

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



BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 1.6
PHÂN TÍCH LOG HỆ THỐNG

Sinh viên thực hiện:

B22DCAT206 PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợt

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

1.	Mục đích.....	3
2.	Nội dung thực hành	3
2.1.	Cơ sở lý thuyết	3
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
2.2.	Nội dung thực hành	7
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
3.	Kết luận	15
4.	Tài liệu tham khảo	15

Danh mục hình ảnh

Hình 1 cài đặt Apache2	12
Hình 2 Xem được port 80 đang mở cho Web Server	13
Hình 3 truy cập từ máy kali	14
Hình 4 tìm kiếm từ khoá test	15
Hình 5 Xem thư mục chứa access_log	16
Hình 7 Ssh đến IP 192.168.100.147 bằng user nam-b22at206	Error! Bookmark not defined.
Hình 8 Trên máy Linux Internal Victim, tiến hành xem file log	18
Hình 9 Sử dụng lệnh grep	19
Hình 10 Sử dụng lệnh gawk	20
Hình 11 Khởi động #hydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list....	21
Hình 12 Kết quả crack mật khẩu từ xHydra.....	21
Hình 13 Xem file log trên máy Windows victim	22

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

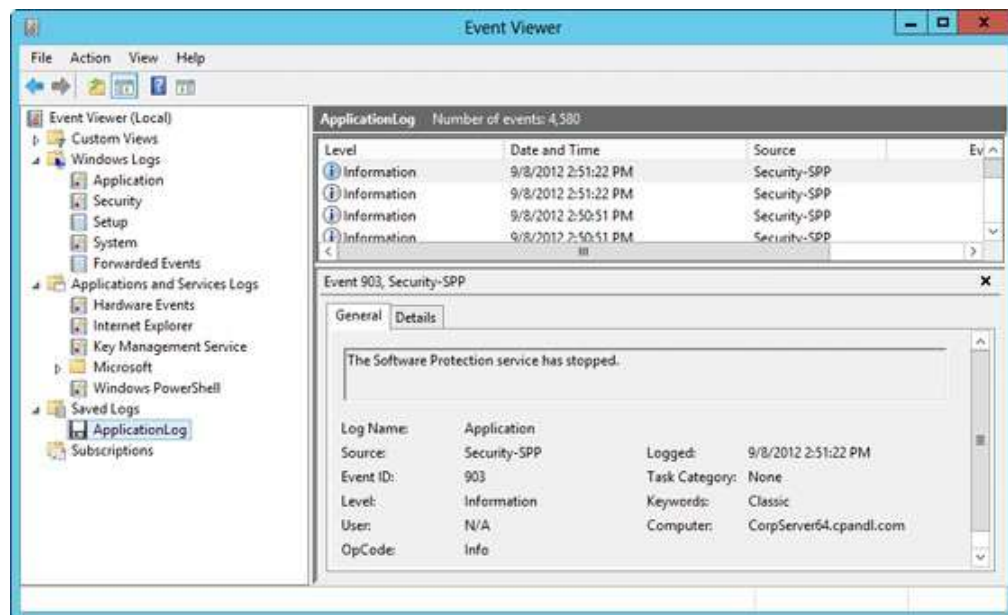
2.1. Cơ sở lý thuyết

2.1.1. Tìm hiểu về Windows Event và Auditing

a. Windows Event

Trong hệ điều hành Windows, một **sự kiện** được định nghĩa là bất kỳ diễn biến quan trọng nào xảy ra trong quá trình vận hành hệ điều hành hoặc các ứng dụng. Những sự kiện này cần được ghi lại để phục vụ mục đích theo dõi và giám sát. Các thông tin được theo dõi bao gồm các cảnh báo, lỗi, hay các sự kiện kiểm toán. Có hai loại tệp nhật ký sự kiện chính:

- Nhật ký Windows: Ghi nhận các sự kiện hệ thống chung liên quan đến ứng dụng, bảo mật, cài đặt và các thành phần hệ thống cốt lõi.
- Nhật ký dịch vụ và ứng dụng: Lưu trữ thông tin về việc sử dụng của một ứng dụng hoặc dịch vụ cụ thể.



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

Để xem các nhật ký sự kiện này, người quản trị sử dụng công cụ **"Event Viewer"** (như minh họa trong hình). Với mỗi sự kiện, chương trình sẽ hiển thị một biểu tượng tương ứng như sau:

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

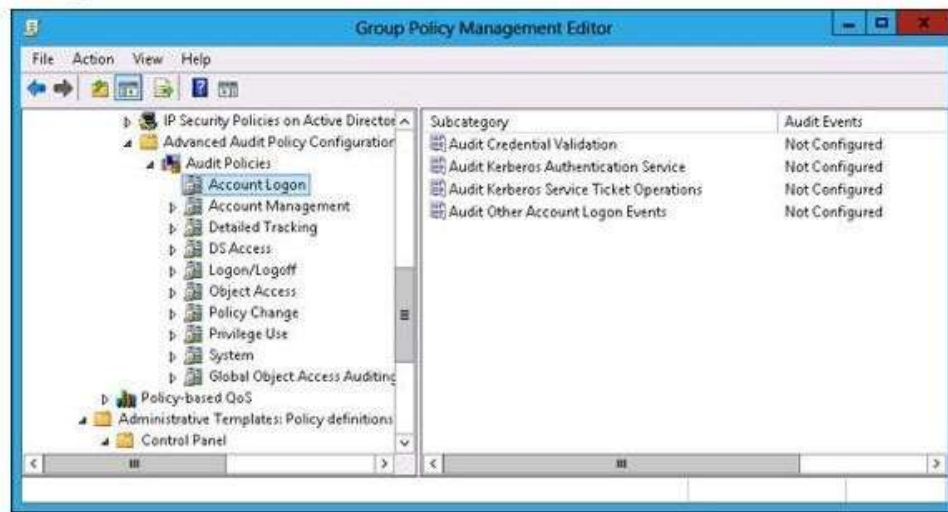
- Cảnh báo: Mô tả một sự kiện không nghiêm trọng nhưng cần được chú ý để ngăn ngừa các vấn đề tiềm ẩn trong tương lai.
- Lỗi: Cho biết một lỗi hoặc vấn đề không nghiêm trọng đã xảy ra.
- Nghiêm trọng: Thể hiện một lỗi nghiêm trọng hoặc một vấn đề rất đáng kể đã phát sinh.
- Kiểm toán thành công: Mô tả một sự kiện kiểm toán an ninh đã diễn ra thành công theo yêu cầu.
- Kiểm toán thất bại: Mô tả một sự kiện kiểm toán an ninh đã không thành công theo yêu cầu.

b. Auditing

Kiểm toán (Auditing) cho phép người quản trị theo dõi cả các truy cập thực tế lẫn các nỗ lực truy cập hoặc sửa đổi đối với các đối tượng và chính sách của hệ thống. Các đối tượng này có thể là thư mục, tệp tin, cũng như các đối tượng bảo mật của hệ thống. Các chính sách kiểm toán đóng vai trò quan trọng trong việc đảm bảo an toàn cho hệ thống, giám sát các thay đổi đối với dữ liệu nhạy cảm hoặc các tài khoản cần được lưu ý đặc biệt.

Có hai nhóm chính sách kiểm toán chính trong một đối tượng Chính sách Nhóm (Group Policy Object - GPO): **chính sách kiểm toán truyền thống** và **chính sách kiểm toán nâng cao**.

Chính sách kiểm toán truyền thống đã tồn tại từ phiên bản Windows Server 2000. Nhược điểm của chúng là không đủ cụ thể và khó cấu hình. Chính sách kiểm toán nâng cao đã khắc phục những hạn chế này, cung cấp 10 nhóm cài đặt với 58 chính sách kiểm toán riêng lẻ, mang lại khả năng kiểm soát chi tiết hơn.



Hình 4-7. Chính sách kiểm toán nâng cao

Các nhóm chính sách tiêu biểu bao gồm:

- Đăng nhập: Theo dõi quá trình xác thực thông tin đăng nhập của người dùng.
- Quản lý tài khoản: Giám sát các thao tác thay đổi liên quan đến tài khoản người dùng, máy tính,...
- Theo dõi chi tiết: Ghi nhận các hoạt động như chạy chương trình, các lời gọi hàm từ xa.

- Truy nhập thư mục động : Theo dõi việc truy cập hoặc các chức năng liên quan đến thư mục động.
- Truy nhập đối tượng : Giám sát việc truy cập các tệp tin, thư mục hoặc ứng dụng cụ thể.

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 cụ thể trong một hoặc nhiều tệp tin được chỉ định. Lệnh này đặc biệt hữu ích khi cần tìm kiếm thông tin trong các tệp nhật ký (log file) có kích thước 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 mà bạn muốn tìm, có thể là một chuỗi văn bản đơn giản hoặc một biểu thức chính quy phức tạp.
- **[tệp...]:** Các tệp mà bạn muốn thực hiện tìm kiếm trong đó. Nếu không chỉ định, grep sẽ đọc dữ liệu từ đầu vào tiêu chuẩn (stdin).

Một số các cách sử dụng lệnh GREP

- Tìm kiếm một chuỗi ký tự trong một tệp 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 ‘a’ 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 dùng để **xử lý và phân tích dữ liệu văn bản**, đặc biệt là dữ liệu dạng bảng, các dòng đơn giản

có thể được chia thành các cột như CSV (Comma-Separated Values) hoặc TSV (Tab-Separated Values).

Một số cách sử dụng tiêu biểu của **gawk**:

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

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

Lệnh này sẽ hiển thị nội dung của cột đầu tiên trong mỗi dòng của tệp "file.csv".

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

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

Đây là ví dụ về cách tính tổng tất cả các giá trị trong cột thứ hai của tệp "file.csv" và hiển thị 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 "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 giá trị của cột thứ ba lớn hơn 100.

2.1.4. Lệnh find

Lệnh **find** là một công cụ mạnh mẽ để tìm kiếm tệp tin và thư mục trong hệ thống Linux. Nó cho phép người dùng tìm kiếm dựa trên nhiều tiêu chí khác nhau như tên tệp, kích thước tệp, thời gian tạo hoặc sửa đổi, quyền truy cập, v.v.

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

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

Một số cách sử dụng thông dụng của lệnh find:

- 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 (ví dụ: tệp tin thông thường):

find /path/to/search -type f

- Lệnh này sẽ tìm kiếm tất cả các tệp tin thông thường (f) 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 (ví dụ: tệp được sửa đổi trong 7 ngày qua):

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 **/path/to/search**.

- Tìm kiếm đệ quy trong tất cả các thư mục con và thực hiện grep:

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

Lệnh này sẽ tìm 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.

- Tìm kiếm và thực hiện các hành động khác trên kết quả tìm thấy

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 tìm thấy.

2.1.5. Lệnh access_log

Lệnh **access_log** được dùng để xem và phân tích tệp nhật ký truy cập (access log) của một máy chủ web. Tệp nhật ký truy cập này ghi lại mọi yêu cầu truy cập đến máy chủ web, bao gồm các thông tin như địa chỉ IP nguồn, URL được yêu cầu, mã trạng thái HTTP và thời gian phản hồi. Lệnh access_log cho phép người dùng xem thông tin này và thực hiện các thao tác phân tích như lọc, đếm, xác định các xu hướng và thống kê về lượt truy cập

2.1.6. Xhydra

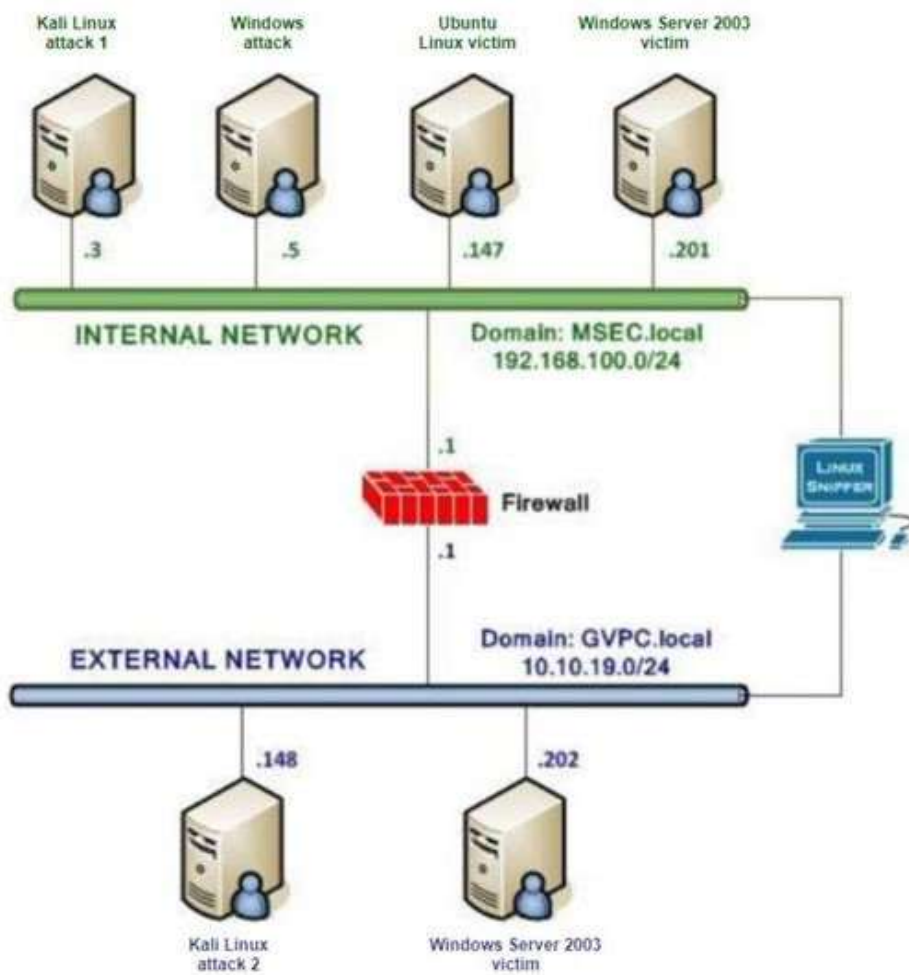
XHydra là một ứng dụng được thiết kế để thực hiện các cuộc tấn công mật khẩu, bao gồm tấn công theo từ điển (dictionary attack) hoặc tấn công vét cạn (brute-force attack), nhằm vào nhiều dịch vụ mạng khác nhau như SSH (Secure Shell), FTP (File Transfer Protocol), Telnet, SMTP (Simple Mail Transfer Protocol), và nhiều dịch vụ khác.

XHydra là một phần của công cụ mạnh mẽ được biết đến với tên gọi **Hydra**, một công cụ kiểm thử xâm nhập (penetration testing tool) rất phổ biến trong cộng đồng bảo mật. XHydra cung cấp **giao diện đồ họa (GUI)** 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 tương tác trực tiếp với dòng lệnh.

2.2. Nội dung thực hành

2.2.1. Chuẩn bị môi trường

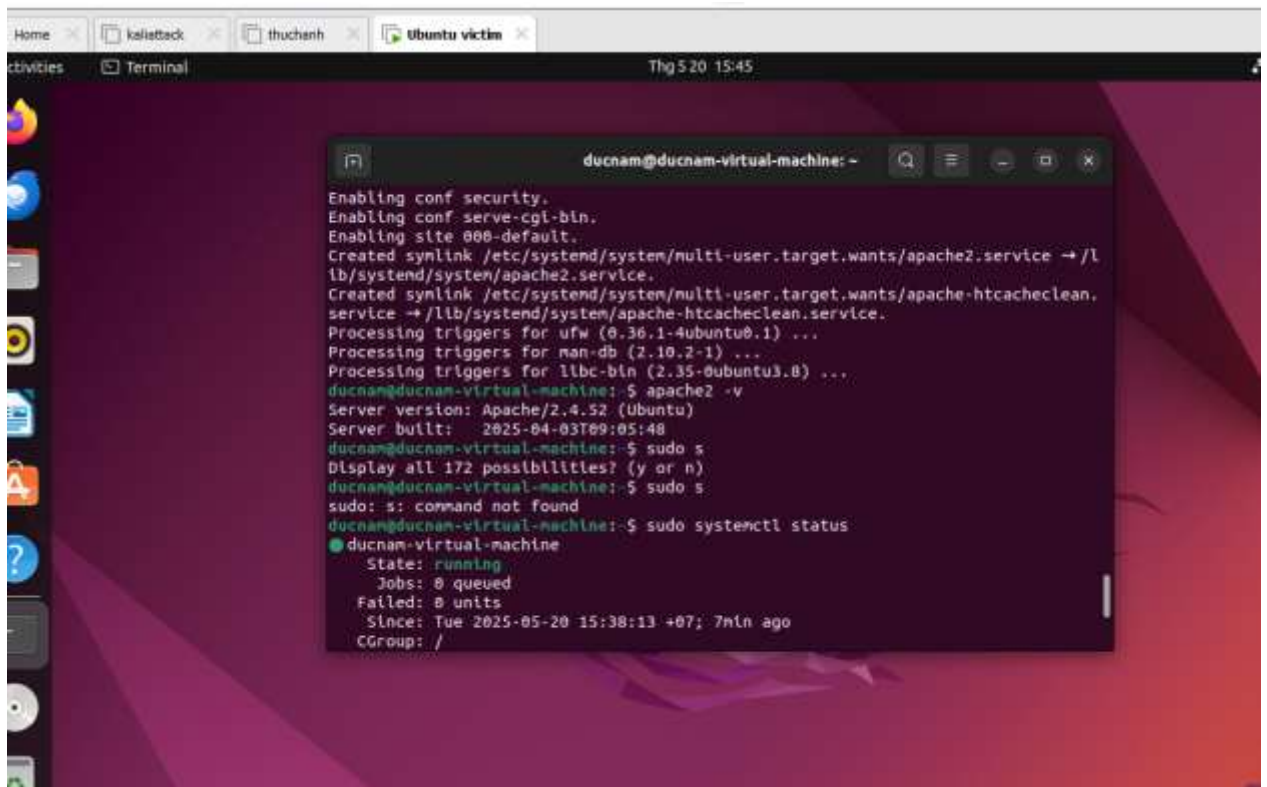
- Phần mềm VMWare Workstation(hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- Topo mạng như đã cấu hình trong bài 5.



Cấu hình topo mạng

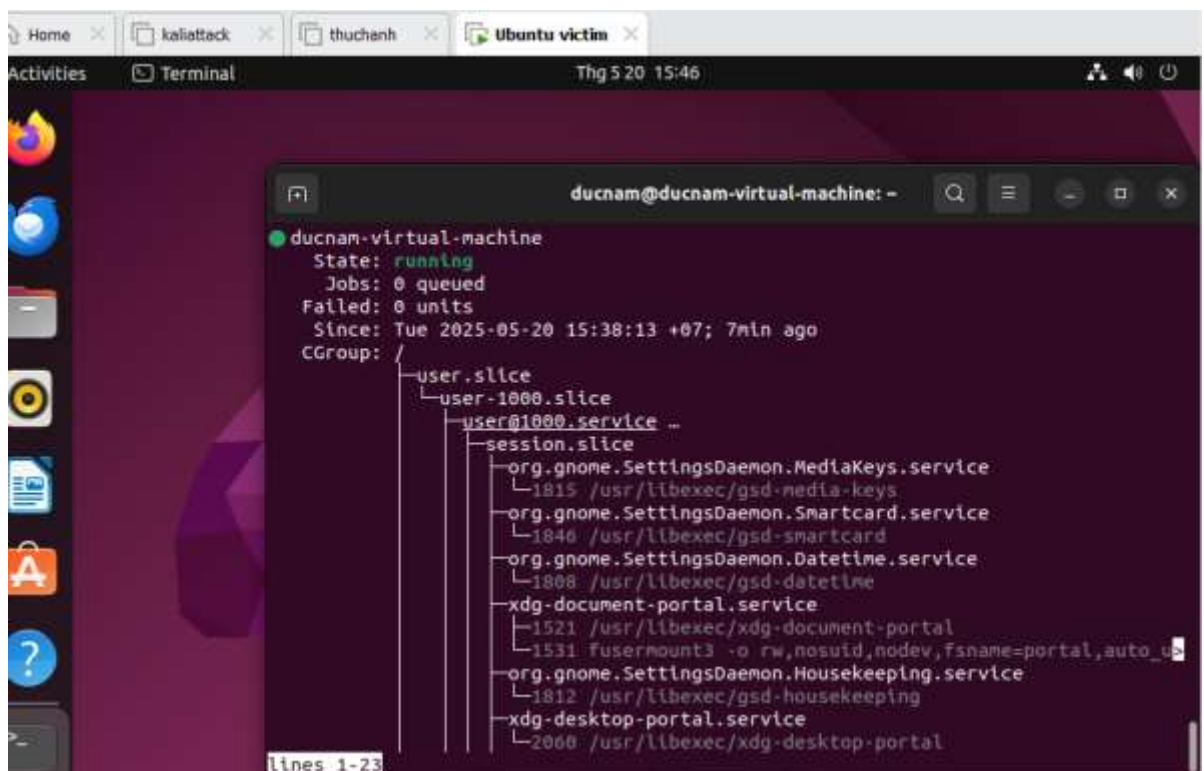
2.2.2. Phân tích log sử dụng grep trong Linux

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



The terminal window shows the process of enabling and starting the Apache2 service. It includes commands for enabling security, CGI-bin, and the default site, creating symlinks, and processing triggers. The user then checks the version of Apache2 and attempts to run it as a daemon. Finally, they use systemctl to start the service and check its status, which shows it is running.

```
ducnam@ducnam-virtual-machine: ~  
Enabling conf security.  
Enabling conf: serve-cgi-bin.  
Enabling site 000-default.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.  
Processing triggers for ufw (0.36.1-4ubuntu0.1) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.8) ...  
ducnam@ducnam-virtual-machine:~$ apache2 -v  
Server version: Apache/2.4.52 (Ubuntu)  
Server built: 2025-04-03T09:05:48  
ducnam@ducnam-virtual-machine:~$ sudo s  
Display all 172 possibilities? (y or n)  
ducnam@ducnam-virtual-machine:~$ sudo s  
sudo: s: command not found  
ducnam@ducnam-virtual-machine:~$ sudo systemctl status  
● ducnam-virtual-machine  
   State: running  
     Jobs: 0 queued  
  Failed: 0 units  
   Since: Tue 2025-05-20 15:38:13 +07; 7min ago  
   CGroup: /
```

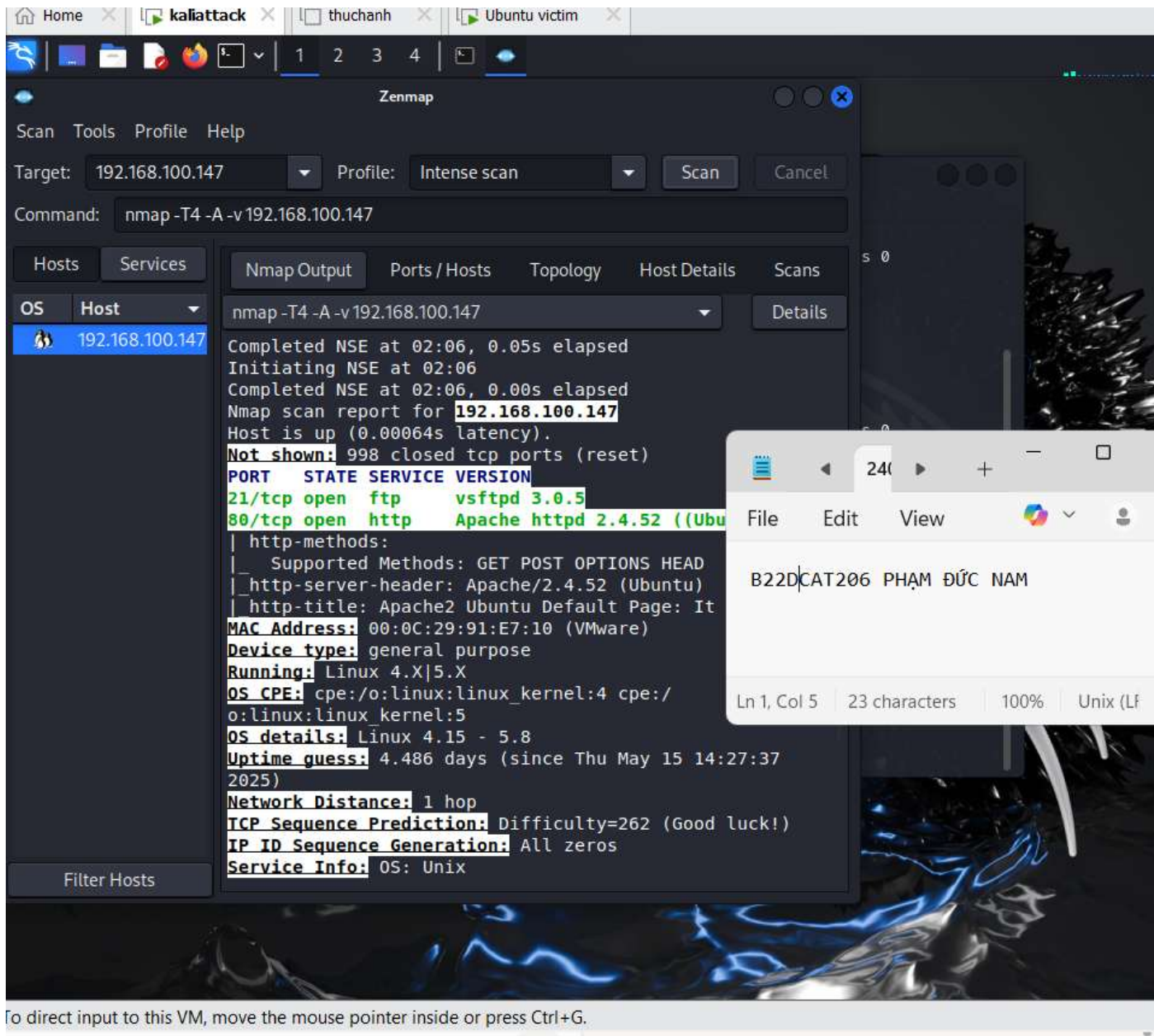


The terminal window shows the detailed status of the Apache2 service. It lists the state as running, with 0 jobs queued and 0 failed units. It also shows the service's CGroup structure, including user.slice, user-1000.slice, and user@1000.service. The service is associated with several other system slices and services, such as org.gnome.SettingsDaemon.MediaKeys.service, org.gnome.SettingsDaemon.Smartcard.service, org.gnome.SettingsDaemon.Datetime.service, xdg-document-portal.service, org.gnome.SettingsDaemon.Housekeeping.service, and xdg-desktop-portal.service.

```
ducnam@ducnam-virtual-machine: ~  
● ducnam-virtual-machine  
   State: running  
     Jobs: 0 queued  
  Failed: 0 units  
   Since: Tue 2025-05-20 15:38:13 +07; 7min ago  
   CGroup: /  
           └─ user.slice  
                └─ user-1000.slice  
                     └─ user@1000.service ...  
                          └─ session.slice  
                               └─ org.gnome.SettingsDaemon.MediaKeys.service  
                                    └─ 1815 /usr/libexec/gsd-media-keys  
                                         └─ org.gnome.SettingsDaemon.Smartcard.service  
                                              └─ 1846 /usr/libexec/gsd-smartcard  
                                                   └─ org.gnome.SettingsDaemon.Datetime.service  
                                                          └─ 1868 /usr/libexec/gsd-datetime  
                                                                └─ xdg-document-portal.service  
                                                                      └─ 1521 /usr/libexec/xdg-document-portal  
                                                                           └─ 1531 fusermount3 -o rw,nosuid,nodev,fsname=portal,auto_...  
                                                                                └─ org.gnome.SettingsDaemon.Housekeeping.service  
                                                                                     └─ 1812 /usr/libexec/gsd-housekeeping  
                                                                                          └─ xdg-desktop-portal.service  
                                                                                               └─ 2060 /usr/libexec/xdg-desktop-portal
```

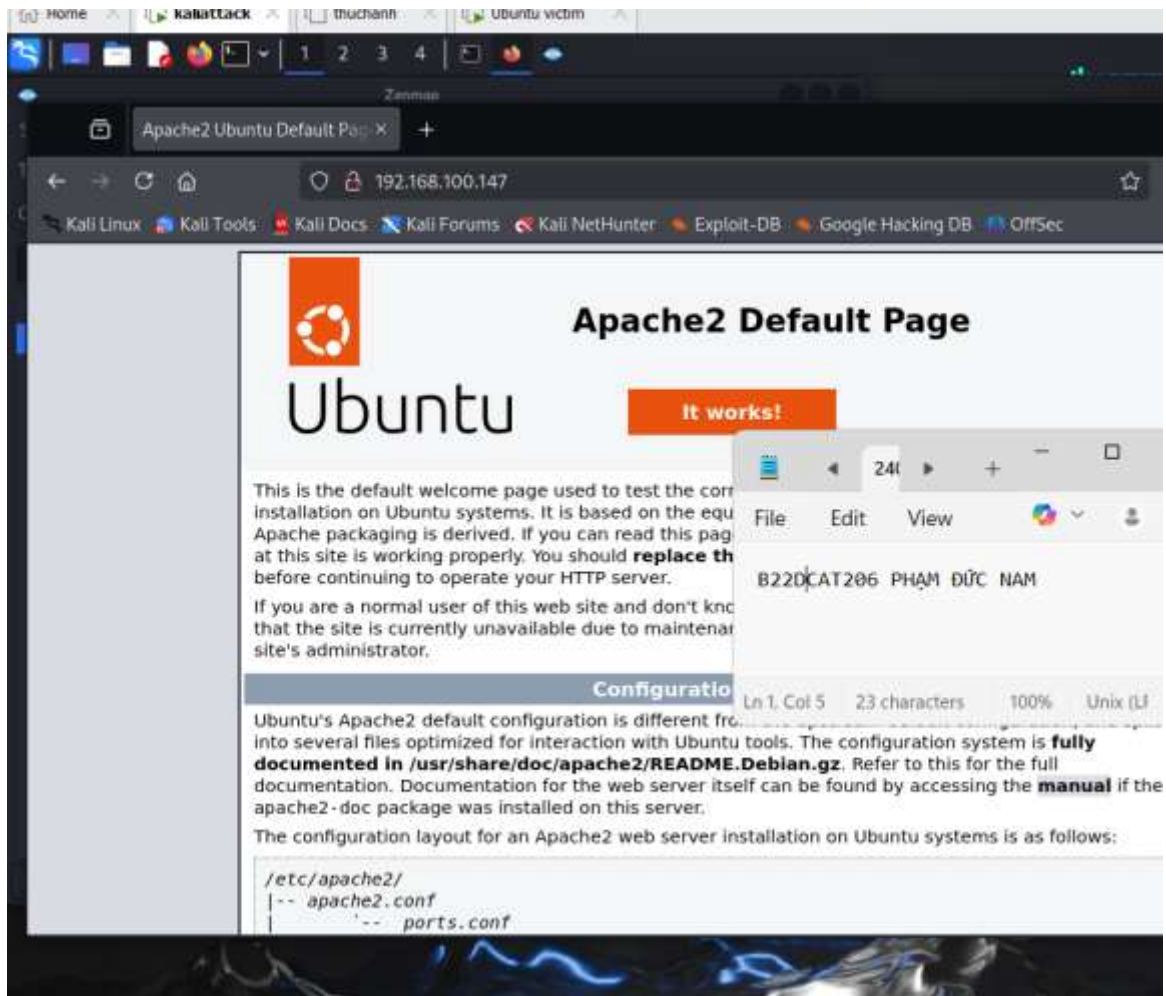
Hình 1 cài đặt Apache2

- 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



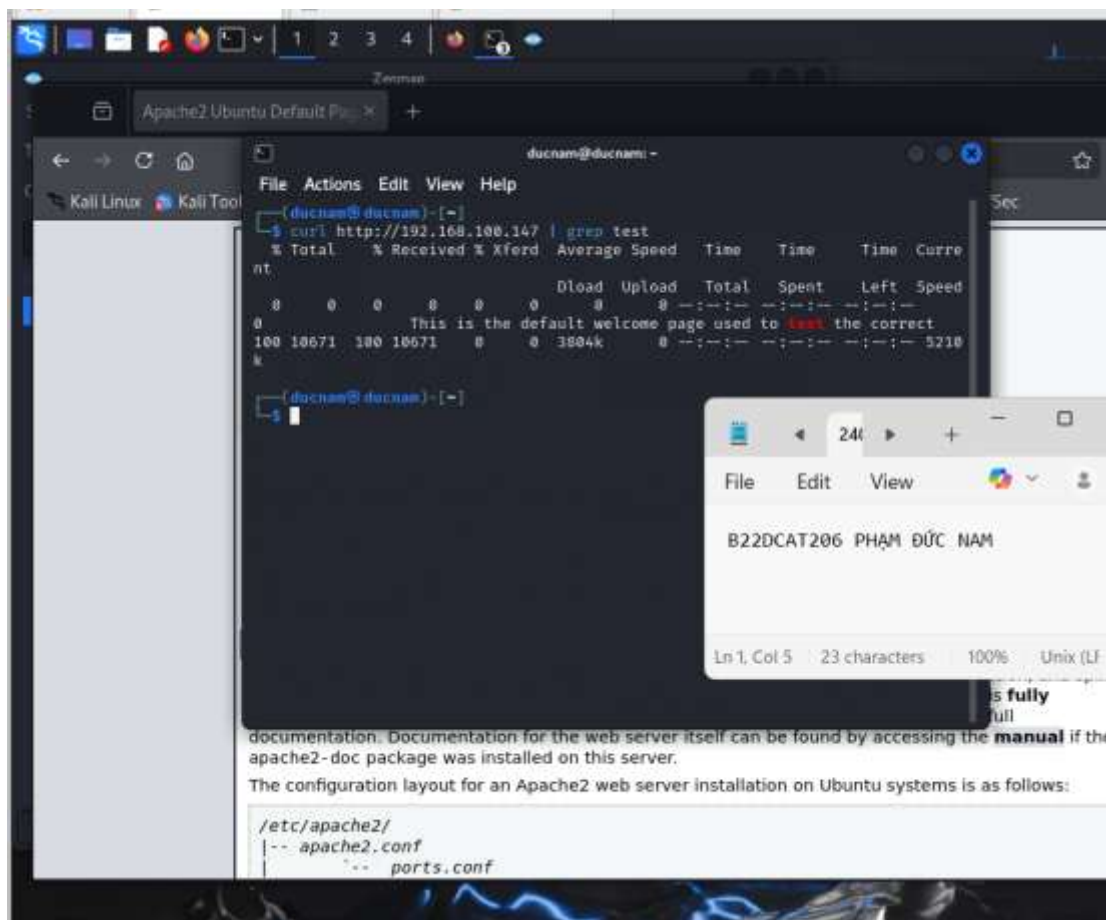
Hình 2 Xem được port 80 đang mở cho Web Server

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



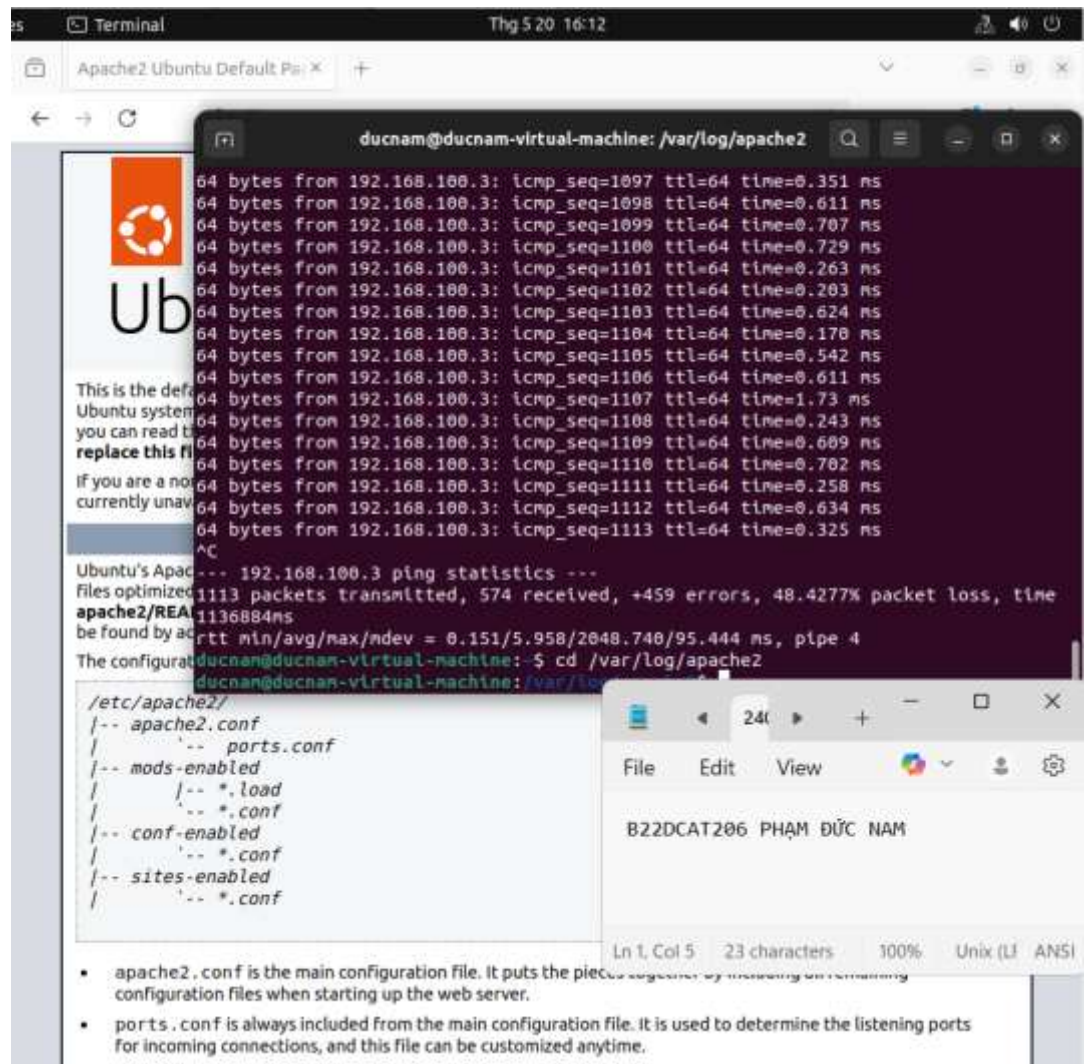
Hình 3 truy cập từ máy kali

- Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test” curl
http://192.168.100.147 | grep test)



Hình 4 tìm kiếm từ khoá test

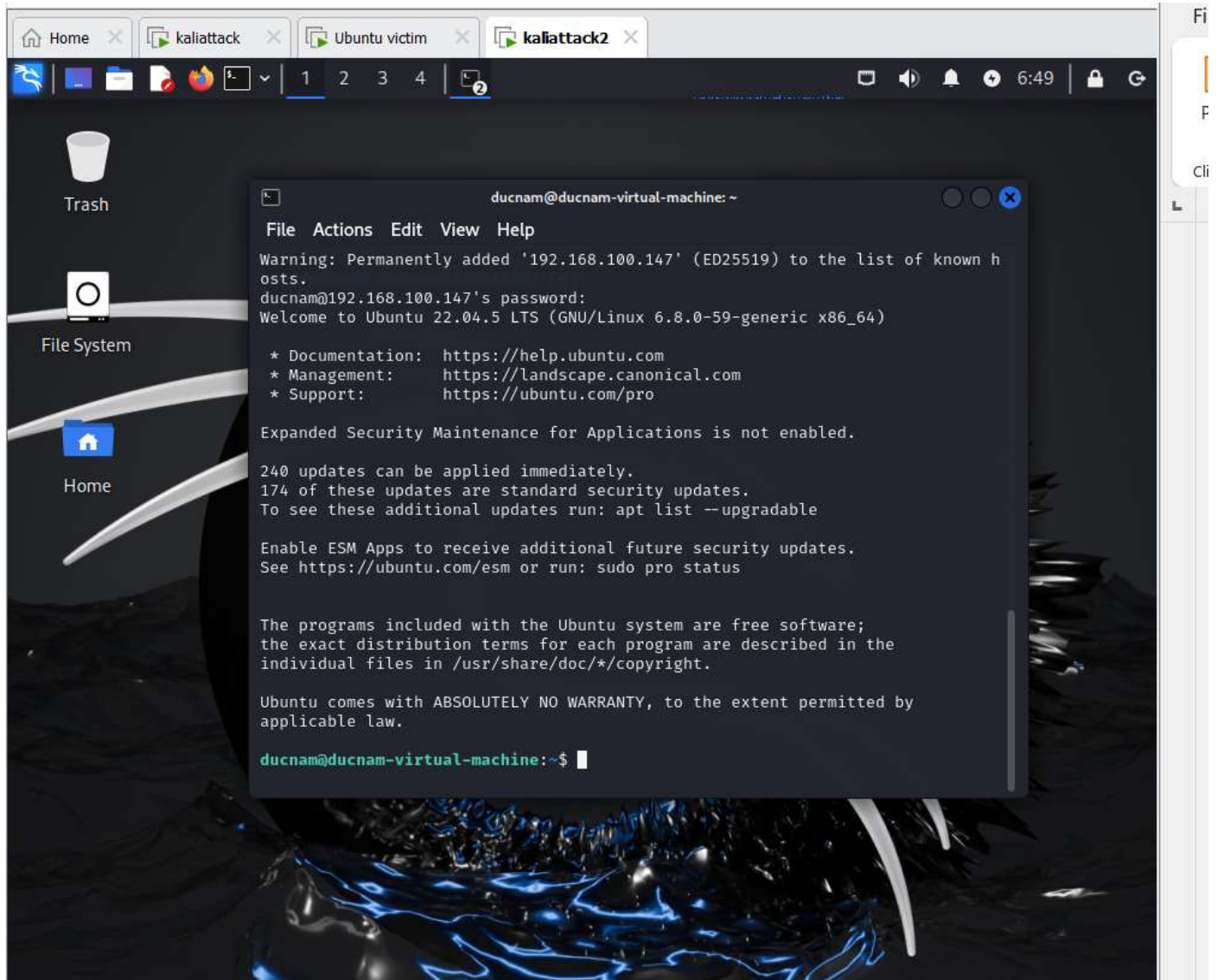
- Trên máy Linux Internal Victim, để xem thư mục chứa access_log dùng lệnh: `cd /var/log/apache2`



Hình 5 Xem thư mục chứa access_log

2.2.3. 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.



Hình 6 Ssh đến IP 192.168.100.147 bằng user nam-b22at206

```
ducnam@ducnam-virtual-machine:~$ sudo useradd nampd206
[sudo] password for ducnam:
ducnam@ducnam-virtual-machine:~$ sudo passwd nampd206
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: password updated successfully
ducnam@ducnam-virtual-machine:~$
```

Tạo một account mới và đổi mật khẩu cho account này

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

```
May 20 16:24:40 ducnam-virtual-machine pkexec[9101]: ducnam: Executing command [USER=root] [TTY=unknown] [CWD=/home/ducnam] [COMMAND=/usr/lib/update-notifier/package-system-locked]
May 20 16:24:42 ducnam-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
May 20 16:24:50 ducnam-virtual-machine sudo: ducnam : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/sbin/netplan apply
May 20 16:24:50 ducnam-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
May 20 16:24:52 ducnam-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
May 20 16:30:01 ducnam-virtual-machine CRON[9276]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May 20 16:30:01 ducnam-virtual-machine CRON[9276]: pam_unix(cron:session): session closed for user root
May 20 20:16:59 ducnam-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
May 20 20:17:01 ducnam-virtual-machine CRON[9443]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
May 20 20:17:01 ducnam-virtual-machine CRON[9443]: pam_unix(cron:session): session closed for user root
May 20 20:17:04 ducnam-virtual-machine sshd[9465]: Accepted password for ducnam from 192.168.100.3 port 46292 ssh2
May 20 20:17:04 ducnam-virtual-machine sshd[9465]: pam_unix(sshd:session): session opened for user ducnam(uid=1000) by (uid=0)
May 20 20:17:04 ducnam-virtual-machine systemd-logind[835]: New session 7 of user ducnam.
May 20 20:17:09 ducnam-virtual-machine sudo: ducnam : TTY=pts/1 ; PWD=/home/ducnam ; USER=root ; COMMAND=/usr/sbin/useradd nampd206
May 20 20:17:09 ducnam-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ducnam(uid=1000)
May 20 20:17:09 ducnam-virtual-machine useradd[9551]: new group: name=nampd206, GID=1001
May 20 20:17:09 ducnam-virtual-machine useradd[9551]: new user: name=nampd206, UID=1001, GID=1001, home=/home/nampd206, shell=/bin/sh, from=/dev/pts/2
May 20 20:17:09 ducnam-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
May 20 20:17:10 ducnam-virtual-machine sudo: ducnam : TTY=pts/1 ; PWD=/home/ducnam ; USER=root ; COMMAND=/usr/bin/passwd nampd206
May 20 20:17:10 ducnam-virtual-machine sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ducnam(uid=1000)
May 20 20:17:10 ducnam-virtual-machine passwd[9562]: pam_unix(passwd:chauthtok): password changed for nampd206
May 20 20:17:10 ducnam-virtual-machine passwd[9562]: gkr-pam: couldn't update the login keyring password: no old password was entered
May 20 20:17:10 ducnam-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
ducnam@ducnam-virtual-machine: /var/log$
```

Hình 6 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.

```
ducnam@ducnam-virtual-machine:~$ grep nampd206 /var/log/auth.log
May 20 20:17:09 ducnam-virtual-machine sudo: ducnam : TTY=pts/1 ; PWD=/home/ducnam ; USER=root ; COMMAND=/usr/sbin/useradd nampd206
May 20 20:17:09 ducnam-virtual-machine useradd[9551]: new group: name=nampd206, GID=1001
May 20 20:17:09 ducnam-virtual-machine useradd[9551]: new user: name=nampd206, UID=1001, GID=1001, home=/home/nampd206, shell=/bin/sh, from=/dev/pts/2
May 20 20:17:10 ducnam-virtual-machine sudo: ducnam : TTY=pts/1 ; PWD=/home/ducnam ; USER=root ; COMMAND=/usr/bin/passwd nampd206
May 20 20:17:10 ducnam-virtual-machine passwd[9562]: pam_unix(passwd:chauthtok): password changed for nampd206
ducnam@ducnam-virtual-machine:~$
```

Hình 7 Sử dụng lệnh grep

```

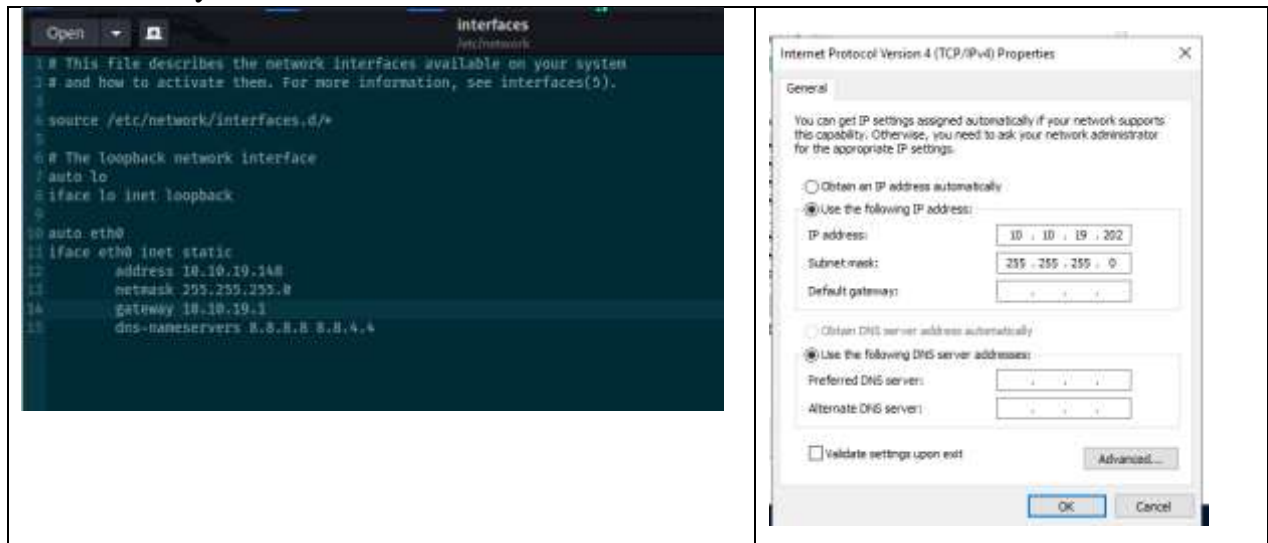
0% [Working]^C
ducnam@ducnam-virtual-machine:/var/log$ gawk '/useradd/ {print}' auth.log^C
ducnam@ducnam-virtual-machine:/var/log$ sudo cat /var/log/auth.log | grep "new user" | grep "nam
pd206" | awk '{print}'
May 20 20:17:09 ducnam-virtual-machine useradd[9551]: new user: name=nampd206, UID=1001, GID=100
1, home=/home/nampd206, shell=/bin/sh, from=/dev/pts/2
ducnam@ducnam-virtual-machine:/var/log$

```

Hình 8 Sử dụng lệnh gawk

2.2.4. Phân tích log sử dụng find trong Windows

- Cấu hình lại IP cho máy kali và Windows Server 2019



- Tạo 1 site mới trong IIS Manager (IP: 10.10.19.202)
- 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

```

Example: hydra -t user -P passlist.txt ftp://192.168.0.1

Welcome to the Hydra Wizard

Enter the service to attack (eg: ftp, ssh, http-post-form): ftp
Enter the target to attack (or filename with targets): 10.10.19.202
Enter a username to test or a filename: administrator
Enter a password to test or a filename: passlist.txt
If you want to test for passwords (s)ame as login, (n)ull or (r)everse login,
  enter these letters without spaces (e.g. "sr") or leave empty otherwise:
Port number (press enter for default): 21

The following options are supported by the service module:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
  military or secret service organizations, or for illegal purposes (this is n
  on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-20 07:
30:46

Help for module ftp:
=====
The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

```

Hình 9 Khởi động #hydra, chọn target là 10.10.19.202, giao thức ftp và cài đặt Password list

```

Help for module ftp:
=====
The Module ftp does not need or support optional parameters

If you want to add module options, enter them here (or leave empty):

The following command will be executed now:
hydra -l administrator -P passlist.txt -u -s 21 10.10.19.202 ftp

Do you want to run the command now? [Y/n] y

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
  military or secret service organizations, or for illegal purposes (this is n
  on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-20 07:
31:24
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), -1
  try per task
[DATA] attacking ftp://10.10.19.202:21/
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-20 07:
31:29
ducmae@ducmae22lcat206:~$

```

Hình 10 Kết quả crack mật khẩu từ xHydra

- Trên máy Windows 2019 Server External Victim, thực hiện điều hướng đến FTP Logfile. 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:\inetpub\logs\LogFiles\FTPSVC2>type exyymmdd.log | find "230")

```
C:\inetpub\logs>cd LogFiles
C:\inetpub\logs\LogFiles>cd FTPSVC2
C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex240317.log | find "230"
The system cannot find the file specified.
C:\inetpub\logs\LogFiles\FTPSVC2>cd ..
C:\inetpub\logs\LogFiles>cd FTPSVC3
C:\inetpub\logs\LogFiles\FTPSVC3>type u_ex240317.log | find "230"
The system cannot find the file specified.
C:\inetpub\logs>type ex250309.log | find "230"
2025-03-09 10:47 21 ControlChannelOpened - - 0 0 230bbace-6108-46f4-b4e2-0b5bfa67823 -
2025-03-09 10:47 21 USER Administrator 331 0 0 230bbace-6108-46f4-b4e2-0b5bfa67823 -
2025-03-09 10:47 21 Administrator 10.10.19.202 21 PASS *** 230 0 0 282f59e5-93aa-48ec-bf4b-
be3e7b327d64 /
2025-03-09 10:47 21 PASS *** 530 1326 41 230bbace-6108-46f4-b4e2-0b5bfa67823 -
2025-03-09 10:47 21 ControlChannelClosed - - 0 0 230bbace-6108-46f4-b4e2-0b5bfa67823 -
```

Hình 11 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
- [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>