

**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: B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên hướng dẫn: PGS.TS Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
DANH MỤC CÁC HÌNH ẢNH	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
I. Mục đích	5
II. Tìm hiểu lý thuyết.....	5
1. Lệnh "grep" - Global Expression Print	5
2. Lệnh “gawk”	6
3. Lệnh “find”	6
4. File Secure	7
5. Tập access.log	7
6. Lệnh xhydra	7
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	8
I. Chuẩn bị môi trường	8
II. Các bước thực hiện	8
a. Phân tích log sử dụng grep trong Linux	8
b. Phân tích log sử dụng gawk trong Linux	13
b. Phân tích log sử dụng find trong Linux	16
TÀI LIỆU THAM KHẢO	21

DANH MỤC CÁC HÌNH ẢNH

Hình 1 – Ví dụ về lệnh <code>grep</code>	5
Hình 2 – Ví dụ về lệnh <code>gawk</code>	6
Hình 3 – Ví dụ về lệnh <code>find</code>	6
Hình 4 – Kiểm tra IP của 2 máy Ubuntu và Kali Linux	9
Hình 5 – Khởi chạy Zenmap	10
Hình 6 – Truy cập địa chỉ web 192.168.126.142	10
Hình 7 – Sao chép website và tìm kiếm từ khóa “test”	11
Hình 8 – Xem nội dung <code>access.log</code>	12
Hình 9 – Lọc kết quả với từ khóa Firefox	12
Hình 10 – Lọc kết quả với từ khóa <code>curl</code>	13
Hình 11 – Remote sang máy Linux thành công	13
Hình 12 – Tạo user mới <code>linh2004</code> thành công	14
Hình 13 – Tiến hành xem file <code>auth.log</code>	15
Hình 14 – Tìm kiếm người dùng vừa tạo bằng <code>grep</code>	15
Hình 15 – Dùng lệnh <code>gawk</code> in một hoặc nhiều dòng dữ liệu	16
Hình 16 – Dùng lệnh <code>gawk</code> ‘/useradd/’	16
Hình 17 – Bắt đầu cấu hình xHydra	17
Hình 18 – Chọn file mật khẩu	17
Hình 19 – Lấy được mật khẩu của tài khoản Administrator	18
Hình 20 – Tiến hành điều hướng đến FTP LogFile	18
Hình 21 – Hiện thị tất cả các file log đang có	19
Hình 22 – Mở file <code>u_ex250224.log</code>	19
Hình 23 – Kết quả đạt được sau khi tấn công login	20

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SCP	Secure Copy	Giao thức chia sẻ file an toàn
FTP	File Transfer Protocol	Giao thức trao đổi tệp tin
SSH	Secure Shell	Giao thức truy cập từ xa
HTTP	Hyper Text Transfer Protocol	Giao thức truyền tải siêu văn bản
Grep	Global Expression Print	Lệnh tìm kiếm

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

I. Mục đích

Nắm vững 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

II. Tìm hiểu lý thuyết

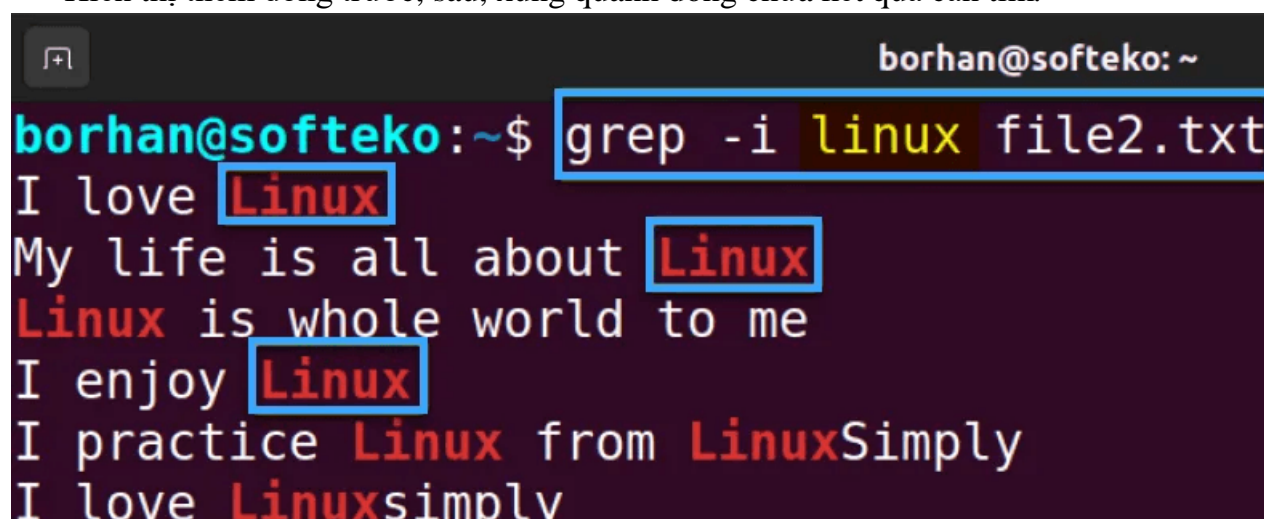
1. Lệnh grep

grep (Global Expression Print): là công cụ cho phép bạn tìm kiếm thông qua một số lượng lớn các tệp và thư mục cho văn bản được chỉ định.

Cú pháp : **grep [tùy chọn] <file>**

Một số chức năng nổi bật của grep:

- Tìm một chuỗi trong file.
- Tìm kiếm chuỗi trong nhiều file.
- Tìm kiếm không phân biệt hoa thường.
- Tìm kiếm ngược sử dụng tùy chọn -v
- Hiển thị số dòng, số lượng, giới hạn số dòng đầu ra.
- Tìm kiếm nhiều chuỗi.
- Tìm kiếm trên tệp.
- Hiển thị thêm dòng trước, sau, xung quanh dòng chứa kết quả cần tìm.



```
borhan@softeko:~$ grep -i linux file2.txt
I love Linux
My life is all about Linux
Linux is whole world to me
I enjoy Linux
I practice Linux from LinuxSimply
I love Linuxsimply
```

Hình ảnh 1 : Lệnh grep.

2. Lệnh gawk

gawk là giao thức cho phép bạn hiển thị đầu ra ở định dạng dễ hiển thị mà con người có thể đọc được.

Sử dụng gawk cho phép bạn:

- Quản lý cơ sở dữ liệu nhỏ, cá nhân.
- Tạo báo cáo.
- Xác thực dữ liệu.
- Tạo chỉ mục và thực hiện các công việc chuẩn bị tài liệu khác.

- Thử nghiệm với các thuật toán mà bạn có thể thích ứng sau này với các ngôn ngữ máy tính khác.

Ngoài ra, gawk cung cấp các tiện ích giúp bạn dễ dàng:

- Trích xuất các bit và phần dữ liệu để xử lý.
- Sắp xếp dữ liệu.
- Thực hiện các giao tiếp mạng đơn giản.

Cú pháp:

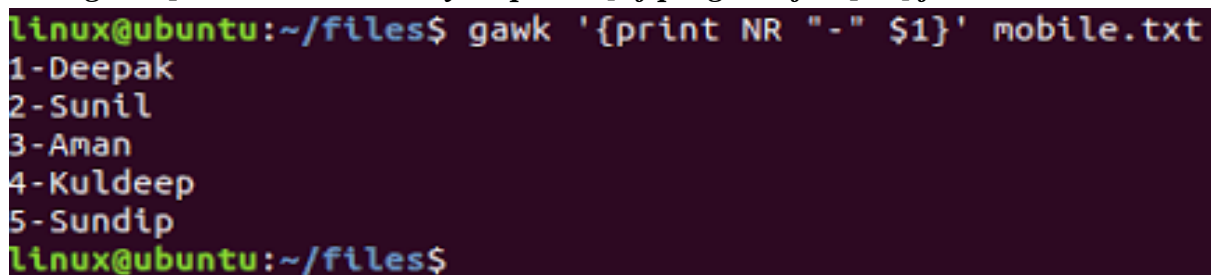
gawk [POSIX or GNU style options] -f program-file [--] file ...

gawk [POSIX or GNU style options] [--] program-text file ...

pgawk [POSIX or GNU style options] -f program-file [--] file ...

pgawk [POSIX or GNU style options] [--] program-text file ...

dgawk [POSIX or GNU style options] -f program-file [--] file ...



```
linux@ubuntu:~/files$ gawk '{print NR "-" $1}' mobile.txt
1-Deepak
2-Sunil
3-Aman
4-Kuldeep
5-Sundip
linux@ubuntu:~/files$
```

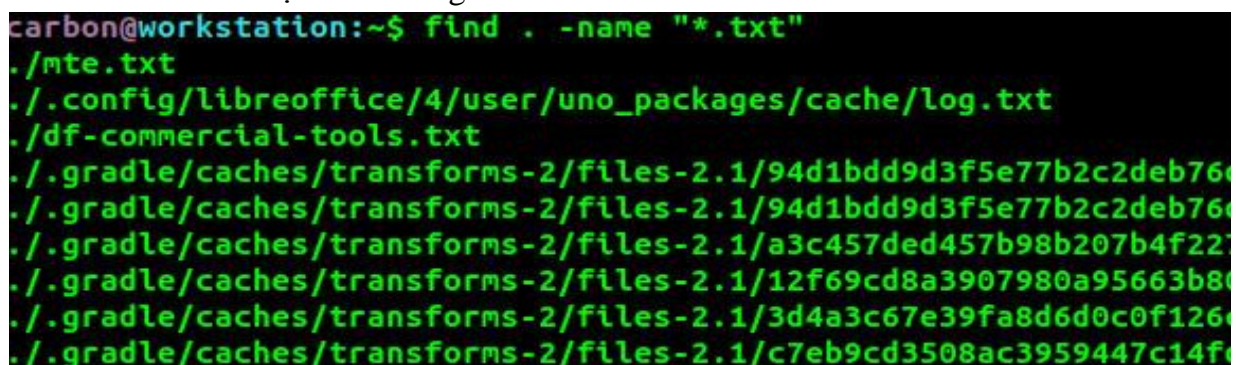
Hình ảnh 2: Ví dụ về câu lệnh “gawk”.

3.Lệnh find

find là lệnh trong Unix cho phép bạn tìm kiếm một chuỗi cụ thể trong một nhóm lớn các giá trị.

Một số khả năng nổi bật của lệnh find:

- Tìm kiếm dựa trên phân quyền và nhóm quyền.
- Tìm file theo tên trong thư mục.
- Tìm file trong thư mục cụ thể.
- Tìm file với một số quyền nhất định.
- Tìm file và thư mục dựa trên ngày giờ, dung lượng.
- Tìm kiếm dựa trên thời gian.



```
carbon@workstation:~$ find . -name "*.txt"
./mte.txt
./config/libreoffice/4/user/uno_packages/cache/log.txt
./df-commercial-tools.txt
./gradle/caches/transforms-2/files-2.1/94d1bdd9d3f5e77b2c2deb76...
./gradle/caches/transforms-2/files-2.1/94d1bdd9d3f5e77b2c2deb76...
./gradle/caches/transforms-2/files-2.1/a3c457ded457b98b207b4f22...
./gradle/caches/transforms-2/files-2.1/12f69cd8a3907980a95663b8...
./gradle/caches/transforms-2/files-2.1/3d4a3c67e39fa8d6d0c0f126...
./gradle/caches/transforms-2/files-2.1/c7eb9cd3508ac3959447c14f...
```

Hình ảnh 3: Ví dụ về lệnh find

4. File Secure:

Secure là tập nhật ký theo dõi các kết nối SSH hoặc Secure Shell. Nó cung cấp thông tin như địa chỉ IP, ngày giờ,... Nó cũng theo dõi các sự kiện khác liên quan đến bảo mật như: tạo tài khoản người dùng mới và tài khoản nhóm mới.

Đối với các hệ thống sử dụng RedHat và CentOS thì file log này thay thế cho file log */var/log/auth.log*.

Filde Secure chứa các thông tin về xác thực trên hệ thống và cả lưu trữ tất cả thông tin liên quan đến bảo mật, các lỗi xác thực. File log này giúp theo dõi thông tin đăng nhập sudo, đăng nhập SSH và các lỗi khác được ghi bởi tiến trình chạy nền của dịch vụ bảo mật hệ thống. Ngoài ra còn giúp chúng ta thấy được chi tiết về các lần đăng nhập trái phép hoặc thất bại và nó cũng lưu trữ thông tin đăng nhập thành công và theo dõi các hoạt động của người dùng hợp lệ.

5. Tập *access_log*:

Access_log là tập nhật ký theo dõi các kết nối HTTP hoặc Giao thức truyền siêu văn bản. Nó cung cấp thông tin như: địa chỉ IP, tác nhân người dùng và tem ngày giờ.

Phân tích nhật ký truy cập có thể cung cấp thông tin:

- *Số lượng* khách truy cập (yêu cầu lần đầu tiên duy nhất) vào một trang chủ cụ thể.
- *Nguồn gốc* của khách truy cập, gồm cả tên miền của máy chủ được liên kết của họ.
- *Có bao nhiêu yêu cầu* cho mỗi trang trên trang web
- *Sử dụng các mẫu liên quan* đến thời gian trong ngày, ngày trong tuần và năm.

Các loại nhật ký truy cập khác nhau thu thập các loại dữ liệu khác nhau:

- *Nhật ký chống virus*: chứa dữ liệu về các đối tượng được quét, các cài đặt được sử dụng cho mỗi tác vụ và lịch sử các hành động được thực hiện trên mỗi tệp.
- *Nhật ký tường lửa*: cung cấp thông tin về địa chỉ IP nguồn và đích, số cổng và có thể được sử dụng để phân tích một cuộc tấn công.
- *Nhật ký bộ lọc web*: cho thấy người dùng đang cố gắng truy cập vào các URL bị hạn chế và cách hệ thống phản hồi.

6. Lệnh *xhydra*

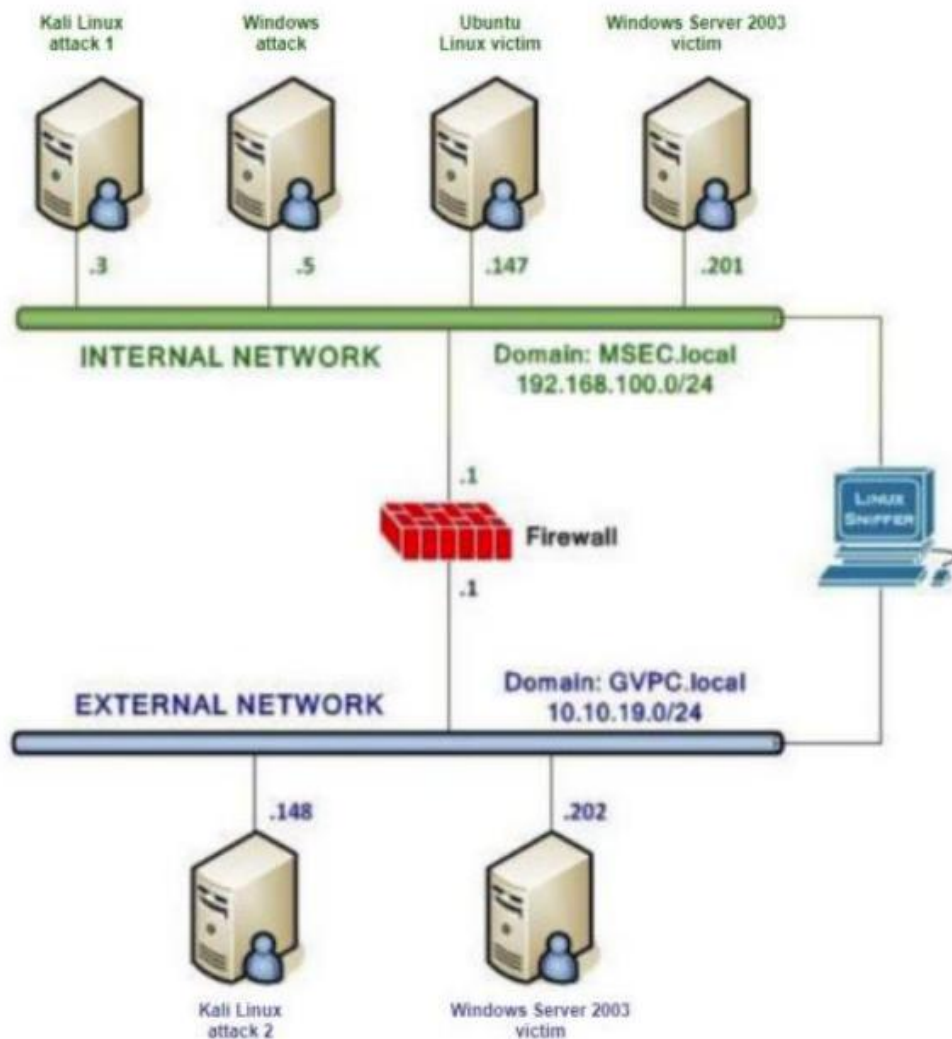
xhydra là một công cụ phục vụ cho việc tấn công từ điển (*brute-force*) trong nhiều giao thức khác nhau như SSH (*Secure Shell*), FTP (*File Transfer Protocol*), Telnet,.... Một số tính năng chính của *xhydra*:

- *Tấn công từ điển đa giao thức*: *xhydra* cho phép thực hiện các cuộc tấn công từ điển trên nhiều giao thức như SSH, FTP, Telnet, MySQL, SMB,...
- *Hỗ trợ tùy chỉnh từ điển*: có thể chỉ định các từ điển hoặc tập hợp từ để sử dụng trong cuộc tấn công từ điển.
- *Tùy chọn cấu hình phong phú*: *xhydra* cung cấp một loạt các tùy chọn cấu hình để điều chỉnh cách thức thực hiện các cuộc tấn công, bao gồm số lần thử, thời gian giữa các thử nghiệm, và nhiều hơn nữa.
- *Giao diện đồ họa*: *xhydra* được thiết kế với giao diện đồ họa (*GUI*) để dễ dàng sử dụng và cấu hình.
- *Hỗ trợ hàng loạt giao thức*: có thể tấn công từ điển trên nhiều loại giao thức mạng phổ biến, giúp kiểm tra tính bảo mật của các hệ thống mạng.

CHƯƠNG 2 : NỘI DUNG THỰC HÀNH

I. Chuẩn bị môi trường

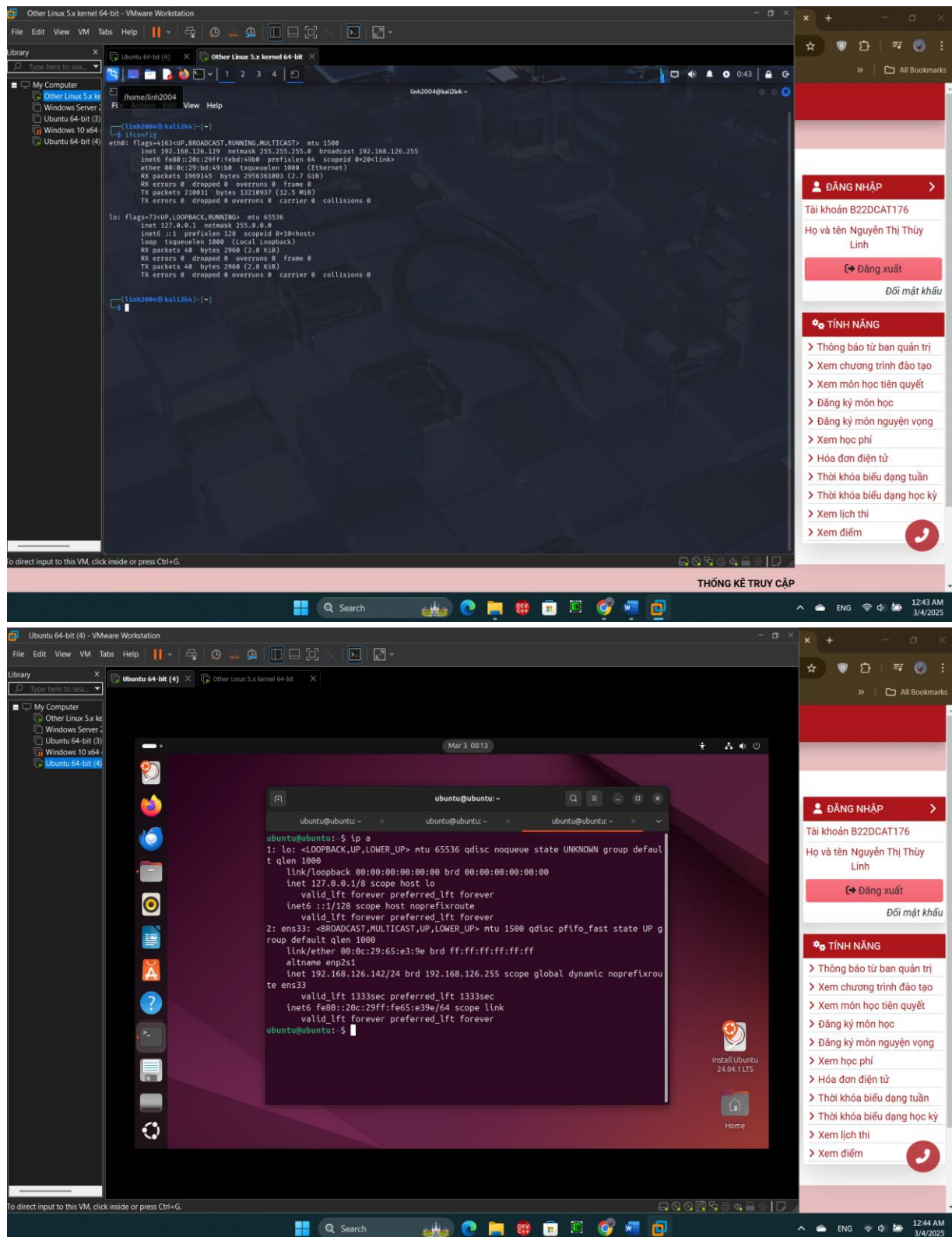
- Các file máy ảo VMWare và hệ thống mạng đã cài đặt trong bài lab trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux.
- Download máy trạm Windows 7 (hoặc Windows 10/11)
- Download phần mềm máy ảo : VMWare Workstation.
- Topo mạng như đã cấu hình trong bài 5.



II. Các bước thực hiện

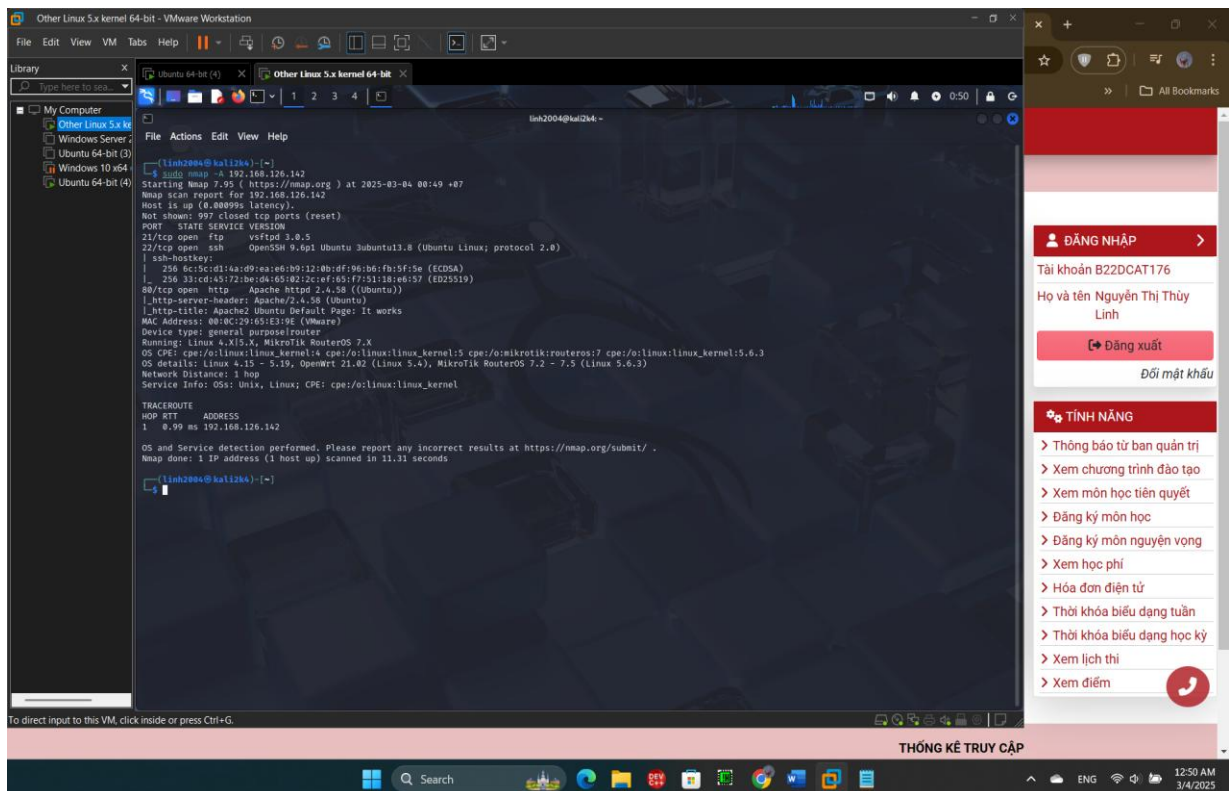
a. Phân tích log sử dụng grep trong Linux

- Kiểm tra IP của 2 máy Kali Linux và Ubuntu.



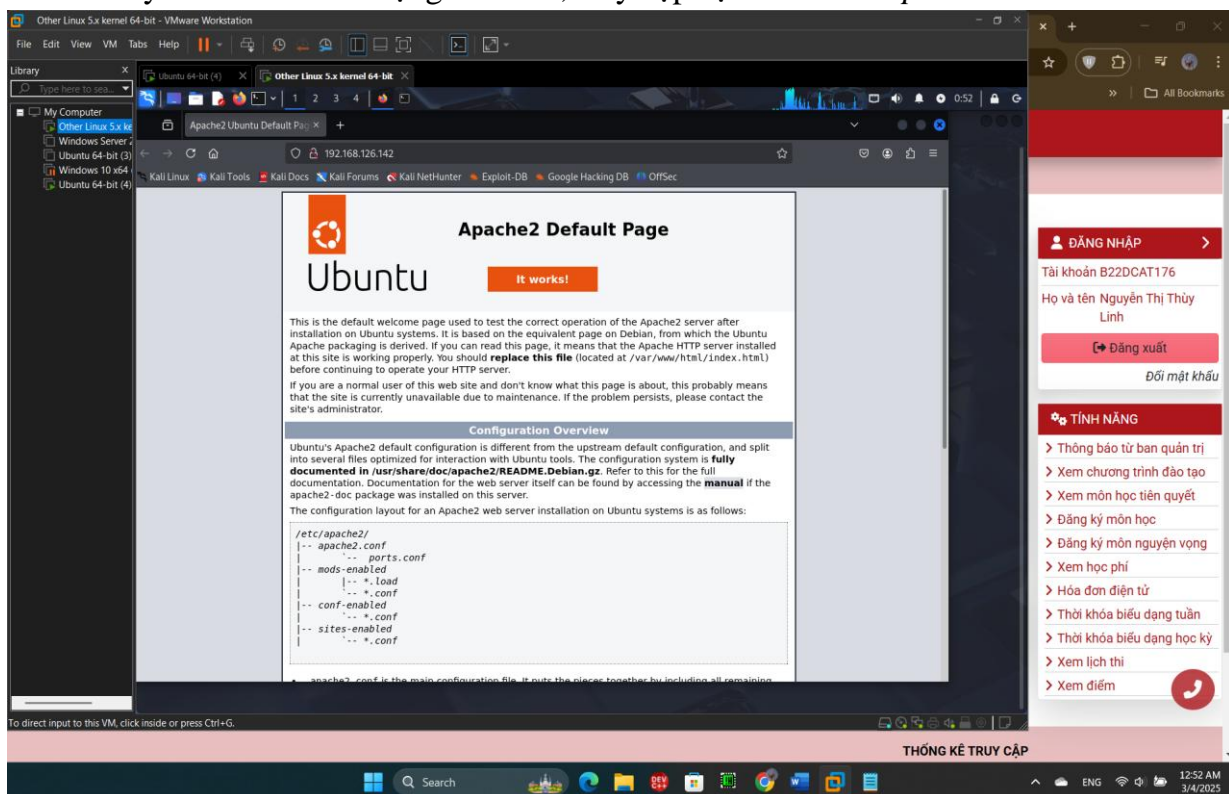
Hình ảnh 4 : Kiểm tra IP của 2 máy Ubuntu và Kali Linux

- Trên máy Kali Attack trong mạng Internal, khởi chạy Zenmap và scan cho địa chỉ 192.168.126.142 (Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.4.58



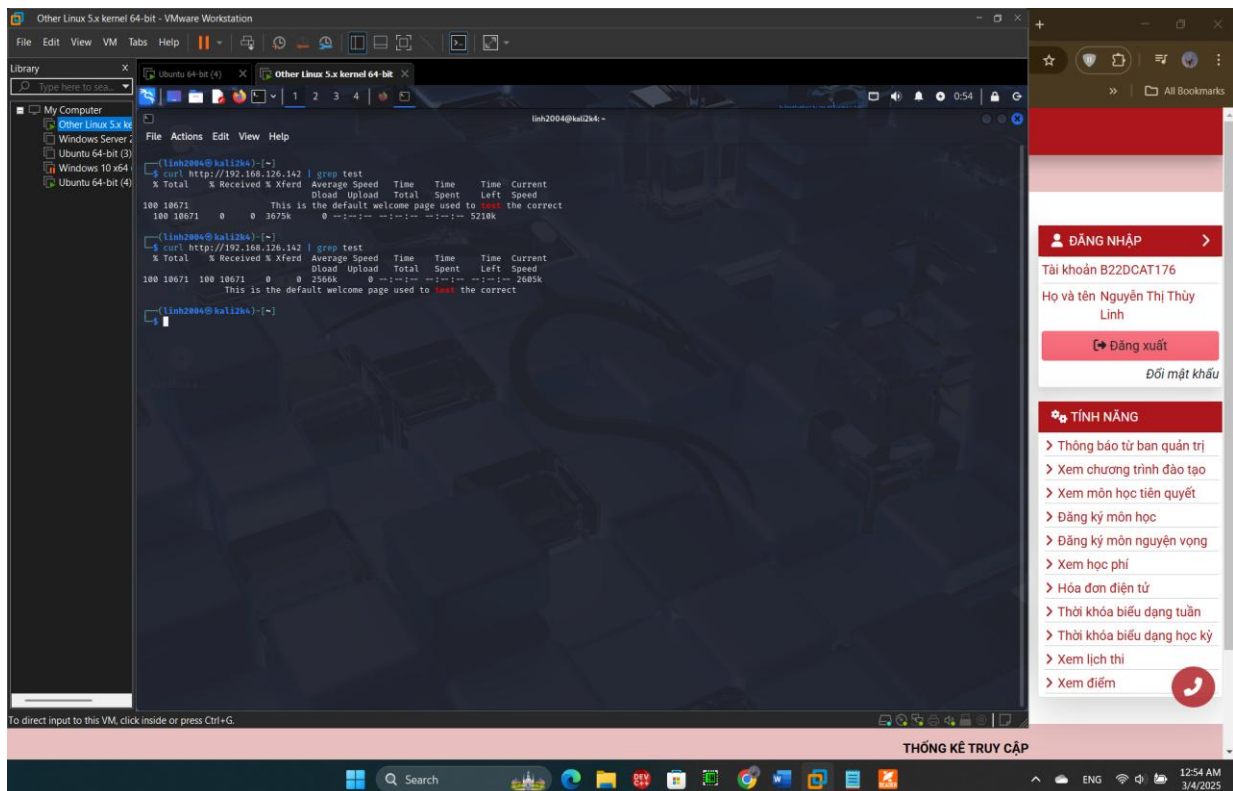
Hình ảnh 5 : Khởi chạy Zenmap

- Trên máy Kali Attack ở mạng Internal, truy cập địa chỉ web <http://192.168.126.142>



Hình ảnh 6 : Truy cập địa chỉ web 192.168.126.142

- Trên Terminal tiến hành sao chép website và tìm kiếm từ khóa “test”: `curl http://192.168.126.142 | grep test`

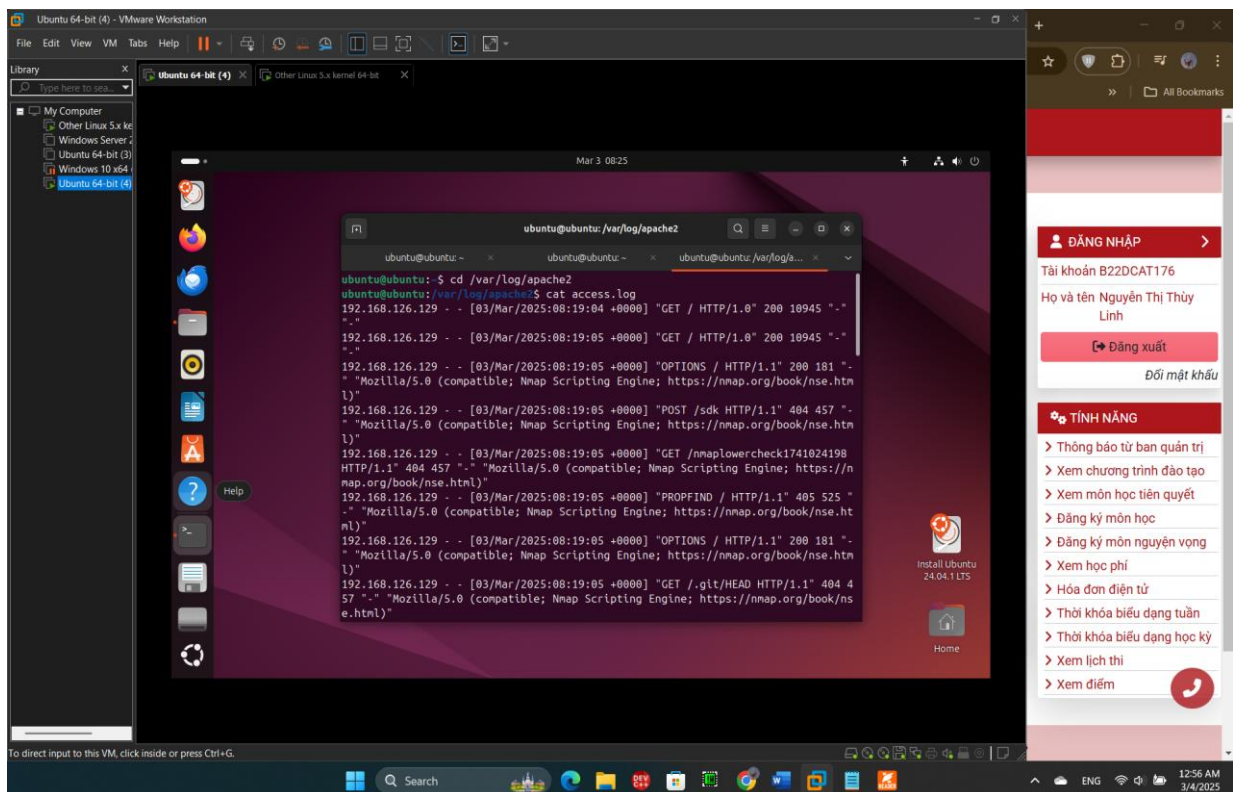


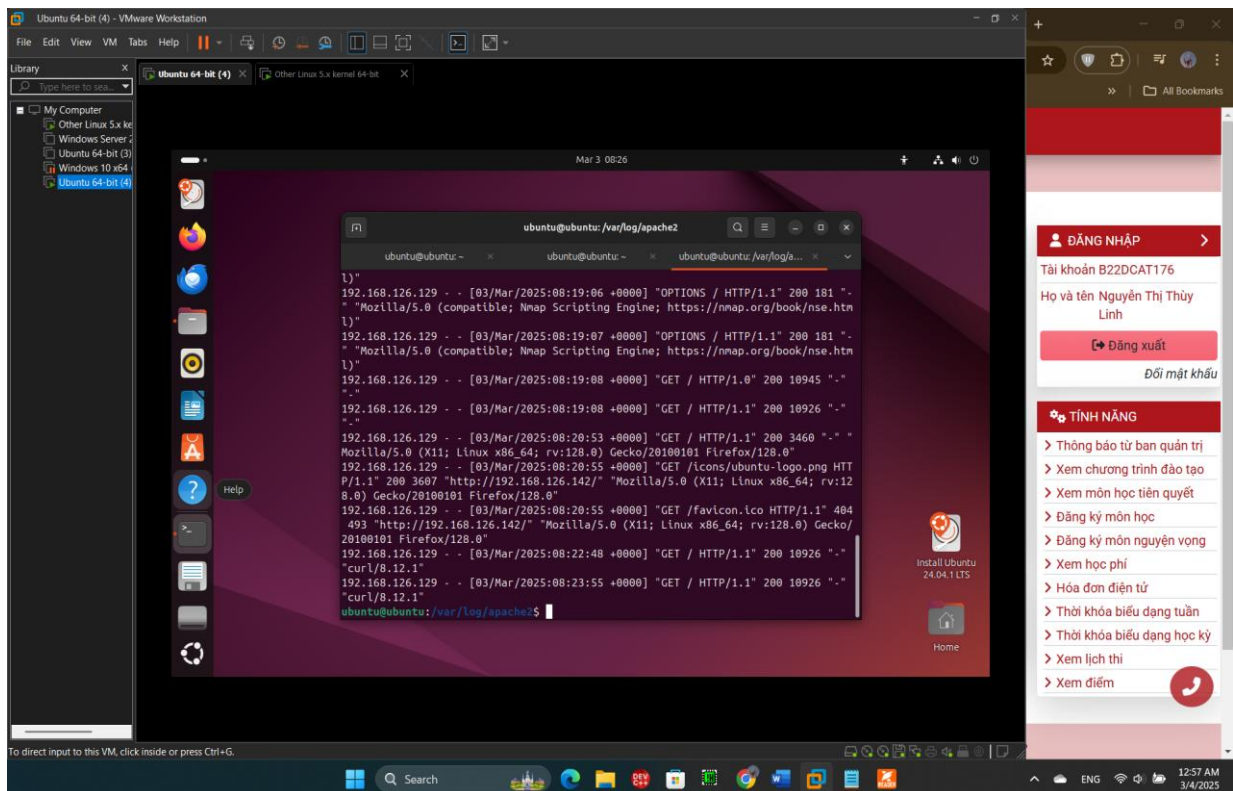
Hình ảnh 7 : Sao chép website và tìm kiếm từ khóa “test”

-Trên máy Linux Internal Victim, để xem access.log dùng lệnh:

`cd /var/log/apache2`

`cat access.log`

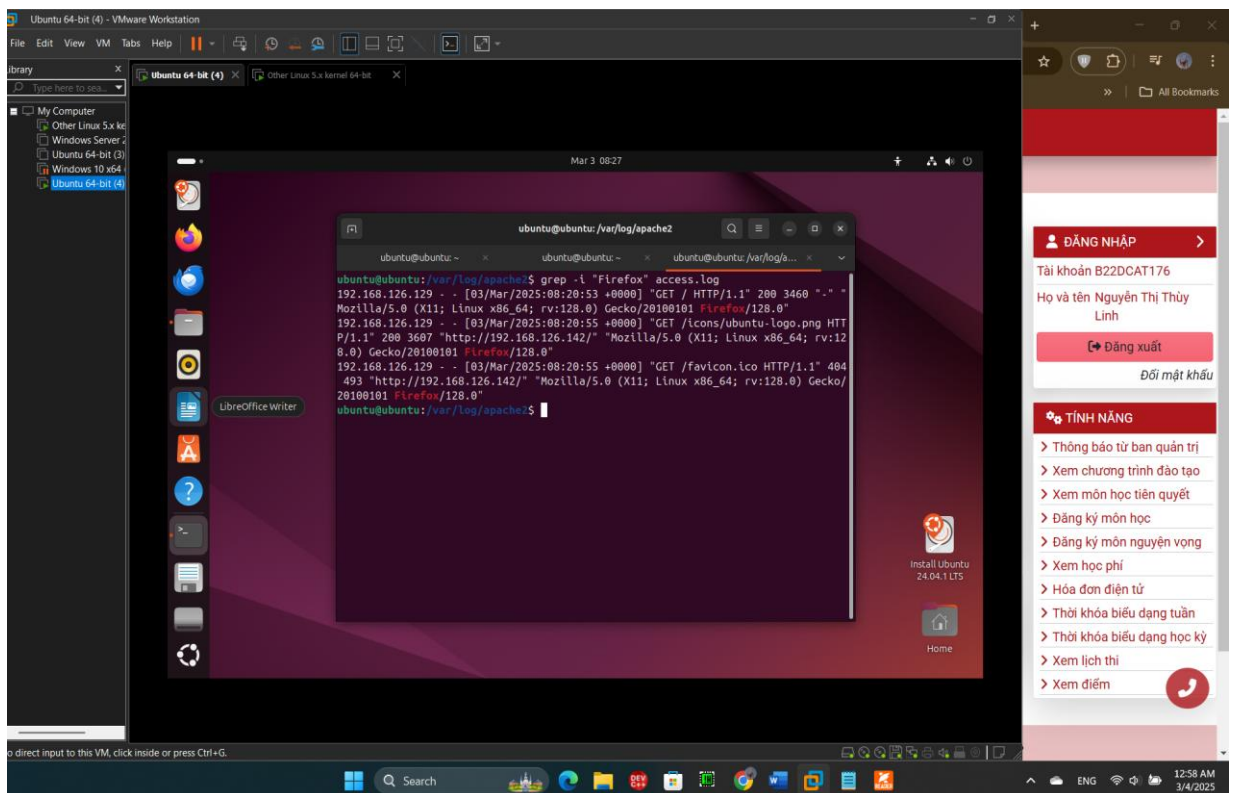




Hình ảnh 8: Xem nội dung access.log

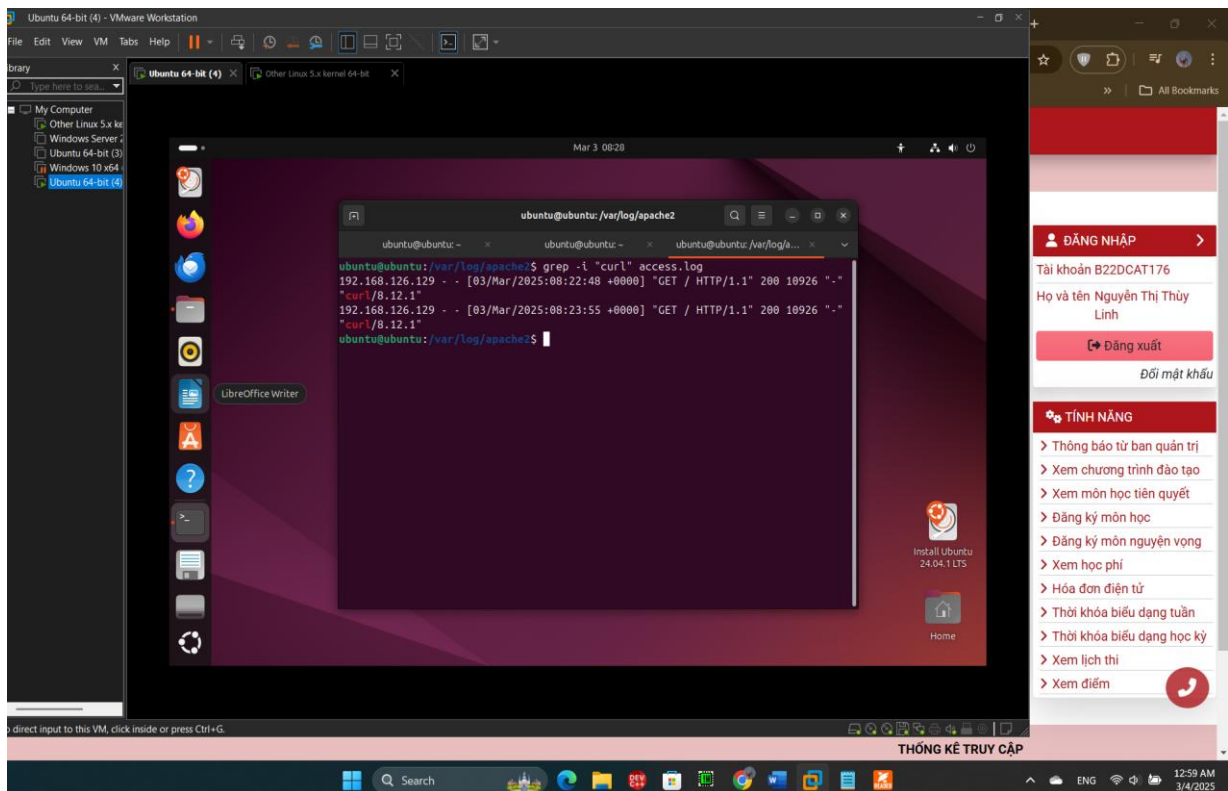
- Khi đã mở được file access_log trên máy nạn nhân, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm như: Nmap, Firefox,...

- Firefox:



Hình ảnh 9: Lọc kết quả với từ khóa tìm kiếm Firefox.

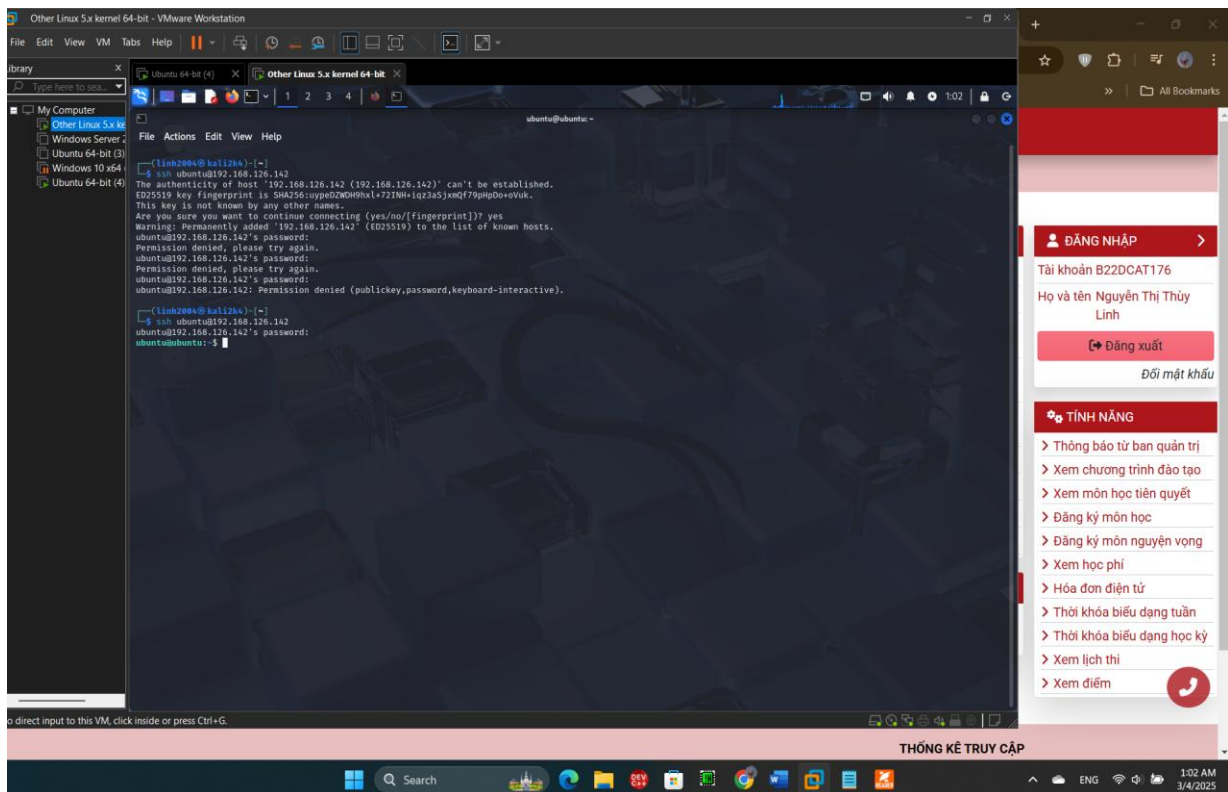
- Curl:



Hình ảnh 10: Lọc kết quả với từ khóa tìm kiếm curl.

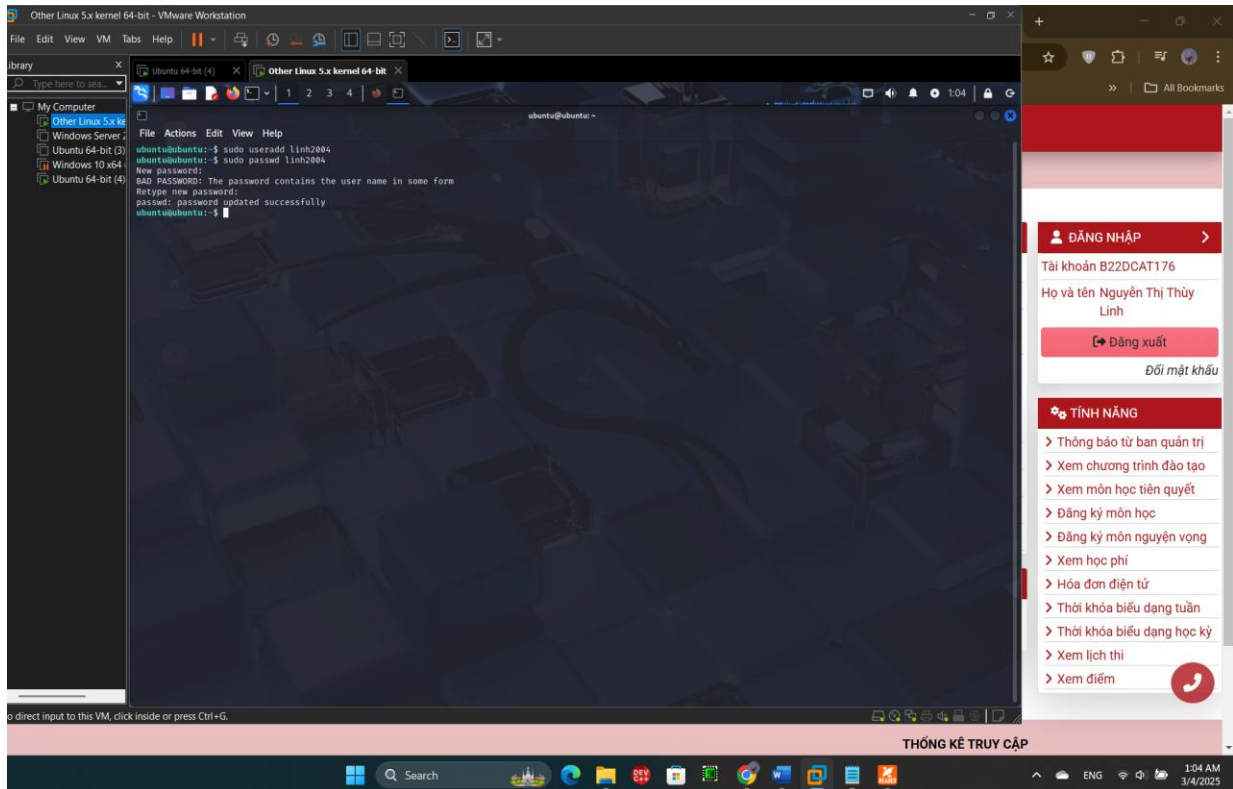
b. Phân tích log sử dụng gawk trong Linux

- 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.



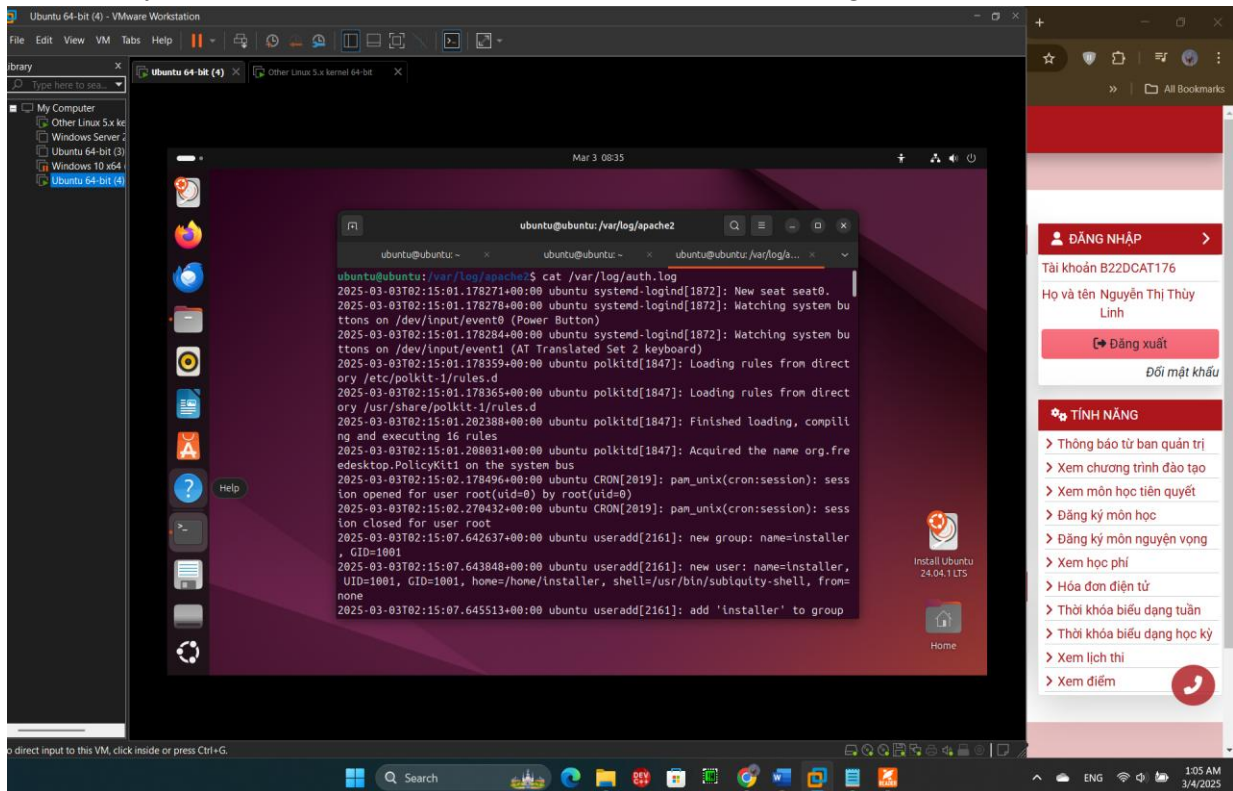
Hình ảnh 11: Remote sang máy Linux thành công.

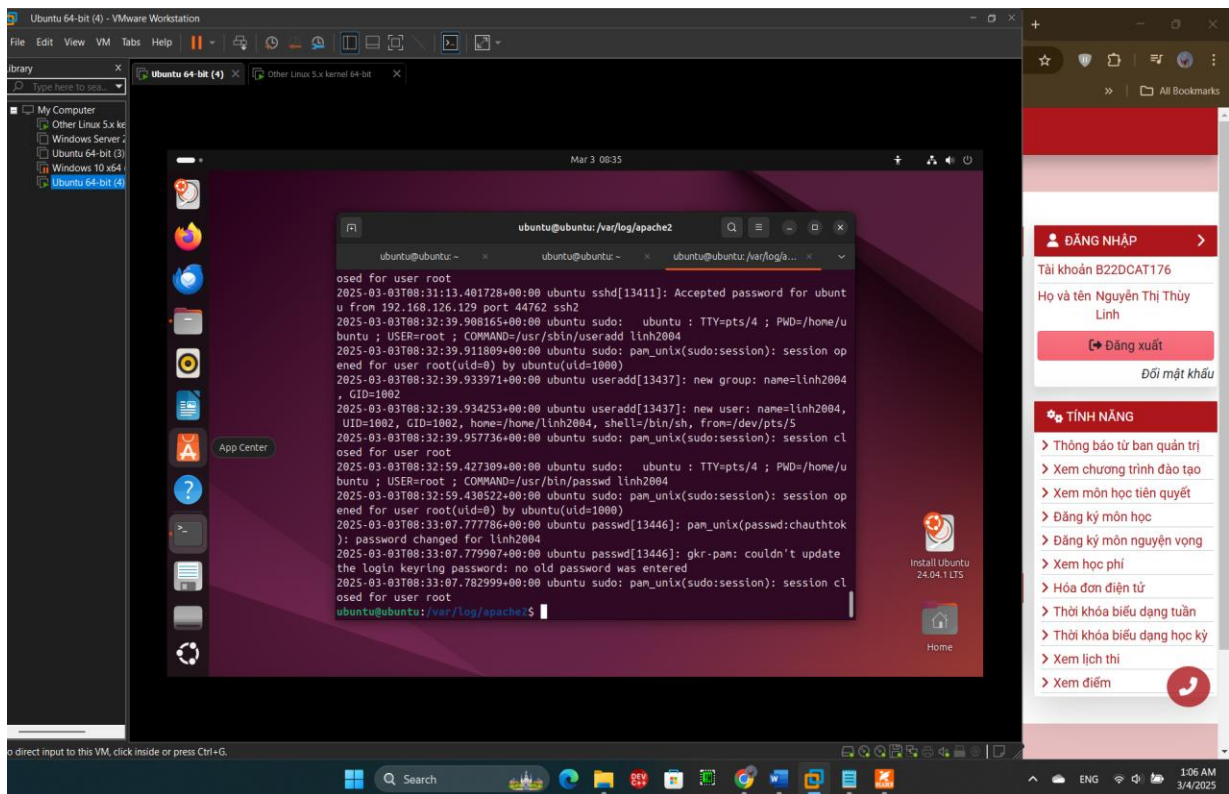
- Tạo user mới : *linh2004*



Hình ảnh 12: Tạo user mới *linh2004* thành công.

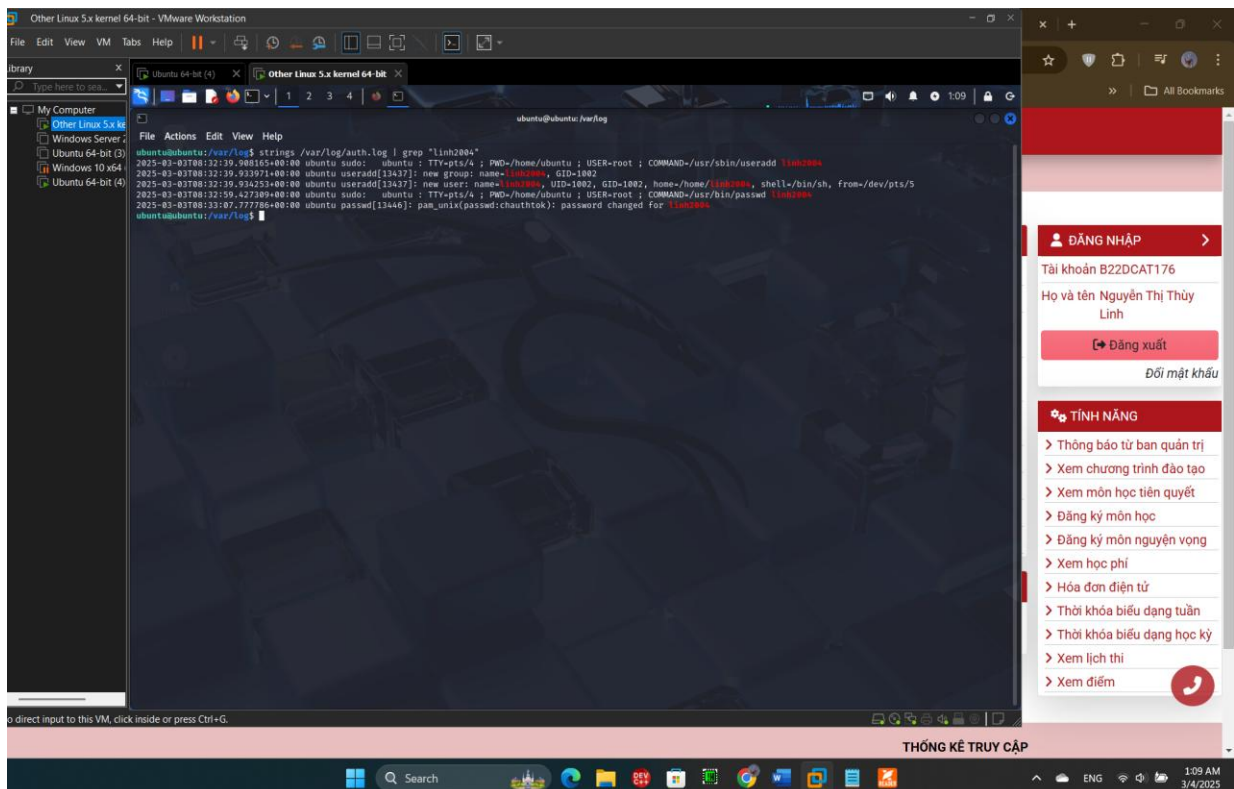
- Trên máy Linux Internal Victim, tiến hành xem file *auth.log*





Hình ảnh 13 :Tiến hành xem file auth.log

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

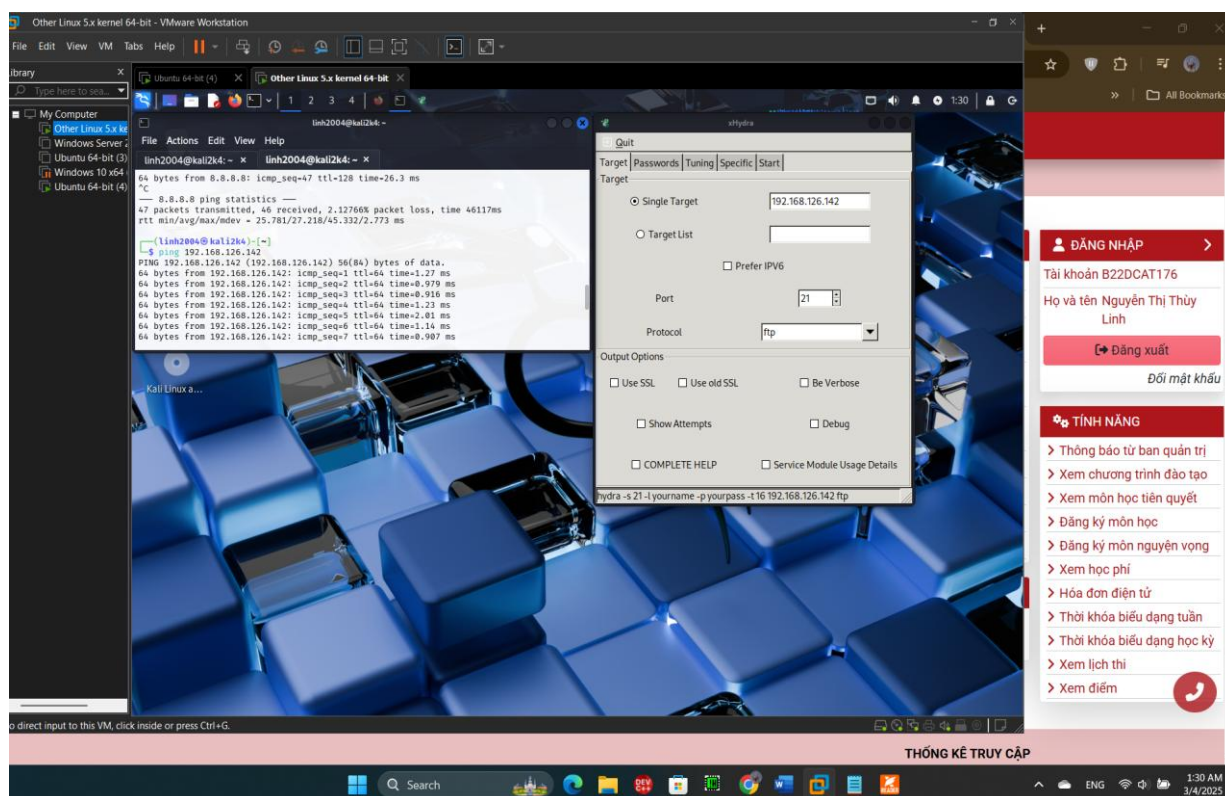


Hình ảnh 14 : Tìm kiếm người dùng vừa tạo bằng grep.

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

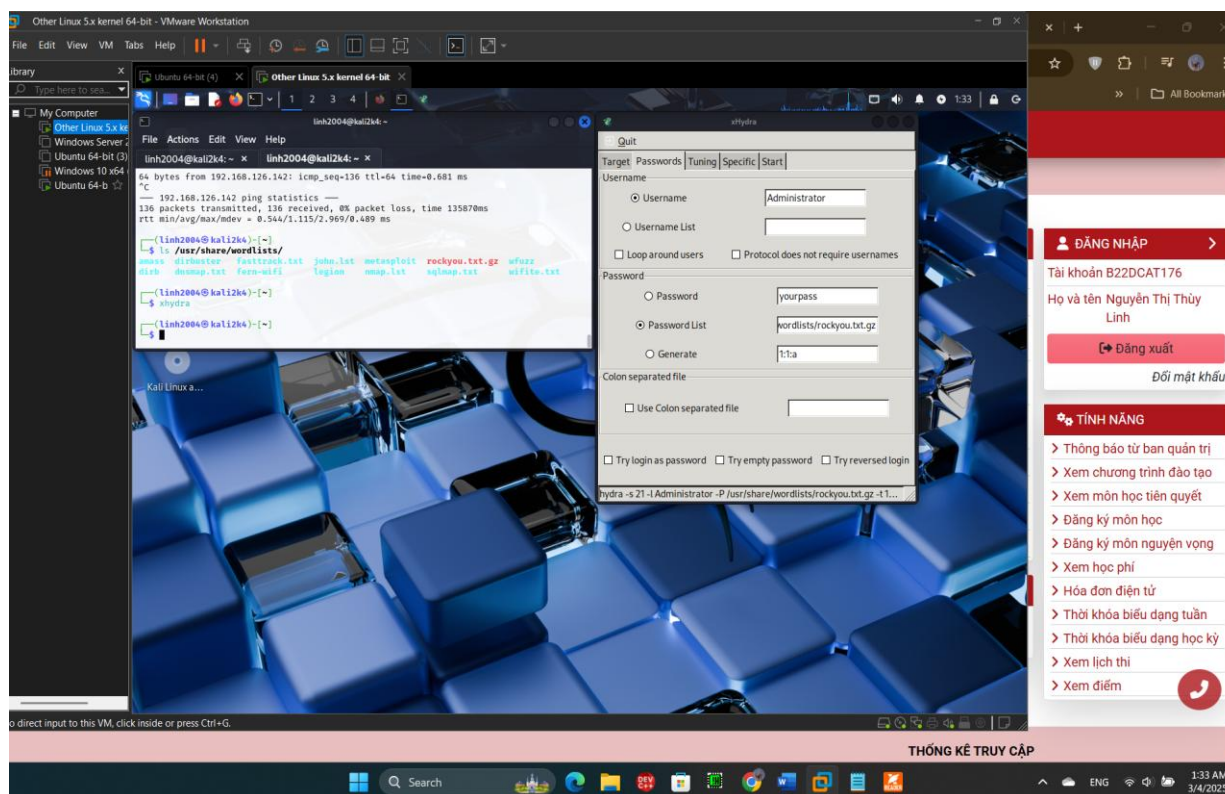
gawk 'linh2004/' /var/log/auth.log

-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.



Hình ảnh 17 : Bắt đầu cấu hình xHydra.

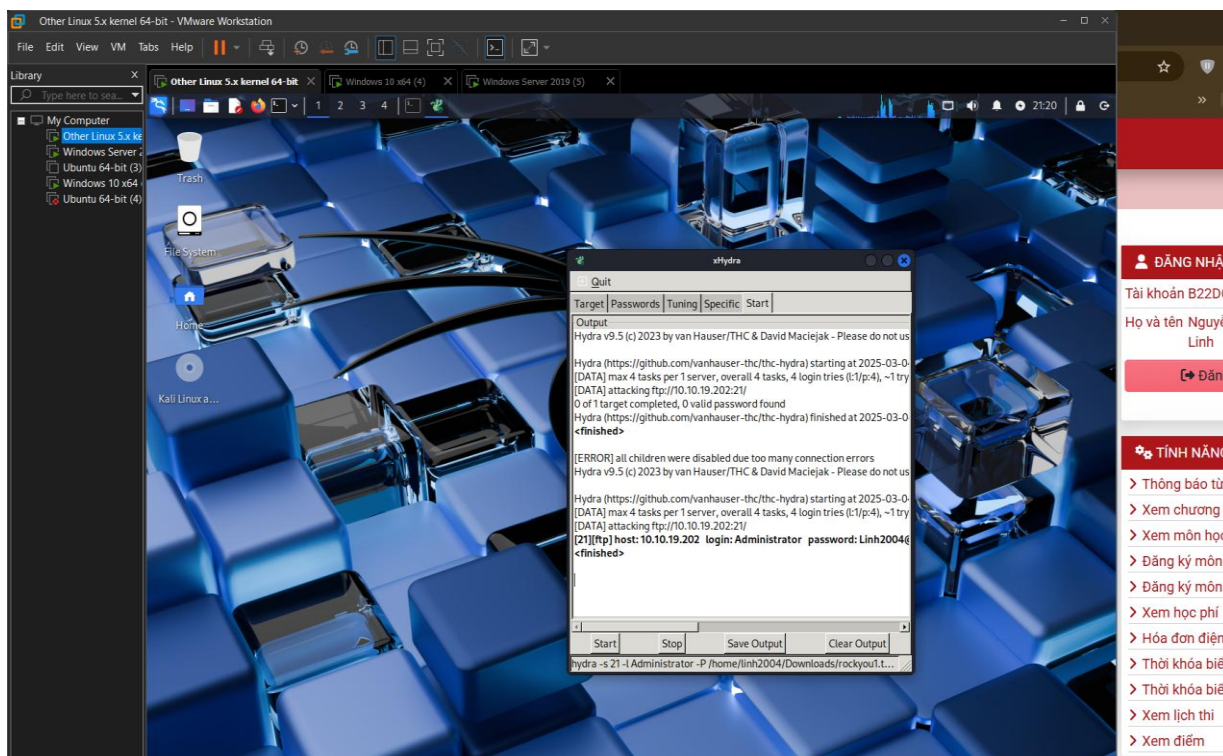
-Tạo 1 file rockyou1.txt chứa nhiều mật khẩu, trong đó có mật khẩu của tài khoản định sử dụng xHydra để bẻ mật khẩu.



Hình ảnh 18 : Chọn file mật khẩu

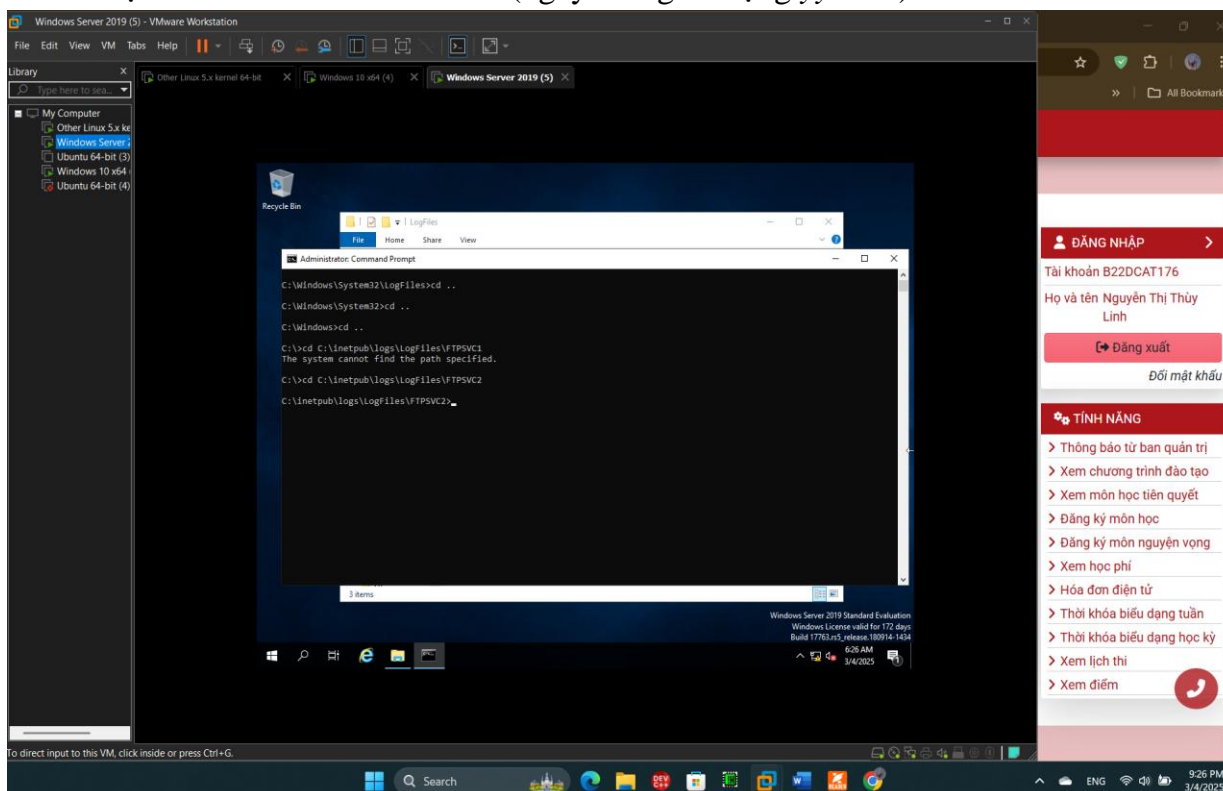
(File rockyou1.txt là file chỉnh sửa của file rockyou.txt.gz như trong ảnh)

- Trên Windows Server, thay đổi IP thành *10.10.19.202* và đổi *Defaule Gateway* thành *10.10.19.1* và thử *ping 10.10.19.202* trên máy Kali Linux đến khi ping được thì bắt đầu ấn “*Start*” trong xHydra. Như trong hình, sau khi Start chúng ta thu được password của tài khoản *Administrator* là *Linh2004@*.



Hình ảnh 19 : Lấy được mật khẩu của tài khoản *Administrator*.

- Trên máy Windows 2019 Server External Victim, thực hiện điều hướng đến FTP Logfile (“*cd 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 *yymmđ*).

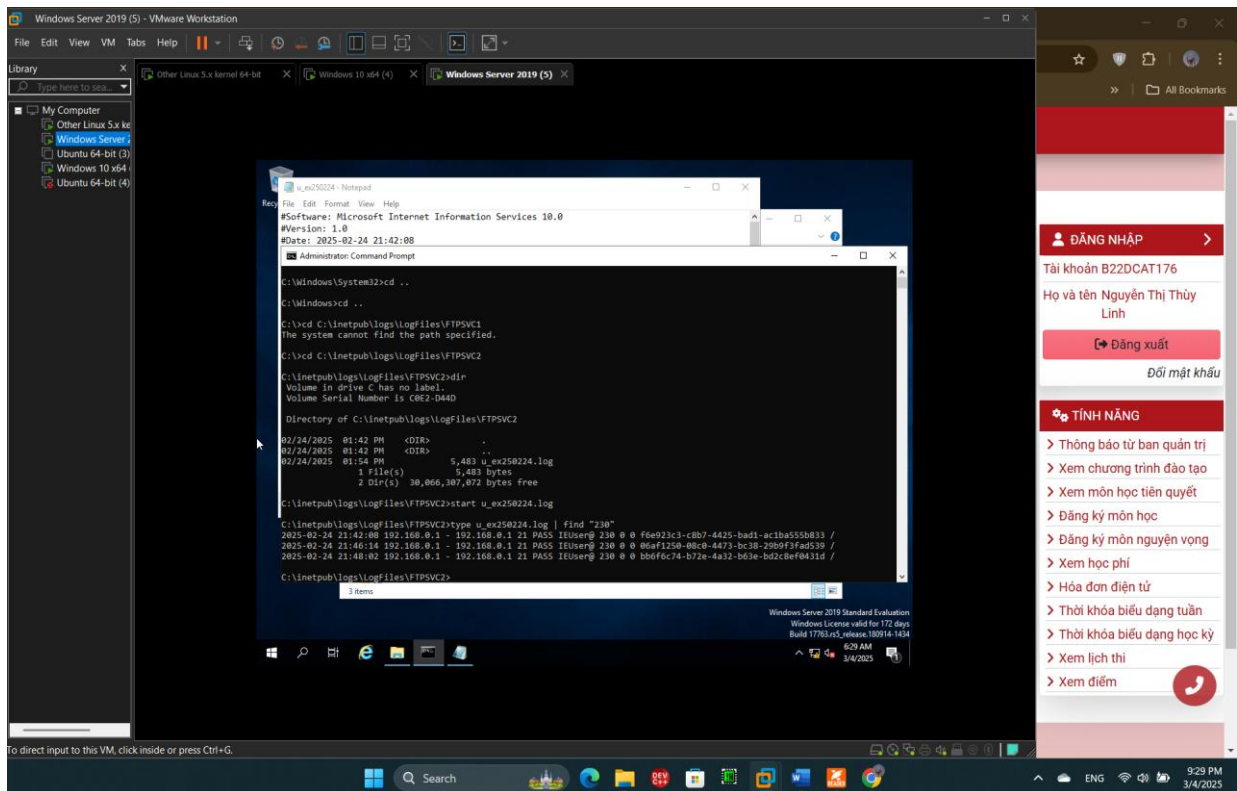


- Hiển thị tất cả các file log đang có bằng lệnh “*dir*”.

[illegible]

19

-Tìm kiếm kết quả tấn công login thành công bằng lệnh: `type u_ex250224.log | find "230"`.



Hình ảnh 23: Kết quả đạt được sau khi tấn công login.

III. Kết quả đạt được

- Học cách sao lưu tới ổ đĩa mạng.
- Sao lưu tệp qua FTP Server
- Chia sẻ file an toàn bằng SCP (Secure Copy)

TÀI LIỆU THAM KHẢO

- [1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.