

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



BÁO CÁO THỰC HÀNH

Bài 9: Phân tích log hệ thống

Họ và tên: Vũ Thành Long

Mã sinh viên: B21DCAT012

Nhóm: 06

Môn học: Thực tập cơ sở

Giảng viên giảng dạy: Nguyễn Hoa Cương

Hà Nội, 2024

Mục lục

I. Tìm hiểu lý thuyết.....	2
1. grep.....	2
2. gawk và awk.....	2
3. find.....	2
4. hydra và xhydra.....	2
II. Mô tả cài đặt & kết quả	3
1. Phân tích log sử dụng grep trong Linux.....	3
2. Phân tích log sử dụng gawk trong Linux	6
3. Phân tích log sử dụng find trong Windows.....	9
III. Tài liệu tham khảo.....	13

Bài 9: Phân tích log hệ thống

I. Tìm hiểu lý thuyết:

1. grep:

- grep là công cụ tìm kiếm các dòng văn bản trong một tệp văn bản chứa nội dung khớp với cụm từ mà người dùng yêu cầu tìm.
- grep ban đầu được phát triển cho hệ điều hành Unix, nhưng sau đó có sẵn cho tất cả các hệ điều hành họ Unix và một số hệ thống khác như OS-9.
- Trong bài thực hành bên dưới, sinh viên sử dụng lệnh **grep <từ khoá> <tên file>** để in ra các dòng có chứa từ khoá trong file văn bản.

2. gawk và awk:

- gawk là một phiên bản của ngôn ngữ lập trình Awk, do GNU phát triển.
- AWK (awk) là ngôn ngữ lập trình được thiết kế để xử lý văn bản và thường được sử dụng làm công cụ báo cáo và trích xuất dữ liệu.
- Trong bài thực hành bên dưới, sinh viên sử dụng lệnh **awk '/từ khoá/ {print}' <tên file>** để in ra màn hình các dòng chứa từ khoá tương ứng trong file văn bản.

3. find:

- find là một lệnh có trong shell hoặc terminal của một số hệ điều hành như DOS, ReactOS, Microsoft Windows, v.v
- Nó được sử dụng để tìm kiếm một chuỗi văn bản cụ thể trong một tệp hoặc các tệp.
- Nếu tìm kiếm thành công, find sẽ in ra các dòng chứa nội dung trùng khớp ra màn hình terminal (cmd).
- Cần lưu ý rằng lệnh find trên Windows và find trên Linux có tác dụng hoàn toàn khác nhau.
- Trong bài thực hành bên dưới, sinh viên dùng lệnh **type <tên file> | find "<từ khoá>"** để lọc và in ra các dòng có chứa từ khoá trong file văn bản.

4. hydra và xhydra:

- hydra là một trình bẻ khóa đăng nhập mạng được có sẵn trong các hệ điều hành khác nhau như Kali Linux, Parrot và các môi

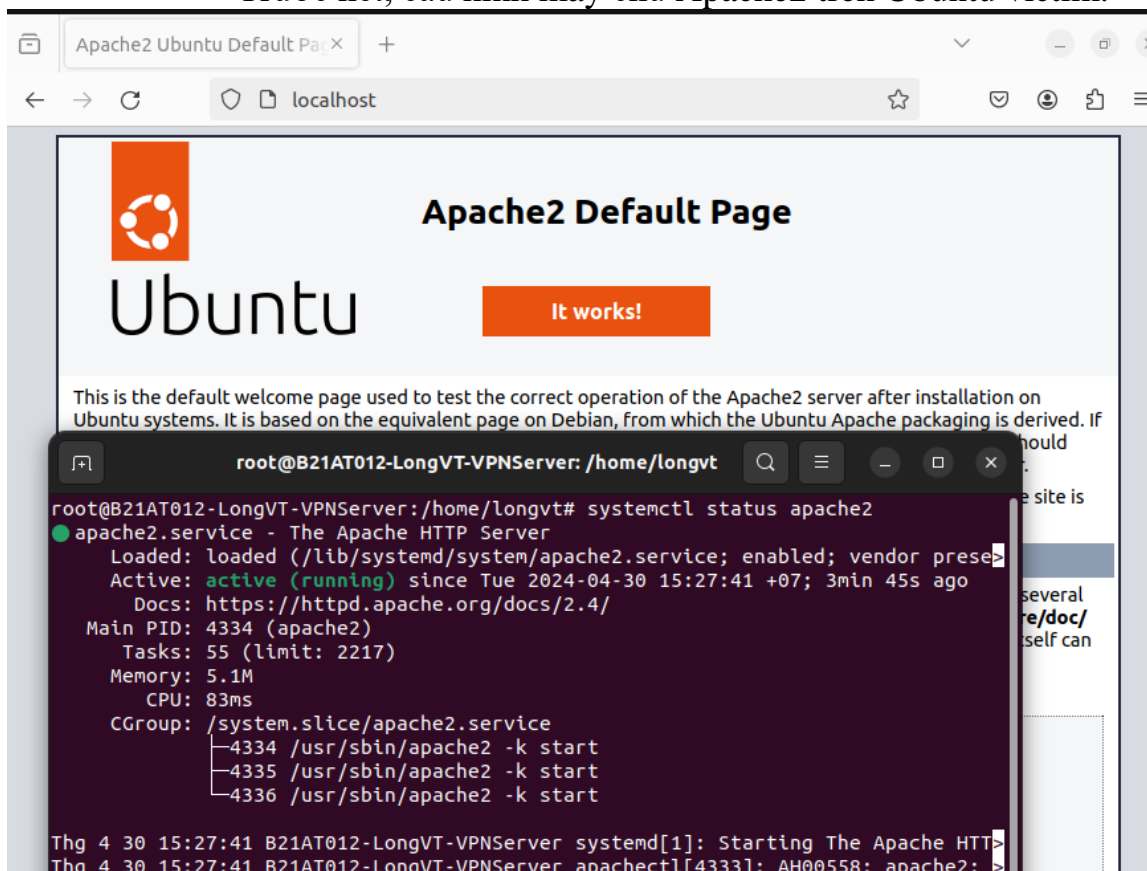
trường thử nghiệm thâm nhập lớn khác.

- hydra hoạt động bằng cách sử dụng các cách tiếp cận khác nhau để thực hiện các cuộc tấn công brute-force nhằm đoán đúng các cặp tên người dùng và mật khẩu.
- hydra hỗ trợ nhiều giao thức đăng nhập phổ biến như biểu mẫu trên trang web, FTP, SMB, POP3, IMAP, MySQL, VNC, SSH, v.v
- xhydra là giao diện đồ họa (GUI) của hydra.

II. Mô tả cài đặt & kết quả:

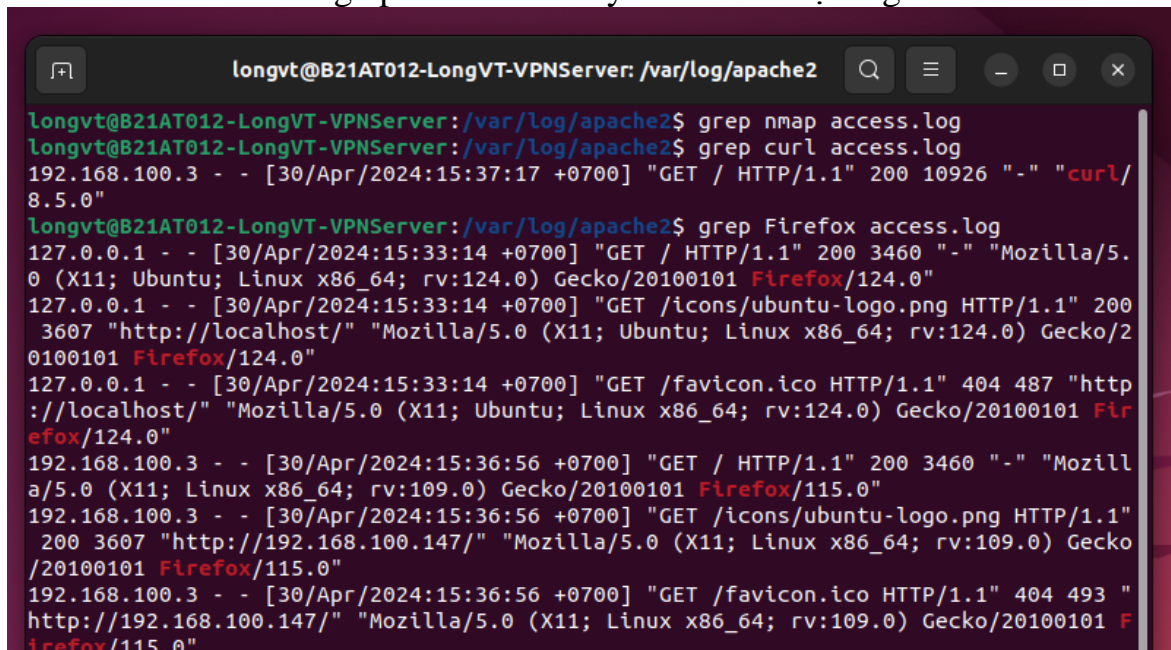
1. Phân tích log sử dụng grep trong Linux:

- Trước hết, cấu hình máy chủ Apache2 trên Ubuntu victim.



- Sau khi cấu hình thành công, truy cập trang web trên trình duyệt Firefox và chạy lệnh `curl http://192.168.100.147 | grep test`

- Sau khi thực hiện các bước trên, truy cập thư mục `/var/log/apache2` trên máy Ubuntu để lọc log.



```
longvt@B21AT012-LongVT-VPNServer: /var/log/apache2
longvt@B21AT012-LongVT-VPNServer:/var/log/apache2$ grep nmap access.log
longvt@B21AT012-LongVT-VPNServer:/var/log/apache2$ grep curl access.log
192.168.100.3 - - [30/Apr/2024:15:37:17 +0700] "GET / HTTP/1.1" 200 10926 "-" "curl/8.5.0"
longvt@B21AT012-LongVT-VPNServer:/var/log/apache2$ grep Firefox access.log
127.0.0.1 - - [30/Apr/2024:15:33:14 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
127.0.0.1 - - [30/Apr/2024:15:33:14 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
127.0.0.1 - - [30/Apr/2024:15:33:14 +0700] "GET /favicon.ico HTTP/1.1" 404 487 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
192.168.100.3 - - [30/Apr/2024:15:36:56 +0700] "GET / HTTP/1.1" 200 3460 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [30/Apr/2024:15:36:56 +0700] "GET /icons/ubuntu-logo.png HTTP/1.1" 200 3607 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
192.168.100.3 - - [30/Apr/2024:15:36:56 +0700] "GET /favicon.ico HTTP/1.1" 404 493 "http://192.168.100.147/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

2. Phân tích log sử dụng gawk trong Linux:

- Dùng SSH trên máy Kali, đăng nhập vào tài khoản trên máy Ubuntu.
- Sau đó, chạy lệnh **sudo useradd -m -g <group> <tênSV>** để tạo một tài khoản người dùng mới trên máy Ubuntu.
- Chạy lệnh **sudo passwd <tên tài khoản>** để đổi mật khẩu của tài khoản.

```
kali@B21AT012-LongVT-Kali-Internal: ~
File Actions Edit View Help

(kali@B21AT012-LongVT-Kali-Internal)-[~]
$ ssh longvt@192.168.100.147
The authenticity of host '192.168.100.147 (192.168.100.147)' can't be established.
ED25519 key fingerprint is SHA256:PWE6yQP+GTcx0Xht252G7fJzJMGcwRaAg1pumbCGxcM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.100.147' (ED25519) to the list of known hosts.
longvt@192.168.100.147's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-26-generic x86_64)

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

Expanded Security Maintenance for Applications is not enabled.

107 updates can be applied immediately.
55 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Mar 23 17:52:54 2024 from 10.10.19.148
longvt@B21AT012-LongVT-VPNServer:~$ sudo useradd -m -g users B21AT012-VuThanhLong
[sudo] password for longvt:
longvt@B21AT012-LongVT-VPNServer:~$ sudo passwd B21AT012-VuThanhLong
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
longvt@B21AT012-LongVT-VPNServer:~$ exit
logout
Connection to 192.168.100.147 closed.
```

- Trên máy Ubuntu, truy cập vào thư mục /var/log và lọc kết quả trong tệp tin auth.log bằng grep.

```
longvt@B21AT012-LongVT-VPNServer: /var/log
longvt@B21AT012-LongVT-VPNServer:/var/log$ grep B21AT012-VuThanhLong auth.log
Apr 30 15:43:50 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USER=root ; COMMAND=/usr/sbin/useradd -m -g users B21AT012-VuThanhLong
Apr 30 15:43:50 B21AT012-LongVT-VPNServer useradd[7033]: new user: name=B21AT012-VuThanhLong, UID=1001, GID=100, home=/home/B21AT012-VuThanhLong, shell=/bin/sh, from=/dev/pts/2
Apr 30 15:44:03 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USER=root ; COMMAND=/usr/bin/passwd B21AT012-VuThanhLong
Apr 30 15:44:10 B21AT012-LongVT-VPNServer passwd[7074]: pam_unix(passwd:chauthtok): password changed for B21AT012-VuThanhLong
longvt@B21AT012-LongVT-VPNServer:/var/log$
```


- Dùng SSH trên máy Kali đăng nhập vào tài khoản người dùng trên máy Ubuntu, rồi chạy lệnh **grep <tên tài khoản> /var/log/auth.log** để lọc log tương tự bước trên.
- Có thể dùng lệnh **awk '/từ khoá/ {print}' <tên file>** để xuất kết quả tương tự lệnh grep bên trên.

```

longvt@B21AT012-LongVT-VPNServer: ~
File Actions Edit View Help
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

107 updates can be applied immediately.
55 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

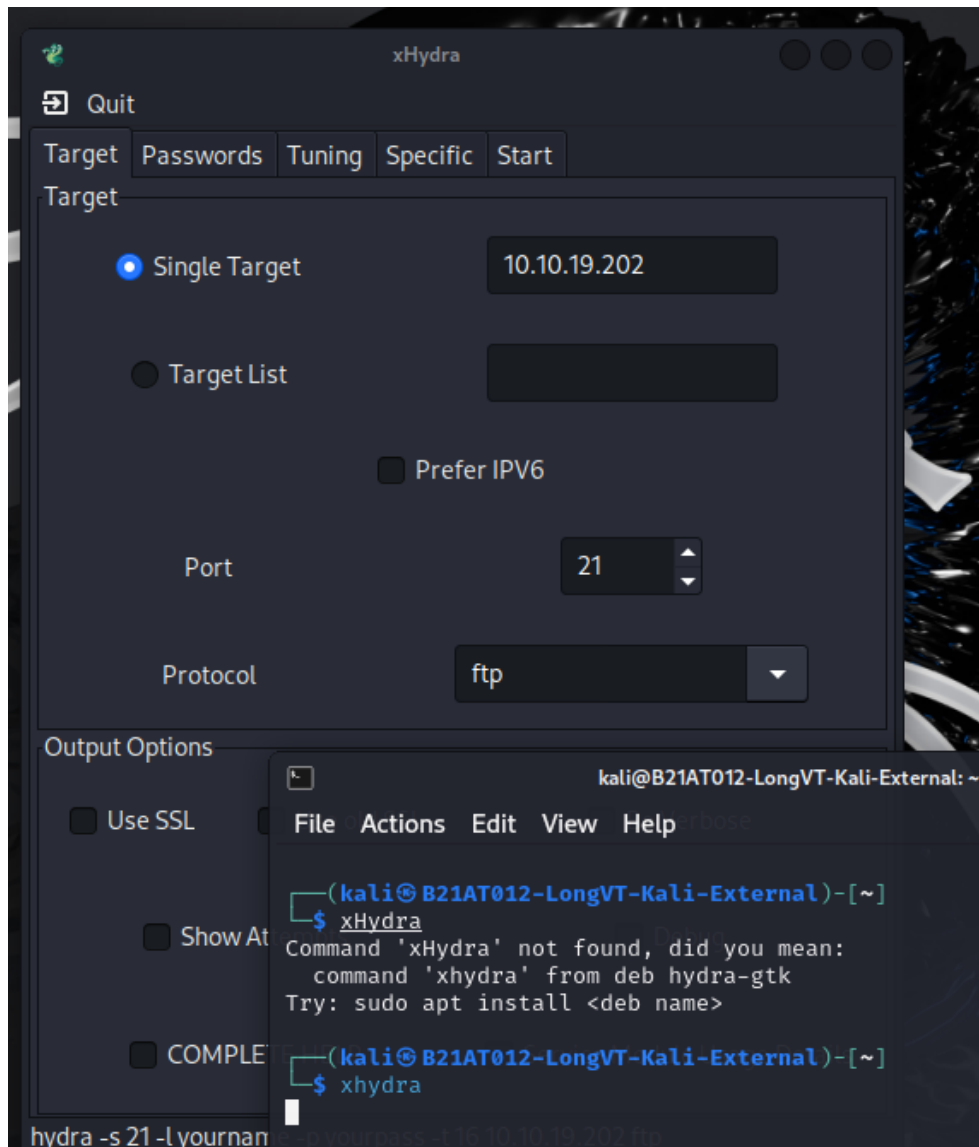
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Apr 30 15:43:02 2024 from 192.168.100.3
longvt@B21AT012-LongVT-VPNServer:~$ grep B21AT012-VuThanhLong /var/log/auth.log
Apr 30 15:43:50 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USE
R=root ; COMMAND=/usr/sbin/useradd -m -g users B21AT012-VuThanhLong
Apr 30 15:43:50 B21AT012-LongVT-VPNServer useradd[7033]: new user: name=B21AT012-VuThanhLong,
UID=1001, GID=100, home=/home/B21AT012-VuThanhLong, shell=/bin/sh, from=/dev/pts/2
Apr 30 15:44:03 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USE
R=root ; COMMAND=/usr/bin/passwd B21AT012-VuThanhLong
Apr 30 15:44:10 B21AT012-LongVT-VPNServer passwd[7074]: pam_unix(passwd:chauthtok): password
changed for B21AT012-VuThanhLong
longvt@B21AT012-LongVT-VPNServer:~$ awk '/B21AT012-VuThanhLong/ {print}' /var/log/auth.log
Apr 30 15:43:50 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USE
R=root ; COMMAND=/usr/sbin/useradd -m -g users B21AT012-VuThanhLong
Apr 30 15:43:50 B21AT012-LongVT-VPNServer useradd[7033]: new user: name=B21AT012-VuThanhLong,
UID=1001, GID=100, home=/home/B21AT012-VuThanhLong, shell=/bin/sh, from=/dev/pts/2
Apr 30 15:44:03 B21AT012-LongVT-VPNServer sudo: longvt : TTY=pts/1 ; PWD=/home/longvt ; USE
R=root ; COMMAND=/usr/bin/passwd B21AT012-VuThanhLong
Apr 30 15:44:10 B21AT012-LongVT-VPNServer passwd[7074]: pam_unix(passwd:chauthtok): password
changed for B21AT012-VuThanhLong
longvt@B21AT012-LongVT-VPNServer:~$

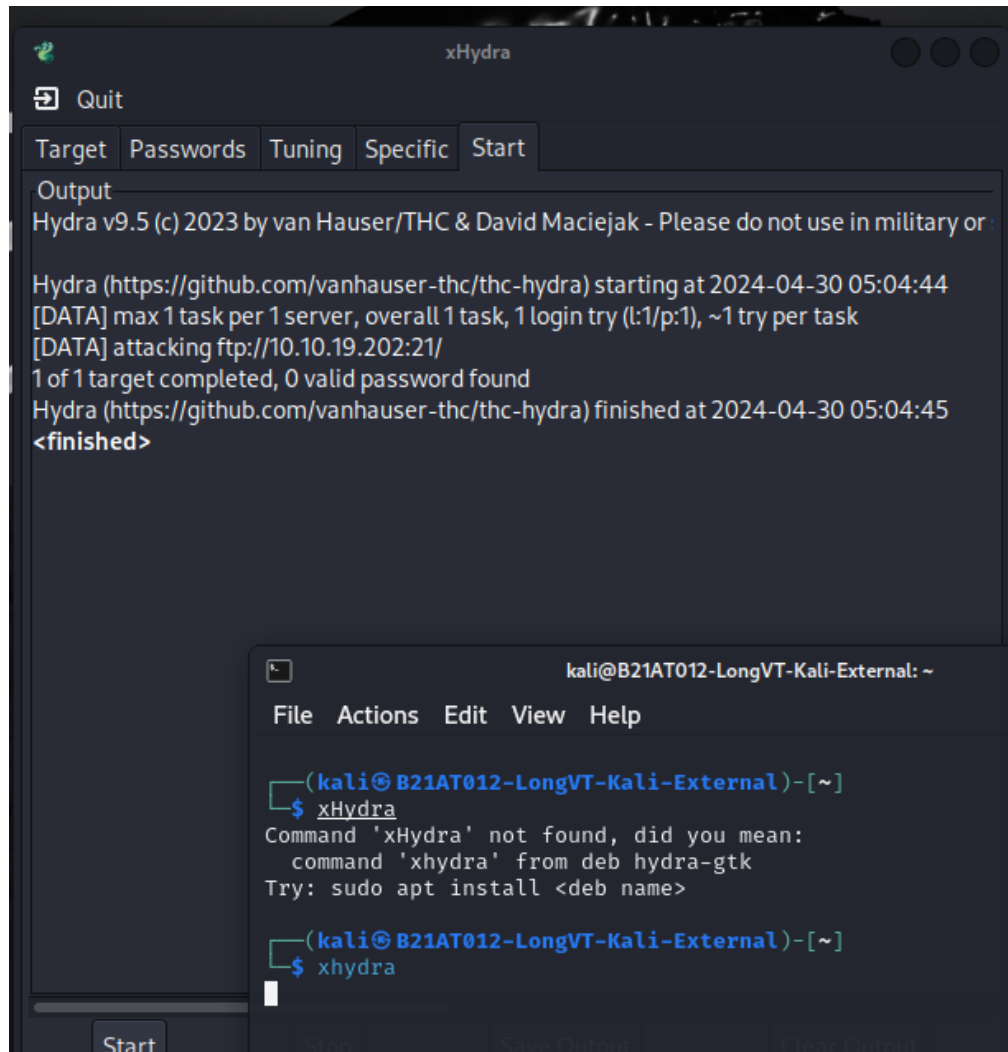
```

3. Phân tích log sử dụng find trong Windows:

- Khởi động máy chủ Windows Server (đã cài đặt FTP site). Khởi động giao diện xHydra. Mục Single Target chọn 10.10.19.202, port chọn 21 (có thể kiểm tra port bằng nmap), protocol chọn ftp.
- Mục Password list, chỉ đến tệp tài liệu ghi lại danh sách các password có thể xảy ra nhất. Mục Username chọn tên người dùng mình muốn tấn công, trong trường hợp này là Administrator.
- Tóm lại, lệnh chạy hydra sẽ là **hydra -s 21 -l Administrator -P /home/kali/Downloads/pass -t 16 10.10.19.202 ftp**



- Bấm Start để bắt đầu tấn công. Nếu thành công, chương trình sẽ hiển thị tên tài khoản và mật khẩu ra màn hình như hình dưới. Thời điểm tấn công thành công là 05:04:44.



- Trên máy chủ Windows Server, mở thư mục log (tùy theo cài đặt của quản trị viên, mặc định là C:\inetpub\logs\LogFiles\FTPSVC2). Tìm thấy 1 file log là u_ex240430.log.
- Dùng lệnh **type u_ex240430.log | find "530"** để lọc file log.
- Có được kết quả là vào 09:04:46, địa chỉ IP 10.10.19.148 đã đăng nhập thành công vào FTP Server.
- Do bất cẩn, sinh viên để file log dùng múi giờ GMT còn múi giờ máy tính là GMT+7 nên mới xảy ra lệnh 7 giờ

```
Administrator: C:\Windows\system32\cmd.exe

C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex240430.log | find "530"
2024-04-30 09:04:46 10.10.19.148 - 10.10.19.202 21 PASS *** 530 1326 41 5f366f4e-f5c7-40c9-ab0c-aba0fd4164a5 -

C:\inetpub\logs\LogFiles\FTPSVC2>echo B21DCAT012-VuThanhLong
B21DCAT012-VuThanhLong

C:\inetpub\logs\LogFiles\FTPSVC2>
```

III. Tài liệu tham khảo:

- gawk Documentation:
<http://www.gnu.org/software/gawk/manual/gawk.html>
- hydra Ubuntu Documentation:
<https://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>