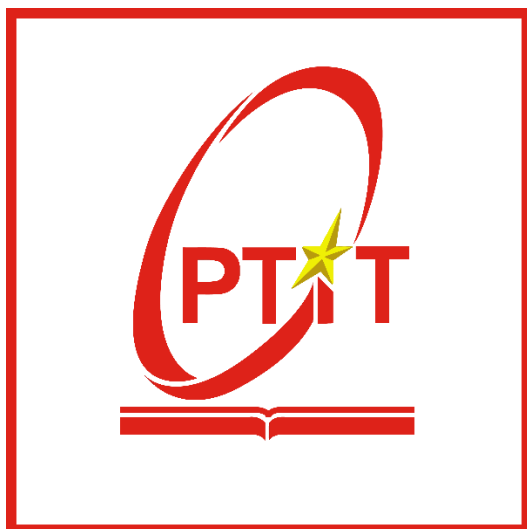


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: THỰC TẬP CƠ SỞ
BÁO CÁO BÀI THỰC HÀNH SỐ 9
PHÂN TÍCH LOG HỆ THỐNG

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 5/2024 ~

Mục Lục

1	Mục đích	2
2	Nội dung thực hành.....	2
2.1	Tìm hiểu lý thuyết.....	2
2.2	Các bước thực hiện.....	6
2.2.1	Phân tích log sử dụng grep trong Linux.....	6
2.2.2	Phân tích log sử dụng gawk trong linux	12
2.2.3	Phân tích log sử dụng find trong Windows.....	14
3	Kết luận	19
4	Tài liệu tham khảo	19

Bài 9: Phân tích log hệ thống

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 Tìm hiểu lý thuyết

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 được chỉ định. Lệnh grep trong Linux sẽ rất tiện lợi khi tìm kiếm các file log lớn.

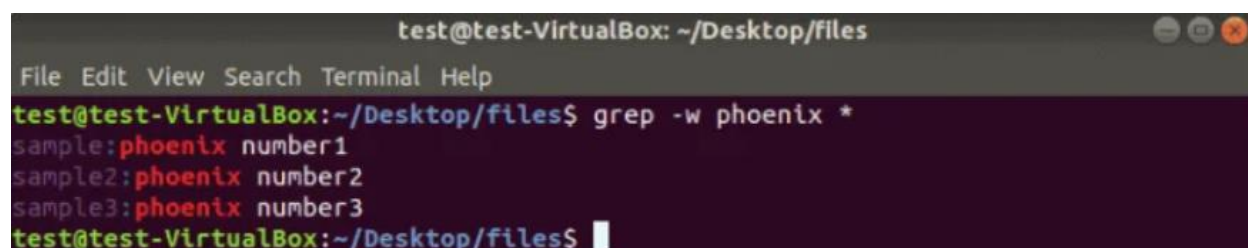
Cú pháp: **grep [OPTIONS] PATTERN [FILE...]**

OPTIONS: Không hoặc nhiều tùy chọn. Grep bao gồm một số tùy chọn để điều khiển hành vi của nó.

PATTERN: mẫu tìm kiếm file

FILE : Không hoặc nhiều tên tập tin đầu vào. □

Ví dụ :



```
test@test-VirtualBox: ~/Desktop/files
File Edit View Search Terminal Help
test@test-VirtualBox:~/Desktop/files$ grep -w phoenix *
sample:phoenix number1
sample2:phoenix number2
sample3:phoenix number3
test@test-VirtualBox:~/Desktop/files$
```

Hình 1: In các dòng có kết quả khớp toàn bộ từ và tên của các file mà nó tìm thấy

Find:

Là một trong những lệnh quan trọng và tiện dụng nhất trên hệ thống Linux.

Lệnh có thể tìm các file trên PC Linux dựa trên khá nhiều điều kiện và biến số bạn đặt. Có thể tìm file theo quyền, người dùng, nhóm, loại file, ngày tháng, dung lượng và các tiêu

chỉ có thể có khác bằng cách sử dụng lệnh find. Kết quả của nó trả về là tên đường dẫn mà bạn đang muốn tìm.

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

options : điều khiển xử lý các liên kết tượng trưng, tùy chọn gỡ lỗi và phương pháp tối ưu hóa.

path: xác định thư mục hoặc các thư mục khởi đầu mà find sẽ tìm kiếm các tập tin.

expression: được tạo thành từ các tùy chọn, mẫu tìm kiếm và các hành động được phân tách bằng các toán tử.

Ví dụ:

```
gary@gary-lubuntu:~$ find -name photo.png
./Pictures/photo.png
gary@gary-lubuntu:~$
```

Hình 2: Tìm file theo tên trong thư mục hiện tại

Gawk:

Gawk là một ngôn ngữ lập trình giúp chúng ta thao tác dễ dàng với kiểu dữ liệu có cấu trúc và tạo ra những kết quả được định dạng. Nó được đặt tên bằng cách viết tắt các chữ cái đầu tiên của các tác giả: Aho, Weinberger và Kernighan.

Gawk sử dụng để tìm kiếm và xử lý file text. Nó có thể tìm kiếm một hoặc nhiều file để xem các file có dòng nào bao gồm những pattern cần tìm kiếm và sau đó thực hiện những action.

Cú pháp của lệnh gawk như sau: **gawk [pattern] actions file .**

Trong đó:

pattern: là những biểu thức chính quyactions: là những câu lệnh cần thực hiện

actions: hành động được thực hiện khi mà pattern ăn khớp

file: file cần thực hiện lệnh gawk

Cách lệnh gawk hoạt động:

Lệnh gawk đọc file đầu vào theo từng dòng.

Đối với mỗi dòng, nó sẽ khớp lần lượt với các pattern, nếu khớp thì sẽ thực hiện action tương ứng. Nếu không có pattern nào được so khớp thì sẽ không có action nào thực hiện.

Cú pháp cơ bản làm việc với lệnh gawk thì pattern hoặc action phải có 1 trong 2 không thể thiếu cả 2.

Nếu không có pattern, gawk sẽ thực hiện action đối với mỗi dòng của dữ liệu. Nếu không có action, gawk sẽ mặc định in ra tất cả những dòng khớp với pattern đã cho.

Mỗi câu lệnh trong phần action được phân tách nhau bởi dấu chấm phẩy.

Ví dụ:

```
sara@sara-pnap:~$ gawk '/O/ {print}' people
1. Olivia Johnson 1995
6. Oliver Davis 2005
sara@sara-pnap:~$
```

Hình 3: In ra các dòng trong tệp "people" mà chứa ký tự 'O'

Accesss_log:

Có chức năng ghi lại những lần sử dụng, truy cập, yêu cầu đến apache server.

File log được lưu trữ tại /var/log/httpd/access_log (hoặc /var/log/apache2/access.log).

Định dạng log (LogFormat) cơ bản như sau là : **%h %l %u %t %r %>s %b Refer User_agent**. Trong đó:

%h: địa chỉ của máy client.

%l: nhận dạng người dùng được xác định bởi identd (thường không SD vì không tin cậy).

%u: tên người dùng được xác định bằng xác thức HTTP.

%t: thời gian yêu cầu được nhận. □

%r: là yêu cầu từ người sử dụng (client).

%>s: mã trạng thái được gửi từ máy chủ đến máy khách.

%b: kích cỡ phản hồi đối với client

Refer: tiêu đề Refeer của yêu cầu HTTP (chứa URL của trang mà yêu cầu này được khởi tạo)

User_agent: chuỗi xác định trình duyệt

Event Log trong Windows:

Event: Là một hành động hoặc trạng thái đặc biệt mà hệ thống hoặc ứng dụng muốn báo cáo. Ví dụ: khởi động hệ thống, lỗi ứng dụng, thay đổi quyền hạn người dùng, vv.

Event Log: Là nơi lưu trữ thông tin về các sự kiện. Windows sử dụng ba loại event log chính: Application log (gồm các sự kiện ứng dụng), System log (gồm các sự kiện hệ thống), và Security log (gồm các sự kiện bảo mật).

Event ID: Mỗi sự kiện được định danh bằng một mã số gọi là Event ID. Mã này là duy nhất cho mỗi loại sự kiện và có thể được sử dụng để xác định loại sự kiện và mức độ nghiêm trọng của nó.

Event Source: Là nguồn tạo ra sự kiện. Mỗi ứng dụng hoặc thành phần của hệ thống có thể tạo ra các sự kiện và đăng ký chúng với event log.

Log Entries: Là các bản ghi cụ thể trong event log, chứa thông tin chi tiết về một sự kiện nhất định.

Log Files: Event log được lưu trữ trong các tập tin có định dạng .evt hoặc .evtx trên hệ thống. Đối với phiên bản mới hơn của Windows (Windows Vista trở đi), log files thường được lưu dưới định dạng XML và có đuôi .evtx.

Event Viewer: Là công cụ trong Windows giúp người dùng xem và quản lý event log. Nó cho phép xem sự kiện, lọc, tìm kiếm, và theo dõi các sự kiện quan trọng.

Auditing trong Windows: là quá trình ghi lại và theo dõi các hoạt động hệ thống, ứng dụng và tài khoản người dùng để đảm bảo an ninh, tuân thủ và giải quyết sự cố trong môi trường hệ thống. Chức năng kiểm toán (auditing) giúp quản trị viên xác định những thay đổi quan trọng, sự cố bảo mật, hoặc các hoạt động không phù hợp trên hệ thống.

Audit Policy: Là các cài đặt mà quản trị viên có thể thiết lập để quyết định loại sự kiện nào sẽ được ghi lại và theo dõi. Có hai loại chính là "Object Access" (theo dõi truy cập đối tượng) và "Account Logon/Audit Logon" (theo dõi đăng nhập tài khoản).

Security Auditing: Đây là loại kiểm toán chủ yếu trong Windows. Nó bao gồm ghi lại các sự kiện liên quan đến bảo mật như đăng nhập, thay đổi mật khẩu, truy cập tài nguyên, và các sự kiện bảo mật khác.

Event Logs: Windows sử dụng Event Logs để lưu trữ thông tin chi tiết về các sự kiện kiểm toán. Các loại sự kiện bảo mật thường được ghi vào Security log, trong khi các sự kiện hệ thống và ứng dụng có thể được ghi vào các log tương ứng.

Event Viewer: Là công cụ giúp quản trị viên xem và phân tích các sự kiện đã được ghi lại trong event logs. Event Viewer cung cấp khả năng lọc, tìm kiếm và xem các sự kiện theo các tiêu chí nhất định.

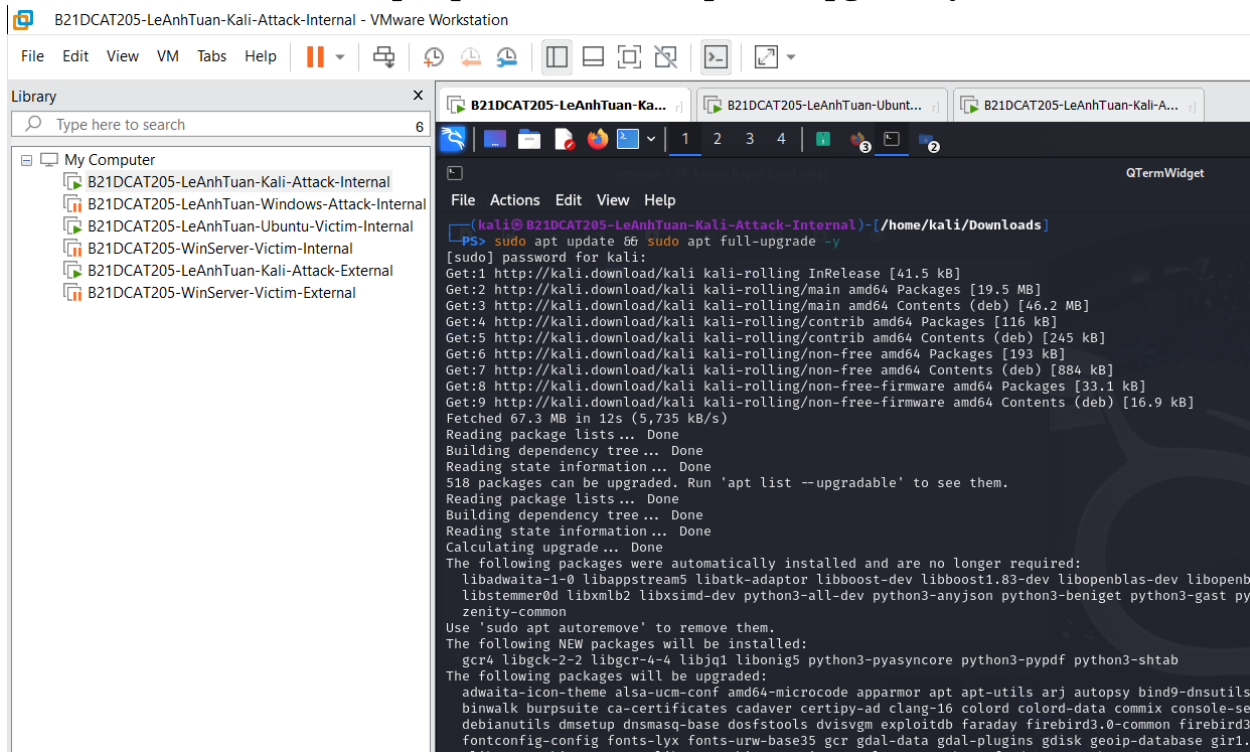
Group Policy: Quản trị viên có thể sử dụng Group Policy để cấu hình các chính sách kiểm toán trên các máy tính trong mạng.

2.2 Các bước thực hiện

2.2.1 Phân tích log sử dụng grep trong Linux

Trên máy **Kali-Attack-Internal** trong mạng **Internal**:

sudo apt update && sudo apt full-upgrade -y

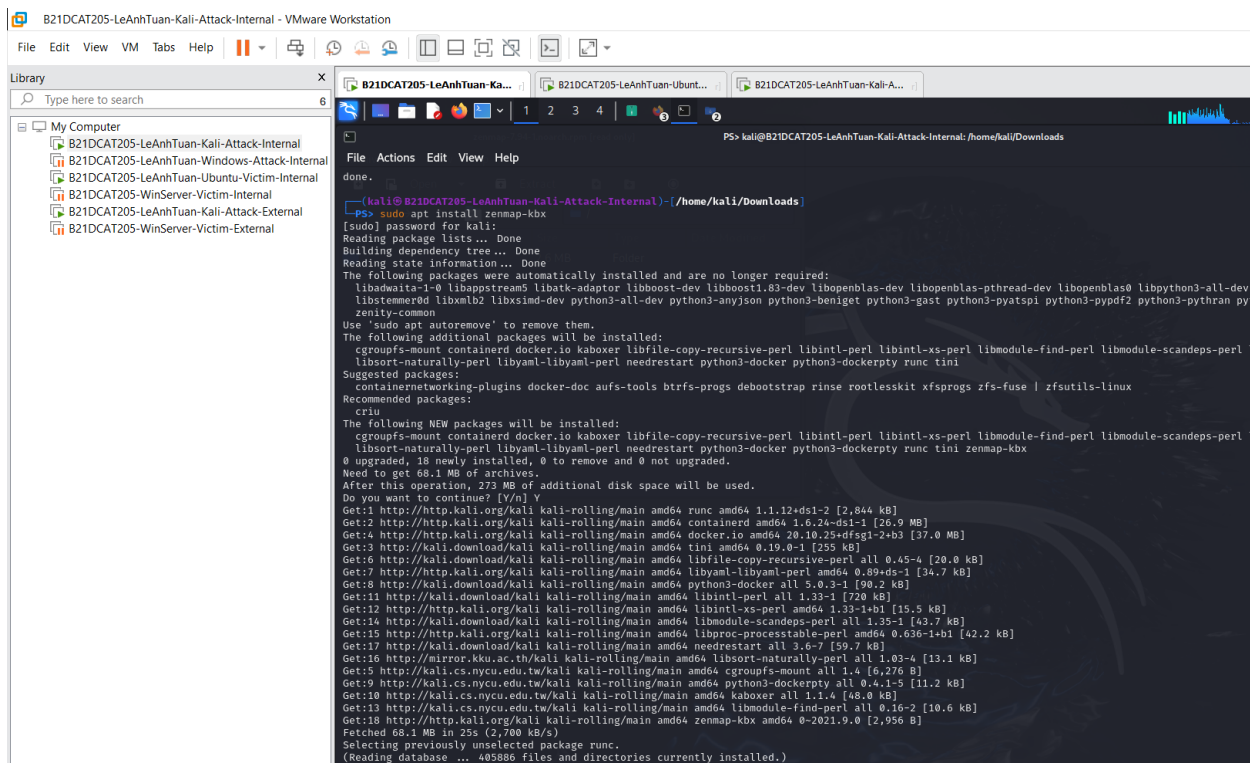


```
(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[/home/kali/Downloads]
PS> sudo apt update && sudo apt full-upgrade -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.2 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [245 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [884 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 67.3 MB in 12s (5,735 kB/s)
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
518 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libopenblas-dev libopenbl
  libstemmer0d libxmb2 libxsimd-dev python3-all-dev python3-anyjson python3-beniget python3-gast py
  zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  gcr4 libgck-2-2 libgcr-4-4 libjq1 libonig5 python3-pyasyncore python3-pypdf python3-shtab
The following packages will be upgraded:
  adwaita-icon-theme alsa-ucm-conf amd64-microcode apparmor apt apt-utils arj autopsy bind9-dnswalk
  binwalk burpsuite ca-certificates cadaver certipy-ad clang-16 colord colord-data commix console-set
  debianutils dmsetup dnsmasq-base dosfstools dvisvgm exploitdb faraday firebird3.0-common firebird3
  fontconfig-config fonts-lyx fonts-urw-base35 gcr gdal-data gdal-plugins gdisk geoip-database girl2
  libnetworking-common libnetworking-common-qa libte-protobufs feed-runs-ruby-common ruby-qa-tem
```

Hình 4: Sử dụng lệnh `sudo apt update && sudo apt full-upgrade -y`

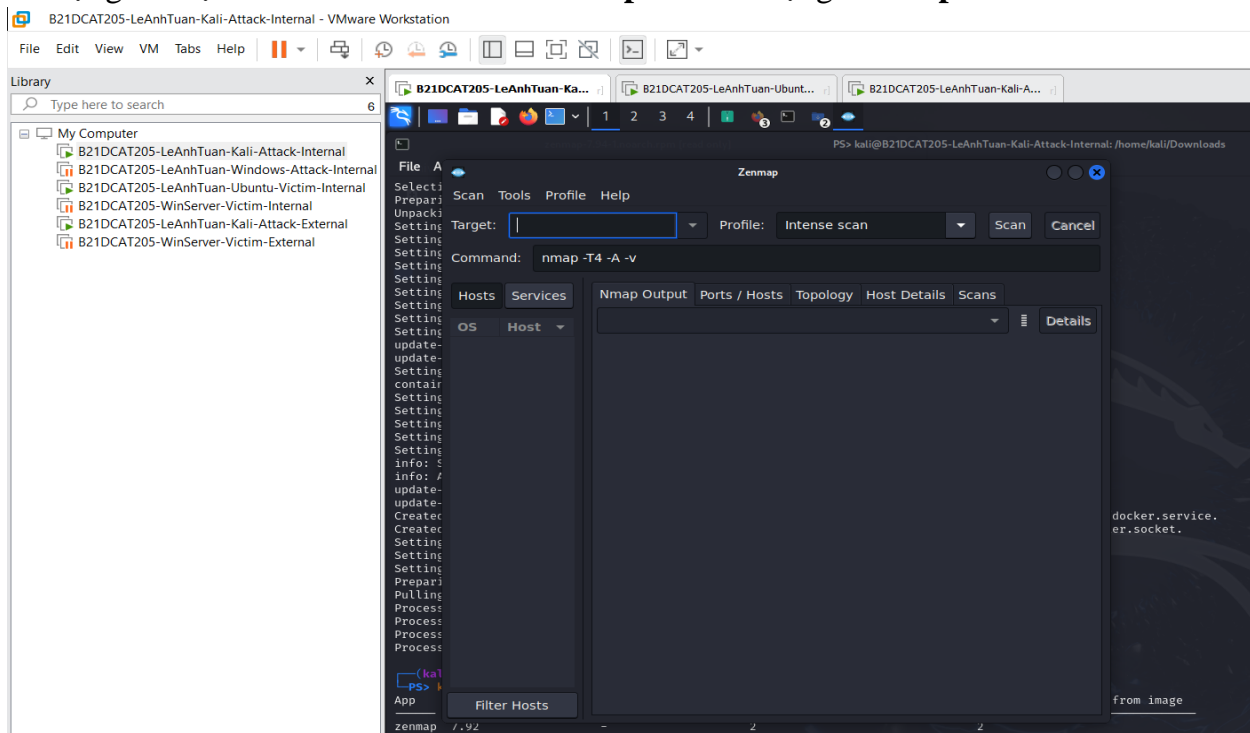
Để tải zenmap sử dụng câu lệnh:

sudo apt install zenmap-kbx



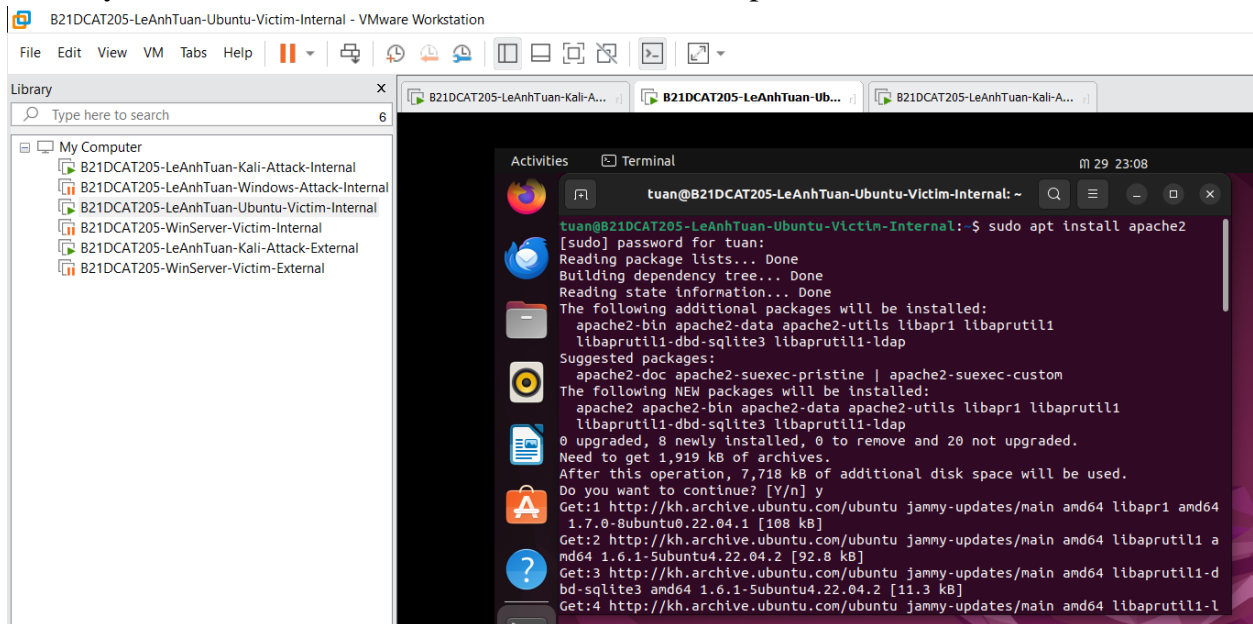
Hình 5: Download zenmap

Sử dụng câu lệnh sudo kaboxer run zenmap để khởi động zenmap:

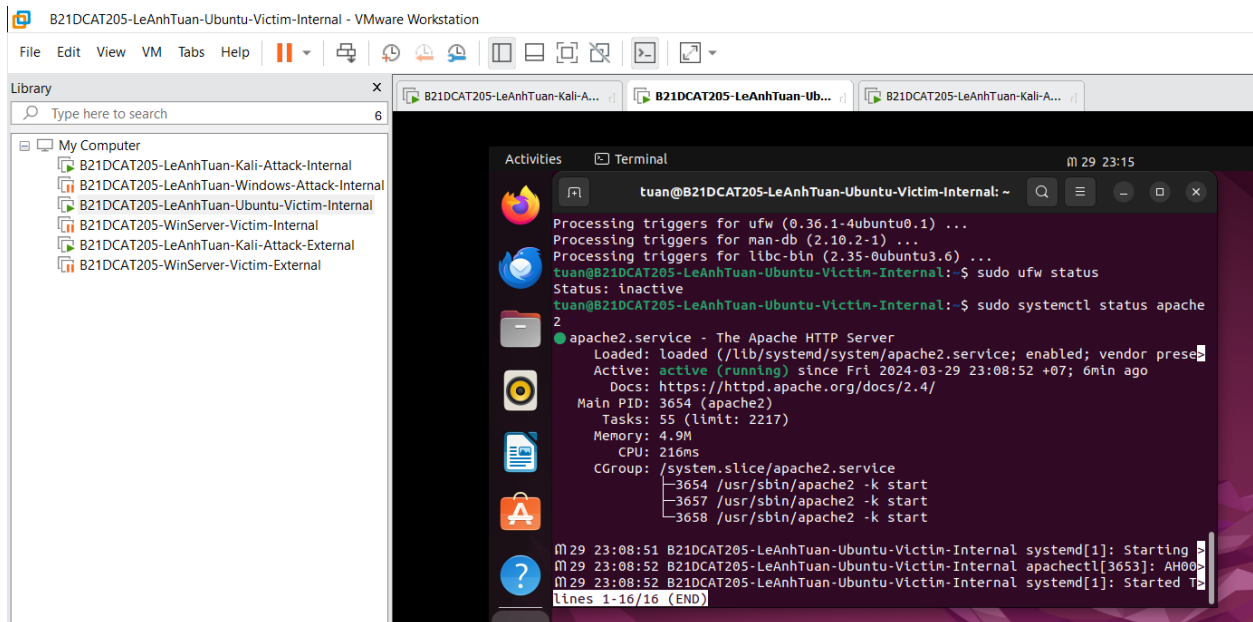


Hình 6: Giao diện zenmap

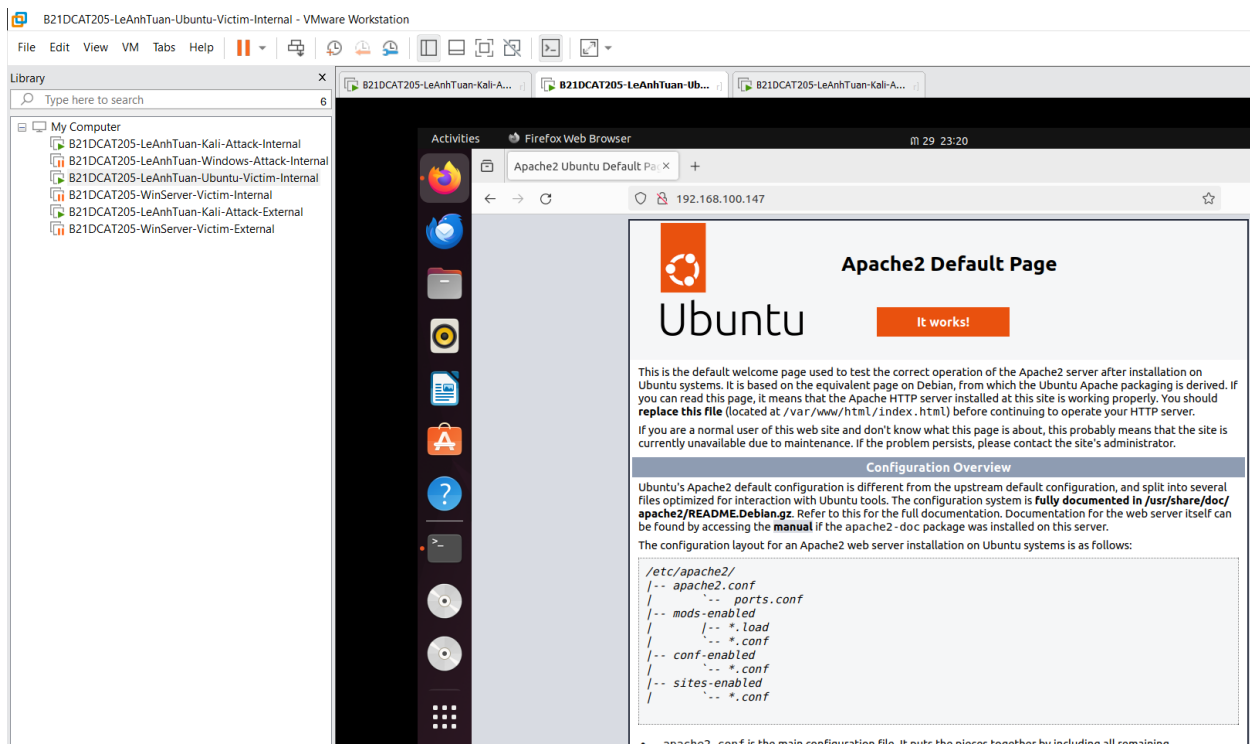
Tại máy **Ubuntu-Victim-Internal** tiến hành cài đặt apache.



Hình 7: Tải apache tại máy Ubuntu-Victim-Internal

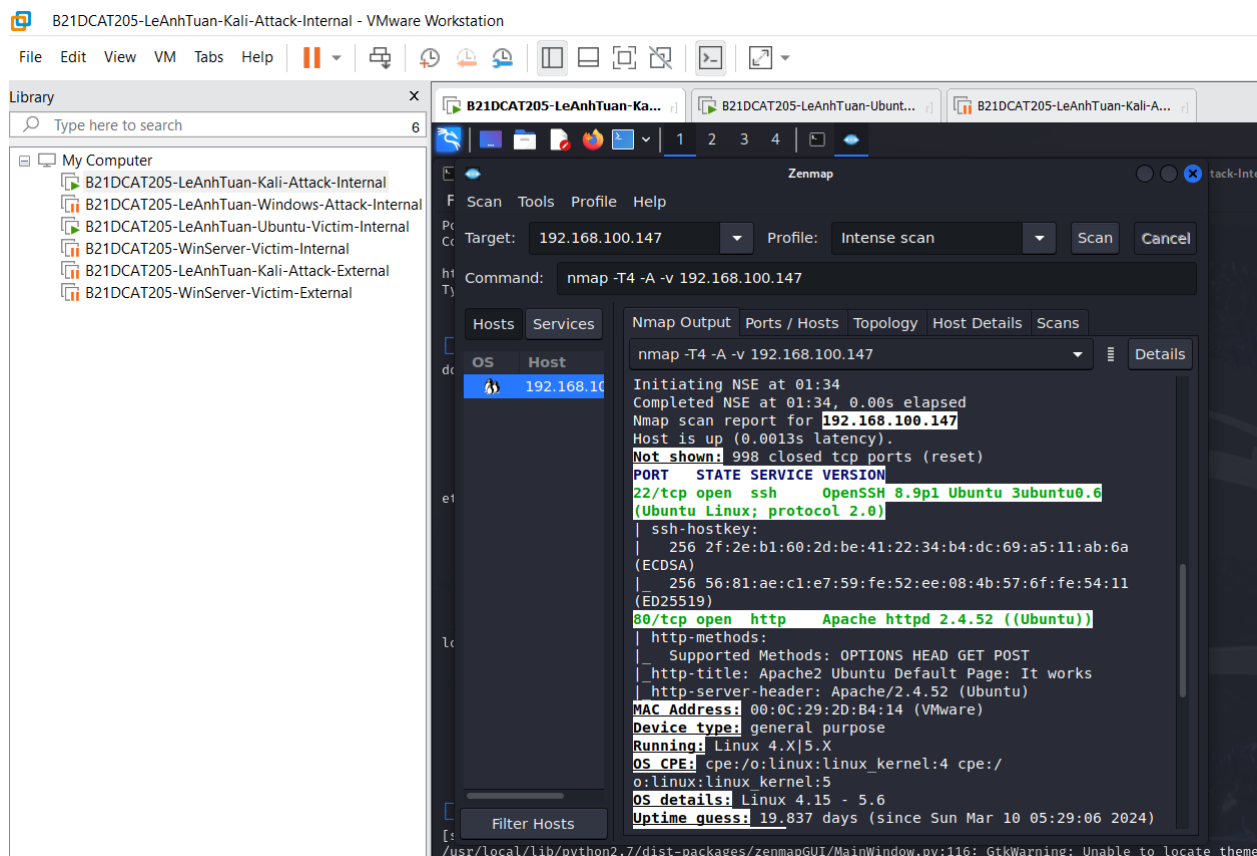


Hình 8: Kiểm tra trạng thái hoạt động của apache



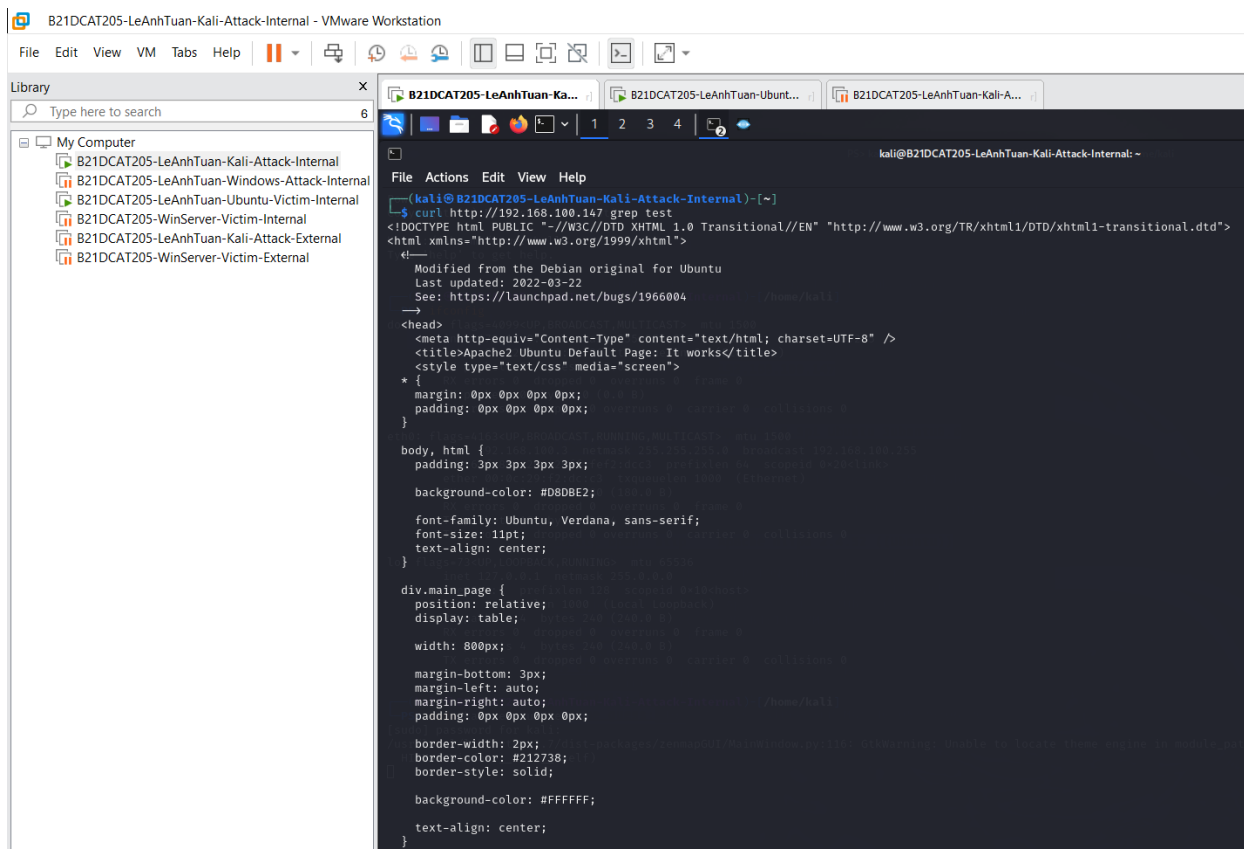
Hình 9: Mở Web Server Apache tại máy Ubuntu-Victim-Internal

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



Hình 10: Tại giao diện zenmap ta thấy cổng 22 và 80 đang mở

Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”(root@bt:~#curl http://192.168.100.147 grep test)

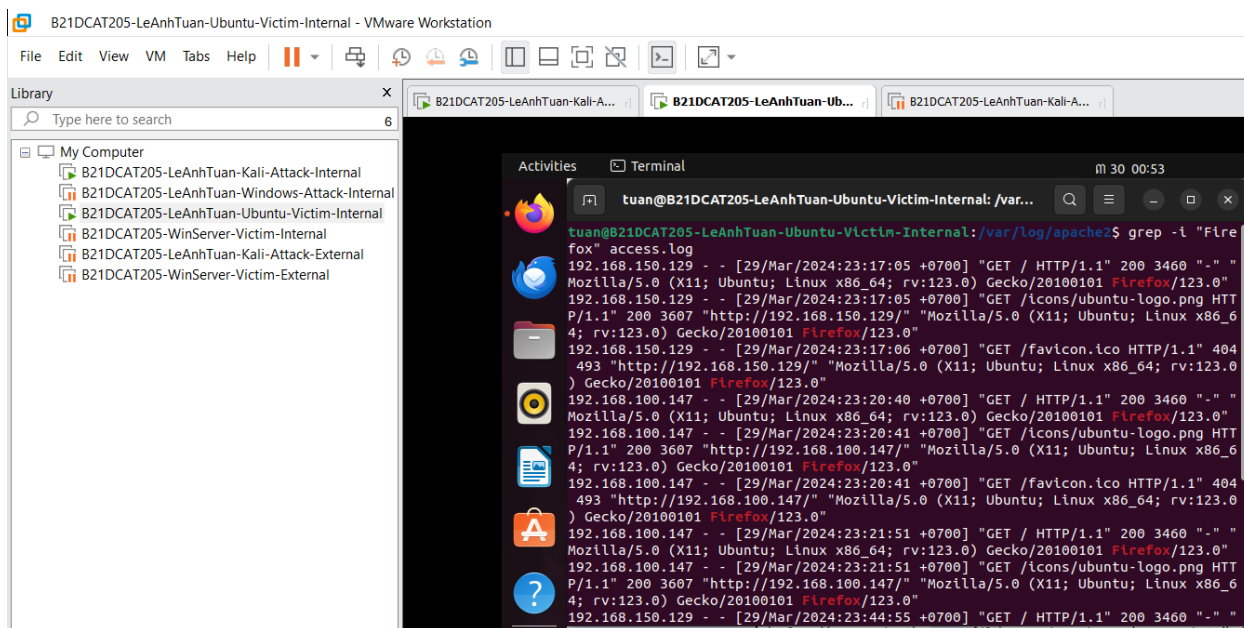


Hình 11: sao chép website và tìm kiếm từ khóa “test”

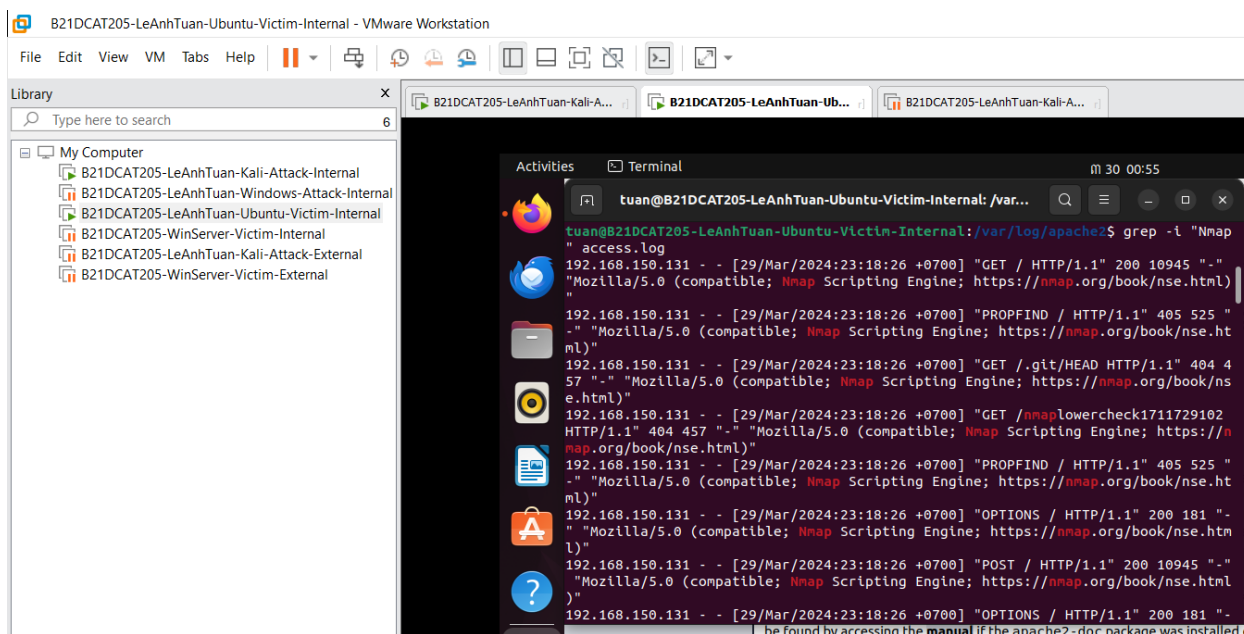
Trên máy **Linux Internal Victim**, để xem thư mục chứa **access_log** dùng lệnh:

cd /var/log/apache2

Sau đó sử dụng **grep -i “Firefox” access.log**



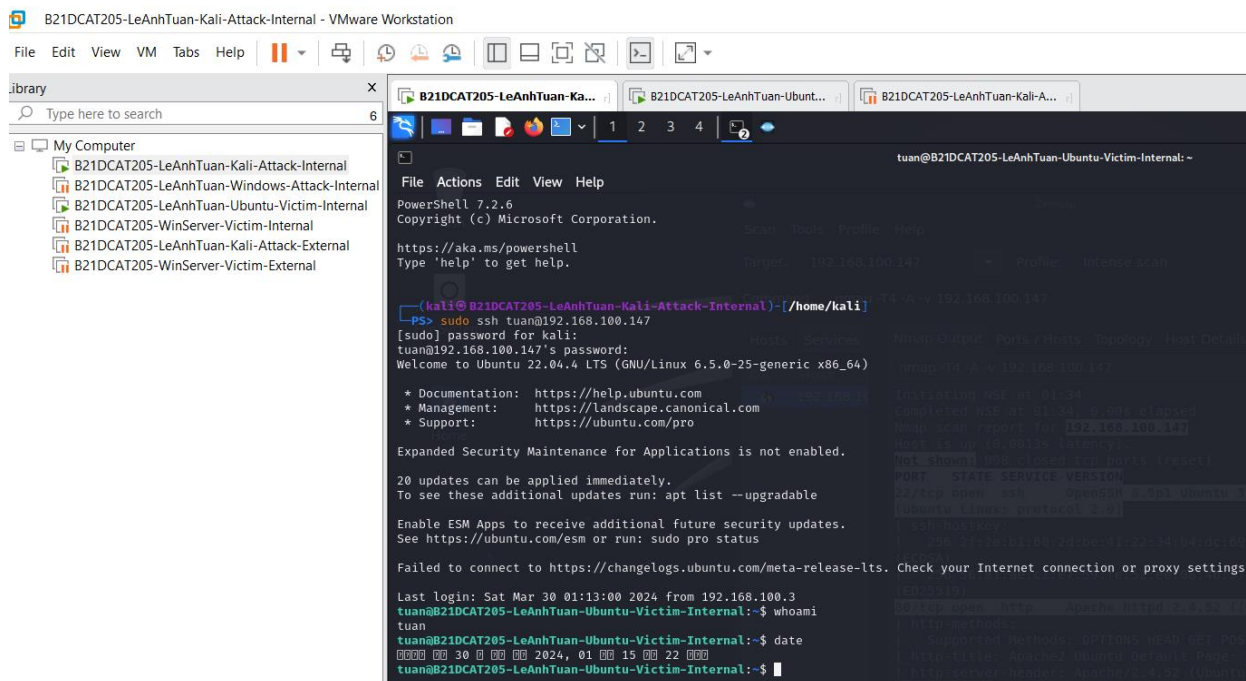
Hình 12: Lọc ra kết quả với từ khóa “Firefox”



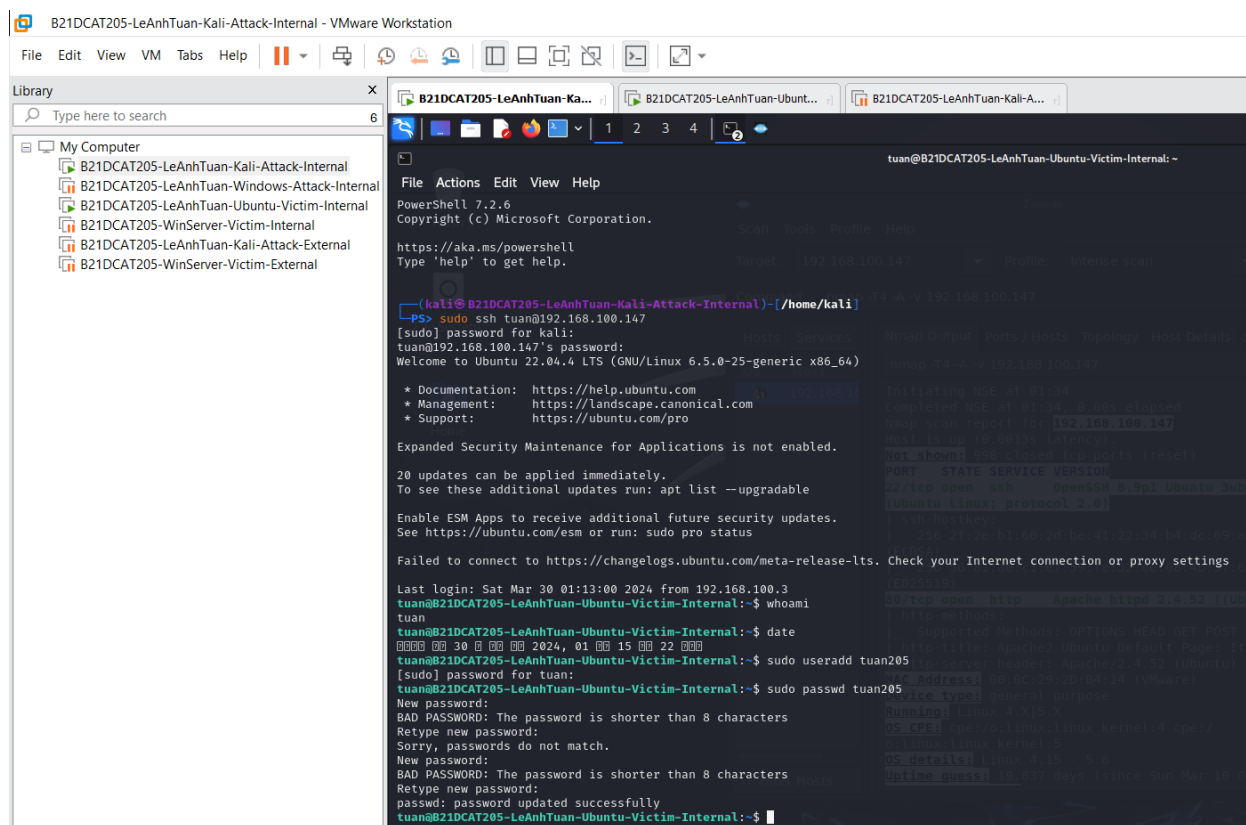
Hình 13: Lọc ra kết quả với từ khóa “Nmap”

2.2.2 Phân tích log sử dụng gawk trong linux

Trên máy **Kali-Attack-Internal** remote máy **Linux-Internal-Victim**. (Sử dụng ssh).
Tạo một account mới.

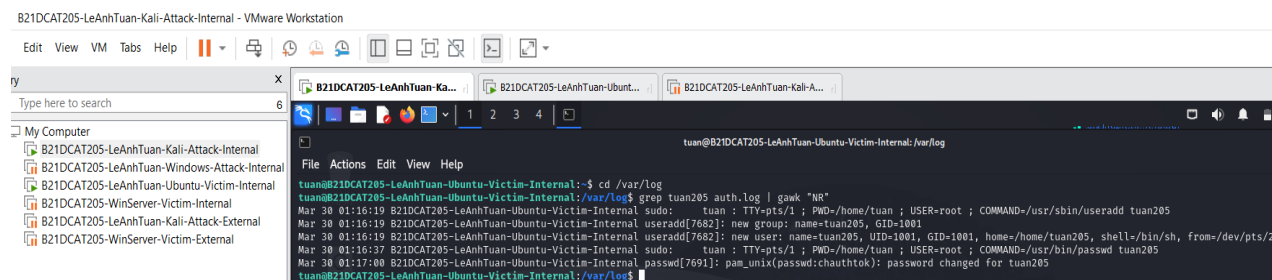


Hình 14: SSH thành công từ máy Kali-Attack-Internal tới Ubuntu-Victim-Internal



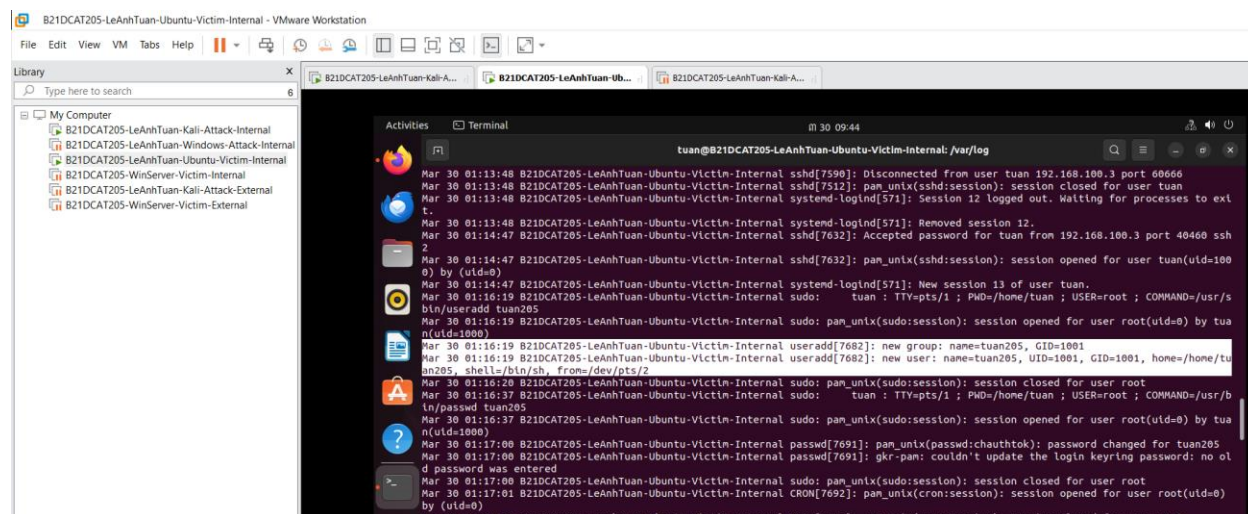
Hình 15: Tạo tài khoản người dùng tuan205

Trên máy **Kali-Attack-Internal**, 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.



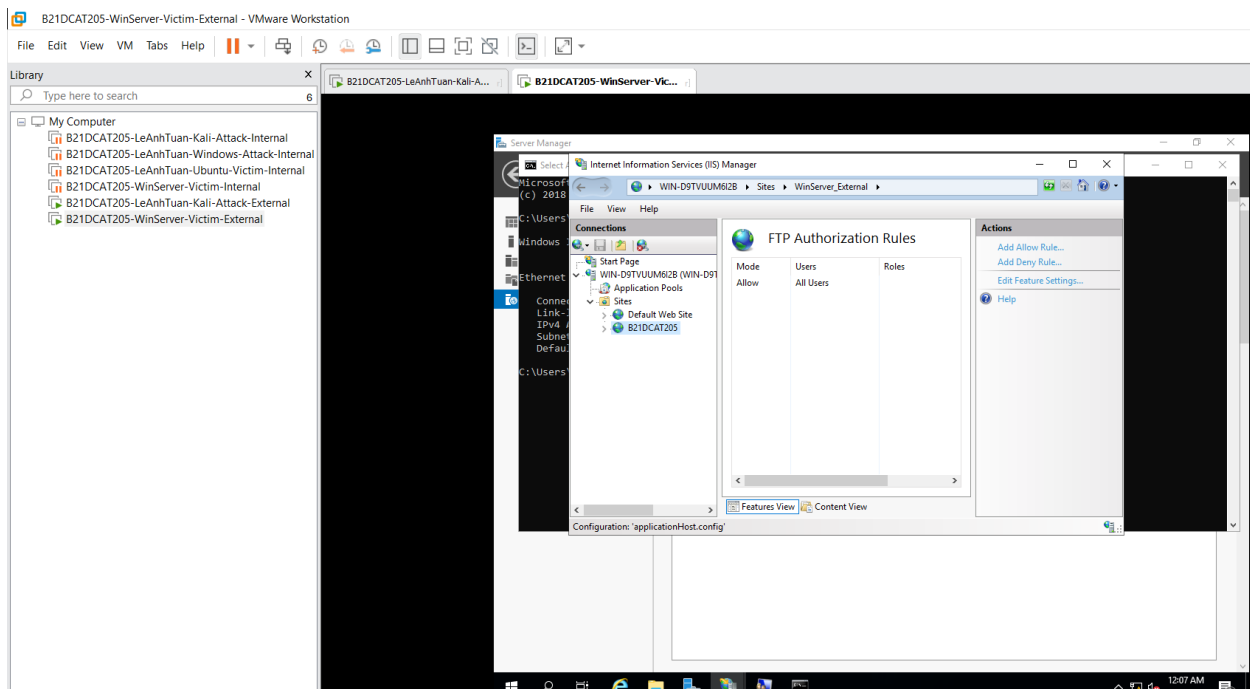
Hình 16: Sử dụng gawk in ra dữ liệu được ghi lại khi tạo account **tuan205**

Tại máy **Ubuntu-Victim-Internal** : `cd /var/log`, sau đó `cat auth.log`, ta sẽ thấy log ghi lại quá trình tạo tài khoản và mật khẩu **tuan205**

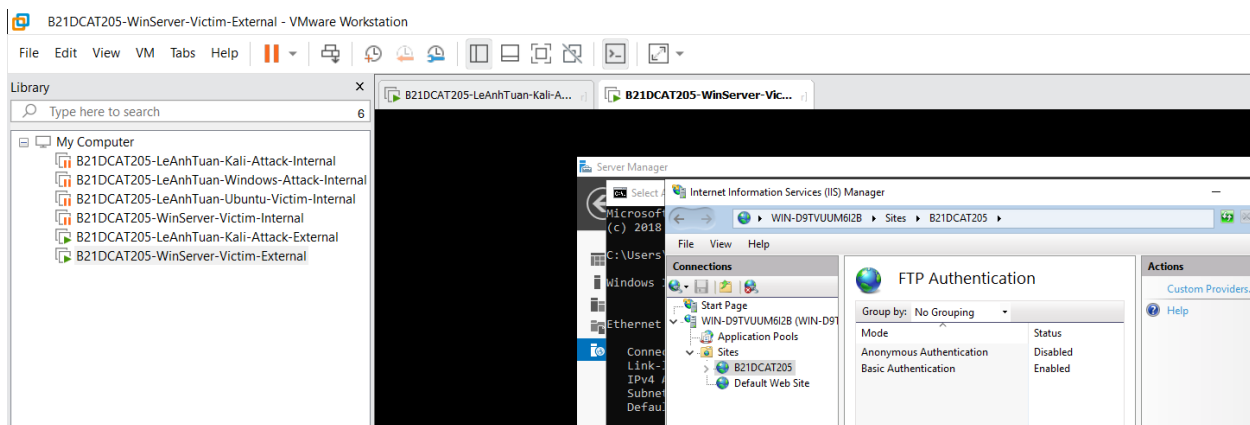


Hình 17: Nội dung trong **auth.log**

2.2.3 Phân tích log sử dụng find trong Windows



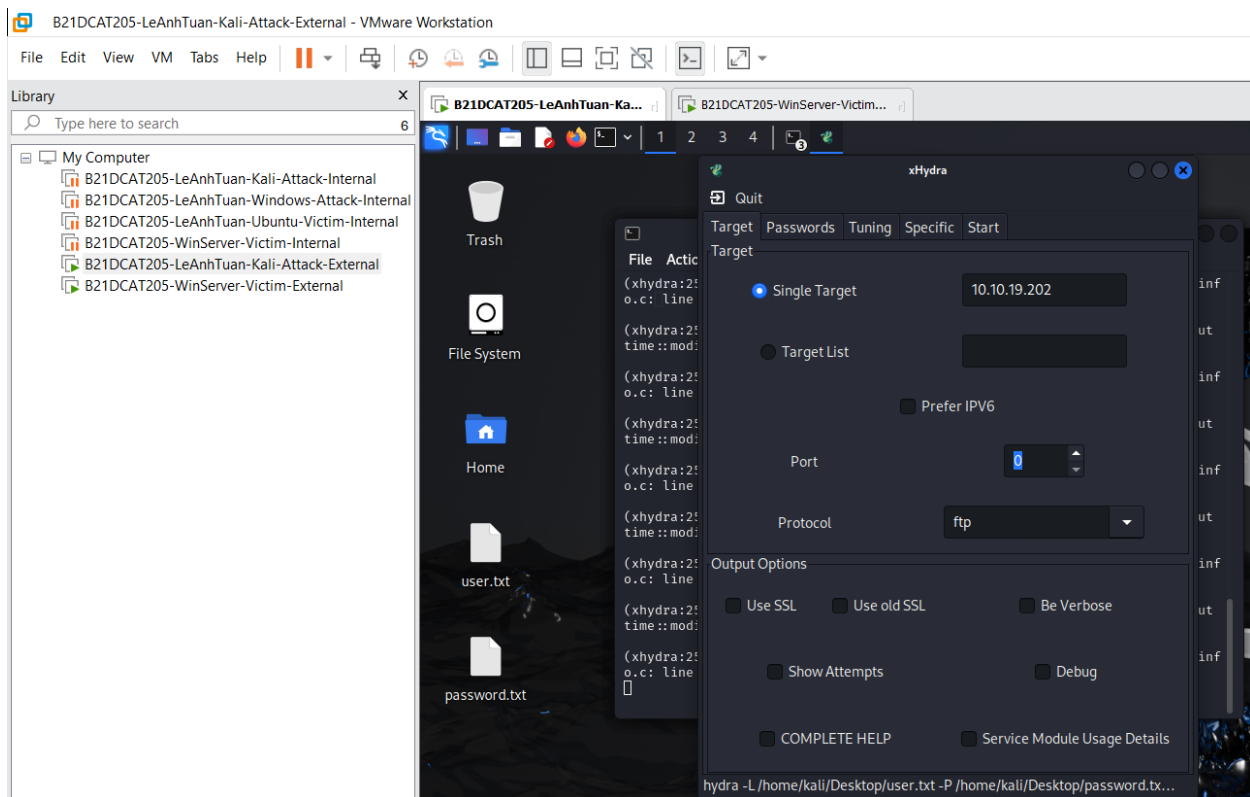
Hình 18: Add FTP site với tên B21DCAT205



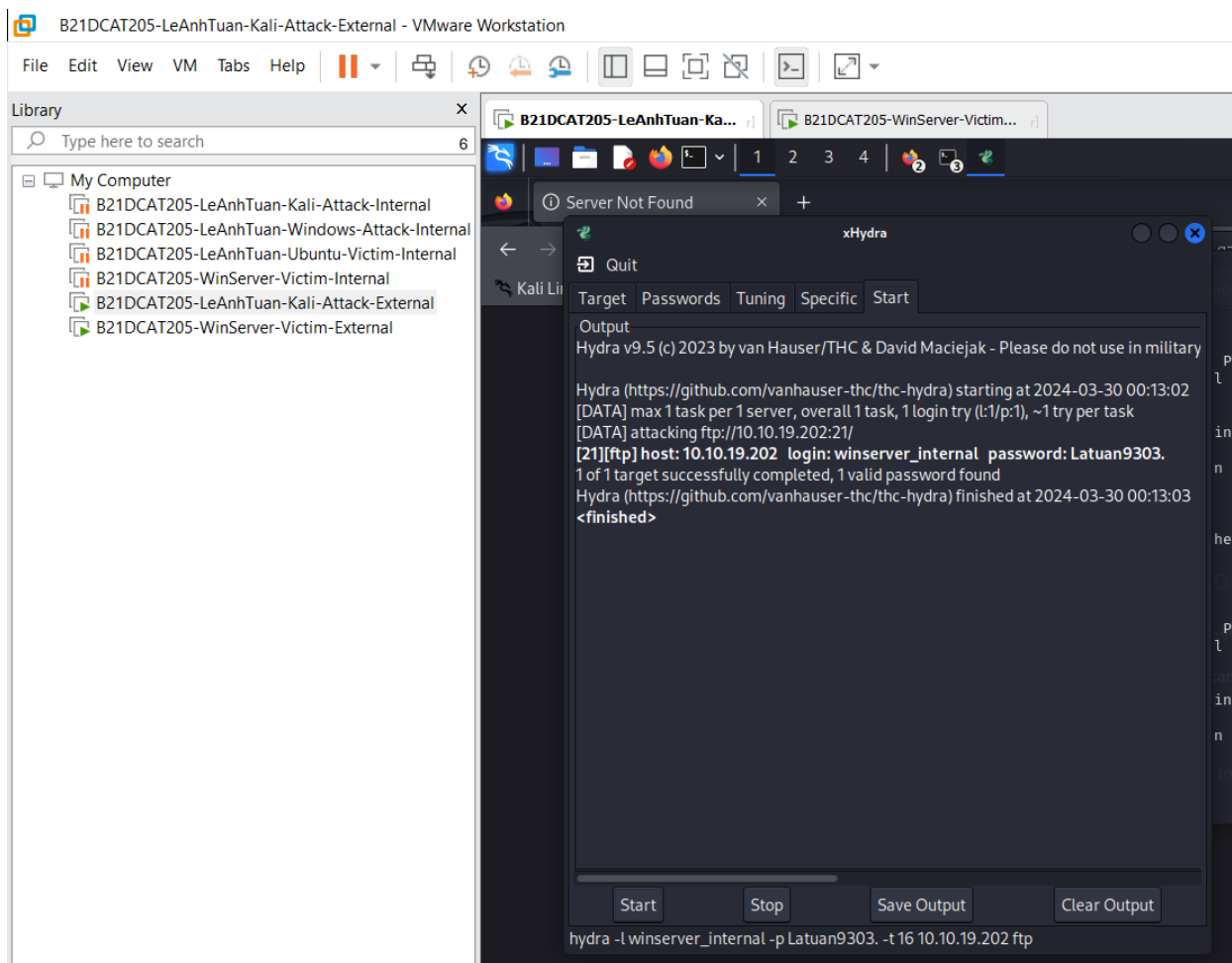
Hình 19: Cấu hình FTP site

Cài đặt xhydra : **sudo apt install hydra-gtk**

Trên máy **Kali-Attack-External** 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

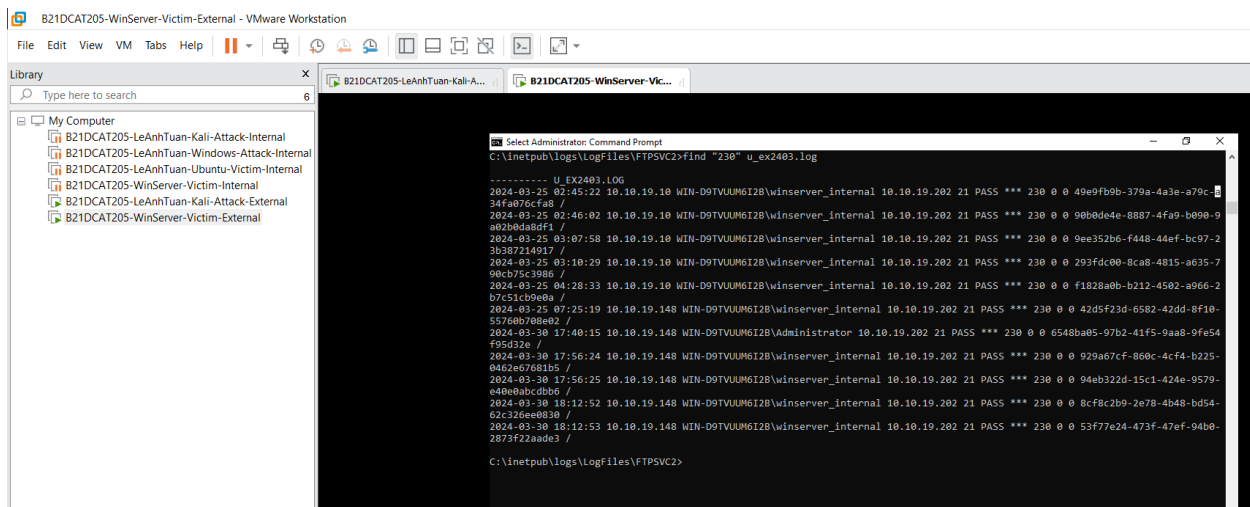


Hình 20:Điền IP là máy WinServer-Victim-External (10.10.19.202)



Hình 22: Tìm mật khẩu thành công

Trên máy **WinServer-Victim-External**, thực hiện điều hướng đến FTP Logfile (**C:\inetpub\logs\LogFiles\FTPSVC2**). 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>find "230" u_ex240124.log**)



Hình 23: Thông tin file u_ex2403.log

3 Kết luận

- Bắt gói tin và các file pcap thông qua tcpdump thành công
- Sử dụng Wireshark để bắt và lọc ra được các gói tin ftp, các file pcap tương ứng thành công
- Bắt được các dữ liệu trong file index.html thành công.

4 Tài liệu tham khảo

- Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021
- <https://www.tcpdump.org/index.html#documentation>
- https://www.wireshark.org/docs/wsug_html/
- <https://docs.securityonion.net/en/2.3/networkminer.html#>