

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

Môn: THỰC TẬP CƠ SỞ
BÁO CÁO BÀI THỰC HÀNH SỐ 9

Họ và tên sinh viên:

Trần Đức Minh

Mã số sinh viên:

B20DCAT127

Họ và tên giảng viên:

TS. Đinh Trường Duy

I. Tìm hiểu lý thuyết:

1. Ý nghĩa lệnh grep:

- Lệnh grep là một công cụ phân tích văn bản dòng lệnh thông dụng trên các hệ thống Unix và Linux, được sử dụng để tìm kiếm và trích xuất các đoạn văn bản có chứa các chuỗi ký tự cụ thể từ một tệp hoặc đầu vào đầu ra.

- Cú pháp của lệnh grep như sau:

`grep [options] pattern [file ...]`

- Trong đó:

+ pattern: là chuỗi ký tự mà bạn muốn tìm kiếm trong tệp log.

+ file: là tên của tệp log mà bạn muốn phân tích.

+ options: là các tùy chọn để điều chỉnh việc tìm kiếm.

- Một số tùy chọn phổ biến của lệnh grep trong phân tích log bao gồm:

+ '-i': tìm kiếm không phân biệt chữ hoa/chữ thường.

+ '-n': hiển thị số dòng của các dòng được tìm thấy.

+ '-r': tìm kiếm đệ quy trong tất cả các file và thư mục con.

+ '-v': hiển thị các dòng không khớp với biểu thức chính quy.

2. Ý nghĩa lệnh gawk:

- Lệnh gawk (GNU awk) là một công cụ mạnh mẽ trong phân tích log. Nó là một công cụ dòng lệnh được sử dụng để xử lý và trích xuất thông tin từ các tập tin văn bản có định dạng cụ thể, chẳng hạn như các tập tin log của máy chủ web hoặc các ứng dụng.

- Các lệnh gawk thường được sử dụng để:

+ Trích xuất thông tin từ các tập tin log: Sử dụng lệnh awk có thể xác định các trường và các giá trị mà bạn muốn trích xuất từ các tập tin log, chẳng hạn như địa chỉ IP, thời gian truy cập, URL được truy cập, tên người dùng và nhiều hơn nữa.

+ Tính toán và thống kê: Sử dụng awk có thể tính toán các giá trị thống kê như tổng, trung bình, số lần xuất hiện của các giá trị, và nhiều hơn nữa.

+ Xử lý và sửa đổi dữ liệu: Bằng cách sử dụng các biểu thức chính quy và các lệnh awk, chúng ta có thể thực hiện các hoạt động như cắt, sao chép, thay thế và sắp xếp các trường và giá trị trong các tập tin log.

3. Ý nghĩa lệnh find:

- Lệnh "find" trong quá trình phân tích log là một trong những lệnh cơ bản được sử dụng để tìm kiếm và lọc ra các thông tin cụ thể trong log file.

- Cú pháp của lệnh "find" là:

find [đường dẫn] [tùy chọn] [biểu thức điều kiện]

- Trong đó:

+ [đường dẫn]: đường dẫn đến thư mục chứa file log cần phân tích.

+ [tùy chọn]: các tùy chọn để chỉ định các hành động cụ thể của lệnh "find", chẳng hạn như "-name", "-type", "-mtime",...

+ [biểu thức điều kiện]: các biểu thức để chỉ định các điều kiện tìm kiếm cụ thể, ví dụ như tìm kiếm tất cả các dòng chứa từ khóa "error" trong file log.

4. Ý nghĩa lệnh secure:

- Lệnh secure có thể liên quan đến nhiều ngữ cảnh khác nhau trong phân tích log. Dưới đây là một số giải thích về các khái niệm liên quan đến secure và cách chúng có thể được áp dụng trong phân tích log:

+ "Secure log": Đây là một tệp log đăng nhập hệ thống trong môi trường Unix/Linux, nơi các sự kiện liên quan đến bảo mật được ghi lại. Trong trường hợp này, lệnh "secure" có thể được sử dụng để đọc và phân tích các sự kiện bảo mật trong tệp log này.

+ "Secure protocol": Đây là một giao thức mạng được thiết kế để đảm bảo tính bảo mật và xác thực trong quá trình truyền tải dữ liệu. Trong trường hợp này, lệnh "secure" có thể được sử dụng để xem và phân tích các thông tin giao tiếp liên quan đến giao thức bảo mật này trong các tệp log.

+ "Security log": Đây là một tệp log chung được sử dụng để ghi lại các sự kiện bảo mật trong các hệ thống và ứng dụng khác nhau. Trong trường hợp này, lệnh "secure" có thể được sử dụng để đọc và phân tích các sự kiện bảo mật trong tệp log này.

5. Ý nghĩa lệnh `access_log`:

- Lệnh "`access_log`" là một lệnh được sử dụng trong các máy chủ web để định cấu hình các tệp log truy cập. Khi một máy khách truy cập trang web của máy chủ, thông tin về truy cập sẽ được ghi lại trong tệp log này.

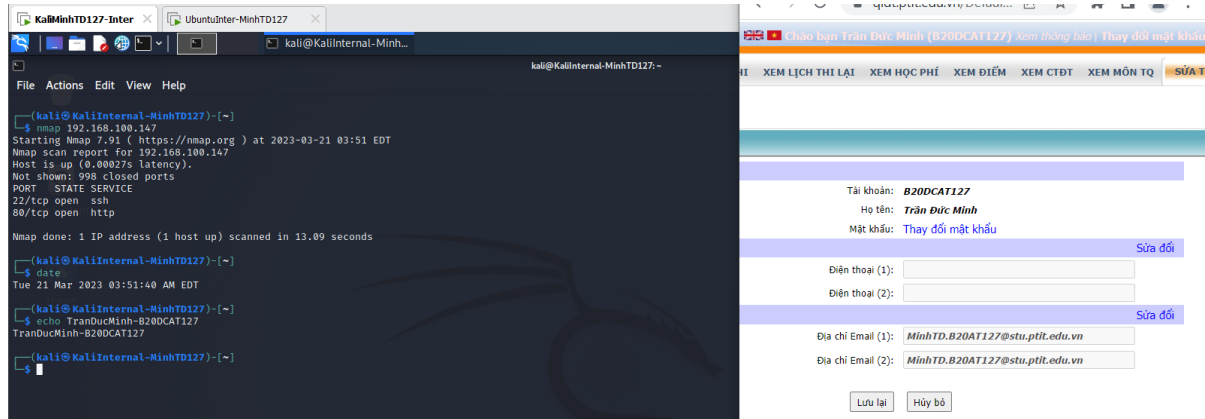
- Trong phân tích log, lệnh "`access_log`" thường được sử dụng để đọc và phân tích các thông tin liên quan đến truy cập trang web. Các thông tin này có thể bao gồm:

- + Địa chỉ IP của máy khách truy cập.
- + Thời gian truy cập.
- + Phương thức HTTP được sử dụng (GET, POST,...).
- + URL được truy cập.
- + Mã trạng thái HTTP (200, 404, 500,...).
- + Kích thước tệp được truy cập.
- + Thông tin về trình duyệt và hệ điều hành được sử dụng bởi máy khách truy cập.

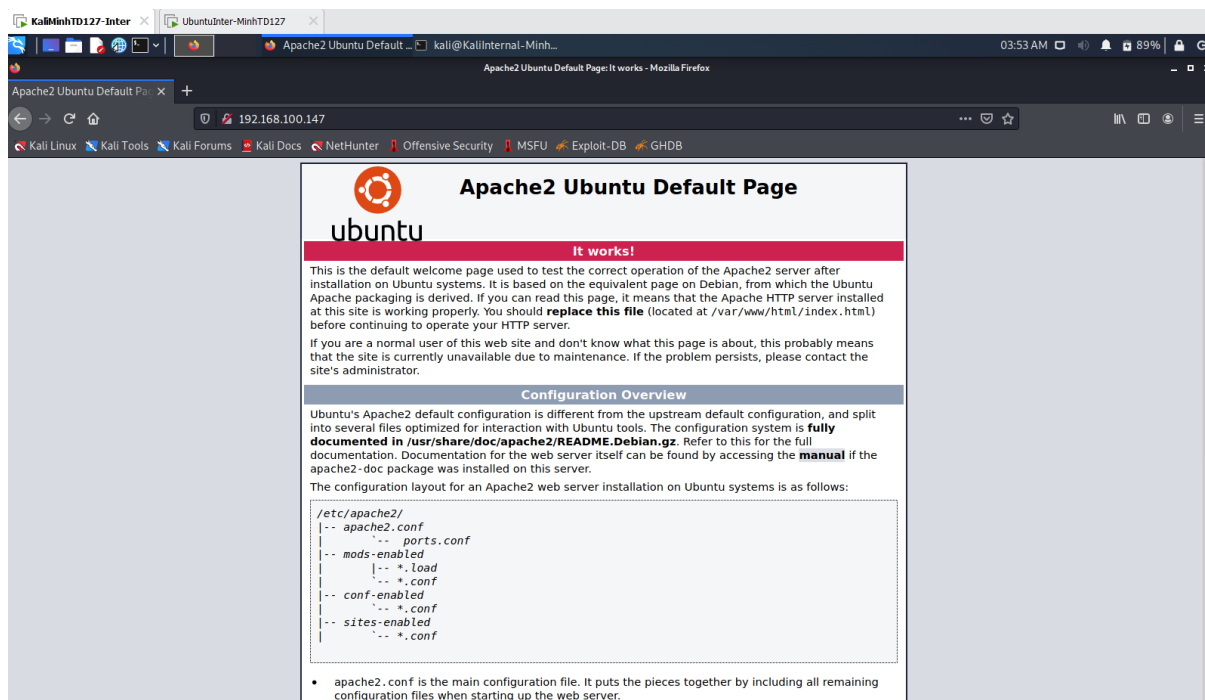
II. Nội dung thực hành:

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) 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”:

```

kali@KaliInternal-MinhTD127:~$ curl http://192.168.100.147/ | grep test
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 11321  100 11321    0     0    0     0    0     0    0     0    0     0    0     0    0
0 10.7M    0 0:00:00 0:00:00 0:00:00 10.7M
This is the default welcome page used to test the correct
(kali@KaliInternal-MinhTD127)~$ date
Tue 21 Mar 2023 03:55:22 AM EDT
(kali@KaliInternal-MinhTD127)~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
(kali@KaliInternal-MinhTD127)~$

```

- Trên máy Linux Internal Victim, vào thư mục chứa access_log và mở file access.log trên máy nạn nhân, dùng grep để lọc ra kết quả với từ khóa Firefox, curl:

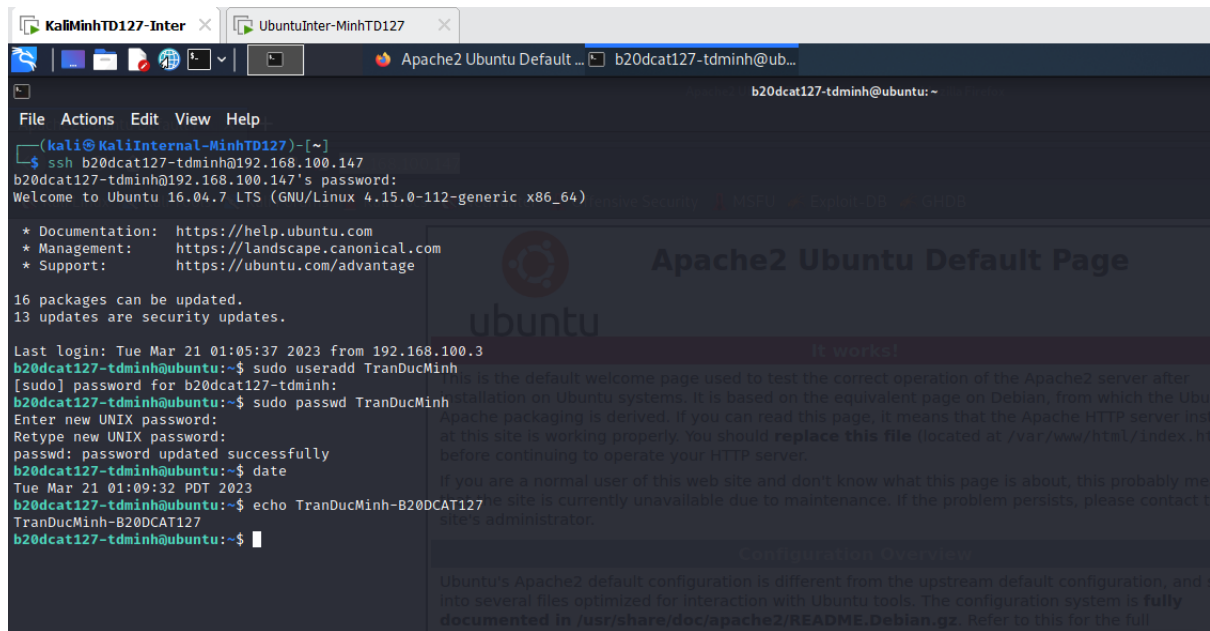
```

b20dcat127-tadmin@ubuntu: /var/log/apache2$ cd /var/log/apache2/
b20dcat127-tadmin@ubuntu: /var/log/apache2$ cat /var/log/apache2/access.log | grep Firefox
192.168.142.145 - - [21/Mar/2023:00:47:36 -0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.142.145 - - [21/Mar/2023:00:47:36 -0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.142.145/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.100.101 - - [21/Mar/2023:00:47:36 -0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.142.145/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.100.147 - - [21/Mar/2023:00:50:44 -0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.100.147 - - [21/Mar/2023:00:50:44 -0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.100.147/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.100.147 - - [21/Mar/2023:00:50:44 -0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.147/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0"
192.168.100.3 - - [21/Mar/2023:00:53:50 -0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.100.3 - - [21/Mar/2023:00:53:51 -0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.100.3 - - [21/Mar/2023:00:53:51 -0700] "GET /favicon.ico HTTP/1.1" 404 493 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.100.3 - - [21/Mar/2023:00:58:32 -0700] "GET / HTTP/1.1" 200 3525 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.100.3 - - [21/Mar/2023:00:58:32 -0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3623 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.100.3 - - [21/Mar/2023:00:58:32 -0700] "GET /favicon.ico HTTP/1.1" 404 493 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
b20dcat127-tadmin@ubuntu: /var/log/apache2$ date
Tue Mar 21 01:01:34 PDT 2023
b20dcat127-tadmin@ubuntu: /var/log/apache2$ echo TranDucMinh_B20DCAT127
TranDucMinh_B20DCAT127
b20dcat127-tadmin@ubuntu: /var/log/apache2$ cat /var/log/apache2/access.log | grep curl
192.168.100.3 - - [21/Mar/2023:00:55:20 -0700] "GET / HTTP/1.1" 200 11576 "-" "curl/7.74.0"

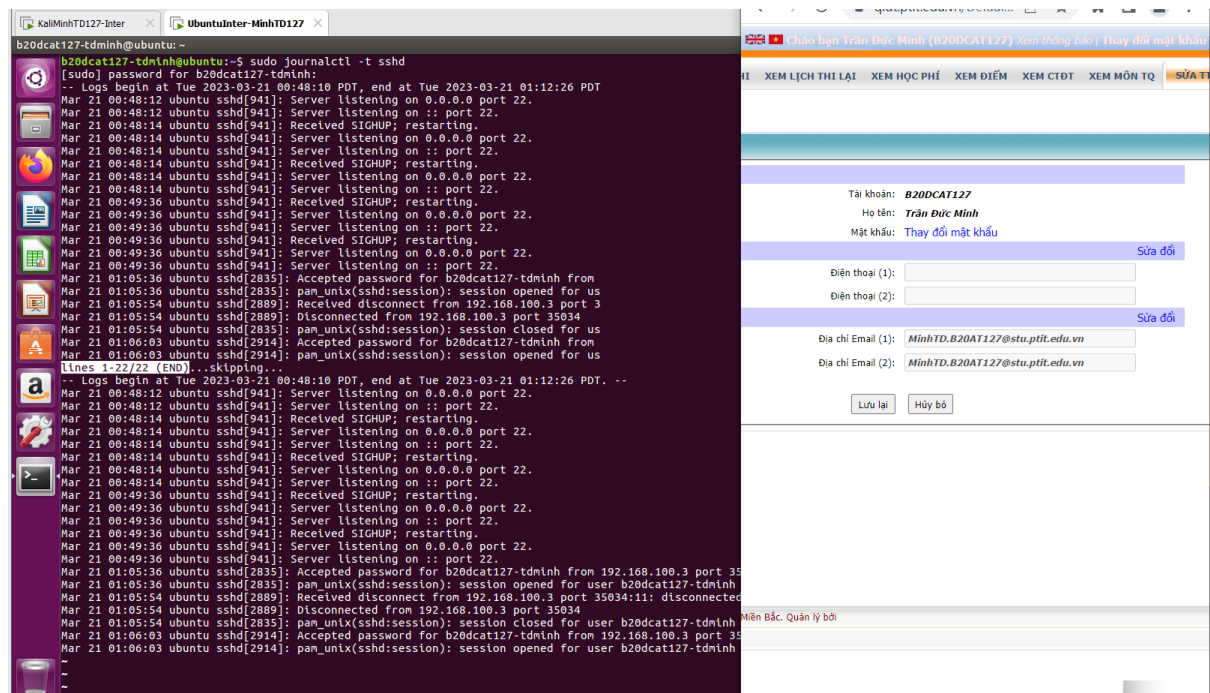
```

2. 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:



- Trên máy Linux Internal Victim, tiến hành xem file log bằng lệnh
`sudo journalctl -t sshd:`



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

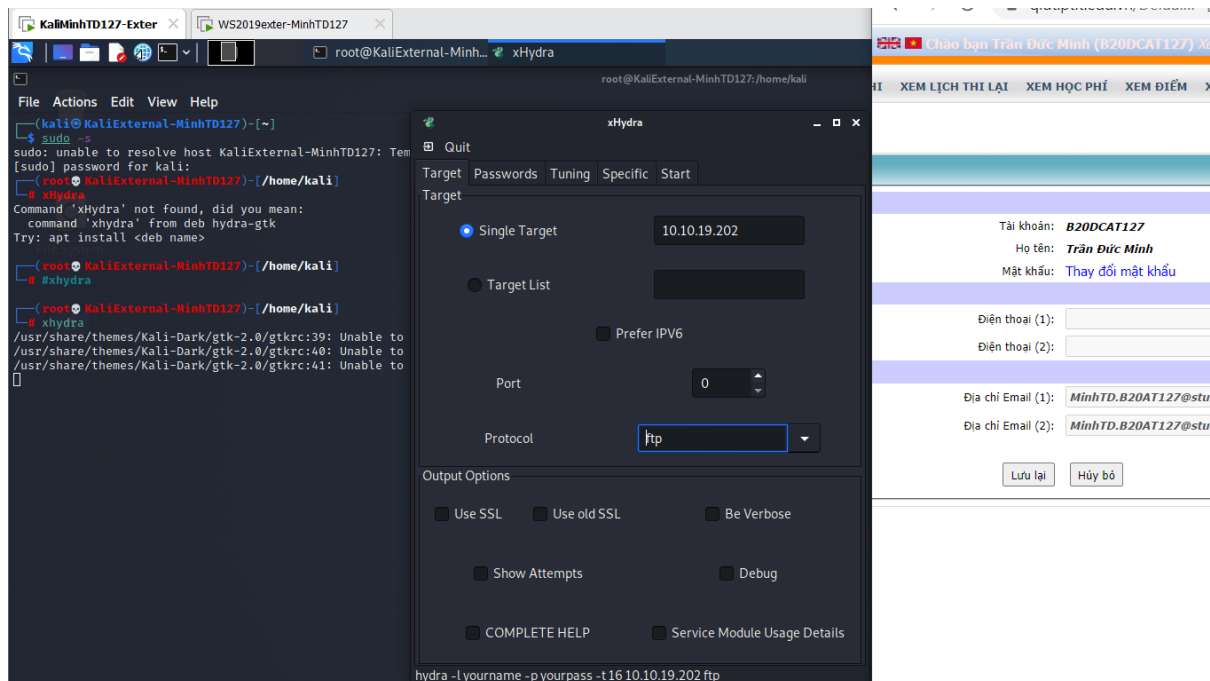
```
b20dcat127-tdminh@ubuntu:~$ cat /var/log/auth.log | grep useradd
Mar 21 01:08:31 ubuntu sudo: b20dcat127-tdminh : TTY=pts/17 ; PWD=/home/b20dcat127-tdminh ; USER=root ; COMMAND=/usr/sbin/useradd TranDucMinh
Mar 21 01:08:31 ubuntu useradd[2965]: new group: name=TranDucMinh, GID=1001
Mar 21 01:08:31 ubuntu useradd[2965]: new user: name=TranDucMinh, UID=1001, GID=1001, home=/home/TranDucMinh, shell=/bin/bash
b20dcat127-tdminh@ubuntu:~$ date
Tue Mar 21 01:14:43 PDT 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$
```

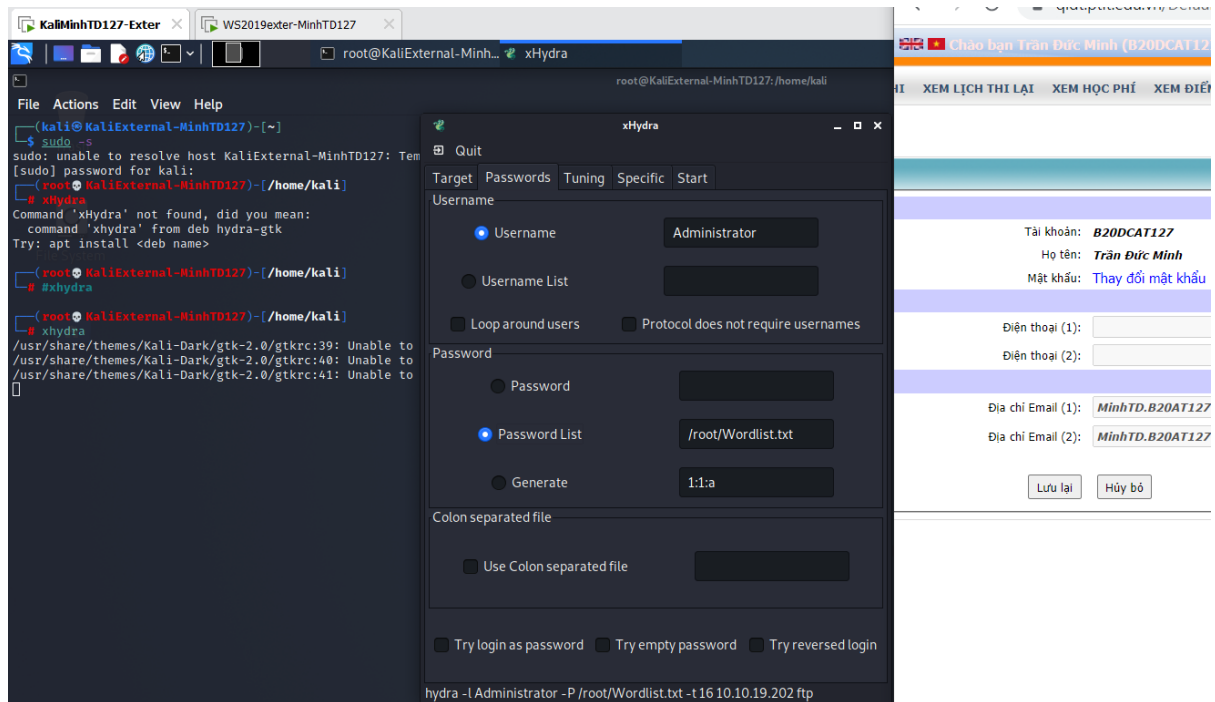
- Dùng lệnh gawk để in một hoặc nhiều dòng dữ liệu tìm được:

```
b20dcat127-tdminh@ubuntu:~$ awk '{print}' /var/log/auth.log
Mar 21 01:08:31 ubuntu sudo: b20dcat127-tdminh : TTY=pts/17 ; PWD=/home/b20dcat127-tdminh ; USER=root ; COMMAND=/usr/sbin/useradd TranDucMinh
Mar 21 01:08:31 ubuntu useradd[2965]: new group: name=TranDucMinh, GID=1001
Mar 21 01:08:31 ubuntu useradd[2965]: new user: name=TranDucMinh, UID=1001, GID=1001, home=/home/TranDucMinh, shell=/bin/bash
b20dcat127-tdminh@ubuntu:~$ date
Tue Mar 21 01:18:20 PDT 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$
```

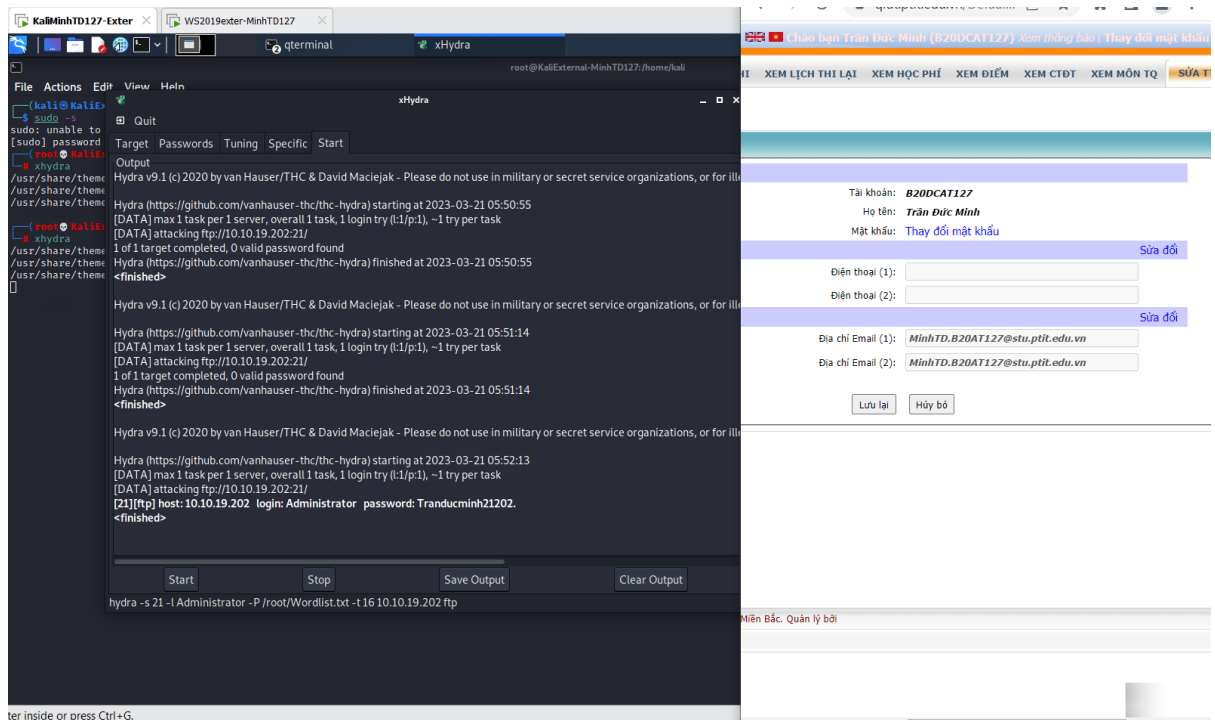
3. Phân tích log sử dụng find trong Windows:

- 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:

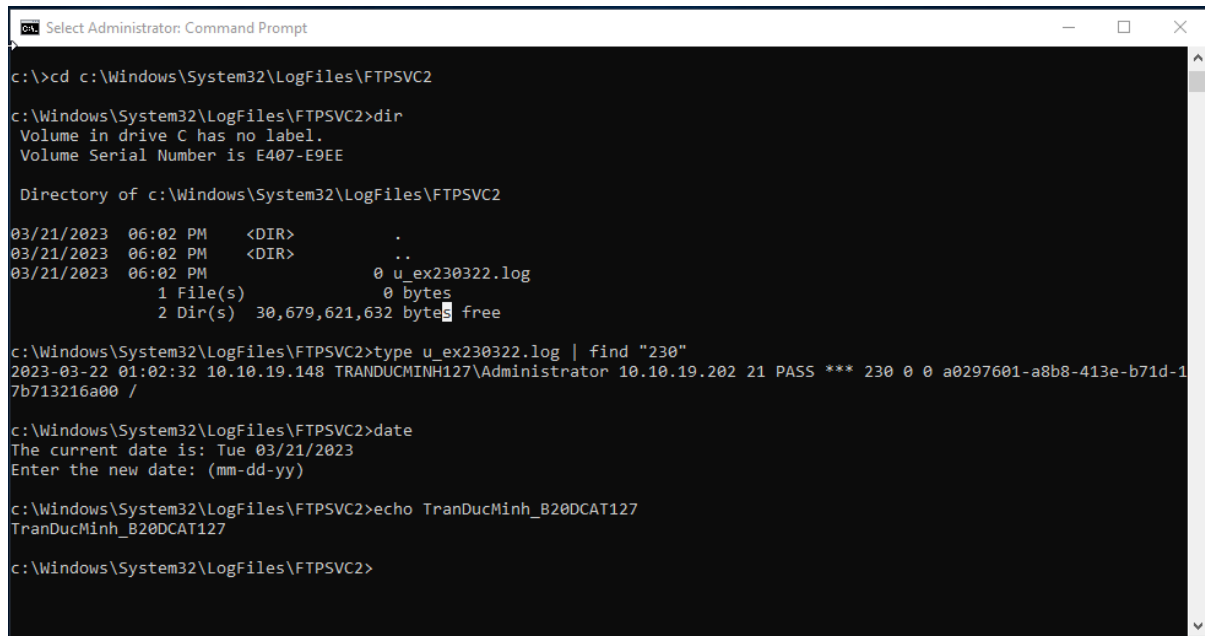




- xHydra tìm ra mật khẩu:



- Trên máy Windows 2003 Server External Victim, điều hướng đến FTP Logfile (C:\Windows\System32\Logfiles\FTPSVC2). Chọn 1 file mới nhất để mở ra (ex230322.log). Gõ lệnh “type u_ex230322.log | find “230” để tìm kiếm kết quả tấn công login thành công:



```

Select Administrator: Command Prompt

c:\>cd c:\Windows\System32\LogFiles\FTPSVC2

c:\Windows\System32\LogFiles\FTPSVC2>dir
Volume in drive C has no label.
Volume Serial Number is E407-E9EE

Directory of c:\Windows\System32\LogFiles\FTPSVC2

03/21/2023  06:02 PM    <DIR>          .
03/21/2023  06:02 PM    <DIR>          ..
03/21/2023  06:02 PM                0 u_ex230322.log
               1 File(s)                0 bytes
               2 Dir(s)  30,679,621,632 byte(s) free

c:\Windows\System32\LogFiles\FTPSVC2>type u_ex230322.log | find "230"
2023-03-22 01:02:32 10.10.19.148 TRANDUCMINH127\Administrator 10.10.19.202 21 PASS *** 230 0 0 a0297601-a8b8-413e-b71d-17b713216a00 /

c:\Windows\System32\LogFiles\FTPSVC2>date
The current date is: Tue 03/21/2023
Enter the new date: (mm-dd-yy)

c:\Windows\System32\LogFiles\FTPSVC2>echo TranDucMinh_B20DCAT127
TranDucMinh_B20DCAT127

c:\Windows\System32\LogFiles\FTPSVC2>
```

