

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



**Môn học: Thực Tập Cơ Sở**  
**Báo Cáo Bài Thực Hành 9**  
**Phân tích log hệ thống**

**Họ và tên:** Trần Thị Thu Phương

**Mã sinh viên:** B21DCAT151

**Nhóm môn học:** 04

**Giảng viên:** Đinh Trường Duy

Hà Nội, 1/2024

## Mục lục

<b>1. Mục đích .....</b>	<b>3</b>
<b>2. Nội dung thực hành .....</b>	<b>3</b>
<b>2.1. Cơ sở lý thuyết.....</b>	<b>3</b>
2.1.1.    Tìm hiểu về Windows Event và Auditing .....	3
a.    Windows Event.....	3
b.    Auditing .....	4
2.1.2.    Lệnh grep .....	5
2.1.3.    Lệnh gawk.....	5
2.1.4.    Lệnh find.....	6
2.1.5.    Lệnh access_log.....	7
2.1.6.    Xhydra .....	7
<b>2.2. Nội dung thực hành .....</b>	<b>7</b>
2.2.1.    Chuẩn bị môi trường.....	7
2.2.2.    Phân tích log sử dụng grep trong Linux .....	8
2.2.3.    Phân tích log sử dụng gawk trong Linux.....	10
2.2.4.    Phân tích log sử dụng find trong Windows .....	13
<b>3. Kết luận .....</b>	<b>15</b>
<b>4. Tài liệu tham khảo.....</b>	<b>15</b>

## Danh mục hình ảnh

Cấu hình topo mạng.....	8
Xem được port 80 đang mở cho Web Server .....	9
Xem thư mục chứa access_log .....	10
Ssh đến IP 192.168.100.147 bằng user tranthithuphuongb21dcat151 .....	11
Tạo một account mới và đổi mật khẩu cho account này .....	11
Trên máy Linux Internal Victim, tiến hành xem file log .....	12
Sử dụng lệnh grep .....	12
Sử dụng lệnh gawk .....	13
Khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list..	13
Kết quả crack mật khẩu từ xHydra.....	14
Xem file log trên máy Windows victim .....	14

## 1. Mục đích

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

- Phân tích log sử dụng grep/gawk trong Linux
- Phân tích log sử dụng find trong Windows
- Tìm hiểu về Windows Event Viewer và auditing
- Phân tích event log trong Windows

## 2. Nội dung thực hành

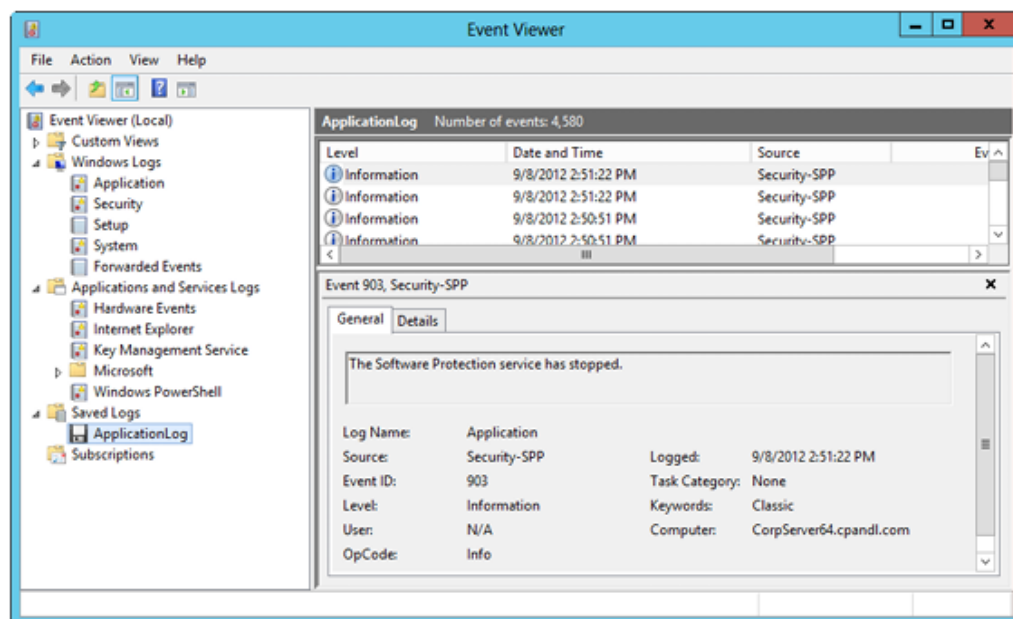
### 2.1. Cơ sở lý thuyết

#### 2.1.1. Tìm hiểu về Windows Event và Auditing

##### a. Windows Event

Hệ điều hành Windows định nghĩa sự kiện là bất cứ điều gì đáng kể xảy ra khi vận hành hệ điều hành hay ứng dụng. Các sự kiện này cần được lưu lại phục vụ mục đích theo dõi. Các thông tin có được theo dõi như cảnh báo, các lỗi, hay các sự kiện kiểm toán. Có hai kiểu file nhật ký sự kiện là:

- Nhật ký Windows: lưu lại các sự kiện hệ thống nói chung liên quan đến ứng dụng, an ninh, cài đặt và các thành phần hệ thống;
- Nhật ký dịch vụ và ứng dụng: lưu lại việc sử dụng của ứng dụng hay dịch vụ cụ thể.



**Hình 4-6. Chương trình xem các sự kiện được lưu lại**

Để xem nhật ký sự kiện, người quản trị sử dụng chương trình “Event Viewer” như trong hình trên. Với mỗi sự kiện chương trình sẽ đánh dấu tương ứng như sau:

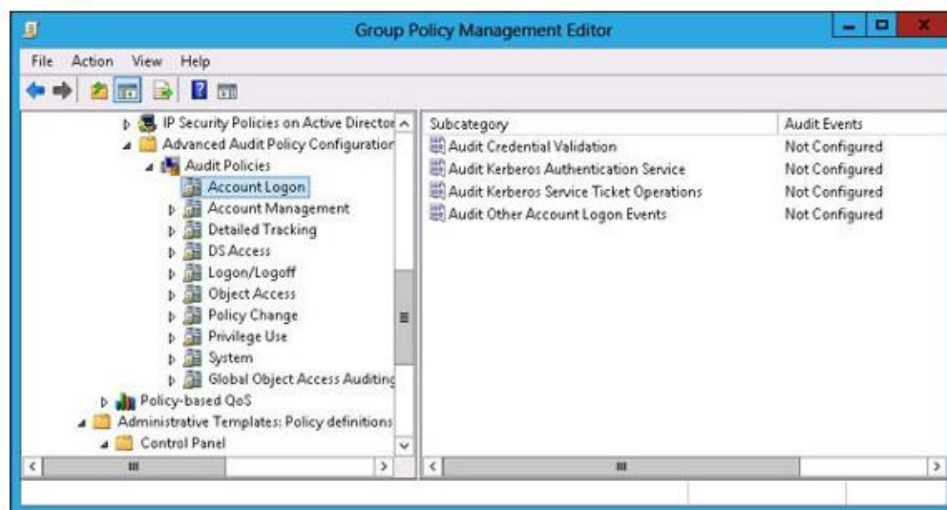
- Thông tin: Thông báo thông thường về thao tác được thực hiện thành công.

- Cảnh báo: Mô tả sự kiện không nghiêm trọng nhưng cần chú ý để tránh các vấn đề xa hơn.
- Lỗi: Cho biết một lỗi hay vấn đề không nghiêm trọng xảy ra.
- Nghiêm trọng: Cho thấy một lỗi nghiêm trọng hay vấn đề rất đáng kể xảy ra.
- Kiểm toán thành công: Mô tả sự kiện kiểm toán an ninh thành công như yêu cầu.
- Kiểm toán thất bại: Mô tả sự kiện kiểm toán an ninh không thành công như yêu cầu.

## b. Auditing

Việc kiểm toán cho phép người quản trị theo dõi cả truy nhập thực tế và cố thử truy nhập hay các sửa đổi các đối tượng và chính sách của hệ thống. Các đối tượng có thể là thư mục và file cũng như các đối tượng an ninh của hệ thống. Cách chính sách kiểm toán hỗ trợ việc đảm bảo an toàn cho hệ thống, theo dõi các sửa đổi các dữ liệu nhạy cảm hay các tài khoản cần đề ý.

Có hai tập chính sách kiểm toán trong một đối tượng chính sách nhóm GPO: chính sách kiểm toán truyền thống và nâng cao. Chính sách truyền thống có từ bản Server 2000. Chính sách này có nhược điểm là chúng không đủ cụ thể và khó cấu hình. Chính sách nâng cao khắc phục nhược điểm này và cung cấp 10 nhóm cài đặt với 58 chính sách kiểm toán riêng lẻ.



**Hình 4-7. Chính sách kiểm toán nâng cao**

Các nhóm chính sách tiêu biểu bao gồm:

- Đăng nhập: theo dõi việc xác thực thông tin đăng nhập
- Quản lý tài khoản: theo dõi các thao tác thay đổi tài khoản như người dùng, máy tính...
- Theo dõi chi tiết: theo dõi việc chạy chương trình, các lời gọi hàm từ xa...

- Truy nhập thư mục động: theo dõi việc truy nhập hay các chức năng của thư mục động.
- Truy nhập đối tượng: theo dõi việc truy nhập các file, thư mục hay ứng dụng.

### 2.1.2. Lệnh grep

Grep là từ viết tắt của Global Regular Expression Print. Lệnh grep trong Linux được sử dụng để tìm kiếm một chuỗi ký tự trong một file hoặc nhiều file được chỉ định. Lệnh grep trong Linux sẽ rất tiện lợi khi tìm kiếm các file log lớn.

**Cú pháp: grep [tùy chọn] [mẫu] [tệp...]**

- [tùy chọn]: Các tùy chọn để tinh chỉnh cách hoạt động của grep, bao gồm -i, -r, -v, và nhiều tùy chọn khác.
- [mẫu]: Mẫu bạn muốn tìm kiếm, có thể là một chuỗi đơn giản hoặc một biểu thức chính quy phức tạp.
- [tệp...]: Các tệp bạn muốn tìm kiếm trong đó. Nếu không chỉ định, grep sẽ đọc từ đầu vào tiêu chuẩn (stdin)

### Một số các cách sử dụng lệnh GREP

- Tìm kiếm một chuỗi ký tự trong một tập tin.  
*grep "chuỗi cần tìm" tên\_file*
- Tìm kiếm chuỗi trong nhiều file cùng lúc.  
*grep 'chuỗi cần tìm' file1 file2 file3. . .*
- Tìm kiếm chuỗi mà không phân biệt chữ hoa/chữ thường.  
*grep -i "chuỗi cần tìm" tên\_file*
- Tìm kiếm chuỗi sử dụng biểu thức chính quy (regular expression).  
*grep -E 'â' example.txt*
- Tìm kiếm chuỗi đúng với từ khóa cụ thể.  
*grep -w "apple" fruits.txt*
- Tìm kiếm chuỗi trong tất cả các file và thư mục con.  
*grep -r "chuỗi tìm kiếm" /đường/dẫn/thư/mục*
- Tìm kiếm chuỗi không có từ khóa cụ thể.  
*grep -v 'pattern' filename*
- Đếm số lần xuất hiện của chuỗi trong file.  
*grep -c "chuỗi" file.txt.*

### 2.1.3. Lệnh gawk

Lệnh **gawk** là một phiên bản mở rộng của lệnh **awk** trong hệ thống Unix/Linux. **gawk** được sử dụng để xử lý và phân tích dữ liệu văn bản, thường là dữ liệu dạng bảng, dòng đơn giản mà có thể được chia thành các cột như CSV (Comma-Separated Values), TSV (Tab-Separated Values),...

Một số cách sử dụng:

- In nội dung của một cột cụ thể trong mỗi dòng của tệp văn bản:

```
gawk '{print $1}' file.csv
```

Lệnh này sẽ in ra nội dung của cột đầu tiên trong mỗi dòng của tệp văn bản "file.csv".

- Tính tổng các giá trị trong một cột cụ thể:

```
gawk 'sum += $2' END {print sum}' file.csv
```

Đây là một ví dụ về cách tính tổng của tất cả các giá trị trong cột thứ hai của tệp văn bản "file.csv" và in kết quả cuối cùng.

- Tìm kiếm và in các dòng phù hợp với một biểu thức chính quy:

```
gawk '/pattern/' file.csv
```

Lệnh này sẽ in ra các dòng trong tệp văn bản "file.csv" mà khớp với biểu thức chính quy "pattern".

- Sử dụng điều kiện để lọc và xử lý dữ liệu:

```
gawk '$3 > 100 {print $1, $3}' file.csv
```

Lệnh này sẽ in ra cột đầu tiên và cột thứ ba của các dòng trong "file.csv" mà cột thứ ba có giá trị lớn hơn 100.

#### 2.1.4. Lệnh find

Lệnh find là một công cụ tìm kiếm tệp tin trong hệ thống Linux. Cho phép người dùng tìm kiếm theo nhiều tiêu chí như tên file, kích thước file, thời gian tạo hoặc sửa đổi file, quyền truy cập file, v.v.

**Cú pháp: find [path] [options] [expression]**

- **path:** Đường dẫn thư mục bắt đầu tìm kiếm. Nếu không chỉ định, lệnh find sẽ tìm kiếm trong thư mục hiện tại.
- **options:** Các tùy chọn để điều chỉnh quá trình tìm kiếm.
- **expression:** Biểu thức tìm kiếm.

**Một số cách sử dụng:**

- Tìm kiếm theo tệp hoặc thư mục

```
find /path/to/search -name "filename"
```

Lệnh này sẽ tìm kiếm tất cả các tệp hoặc thư mục có tên "filename" trong thư mục **/path/to/search** và các thư mục con của nó.

- Tìm kiếm theo loại tệp

```
find /path/to/search -type f
```

Lệnh này sẽ tìm kiếm tất cả các tệp hoặc thư mục có tên "filename" trong thư mục **/path/to/search** và các thư mục con của nó.

- Tìm kiếm theo quyền truy cập

```
find /path/to/search -perm 644
```

Lệnh này sẽ tìm kiếm các tệp hoặc thư mục có quyền truy cập là **644** trong thư mục **/path/to/search** và các thư mục con của nó.

- Tìm kiếm dựa trên thời gian

*find /path/to/search -mtime -7*

Lệnh này sẽ tìm kiếm các tệp hoặc thư mục được sửa đổi trong vòng 7 ngày qua trong thư mục

- Tìm kiếm và thực hiện các hành động khác

*find /path/to/search -name "filename" -exec command {} \;*

Lệnh này sẽ tìm kiếm tệp có tên "filename" trong thư mục **/path/to/search** và thực hiện lệnh **command** trên mỗi tệp được tìm thấy.

- Tìm kiếm đệ quy trong tất cả các thư mục

*find /path/to/search -name "filename" -type f -exec grep "pattern" {} \;*

Lệnh này sẽ tìm kiếm tệp có tên "filename" trong thư mục **/path/to/search** và thực hiện tìm kiếm **grep** cho mẫu "pattern" trong mỗi tệp được tìm thấy.

### 2.1.5. Lệnh access\_log

Lệnh này được sử dụng để xem và phân tích tệp log truy cập (access log) của một máy chủ web. Tệp log truy cập ghi lại tất cả các yêu cầu truy cập đến máy chủ web, bao gồm các thông tin như IP nguồn, URL yêu cầu, trạng thái HTTP và thời gian phản hồi. Lệnh access\_log cho phép bạn xem thông tin này và thực hiện các thao tác phân tích như lọc, đếm, xác định các xu hướng và thống kê.

### 2.1.6. XHydra

XHydra là một ứng dụng dùng để thực hiện tấn công mật khẩu theo từ điển (dictionary attack) hoặc tấn công theo mục tiêu (brute-force attack) vào các dịch vụ mạng như SSH (Secure Shell), FTP (File Transfer Protocol), Telnet, SMTP (Simple Mail Transfer Protocol), và nhiều dịch vụ khác.

XHydra là một phần của công cụ mạnh mẽ được gọi là Hydra, một công cụ thử nghiệm xâm nhập (penetration testing tool) phổ biến trong cộng đồng bảo mật. XHydra cung cấp giao diện đồ họa cho việc sử dụng Hydra, giúp người dùng dễ dàng cấu hình và thực hiện các cuộc tấn công mật khẩu mà không cần phải sử dụng dòng lệnh trực tiếp.

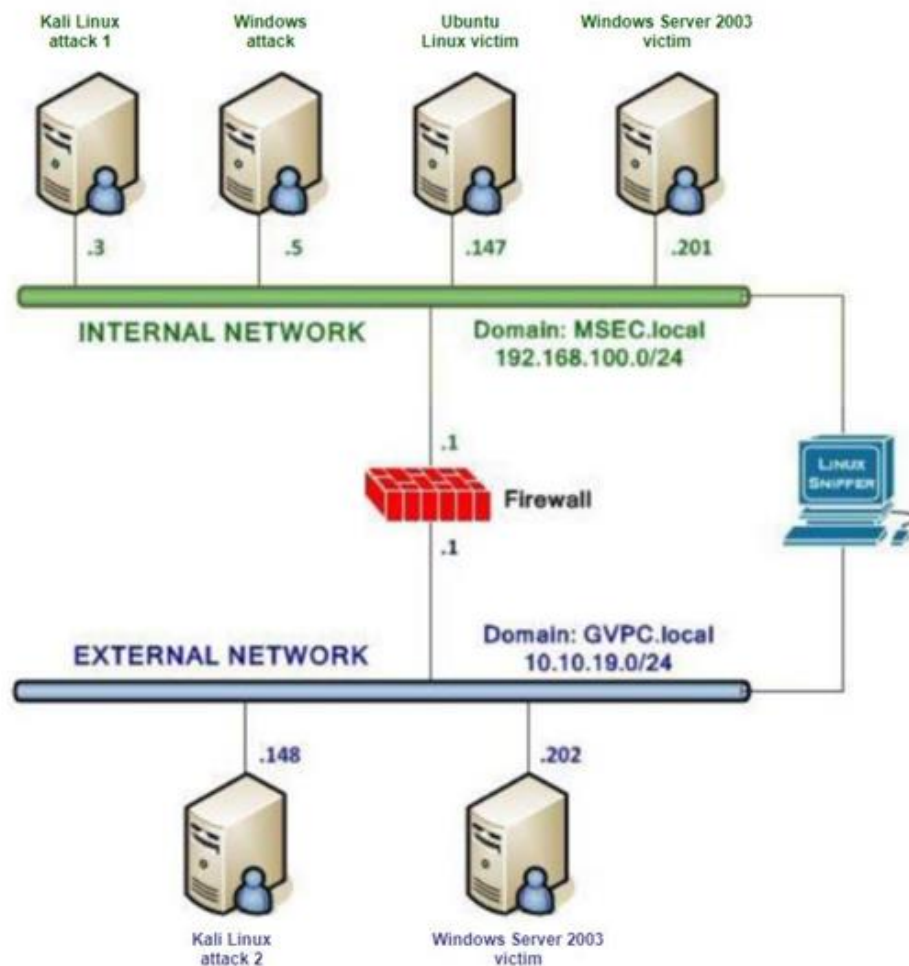
## 2.2. Nội dung thực hành

### 2.2.1. 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 thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- Topo mạng như đã cấu hình trong bài 5.



## Bài 9: Phân tích log hệ thống



Cấu hình topo mạng

### 2.2.2. Phân tích log sử dụng grep trong Linux

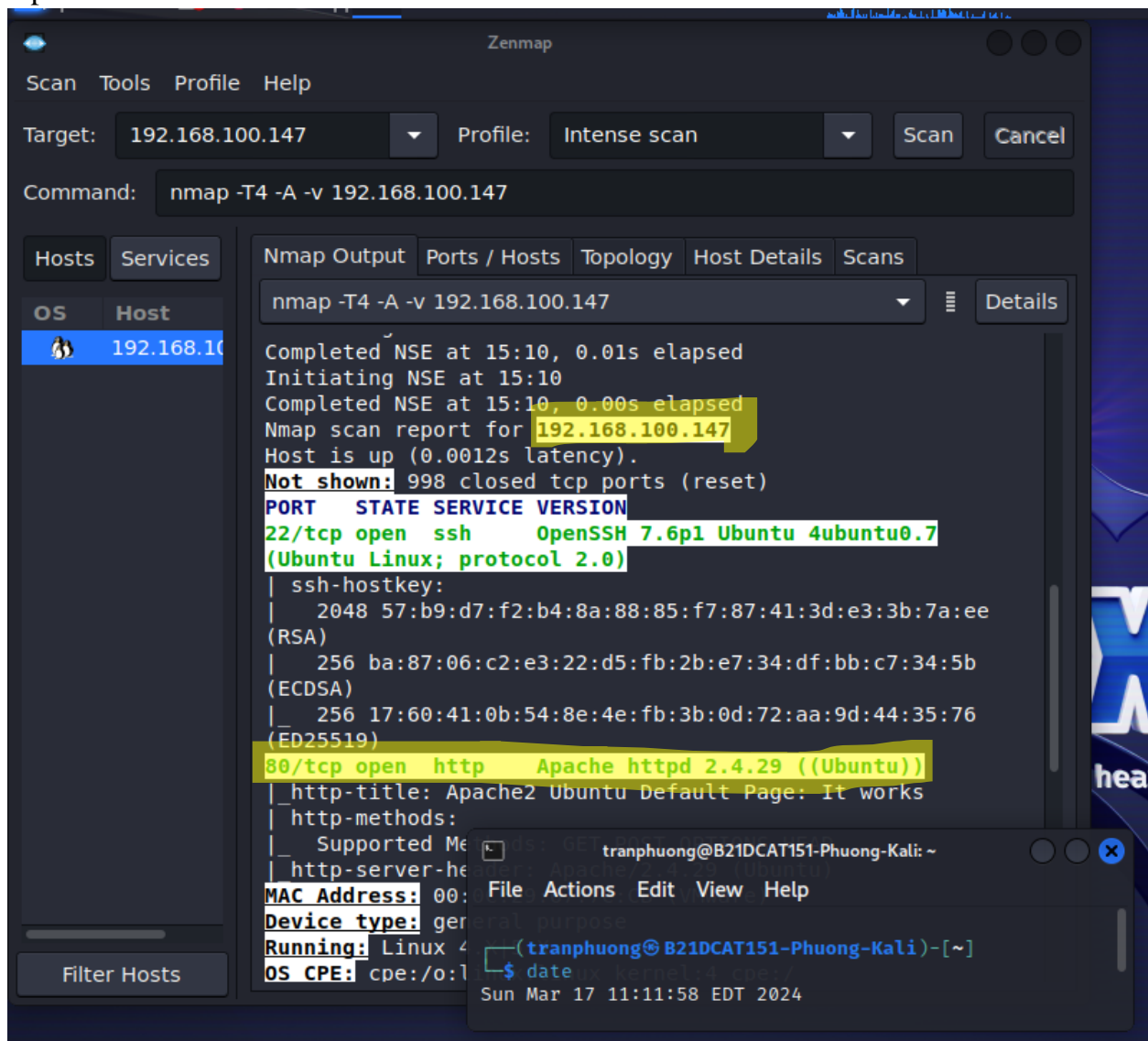
- Đảm bảo máy Ubuntu Internal đã cài đặt dịch vụ apache2

```
tranthithuphuongb21dcat151@slave-1:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: ena
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Sun 2024-03-17 07:39:30 PDT; 2min 35s ago
     Main PID: 3015 (apache2)
       Tasks: 55 (limit: 2281)
    CGroup: /system.slice/apache2.service
            └─3015 /usr/sbin/apache2 -k start
              3016 /usr/sbin/apache2 -k start
              3018 /usr/sbin/apache2 -k start

Mar 17 07:39:30 slave-1 systemd[1]: Starting The Apache HTTP Server...
Mar 17 07:39:30 slave-1 apachectl[3004]: AH00558: apache2: Could not reliably deter
Mar 17 07:39:30 slave-1 systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)
```

## Bài 9: Phân tích log hệ thống

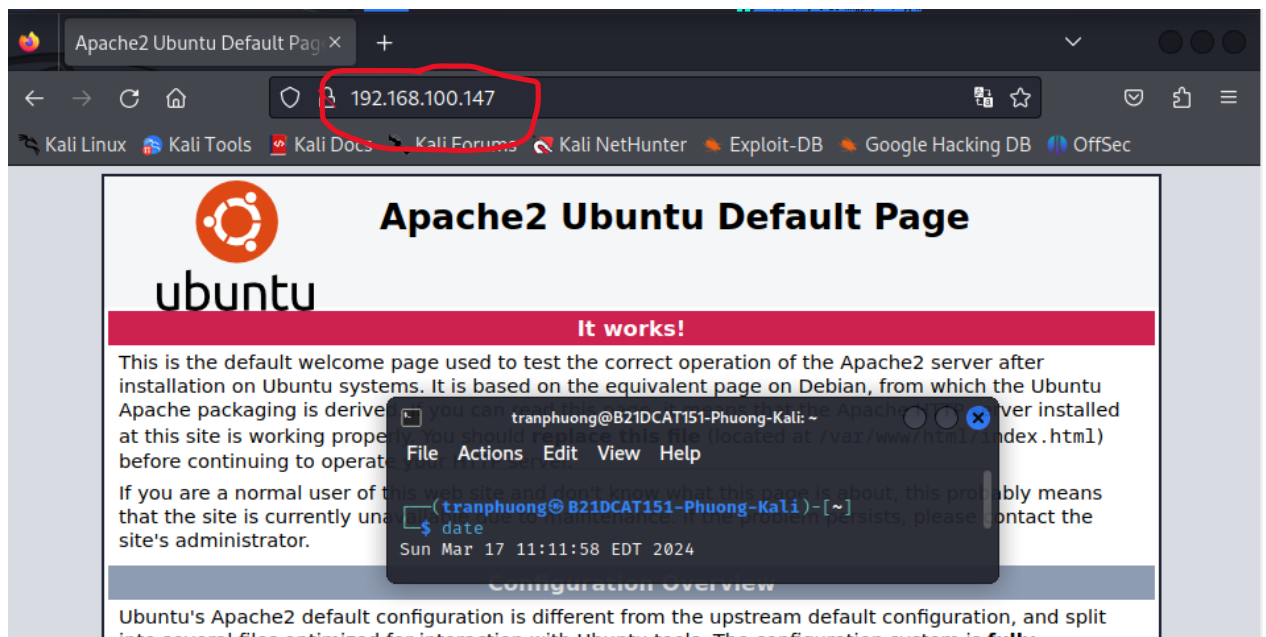
- Trên máy Kali attack trong mạng Internal, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.4.29



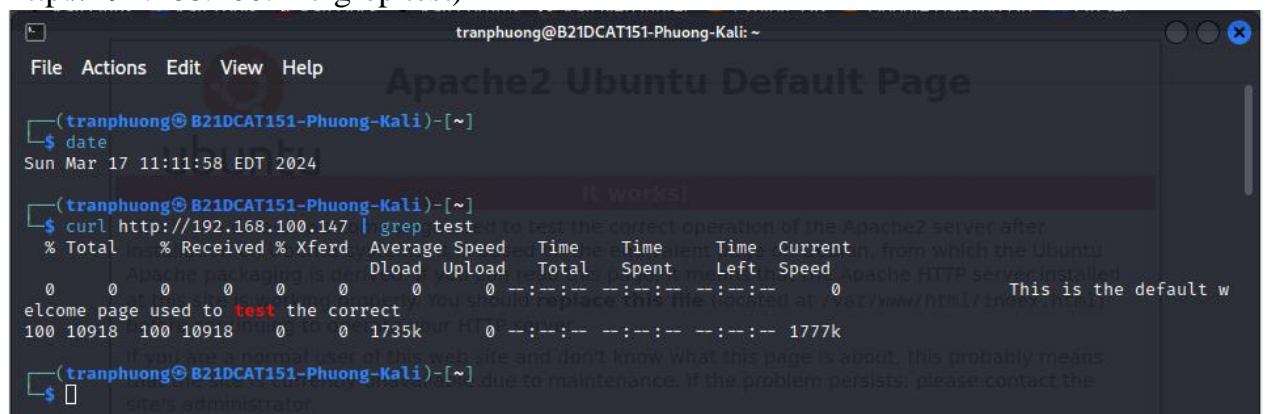
*Xem được port 80 đang mở cho Web Server*

- Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web <http://192.168.100.147>.

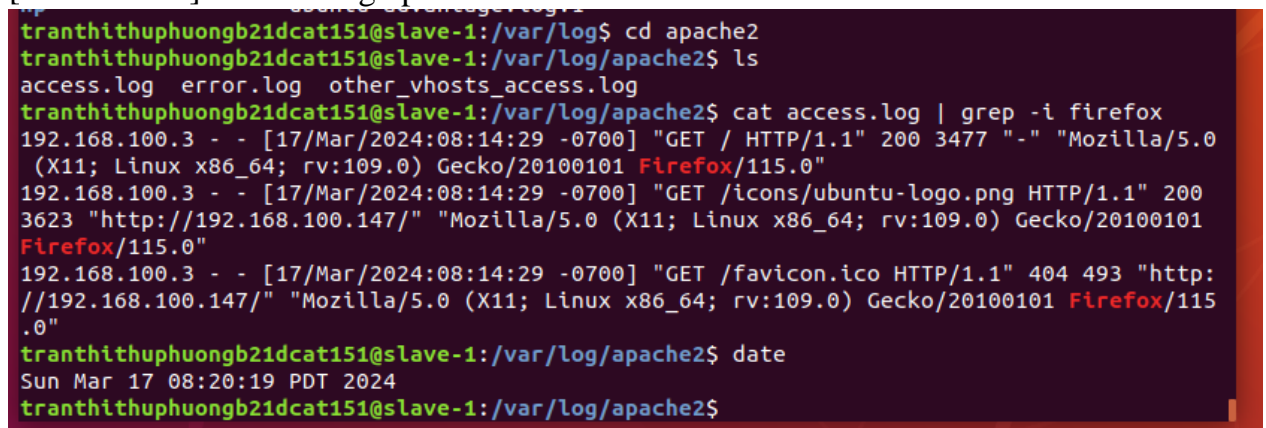
## Bài 9: Phân tích log hệ thống



- 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/apache2



Xem thư mục chứa access\_log

### 2.2.3. Phân tích log sử dụng gawk trong Linux

## Bài 9: Phân tích log hệ thống

- 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.

```
(tranhithuphuong@B21DCAT151-Phuong-Kali)-[~]
$ ssh tranthithuphuongb21dcat151@192.168.100.147
tranthithuphuongb21dcat151@192.168.100.147's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.
6 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

161 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

tranthithuphuongb21dcat151@slave-1:~$
```

*Ssh đến IP 192.168.100.147 bằng user tranthithuphuongb21dcat151*

```
tranthithuphuongb21dcat151@slave-1:~$ sudo useradd phuongttt151
[sudo] password for tranthithuphuongb21dcat151:
tranthithuphuongb21dcat151@slave-1:~$ date
Sun Mar 17 08:27:30 PDT 2024
tranthithuphuongb21dcat151@slave-1:~$ sudo passwd phuongttt151
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
tranthithuphuongb21dcat151@slave-1:~$
```



*Tạo một account mới và đổi mật khẩu cho account này*

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




```
tranthithuphuongb21dcat151@slave-1:/var/log$ journalctl -t sshd | grep "Mar 17 08:"
Mar 17 08:08:25 slave-1 sshd[828]: Received SIGHUP; restarting.
Mar 17 08:08:25 slave-1 sshd[828]: Server listening on 0.0.0.0 port 22.
Mar 17 08:08:25 slave-1 sshd[828]: Server listening on :: port 22.
Mar 17 08:10:11 slave-1 sshd[4458]: Did not receive identification string from 192.168.100.3 port 34580
Mar 17 08:10:18 slave-1 sshd[4459]: Protocol major versions differ for 192.168.100.3 port 39124: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 vs. SSH-1.5-NmapNSE_1.0
Mar 17 08:10:18 slave-1 sshd[4460]: Protocol major versions differ for 192.168.100.3 port 39136: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 vs. SSH-1.5-Nmap-SSH1-Hostkey
Mar 17 08:10:18 slave-1 sshd[4461]: Unable to negotiate with 192.168.100.3 port 39152: no matching host key type found. Their offer: ssh-dss [preauth]
Mar 17 08:10:18 slave-1 sshd[4463]: Connection closed by 192.168.100.3 port 39162 [preauth]
Mar 17 08:10:18 slave-1 sshd[4465]: Connection closed by 192.168.100.3 port 39168 [preauth]
Mar 17 08:10:18 slave-1 sshd[4467]: Unable to negotiate with 192.168.100.3 port 39170: no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
Mar 17 08:10:18 slave-1 sshd[4469]: Unable to negotiate with 192.168.100.3 port 39180: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth]
Mar 17 08:10:18 slave-1 sshd[4471]: Connection closed by 192.168.100.3 port 39188 [preauth]
Mar 17 08:23:28 slave-1 sshd[4511]: pam_unix(sshd:auth): authentication failure; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.3 user=root
Mar 17 08:23:30 slave-1 sshd[4511]: Failed password for root from 192.168.100.3 port 49810 ssh2
Mar 17 08:23:39 slave-1 sshd[4511]: Failed password for root from 192.168.100.3 port 49810 ssh2
Mar 17 08:24:35 slave-1 sshd[4511]: Failed password for root from 192.168.100.3 port 49810 ssh2
Mar 17 08:24:35 slave-1 sshd[4511]: Connection closed by authenticating user root 192.168.100.3 port 49810 [preauth]
Mar 17 08:24:35 slave-1 sshd[4511]: PAM 2 more authentication failures; logname=uid=0 euid=0 tty=ssh ruser= rhost=192.168.100.3 user=root
Mar 17 08:25:00 slave-1 sshd[4518]: Accepted password for tranthithuphuongb21dcat151 from 192.168.100.3 port 47854 ssh2
Mar 17 08:25:00 slave-1 sshd[4518]: pam_unix(sshd:session): session opened for user tranthithuphuongb21dcat151 by (uid=0)
tranthithuphuongb21dcat151@slave-1:/var/log$
```

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

- 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.

```
passwd: password updated successfully
tranthithuphuongb21dcat151@slave-1:~$ cat /var/log/auth.log | grep useradd
Mar 17 08:27:02 slave-1 sudo: tranthithuphuongb21dcat151 : TTY=pts/1 ; PWD=/home/tranthithuphuongb21dcat151 ; USER=root ; COMMAND=/usr/sbin/useradd phuongttt151
Mar 17 08:27:02 slave-1 useradd[4609]: new group: name=phuongttt151, GID=1002
Mar 17 08:27:02 slave-1 useradd[4609]: new user: name=phuongttt151, UID=1002, GID=1002, home=/home/phuongttt151, shell=/bin/sh
tranthithuphuongb21dcat151@slave-1:~$
```



*Sử dụng lệnh grep*

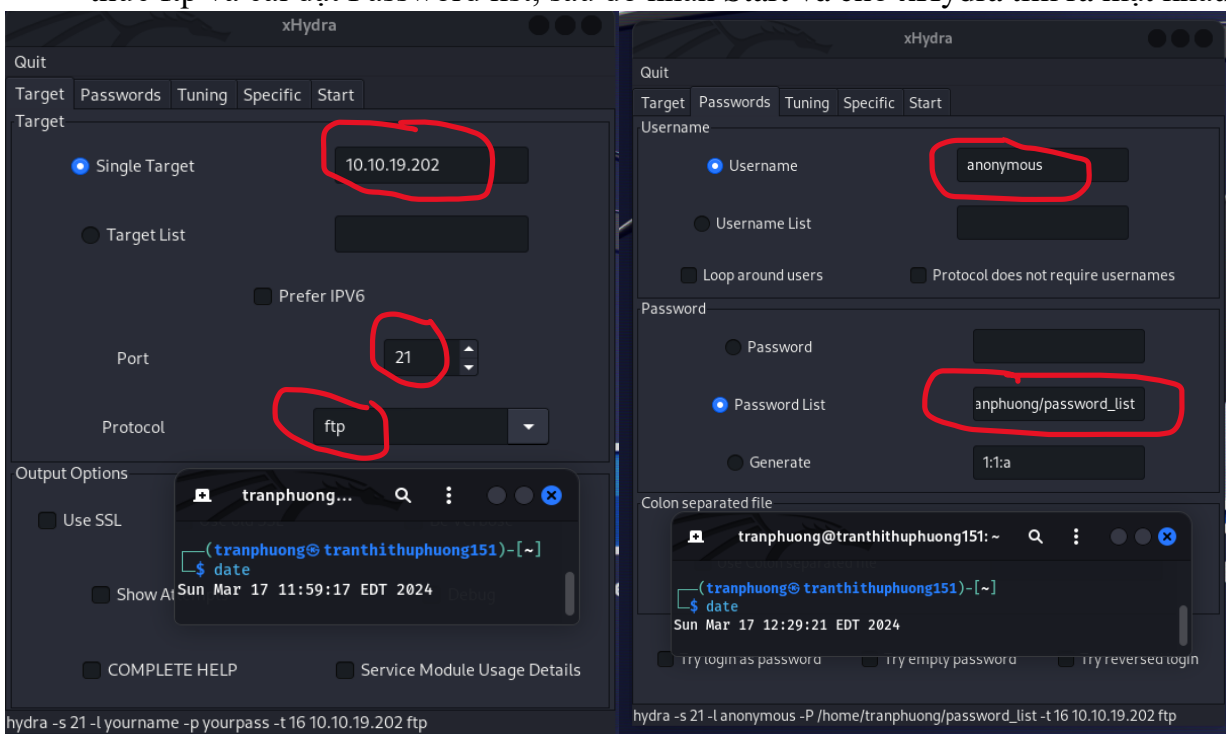
## Bài 9: Phân tích log hệ thống

```
tranthithuphuongb21dcat151@slave-1:~$ gawk '/useradd/ {print}' /var/log/auth.log
Mar 17 08:27:02 slave-1 sudo: tranthithuphuongb21dcat151 : TTY=pts/1 ; PWD=/home/tranthithuphuongb21dcat151 ; USER=
root ; COMMAND=/usr/sbin/useradd phuongttt151
Mar 17 08:27:02 slave-1 useradd[4609]: new group: name=phuongttt151, GID=1002
Mar 17 08:27:02 slave-1 useradd[4609]: new user: name=phuongttt151, UID=1002, GID=1002, home=/home/phuongttt151, sh
ell=/bin/sh
tranthithuphuongb21dcat151@slave-1:~$
```

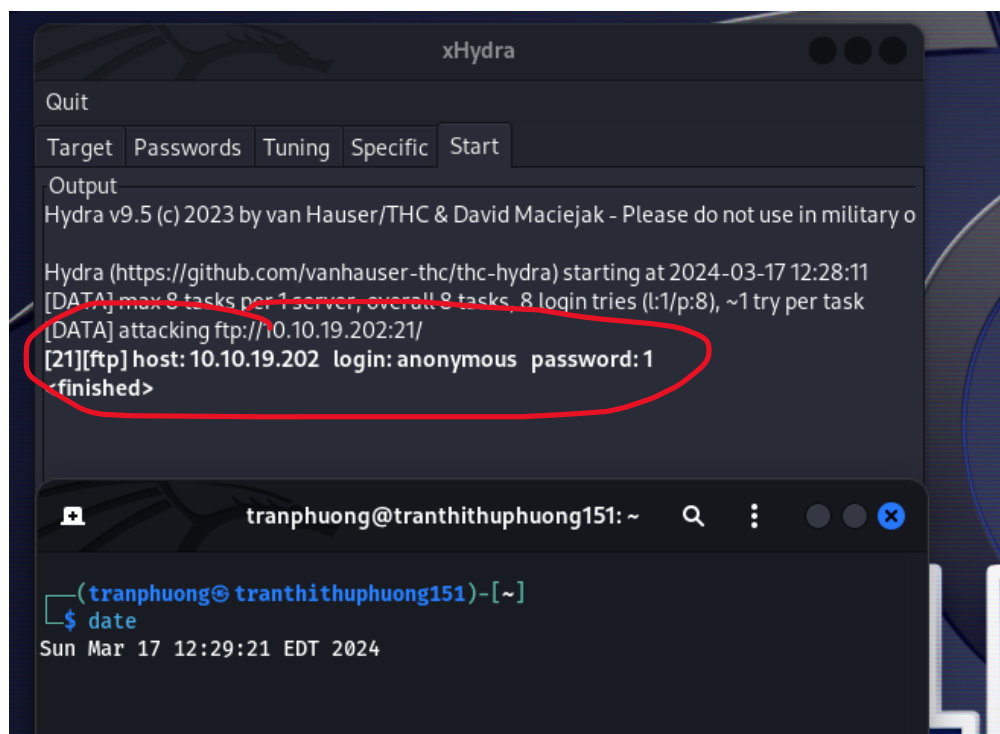
*Sử dụng lệnh gawk*

### 2.2.4. 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

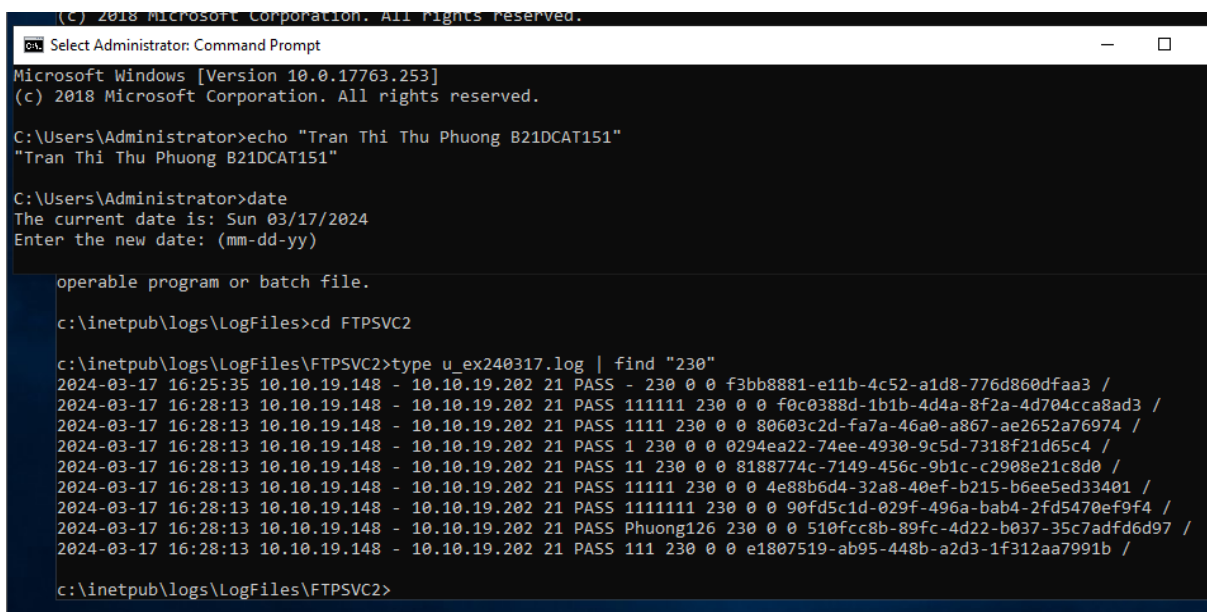


*Khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list*



*Kết quả crack mật khẩu từ xHydra*

- 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")



*Xem file log trên máy Windows victim*

### 3. Kết luận

- Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk, find, secure, access\_log, ...
- Khi đã mở được file access\_log trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm ví dụ: Nmap, Firefox, curl, ...
- Xem được log và tìm được nội dung mong muốn bằng lệnh grep/gawk. In được kết quả mong muốn lên màn hình.
- Lưu được dữ liệu log tấn công mật khẩu và tìm được kết quả tấn công trong file log trên máy victim.

### 4. Tài liệu tham khảo

- [1]. grep: [https://linuxcommand.org/lc3\\_man\\_pages/grep1.html](https://linuxcommand.org/lc3_man_pages/grep1.html)
- [2]. gawk: <http://www.gnu.org/software/gawk/manual/gawk.html>
- [3]. find: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find>
- [4]. xhydra: <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>