tấn công login thành công(C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type exyymmdd.log | find “230”)



```
C:\Users\Administrator>echo "PhuongNM-B19DCAT141"
"PhuongNM-B19DCAT141"
```

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2022-03-28 08:19:55
#Field: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem sc-status sc-win32-status sc-substatus x-session x
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 cd01b402-13ba-424a-899f-c1984b35e15b -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 b40ad238-6c11-4e78-9636-cbaccdaac0d9 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 cf5746e3-9d8c-4838-9ad2-54a01b520f47 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 768384c3-74d0-4255-9cf1-0f5845344515 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 4784d018-dd1a-4083-b6ba-9e5938b484ee -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 cce2e555-999f-486b-8309-b10baff33072 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 7af209cf-91cf-482e-85b1-0187e83a8538 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 e37b7dd7-4456-413e-ba7e-d51c70e98e0b -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 a34e1b76-d537-400d-9778-afcf685760ee -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER administrator 331 0 0 d0fc4093-6ed0-4c70-a20e-0d884cfe0113 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER ad
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER ad
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER ad
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER ad
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER ad
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS **
```

```
C:\Users\Administrator>echo "PhuongNM-B19DCAT141"
"PhuongNM-B19DCAT141"

C:\Users\Administrator>
```

```
C:\inetpub\logs\LogFiles\FTPSVC2>echo "PhuongNM-B19DCAT141"
"PhuongNM-B19DCAT141"

C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex220328.log | find "230"
2022-03-28 13:47:13 192.168.100.3 - 10.10.19.202 21 ControlChannelOpened - - 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:14 192.168.100.3 B19DCAT205\admin 10.10.19.202 21 PASS *** 230 0 0 a2064372-376f-40ce-90e1-e652d6a7172
 /
2022-03-28 13:47:15 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:47:15 192.168.100.3 - 10.10.19.202 21 ControlChannelClosed - - 0 0 c2305cd0-9dc5-4936-a21a-afb289ed0a40 -
2022-03-28 13:48:32 192.168.100.3 - 10.10.19.202 21 ControlChannelOpened - - 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:32 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:32 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:32 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 USER admin 331 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 B19DCAT205\admin 10.10.19.202 21 PASS *** 230 0 0 671ab78f-2fb8-4b8a-a884-18b73c726df
 /
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 USER ./administrator 331 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 USER ./administrator 331 0 0 e922dc27-2307-4649-9582-bca60d7d1811 -
2022-03-28 13:48:33 192.168.100.3 - 10.10.19.202 21 PASS *** 530 1326 41 e922dc27-2307-4649-9582-bca60d7d1811 -
```