HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO THỰC HÀNH MÔN THỰC TẬP CƠ SỞ ATTT

Bài 9: Phân tích log hệ thống

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Hệ: Chính Quy

Giảng viên: Nguyễn Hoa Cương

Hà Nội – 2023

Mục lục

1. Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, baogồm:

1. Phân tích log sử dụng grep/gawk trong Linux
2. Phân tích log sử dụng find trong Windows
3. Tìm hiểu về Windows Event Viewer và auditing
4. Phân tích event log trong Windows

2. Nội dung thực hành

2.1. Tìm hiểu lý thuyết

Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk,find, secure, access_log, …

- **grep**

  Grep (Global Regular Expression Print) là một công cụ dòng lệnh Linux/Unix đượcsử dụng để tìm kiếm một chuỗi ký tự trong một tệp được chỉ định. Khi tìm thấy kếtquả khớp, nó sẽ in dòng kết quả. Lệnh grep rất tiện lợi khi tìm kiếm log

Cú pháp:
grep [OPTION ...] PATTERNS [FILE ...]
grep [OPTION ...] -e PATTERNS ... [FILE ...]
grep [OPTION ...] -f PATTERN_FILE ... [FILE ...] grep

- Lựa chọn
  - đối sánh -E, --extended-regexp : Diễn giải MẪU dưới dạng biểu thức chính quymở rộng
  - -F, --fixed-string : Diễn giải MẪU là chuỗi cố định, không phải biểu thức chínhquy.
  - -G, --basic-regexp : Diễn giải MẪU dưới dạng biểu thức chính quy cơ bản
    - -P, --perl-regex: Giải thích MẪU dưới dạng biểu thức chính quy tương thích với Perl (PCRE). Tùy chọn này là thử nghiệm khi được kết hợp với tùy chọn
  - -z (--null-data) và grep -P có thể cảnh báo về các tính năng chưa được thực hiện

- **gawk**

  – gawk - mô hình quét và xử lý ngôn ngữ

  – Nó có thể được sử dụng như một trình trích xuất trường (như lệnh cắt), một máy tính cơ bản và như một trình so khớp mẫu (như lệnh grep)

- **Find**

  – Đây là một command rất mạnh trong việc tìm kiếm và xác định file đối với thư mục có dạng cây (the directory heirarchy) theo Regex được định nghĩa, ngoài ra còn thực hiện tìm theo các điều kiện chi tiết như thời gian, loại file...

  – Command của Find có dạng như sau:

  $ find [Command-Option] [PATH] [Option] [File/Search_Expresion]

  – Option:

  -P Không đọc Symbolic Link-các lối tắt(tương ứng trong window là short-cut).

  Đây là cấu hình mặc định

  -L Đọc tất cả Symbolic Link

  -H Chỉ đọc Symbolic Link được chỉ định

  -D <sub_option> Hiển thị thông tin Debug

  -O<level> Cấp tối ưu hóa xử lý. Cấp -O1 là cấp tối ưu hóa được cài đặt mặc định.

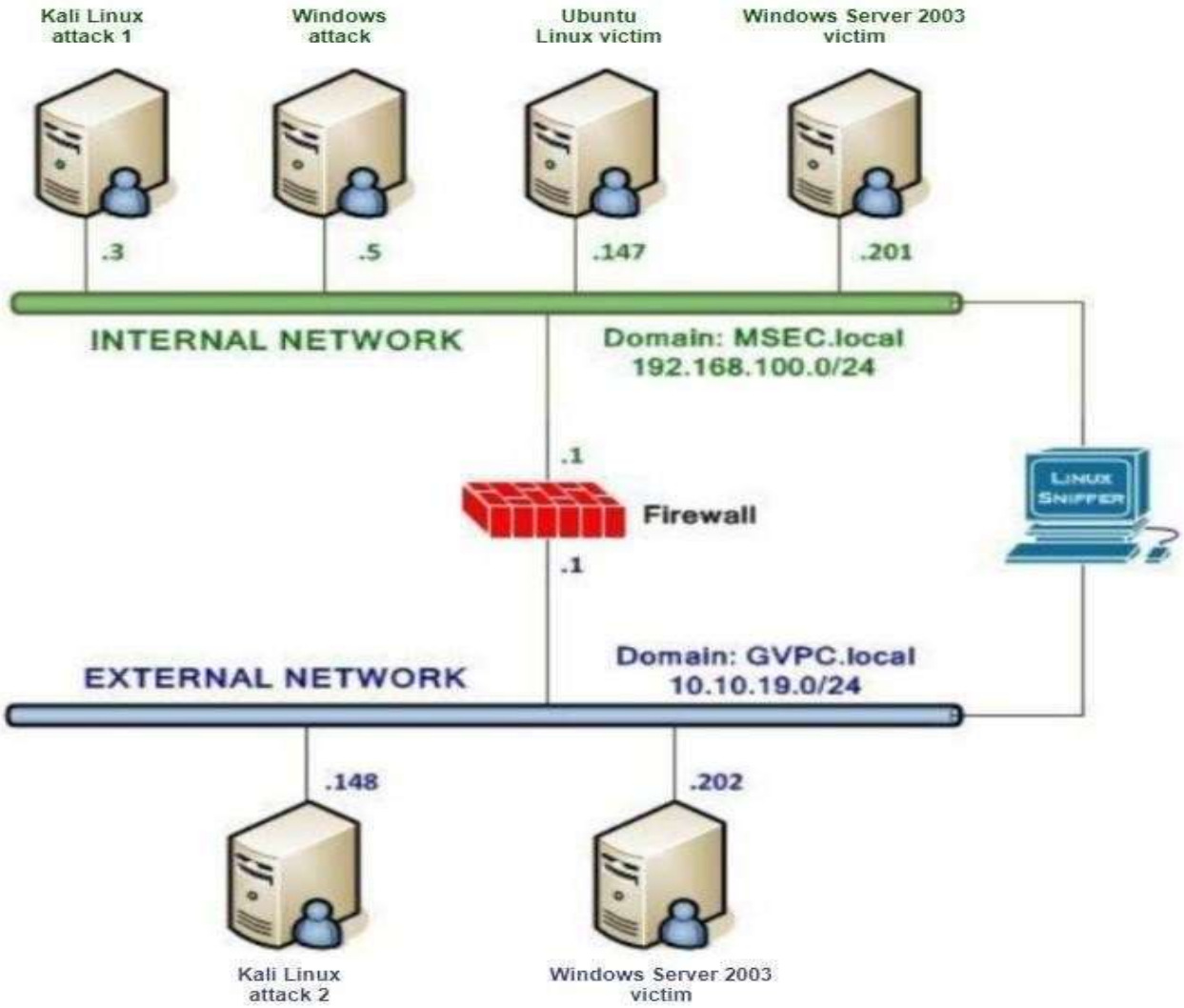
- **Access_log**

  – Log truy cập (access log) ghi lại các thông tin người dùng truy cập vào website. Log lỗi (error log) ghi lại các cảnh báo các lỗi xảy ra với dịch vụ liên quan web server.

2.2. Chuẩn bị môi trường

- Phần mềm VMWare Workstation (hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài lab 05 trước đó: máytrạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cầnsử dụng trong bài thực hành.

- Topo mạng như đã cấu hình trong bài 5



2.3. Các bước thực hiện và kết quả

2.3.1. Phân tích log sử dụng grep trong Linux

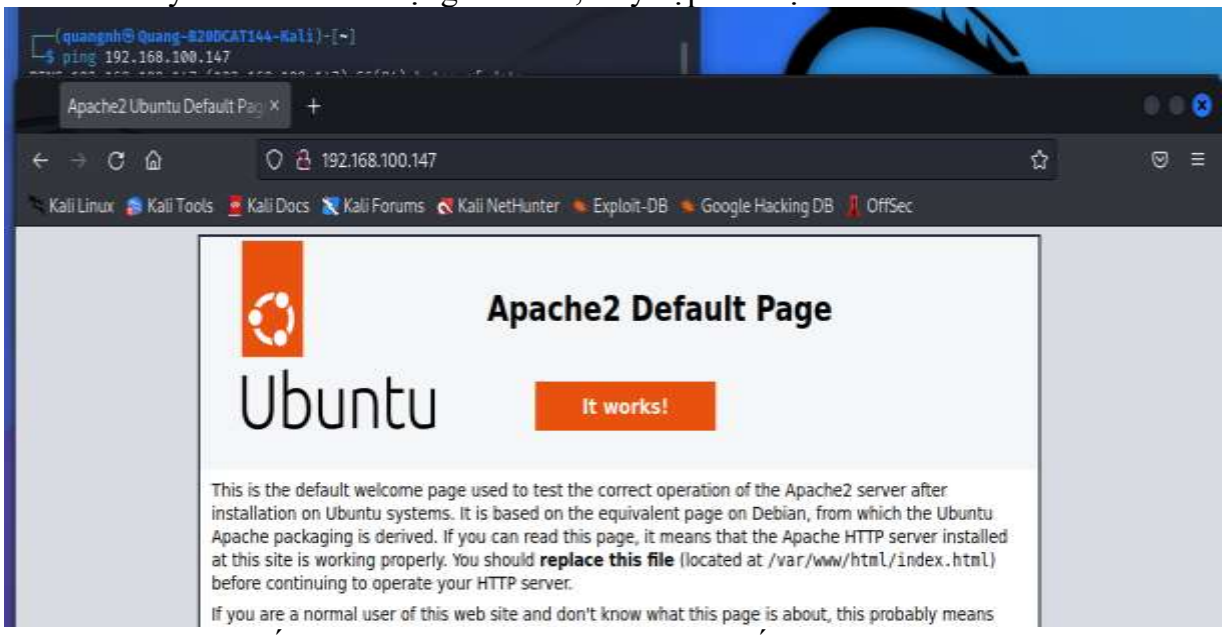
- Trên máy Kali attack trong mạng Internal, khởi chạy nmap và scan cho địa chỉ 192.168.100.147 (Máy Linux Victim Internal) và xem được port 80 đang mở cho Web Server Apache

```
┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~]
└─$ nmap 192.168.100.147
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-04 10:46 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.147
Host is up (0.00022s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~]
```

Trên máy Kali attack ở mạng Internal, truy cập vào địa chỉ web



Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”

Trên máy Linux Internal Victim, xem thư mục chứa access.log

```
┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~]
└─$ curl http://192.168.100.147 | grep test
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curre
nt
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--
100 10671  100 10671    0     0  6595k      0 --:--:-- --:--:-- --:--:-- 10.1
M
               This is the default welcome page used to test the correct

┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~]
```

```
quangnh@Quang-B20DCAT144:/var/log$ cd apache2
quangnh@Quang-B20DCAT144:/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
quangnh@Quang-B20DCAT144:/var/log/apache2$
```

- Khi đã mở được file access.log trên máy Linux Internal Victim, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm:

+ Firefox

```
quangnh@Quang-B20DCAT144:/var/log/apache2$ grep Firefox access.log
192.168.100.3 - - [04/Mar/2023:22:48:08 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mo
zilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
192.168.100.3 - - [04/Mar/2023:22:48:08 +0700] "GET /icons/ubuntu-logo.png HTTP/
1.1" 200 3607 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.
0) Gecko/20100101 Firefox/102.0"
192.168.100.3 - - [04/Mar/2023:22:48:08 +0700] "GET /favicon.ico HTTP/1.1" 404 4
93 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20
100101 Firefox/102.0"
```

+ Curl

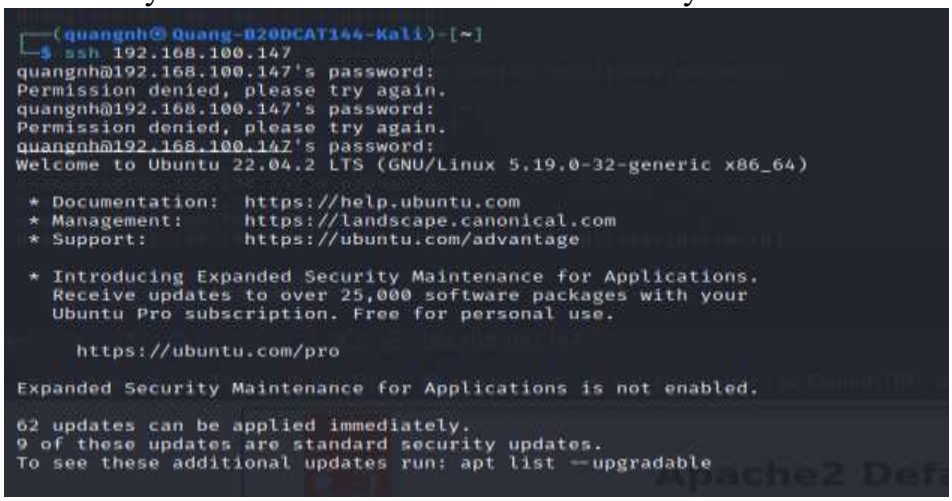
```
quangnh@Quang-B20DCAT144:/var/log/apache2$ grep curl access.log
192.168.100.3 - - [04/Mar/2023:22:50:11 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/7.85
.0"
quangnh@Quang-B20DCAT144:/var/log/apache2$
```

2.3.2. Phân tích log sử dụng gawk trong Linux

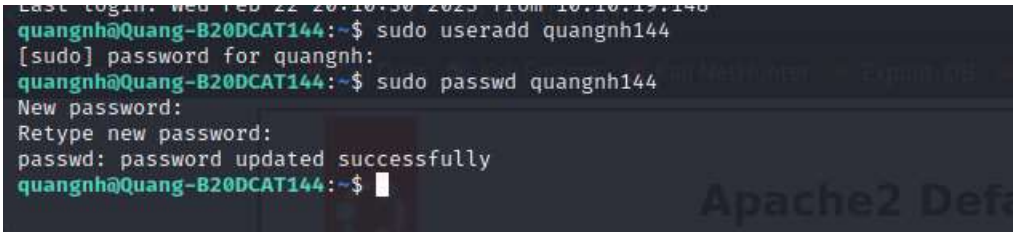
- Kiểm tra cổng SSH trên địa chỉ 192.168.100.147 (Linux Internal Victim)

```
quangnh@Quang-B20DCAT144:~$ sudo apt install gawk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requi
  libflashrom1 libftdi1-2 libllvm13
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libsigsegv2
Suggested packages:
  gawk-doc
The following NEW packages will be installed:
  gawk libsigsegv2
0 upgraded, 2 newly installed, 0 to remove and 63 not upgraded.
Need to get 461 kB of archives.
After this operation, 1.770 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

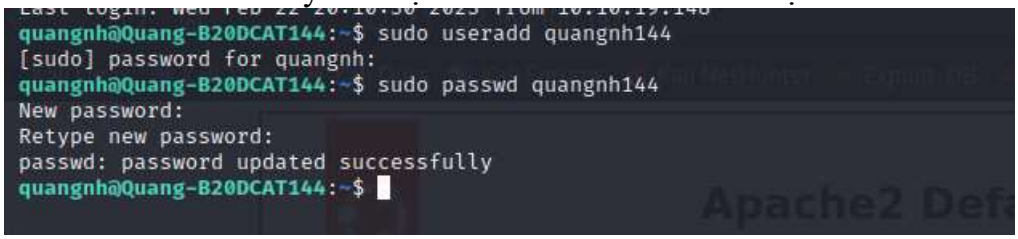
- Trên máy Kali Attack tiến hành remote vào máy Linux Internal Victim



- 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



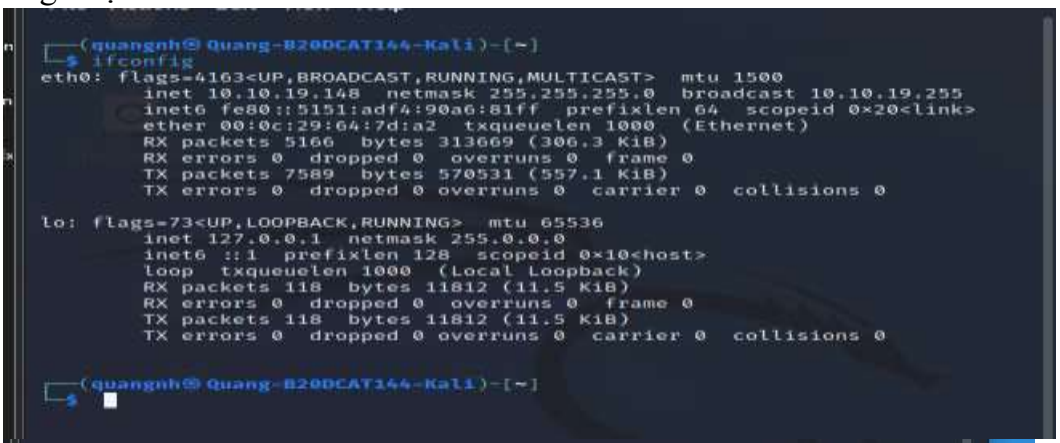
- Trên máy Linux Internal Victim, tiến hành xem file auth.log

- Trên máy Kali Attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep

```
quangnh@Quang-B20DCAT144:~$ cd /var/log
quangnh@Quang-B20DCAT144:/var/log$ sudo grep "quangnh144" auth.log
Mar  4 23:50:17 Quang-B20DCAT144 sudo:  quangnh : TTY=pts/1 ; PWD=/home/quang
nh ; USER=root ; COMMAND=/usr/sbin/useradd quangnh144
Mar  4 23:50:17 Quang-B20DCAT144 useradd[5364]: new group: name=quangnh144, G
ID=1001
Mar  4 23:50:17 Quang-B20DCAT144 useradd[5364]: new user: name=quangnh144, UI
D=1001, GID=1001, home=/home/quangnh144, shell=/bin/sh, from=/dev/pts/2
Mar  4 23:50:39 Quang-B20DCAT144 sudo:  quangnh : TTY=pts/1 ; PWD=/home/quang
nh ; USER=root ; COMMAND=/usr/bin/passwd quangnh144
Mar  4 23:50:45 Quang-B20DCAT144 passwd[5439]: pam_unix(passwd:chauthtok): pa
ssword changed for quangnh144
Mar  4 23:54:17 Quang-B20DCAT144 sudo:  quangnh : TTY=pts/1 ; PWD=/var/log ;
USER=root ; COMMAND=/usr/bin/grep quangnh144 auth.log
quangnh@Quang-B20DCAT144:/var/log$
```

2.3.3. Phân tích log sử dụng find trong Windows

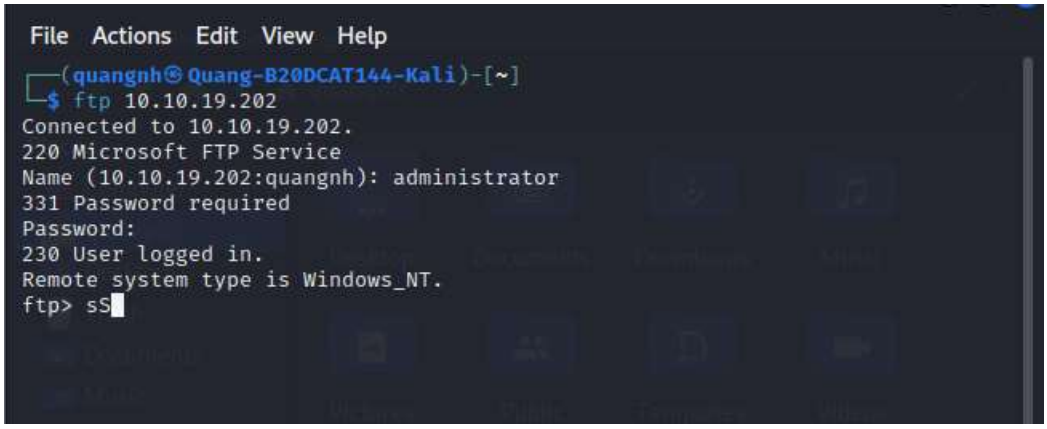
- Trên máy Kali External Attack dùng nmap cho địa chỉ 10.10.202 và xem được port 21 đang được mở



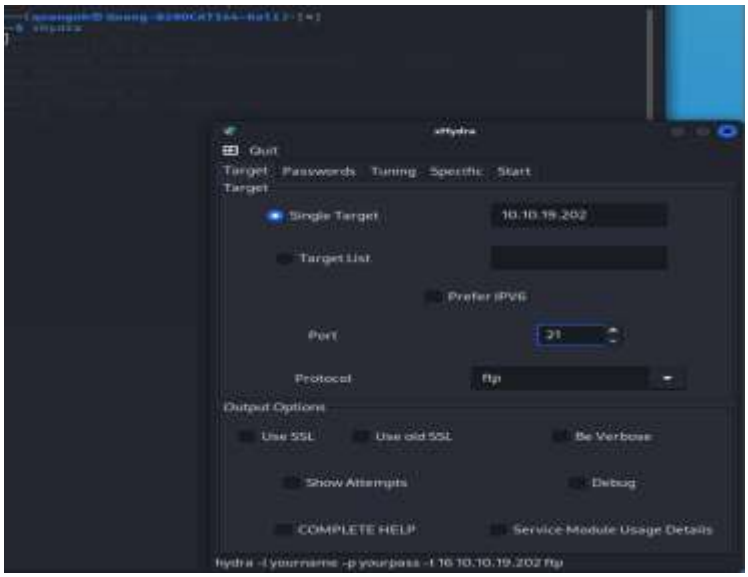

```
(quangnh㉿Quang-B20DCAT144-Kali)-[~]
$ nmap 10.10.19.202
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-05 12:28 EST
Nmap scan report for 10.10.19.202
Host is up (0.000093s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 15.65 seconds
```

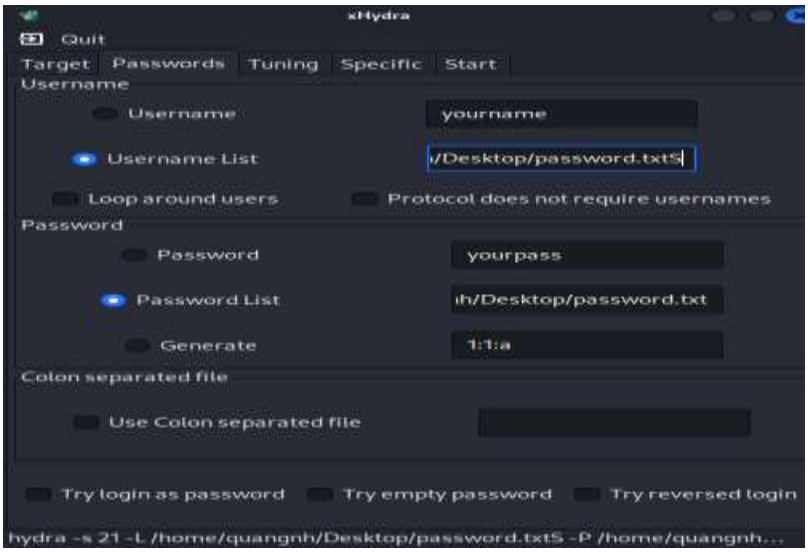
```
C:\Users\Administrator>ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.19.202:(none)): administrator
331 Password required
Password:
230 User logged in.
ftp>
```

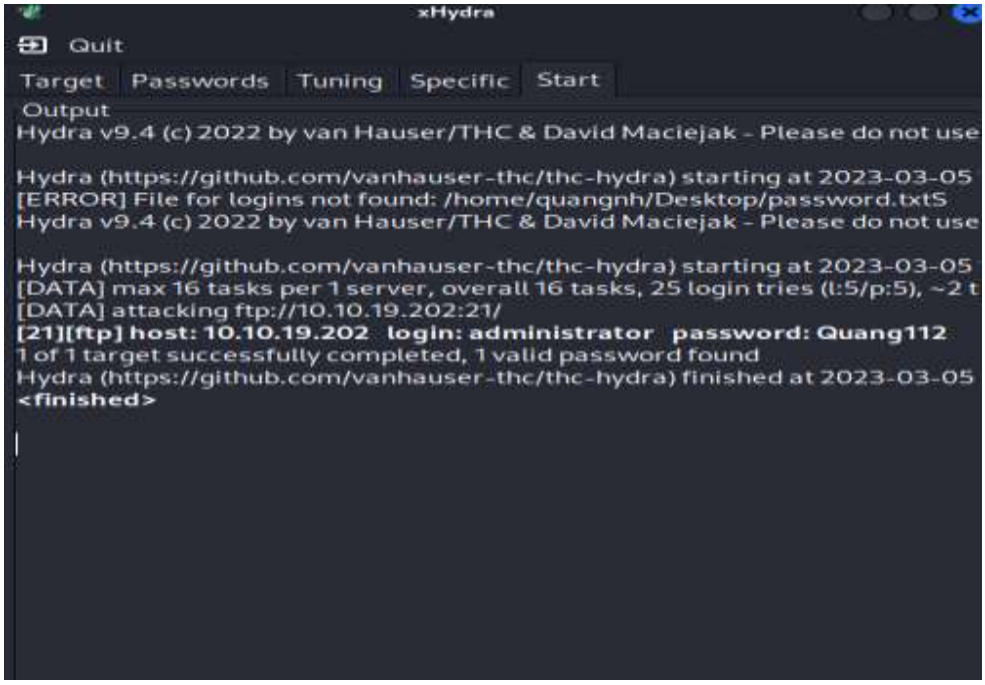


- Trong máy Kali External Attack khởi động #xhydra, chọn target là **10.10.19.202**, giao thức ftp

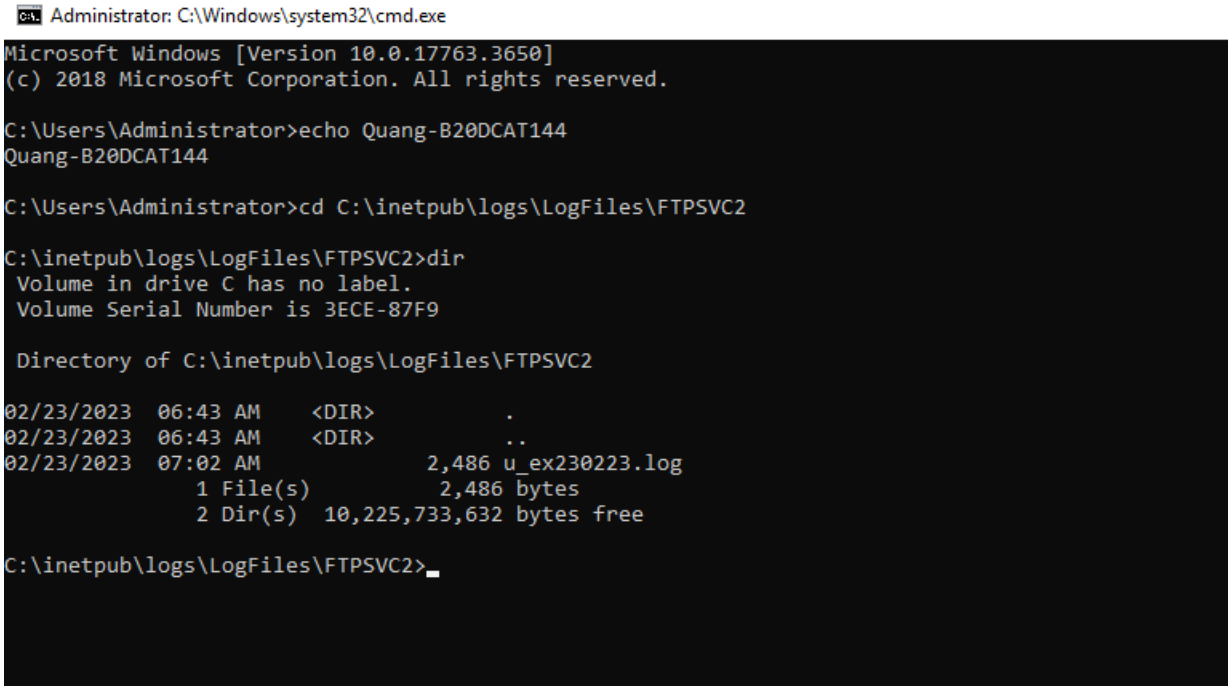


và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu

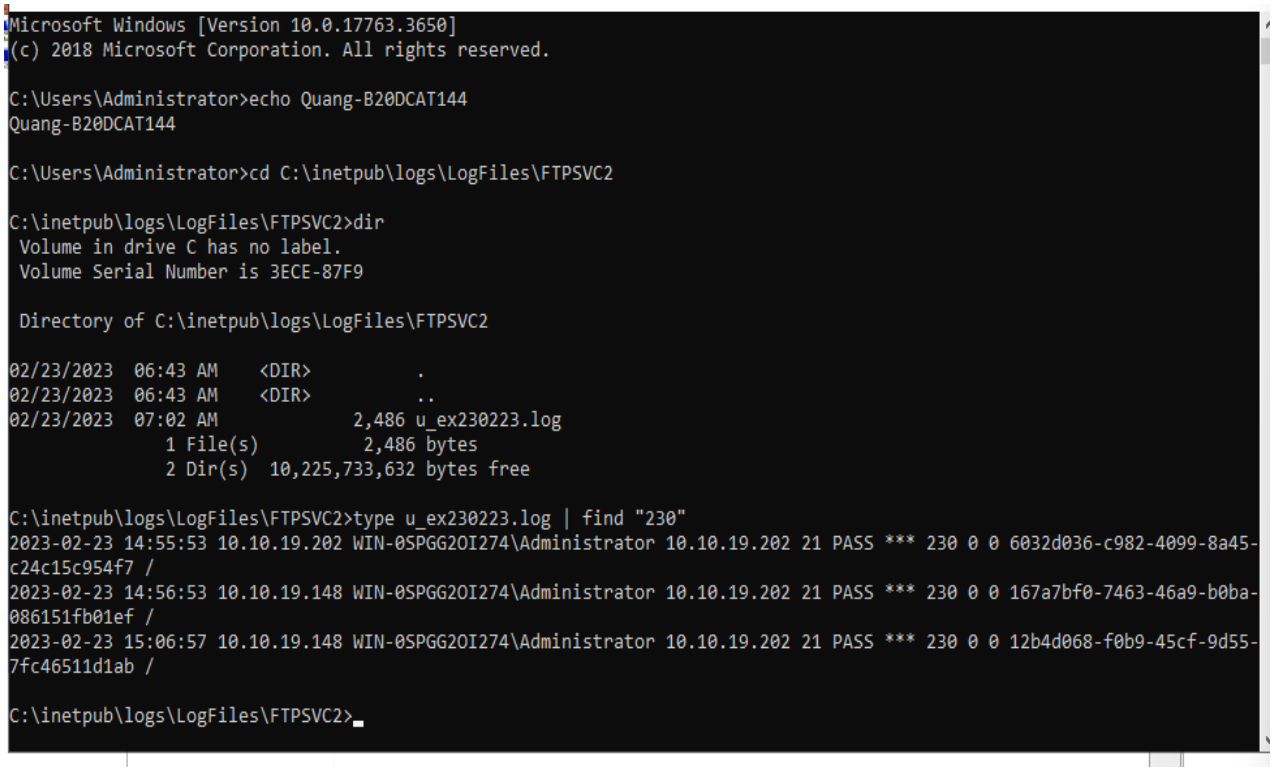




- Trên máy Windows Server External Victim, thực hiện điều hướng đến FPT Logfile: C:\inetpub\logs\Logfiles\FTPSVC2*.log



- Tìm kiếm kết quả login thành công



3. Tài liệu tham khảo

- grep: https://linuxcommand.org/lc3_man_pages/grep1.html
- gawk: http://www.gnu.org/software/gawk/manual/gawk.html
- find:https://docs.microsoft.com/en-us/windowsserver/administration/windows commands/find
- xhydra: http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html