

**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:

B22DCAT063 Lê Tiến Dương

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 VẼ.....	3
DANH MỤC CÁC TỪ VIẾT TẮT.....	4
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	5
1.1 Mục đích.....	5
1.2 Tìm hiểu lý thuyết	5
1.2.1 Tìm hiểu về Windows Event Viewer và auditing	5
1.2.2 Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log	7
1.2.3 Tìm hiểu về Xhydra.....	8
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	9
2.1 Chuẩn bị môi trường	9
2.2 Các bước thực hiện.....	11
2.2.1 Phân tích log sử dụng grep trong Linux	11
2.2.2 Phân tích log sử dụng gawk trong Linux	15
2.2.3 Phân tích log sử dụng find trong Windows	17
TÀI LIỆU THAM KHẢO	21

DANH MỤC CÁC HÌNH VẼ

Hình 1 – Giao diện Windows Event Viewer.....	5
Hình 2 – Topo mạng đã được cấu hình	9
Hình 3 – Máy Ubuntu Linux Victim.....	10
Hình 4 – Máy Kali Linux attack 1.....	10
Hình 5 – Máy Kali Linux attack 2.....	11
Hình 6 – Máy Windows Server victm thuộc External Network	11
Hình 7 – Cài đặt apache2 trên máy Ubuntu	12
Hình 8 – Kiểm tra trạng thái của apache2 trên máy Ubuntu.....	12
Hình 9 – Kết quả sau khi scan.....	13
Hình 10 – Truy cập địa chỉ web trên máy Kali attack 1.....	13
Hình 11 – Sao chép website và tìm kiếm	14
Hình 12 – Mở thư mục chứa access_log, đọc và lọc kết quả theo từ khóa	14
Hình 13 – Tiến hành remote vào máy Linux Internal Victim	15
Hình 14 – Tạo user mới và đổi mật khẩu	15
Hình 15 – Xem file log trên máy Linux Internal Victim	16
Hình 16 – Dùng lệnh grep tìm kiếm người dùng vừa tạo	16
Hình 17 – Sử dụng lệnh gawk.....	17
Hình 18 – Khởi động #xhydra trên máy Kali External Attack	17
Hình 19 – Tạo file password_list	18
Hình 20 – Nhập Username và chọn đường dẫn đến file password_list	18
Hình 21 – xHydra tìm được mật khẩu.....	19
Hình 22 – Điều hướng đến FTP Logfile và mở file log mới nhất.....	19
Hình 23 – Gõ lệnh để tìm kiếm kết quả login thành công	20

DANH MỤC CÁC TỪ VIẾT TẮT

[illegible]

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Mục đích của bài thực hành “1.6: Phân tích log hệ thống” là giúp sinh viên nắm được 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

1.2 Tìm hiểu lý thuyết

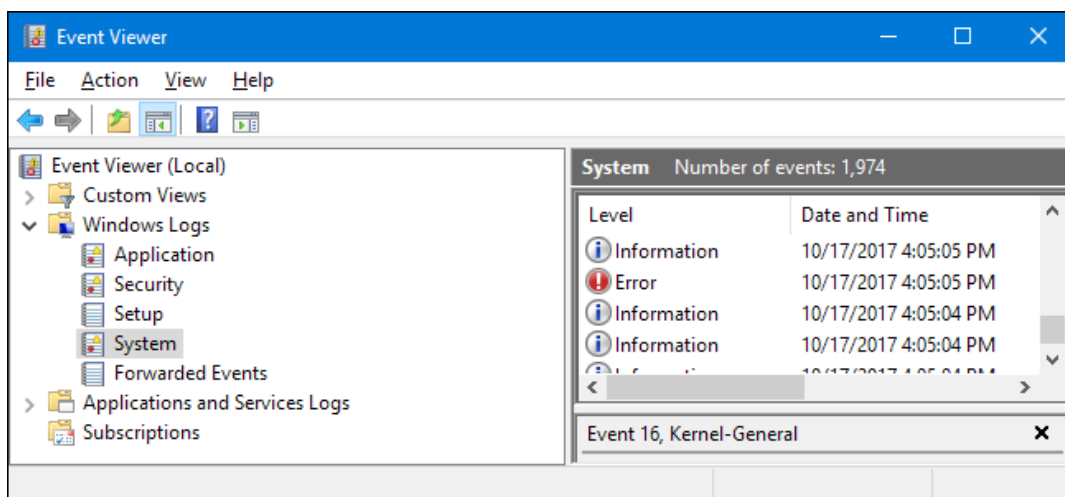
1.2.1 Tìm hiểu về Windows Event Viewer và auditing

1.2.1.1 Windows Event Viewer

Windows Event Viewer là một công cụ tích hợp trong hệ điều hành Windows, cho phép người dùng xem và phân tích các bản ghi sự kiện (event logs) do hệ thống, ứng dụng hoặc phần cứng tạo ra. Công cụ này đóng vai trò quan trọng trong quản trị hệ thống, khắc phục sự cố, giám sát bảo mật và phân tích hiệu suất.

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 1 – Giao diện Windows Event Viewer

Phân loại mức độ sự kiện:

- *Information*: Hoạt động bình thường.
- *Warning*: Vấn đề tiềm ẩn.
- *Error*: Lỗi ảnh hưởng hệ thống/ ứng dụng.

- *Critical*: Lỗi nghiêm trọng.
- *Audit Success/Failure*: Thành công/ Thất bại trong việc kiểm tra bảo mật.

Ưu điểm của Windows Event Viewer:

- *Tích hợp sẵn*: Không cần cài đặt thêm phần mềm.
- *Chi tiết và toàn diện*: Ghi lại mọi hoạt động từ hệ thống, ứng dụng, bảo mật.
- *Giao diện thân thiện*: Dễ sử dụng với khả năng lọc và tìm kiếm.
- *Hỗ trợ mạng*: Thu thập log từ nhiều máy trong domain.

Windows Event Viewer là công cụ mạnh mẽ và không thể thiếu để quản lý và phân tích log trên Windows. Nó cung cấp khả năng giám sát toàn diện, từ lỗi hệ thống đến bảo mật, hỗ trợ quản trị viên trong việc duy trì hệ thống ổn định và an toàn. Tuy nhiên, để khai thác hiệu quả, người dùng cần hiểu cách lọc và tra cứu Event ID.

1.2.1.2 Auditing

Auditing (Kiểm tra) trong lĩnh vực công nghệ thông tin là quá trình ghi lại, theo dõi và phân tích các sự kiện hoặc hành động xảy ra trong hệ thống máy tính, mạng hoặc ứng dụng nhằm đảm bảo tính bảo mật, tuân thủ quy định và phát hiện các vấn đề bất thường. Auditing thường được thực hiện thông qua các công cụ tích hợp sẵn (như Windows Event Viewer) hoặc phần mềm chuyên dụng.

Mục đích của Auditing:

- Giám sát hoạt động của người dùng (đăng nhập, truy cập tệp).
- Phát hiện hành vi đáng nghi (xâm nhập, lạm dụng quyền).
- Đáp ứng yêu cầu pháp lý hoặc tiêu chuẩn bảo mật (ISO 27001, GDPR).

Các loại kiểm tra phổ biến:

- **Audit Logon Events**: Theo dõi đăng nhập/ đăng xuất.
- **Audit Object Access**: Ghi lại truy cập tệp/ thư mục.
- **Audit Policy Change**: Theo dõi thay đổi chính sách bảo mật.
- **Audit Process Tracking**: Giám sát việc tạo/ kết thúc tiến trình.

Ứng dụng thực tế của Auditing:

- *Bảo mật hệ thống*: Phát hiện đăng nhập trái phép. Security Log ghi lại địa chỉ IP và thời gian đăng nhập thất bại.
- *Quản lý tài nguyên*: Theo dõi ai đã truy cập hoặc sửa đổi tệp quan trọng (Audit Object Access).
- *Tuân thủ quy định*: Cung cấp bằng chứng kiểm tra cho các tiêu chuẩn như HIPAA, PCI DSS.

- **Khắc phục sự cố:** Xác định nguyên nhân lỗi hệ thống bằng cách phân tích log kiểm tra.

Auditing là một công cụ quan trọng trong quản trị hệ thống và bảo mật, giúp ghi lại và phân tích các sự kiện để bảo vệ dữ liệu, phát hiện sự cố và đảm bảo tuân thủ. Trong Windows, nó được triển khai dễ dàng qua Event Viewer và Local Security Policy, trong khi Linux cung cấp giải pháp mạnh mẽ hơn với auditd. Để sử dụng hiệu quả, cần cân nhắc loại sự kiện kiểm tra và quản lý dung lượng log.

1.2.2 Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log

1.2.2.1 Lệnh grep

grep (Global Regular Expression Print) là một công cụ dòng lệnh trong Linux/Unix dùng để tìm kiếm các chuỗi văn bản hoặc mẫu (pattern) trong tệp hoặc đầu ra của lệnh khác. Nó hỗ trợ biểu thức chính quy (regular expression) để lọc dữ liệu theo cách linh hoạt. Lệnh này được dùng để lọc nhanh các dòng log chứa các từ khóa cụ thể (lỗi, cảnh báo) hoặc thông tin cần tìm.

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

Ví dụ: *grep "error" /var/log/syslog* . Lệnh này tìm tất cả các dòng chứa từ “error” trong tệp log hệ thống */var/log/syslog*.

Ứng dụng: Phát hiện lỗi hệ thống, tìm kiếm truy cập bất thường trong log máy chủ.

Ưu điểm: Nhanh, dễ sử dụng, hỗ trợ tìm kiếm nâng cao với regex.

1.2.2.2 Lệnh gawk

gawk là phiên bản GNU của *awk*, một ngôn ngữ xử lý văn bản và công cụ dòng lệnh trong Linux/Unix. Nó được dùng để phân tích và trích xuất dữ liệu từ các tệp có cấu trúc (như log) bằng cách chia nhỏ dòng thành các trường (field) dựa trên dấu phân cách. Lệnh này được dùng để trích xuất thông tin chi tiết như thời gian, địa chỉ IP, hoặc mã trạng thái từ log.

Ví dụ: *gawk '{print \$1, \$4}' /var/log/auth.log* . Lệnh này in trường đầu tiên (thường là ngày) và trường thứ tư (thời gian) từ tệp log xác thực.

Ứng dụng: Phân tích log máy chủ web (access log), thống kê hành vi người dùng.

Ưu điểm: Xử lý dữ liệu có cấu trúc tốt, hỗ trợ lập trình logic phức tạp.

1.2.2.3 Lệnh find

find là một lệnh trong Linux/Unix dùng để tìm kiếm tệp hoặc thư mục trong hệ thống tệp dựa trên các tiêu chí như tên, kích thước, thời gian sửa đổi, v.v.

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

Ví dụ: *find /var/log -name "*.log" -mtime +7* . Lệnh này tìm các tệp *.log* trong */var/log* được sửa đổi cách đây hơn 7 ngày.

Ứng dụng: Quản lý không gian lưu trữ log, tìm log liên quan đến sự cố cụ thể.

Ưu điểm: Linh hoạt, hiệu quả khi cần tìm tệp trong nhiều thư mục.

1.2.2.4 *secure*

secure là tên tệp log, thường là `/var/log/secure`, xuất hiện trong các hệ thống dựa trên Red Hat (như CentOS, RHEL). Tệp này ghi lại các sự kiện bảo mật như đăng nhập SSH, thay đổi quyền, hoặc xác thực người dùng. *Secure* theo dõi các hoạt động bảo mật để phát hiện xâm nhập hoặc lỗi xác thực.

Ví dụ: `cat /var/log/secure | grep "Failed password"`. Lệnh này lọc các dòng liên quan đến đăng nhập thất bại trong `/var/log/secure`.

Ứng dụng: Kiểm tra bảo mật hệ thống, phát hiện truy cập trái phép.

Ưu điểm: Tập trung vào dữ liệu bảo mật, dễ phân tích với các công cụ như `grep`.

1.2.2.5 *access_log*

access_log là tên tệp log phổ biến trong máy chủ web (Apache, Nginx), thường nằm tại `/var/log/apache2/access.log` hoặc `/var/log/nginx/access.log`. Tệp này ghi lại mọi yêu cầu truy cập (HTTP requests) đến máy chủ, bao gồm địa chỉ IP, thời gian, URL, mã trạng thái. Cung cấp thông tin về lưu lượng truy cập web, phát hiện lỗi hoặc hành vi bất thường.

Ví dụ: `grep "404" /var/log/apache2/access.log`. Lệnh này tìm các yêu cầu trả về mã lỗi 404 (Not Found).

Ứng dụng: Phân tích hiệu suất web, phát hiện tấn công DDoS, tối ưu trải nghiệm người dùng.

Ưu điểm: Chi tiết về hoạt động web, dễ tích hợp với công cụ phân tích.

1.2.3 *Tìm hiểu về Xhydra*

XHydra là phiên bản giao diện đồ họa (GUI) của Hydra, một công cụ mã nguồn mở dùng để tấn công brute-force (dò mật khẩu) trên các giao thức mạng như SSH, FTP, HTTP, v.v. Nó được thiết kế để kiểm tra bảo mật bằng cách thử nhiều tổ hợp tên người dùng và mật khẩu, thường được sử dụng bởi các chuyên gia bảo mật hoặc hacker mũ trắng.

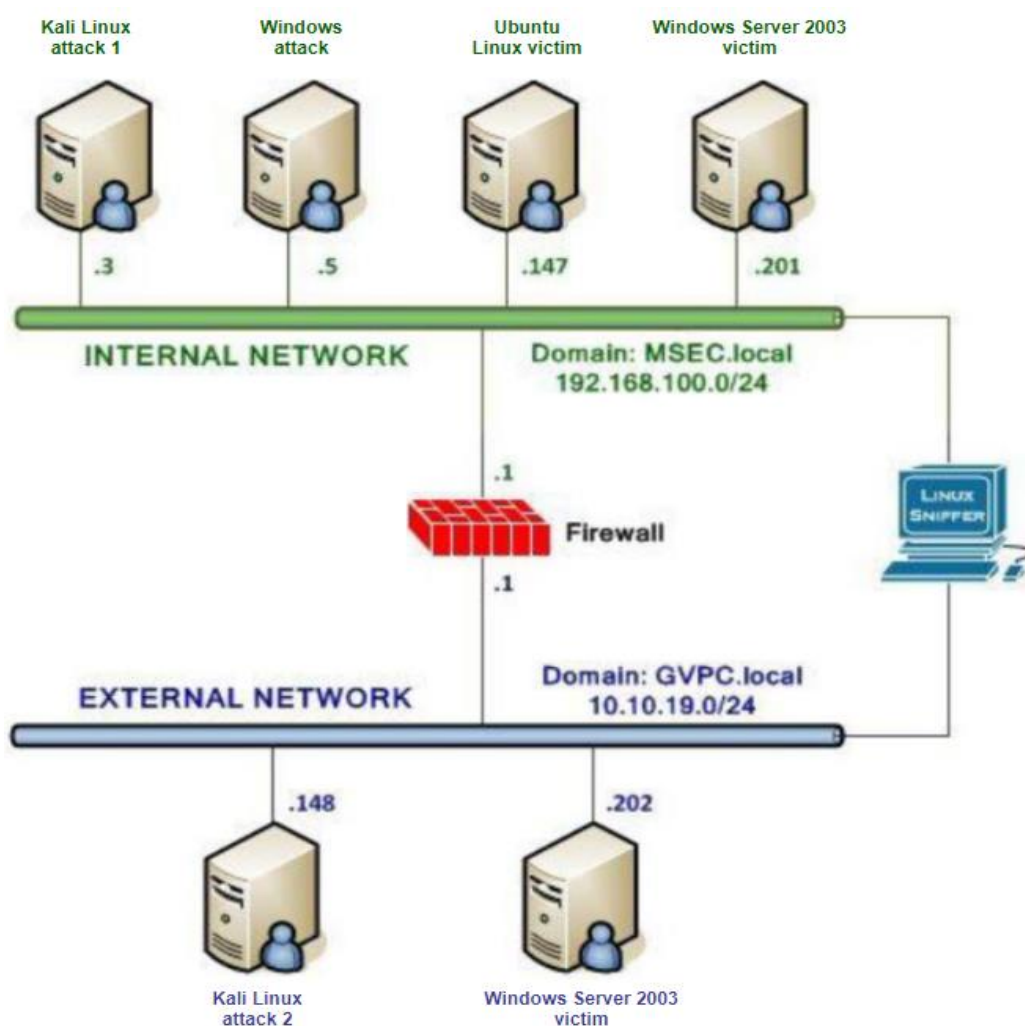
Ý nghĩa và ứng dụng:

- **Ý nghĩa:** Cung cấp giao diện trực quan thay vì dòng lệnh như Hydra, giúp người dùng dễ dàng cấu hình mục tiêu, danh sách mật khẩu và giao thức.
- **Ứng dụng:**
 - Kiểm tra độ mạnh của mật khẩu trên hệ thống.
 - Phát hiện lỗ hổng bảo mật trong các dịch vụ mạng.
 - Hỗ trợ pen-testing (kiểm tra xâm nhập).

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

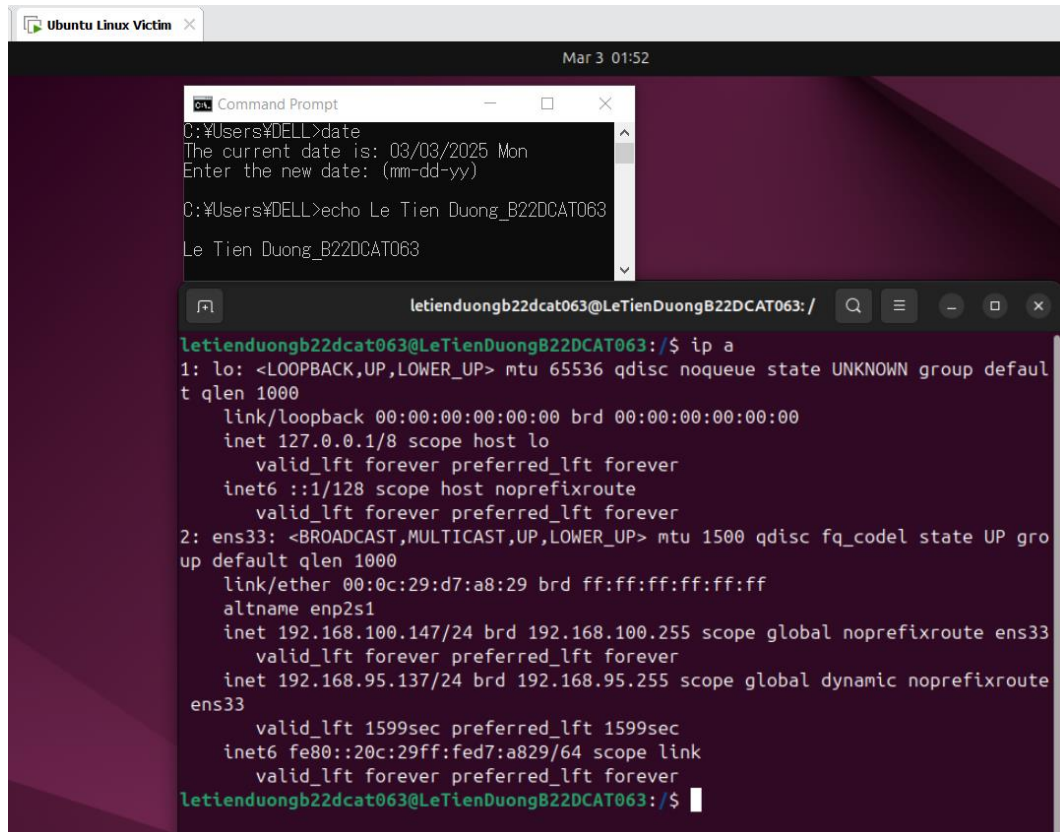
2.1 Chuẩn bị môi trường

- 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 lab 05 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: Chỉ cần bật các máy cần sử dụng trong bài thực hành.
- Topo mạng như đã cấu hình trong bài 5. Trong bài này sử dụng máy Ubuntu Linux victim, Kali Linux attack 1 thuộc Internal Network và máy Kali Linux attack 2, Windows Server 2003 victim thuộc mạng External Network.



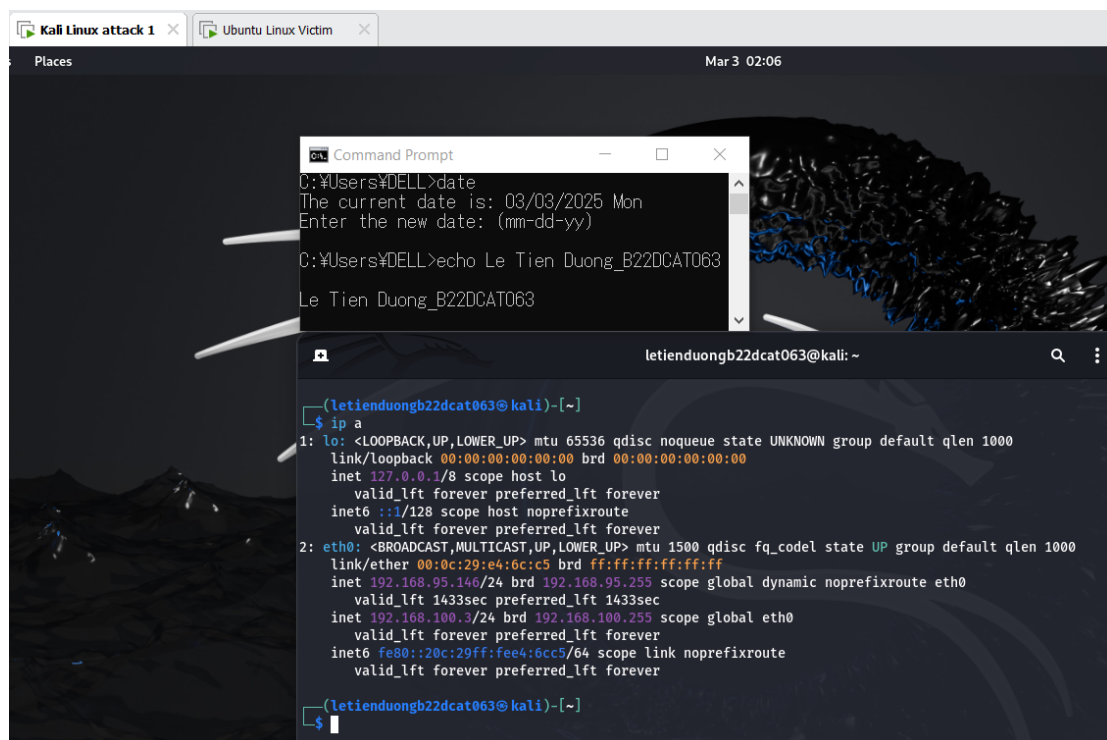
Hình 2 – Topo mạng đã được cấu hình

- Máy Ubuntu Linux Victim thuộc Internal Network có địa chỉ IP 192.168.100.147



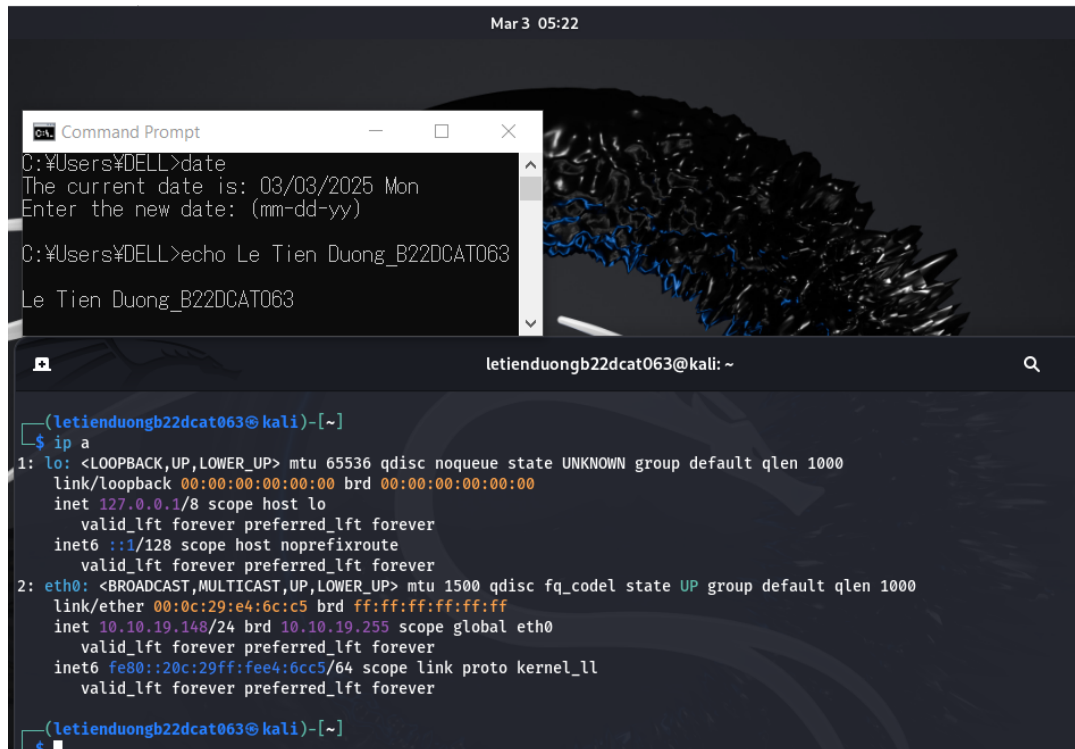
Hình 3 – Máy Ubuntu Linux Victim

- Máy Kali Linux attack 1 thuộc Internal Network có địa chỉ IP 192.168.100.3



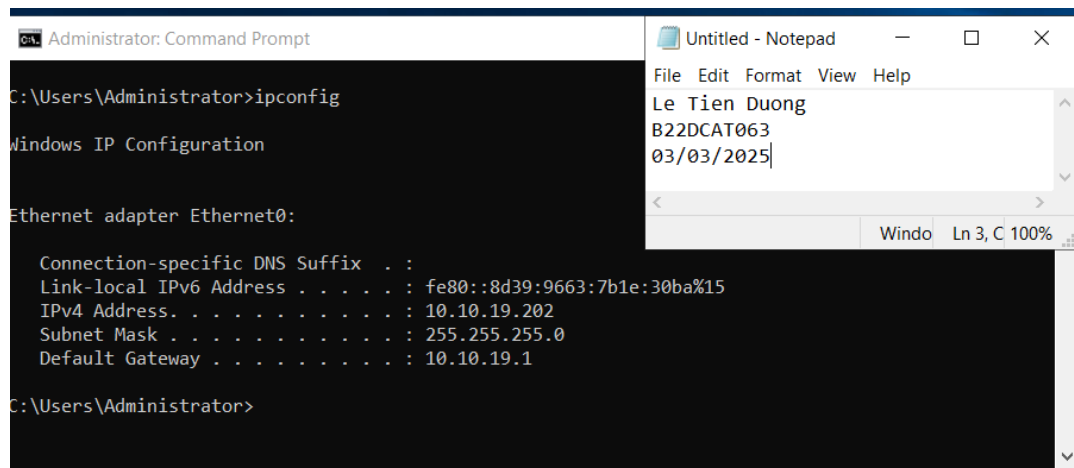
Hình 4 – Máy Kali Linux attack 1

- Máy Kali Linux attack 2 thuộc External Network có địa chỉ IP 10.10.19.148



Hình 5 – Máy Kali Linux attack 2

- Máy Windows Server 2019 victim thuộc External Network có địa chỉ IP 10.10.19.202

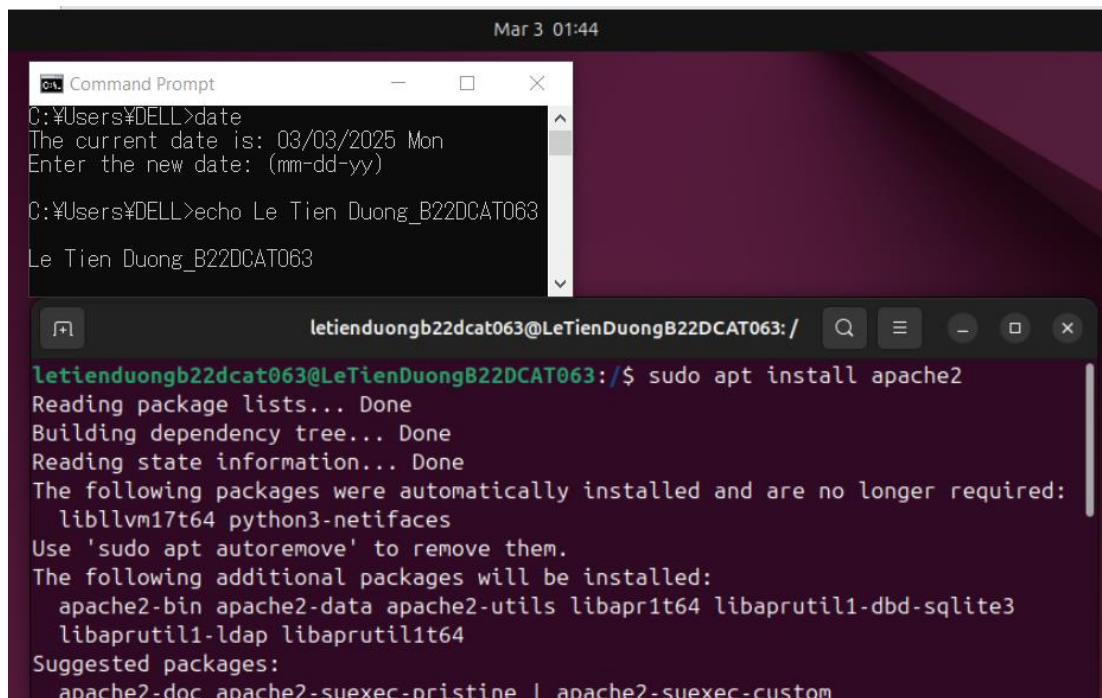


Hình 6 – Máy Windows Server victim thuộc External Network

2.2 Các bước thực hiện

2.2.1 Phân tích log sử dụng grep trong Linux

- Cài đặt và kiểm tra trạng thái của dịch vụ apache2 trên máy Ubuntu Linux victim.



```
Mar 3 01:44

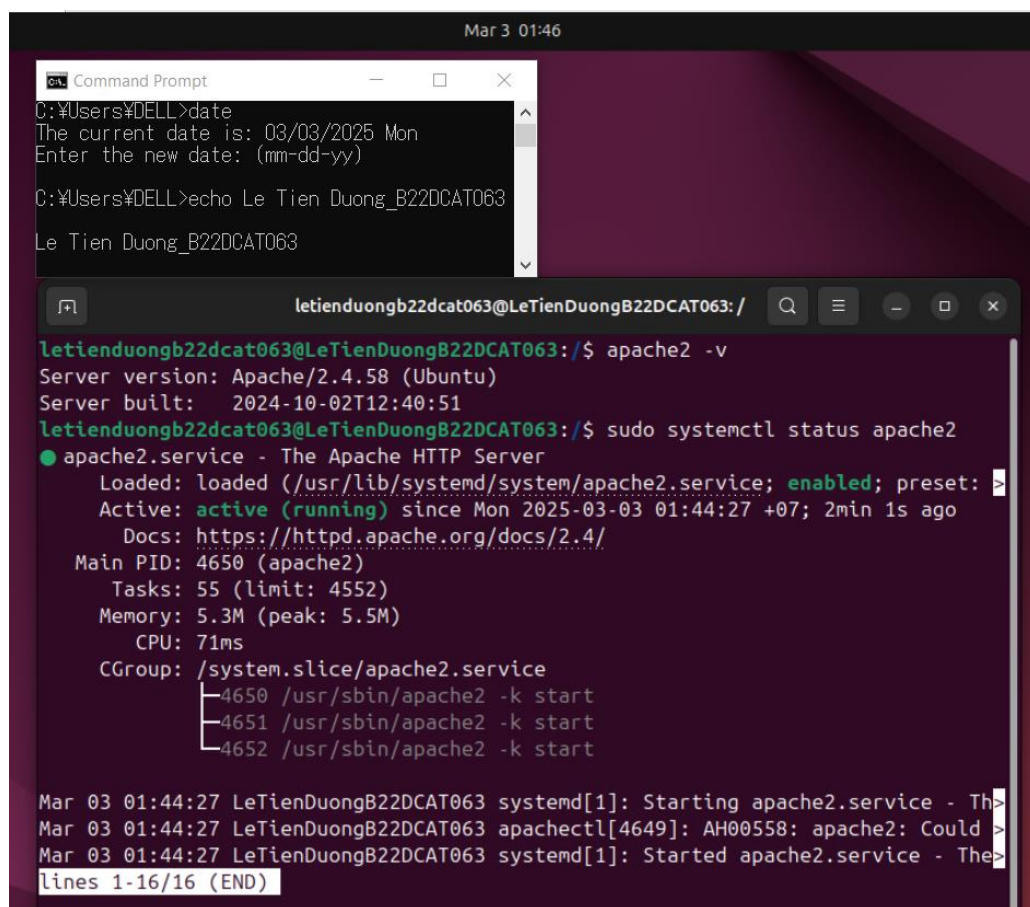
C:\Users\YDELL>date
The current date is: 03/03/2025 Mon
Enter the new date: (mm-dd-yy)

C:\Users\YDELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

lettienduongb22dcat063@LeTienDuongB22DCAT063: /
lettienduongb22dcat063@LeTienDuongB22DCAT063:/$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libllvm17t64 python3-netifaces
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

Hình 7 – Cài đặt apache2 trên máy Ubuntu

- Kiểm tra trạng thái của apache2 trên máy Ubuntu.



```
Mar 3 01:46

C:\Users\YDELL>date
The current date is: 03/03/2025 Mon
Enter the new date: (mm-dd-yy)

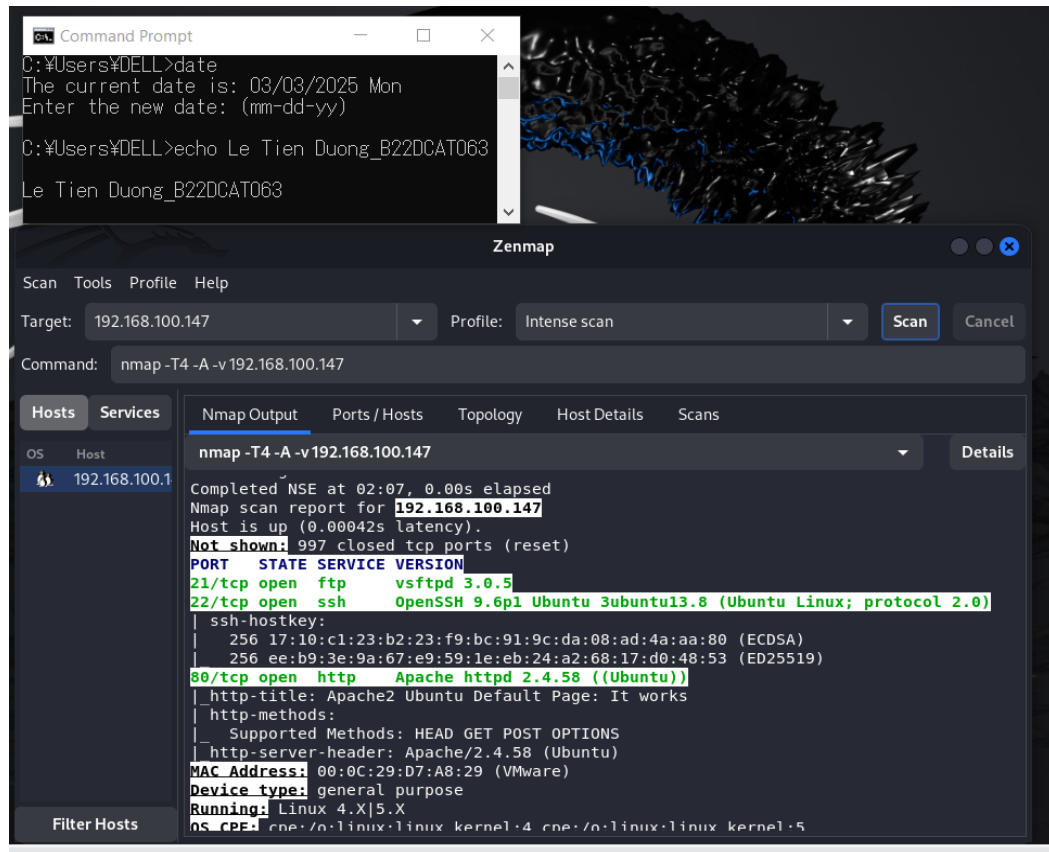
C:\Users\YDELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

lettienduongb22dcat063@LeTienDuongB22DCAT063: /
lettienduongb22dcat063@LeTienDuongB22DCAT063:/$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built: 2024-10-02T12:40:51
lettienduongb22dcat063@LeTienDuongB22DCAT063:/$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: >
   Active: active (running) since Mon 2025-03-03 01:44:27 +07; 2min 1s ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 4650 (apache2)
      Tasks: 55 (limit: 4552)
     Memory: 5.3M (peak: 5.5M)
        CPU: 71ms
    CGroup: /system.slice/apache2.service
            └─4650 /usr/sbin/apache2 -k start
              └─4651 /usr/sbin/apache2 -k start
                └─4652 /usr/sbin/apache2 -k start

Mar 03 01:44:27 LeTienDuongB22DCAT063 systemd[1]: Starting apache2.service - Th>
Mar 03 01:44:27 LeTienDuongB22DCAT063 apachectl[4649]: AH00558: apache2: Could >
Mar 03 01:44:27 LeTienDuongB22DCAT063 systemd[1]: Started apache2.service - The>
lines 1-16/16 (END)
```

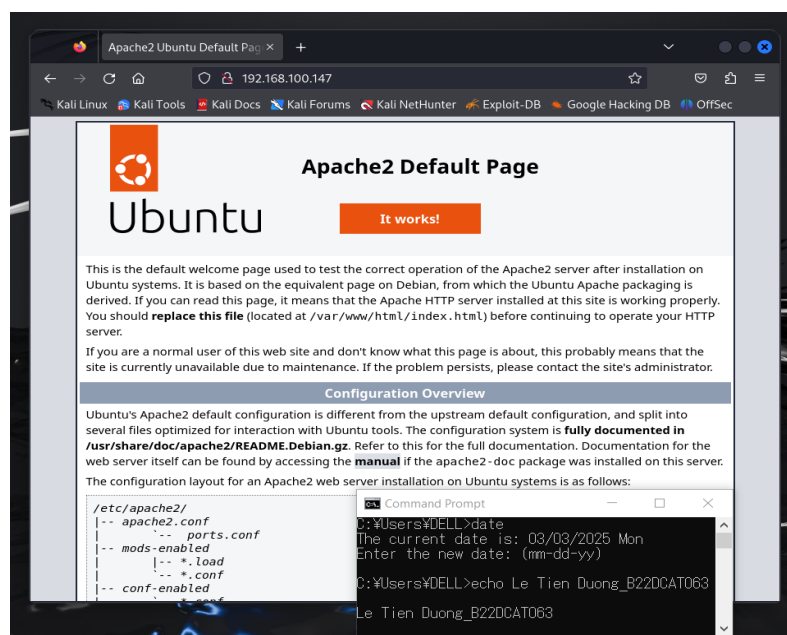
Hình 8 – Kiểm tra trạng thái của apache2 trên máy Ubuntu

- 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 2.2.3
- Sử dụng lệnh *zenmap* trong terminal để khởi chạy zenmap. Nhập Target là 192.168.100.147 và chọn Scan.



Hình 9 – Kết quả sau khi scan

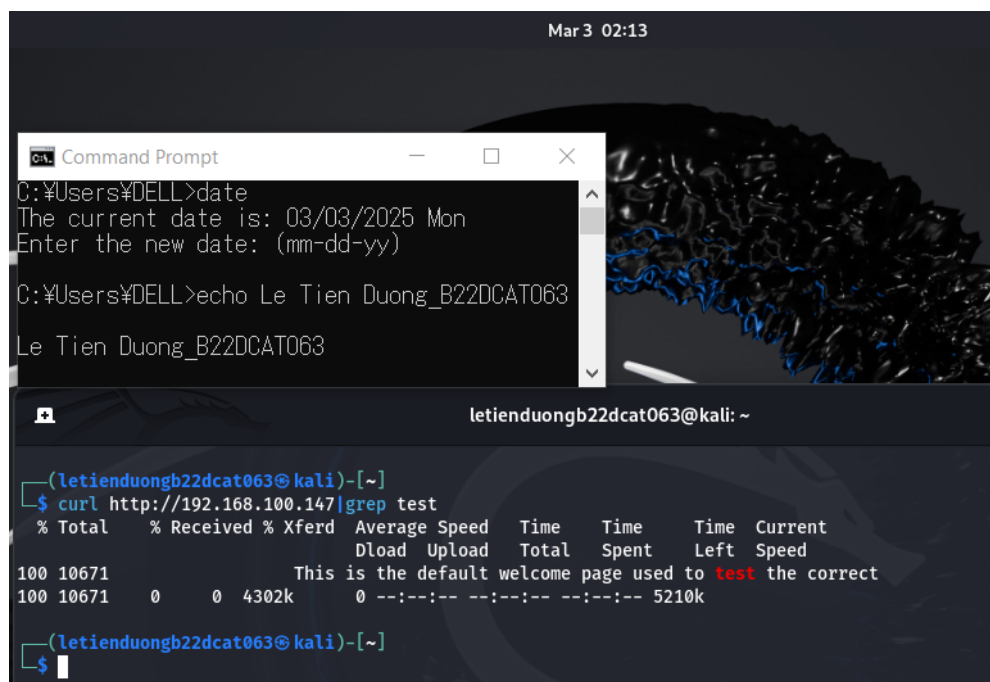
- Trên máy Kali attack 1 ở mạng Internal, truy cập địa chỉ web <http://192.168.100.147>.



Hình 10 – Truy cập địa chỉ web trên máy Kali attack 1

- Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test” dùng lệnh:

`curl http://192.168.100.147 | grep test`

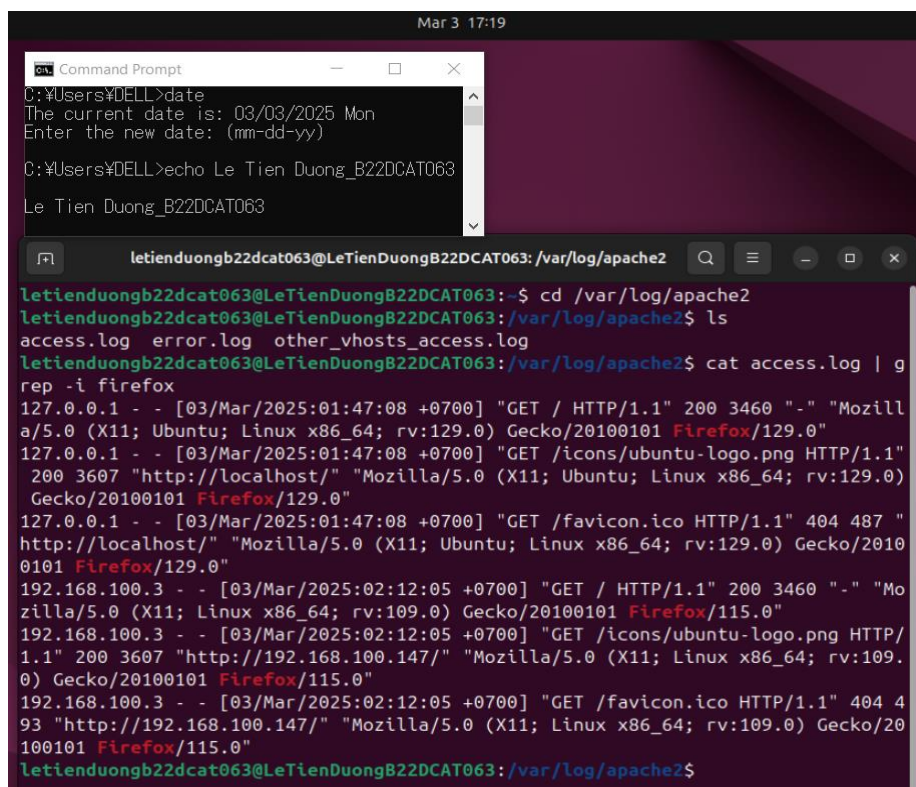


Hình 11 – Sao chép website và tìm kiếm

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

`cd /var/log/apache2`

`cat access.log | grep -i firefox #lọc kết quả theo từ khóa tìm kiếm “firefox”`

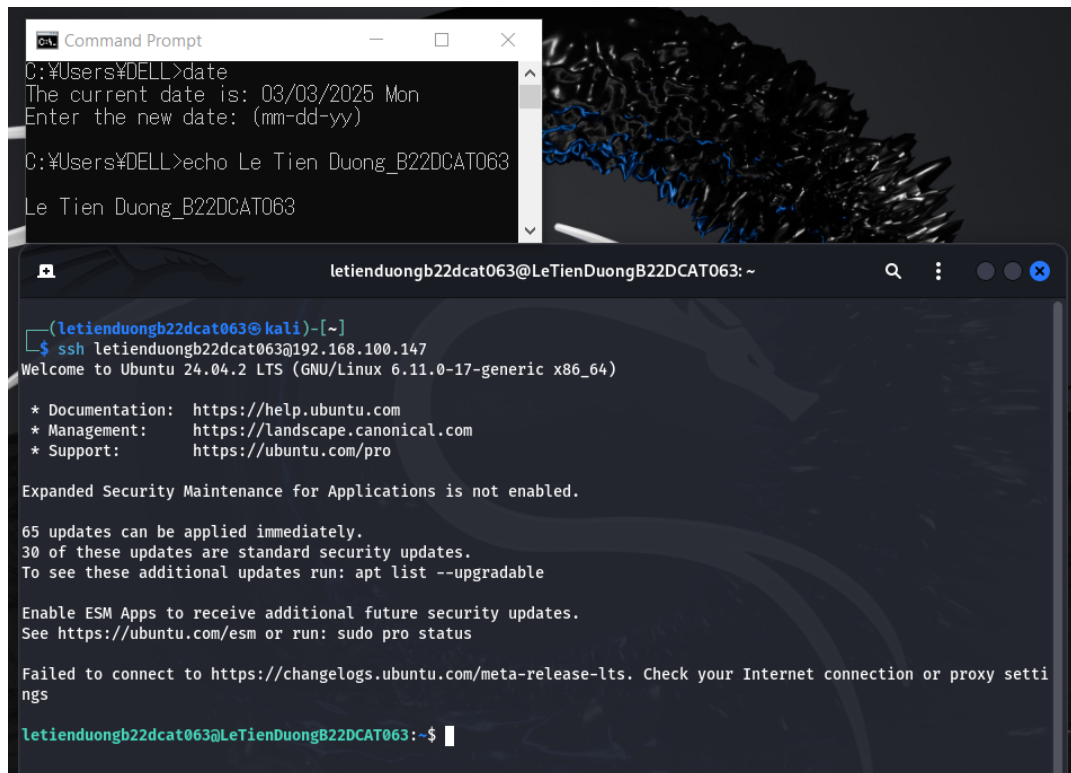


Hình 12 – Mở thư mục chứa access_log, đọc và lọc kết quả theo từ khóa

2.2.2 Phân tích log sử dụng gawk trong Linux

- Trên máy Kali attack tiến hành remote vào máy Linux Internal Victim.

ssh letienduongb22dcat063@192.168.100.147

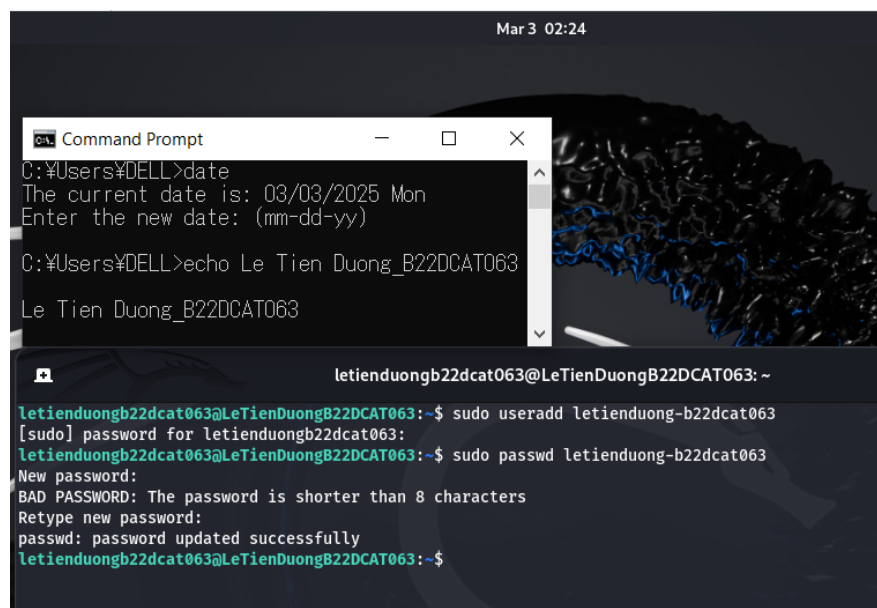


Hình 13 – Tiến hành remote vào máy Linux Internal Victim

- Tạo một account mới với tên sinh viên mà mật khẩu tùy chọn. Sau đó tiến hành thay đổi mật khẩu cho tài khoản vừa tạo.

sudo useradd letienduong-b22dcat063

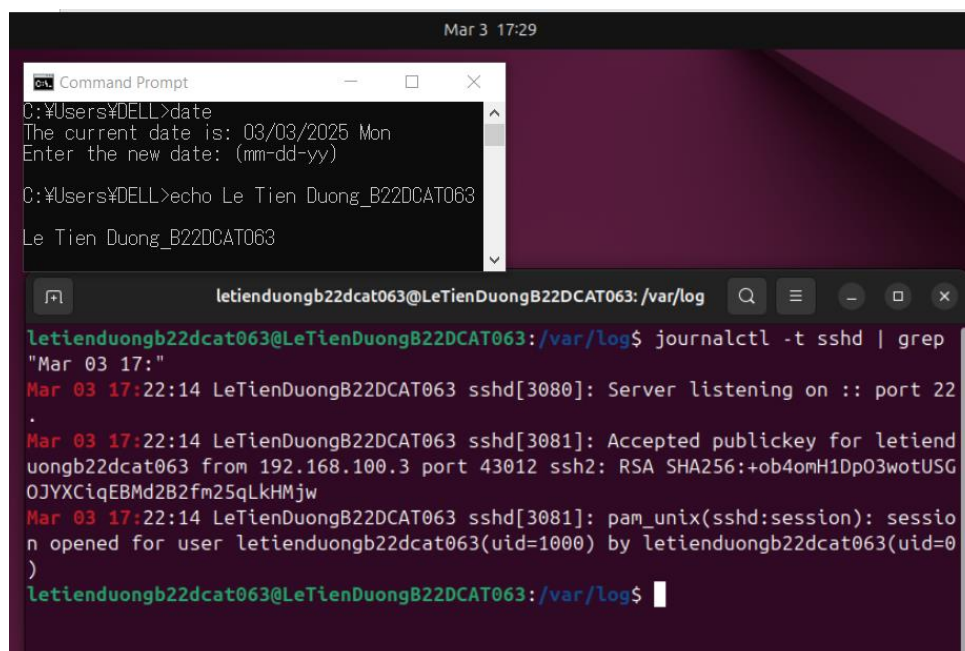
sudo passwd letienduong-b22dcat063



Hình 14 – Tạo user mới và đổi mật khẩu

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

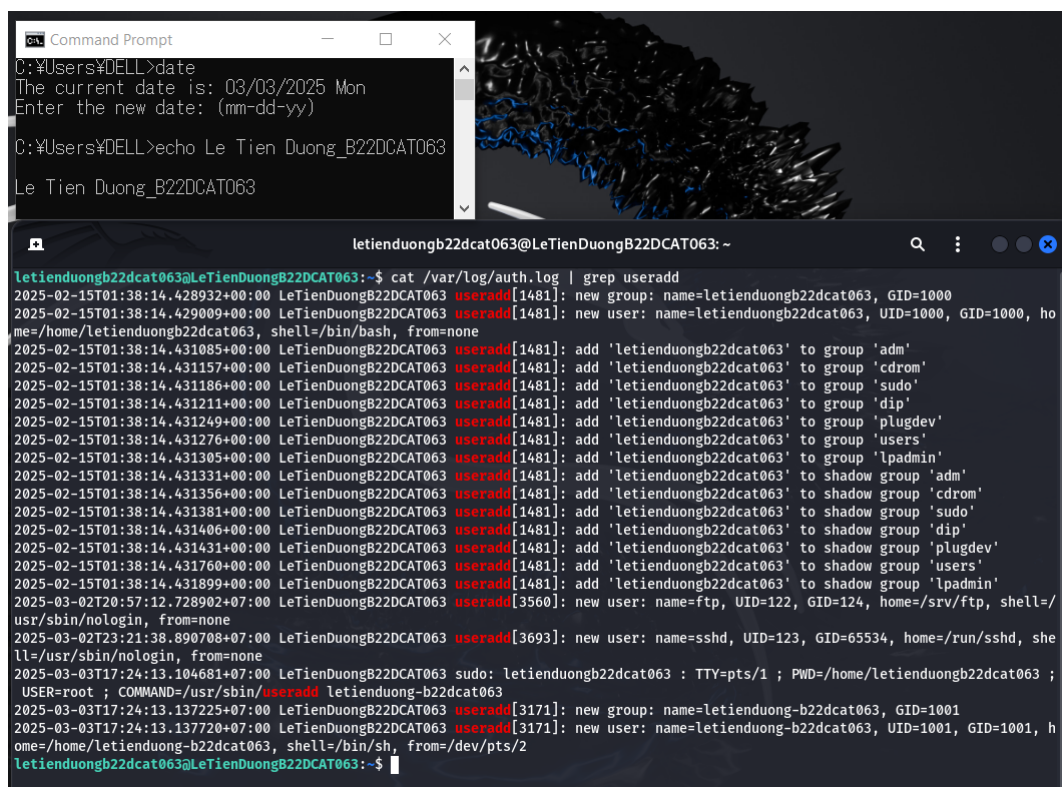
journalctl -t sshd | grep "Mar 03 17:"



Hình 15 – Xem file log trên máy Linux Internal Victim

- Trên máy Kali attack 1, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep.

cat /var/log/auth.log | grep useradd



Hình 16 – Dùng lệnh grep tìm kiếm người dùng vừa tạo

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

gawk '/useradd/ {print}' /var/log/auth.log

```

C:\Users\DELL>date
The current date is: 03/03/2025 Mon
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

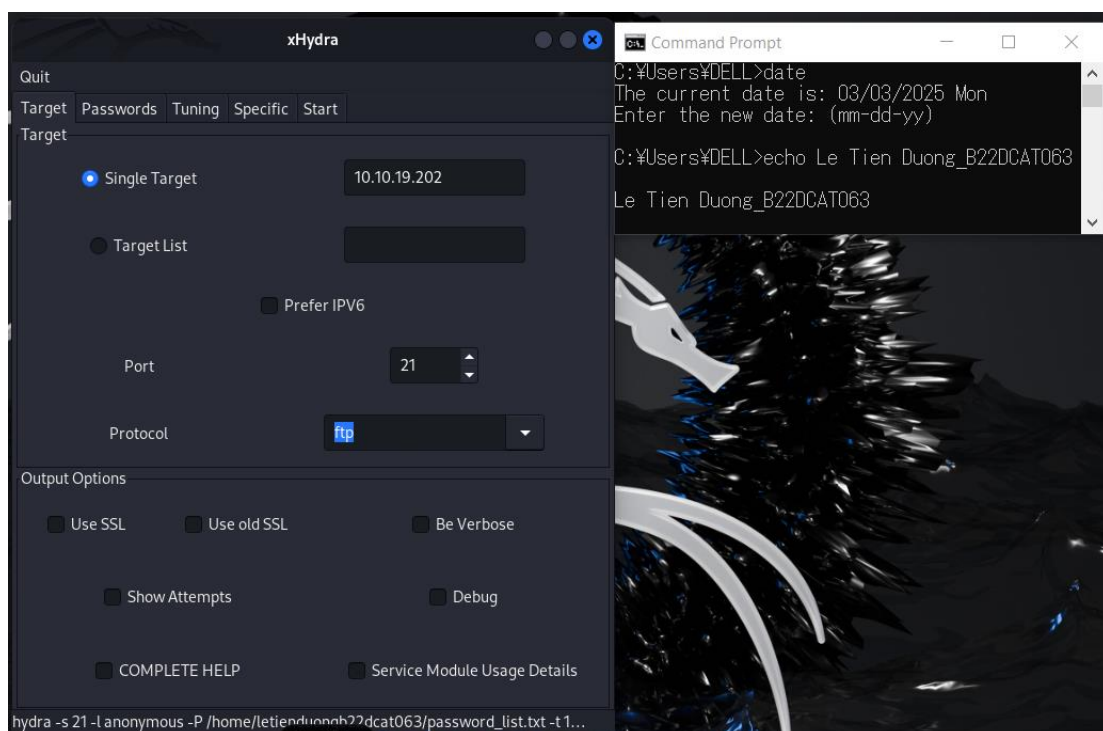
letiendaungb22dcat063@LeTienDuongB22DCAT063:~$ gawk '/useradd/ {print}' /var/log/auth.log
2025-02-15T01:38:14.428932+00:00 LeTienDuongB22DCAT063 useradd[1481]: new group: name=letiendaungb22dcat063, GID=1000
2025-02-15T01:38:14.429009+00:00 LeTienDuongB22DCAT063 useradd[1481]: new user: name=letiendaungb22dcat063, UID=1000, GID=1000, home=/home/letiendaungb22dcat063, shell=/bin/bash, from=none
2025-02-15T01:38:14.431085+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'adm'
2025-02-15T01:38:14.431157+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'cdrom'
2025-02-15T01:38:14.431186+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'sudo'
2025-02-15T01:38:14.431211+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'dip'
2025-02-15T01:38:14.431249+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'plugdev'
2025-02-15T01:38:14.431276+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'users'
2025-02-15T01:38:14.431305+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to group 'lpadmin'
2025-02-15T01:38:14.431331+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'adm'
2025-02-15T01:38:14.431356+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'cdrom'
2025-02-15T01:38:14.431381+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'sudo'
2025-02-15T01:38:14.431406+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'dip'
2025-02-15T01:38:14.431431+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'plugdev'
2025-02-15T01:38:14.431760+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'users'
2025-02-15T01:38:14.431899+00:00 LeTienDuongB22DCAT063 useradd[1481]: add 'letiendaungb22dcat063' to shadow group 'lpadmin'
2025-03-02T20:57:12.728902+07:00 LeTienDuongB22DCAT063 useradd[3560]: new user: name=ftp, UID=122, GID=124, home=/srv/ftp, shell=/usr/sbin/nologin, from=none
2025-03-02T23:21:38.890708+07:00 LeTienDuongB22DCAT063 useradd[3693]: new user: name=sshd, UID=123, GID=65534, home=/run/sshd, shell=/usr/sbin/nologin, from=none
2025-03-03T17:24:13.104681+07:00 LeTienDuongB22DCAT063 sudo: letiendaungb22dcat063 : TTY=pts/1 ; PWD=/home/letiendaungb22dcat063 ; USER=root ; COMMAND=/usr/sbin/useradd letiendaung-b22dcat063
2025-03-03T17:24:13.137225+07:00 LeTienDuongB22DCAT063 useradd[3171]: new group: name=letiendaung-b22dcat063, GID=1001
2025-03-03T17:24:13.137720+07:00 LeTienDuongB22DCAT063 useradd[3171]: new user: name=letiendaung-b22dcat063, UID=1001, GID=1001, home=/home/letiendaung-b22dcat063, shell=/bin/sh, from=/dev/pts/2
letiendaungb22dcat063@LeTienDuongB22DCAT063:~$

```

Hình 17 – Sử dụng lệnh gawk

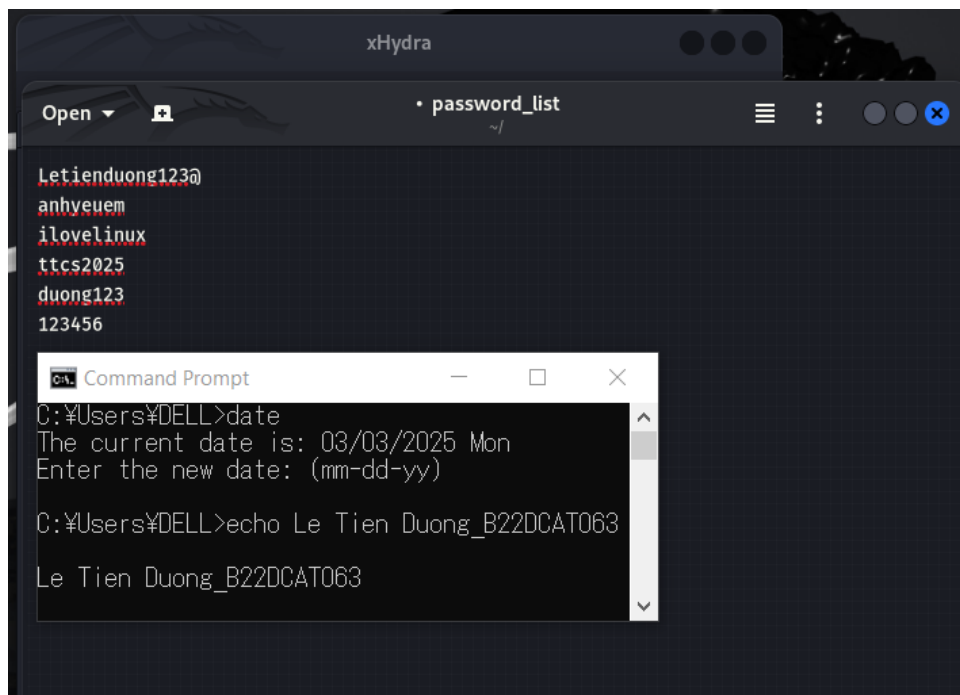
2.2.3 Phân tích log sử dụng find trong Windows

- Trên máy Kali External Attack khởi động #xhydra, chọn target là 10.10.19.202, giao thức ftp, cổng 21.



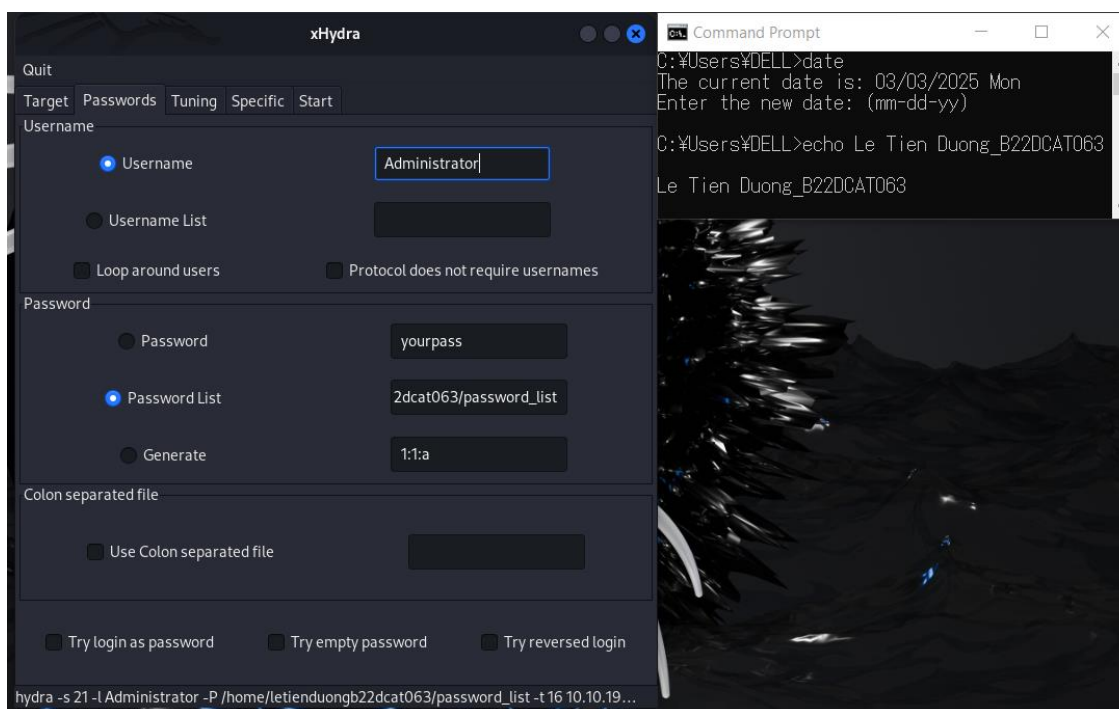
Hình 18 – Khởi động #xhydra trên máy Kali External Attack

- Tạo file password_list chứa mật khẩu.



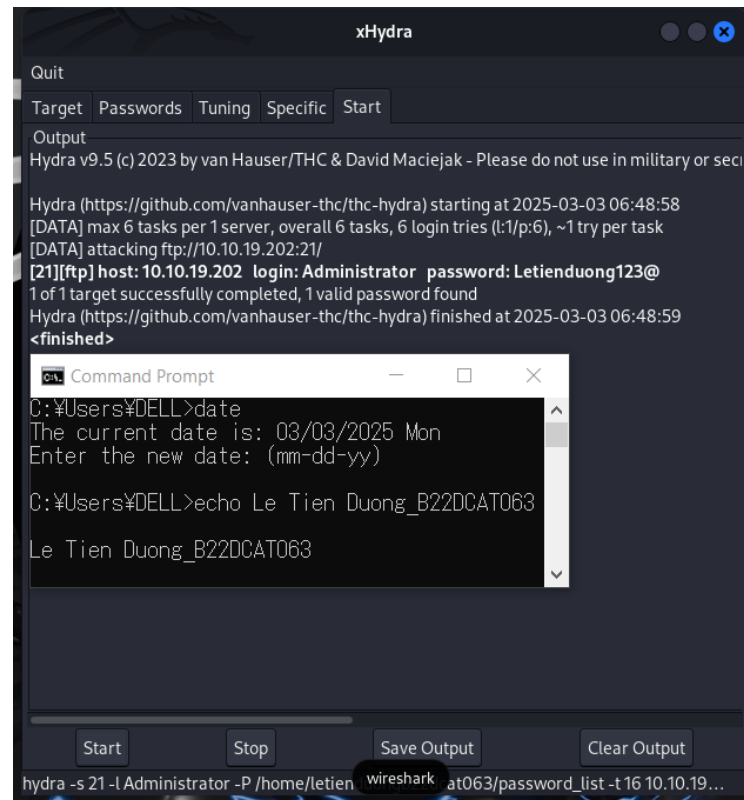
Hình 19 – Tạo file password_list

- Quay về giao diện #xhydra, nhập Username của máy Windows Server 2019 External Victim, chọn cài đặt Password list, sau đó chọn đường dẫn đến file password_list đã tạo.



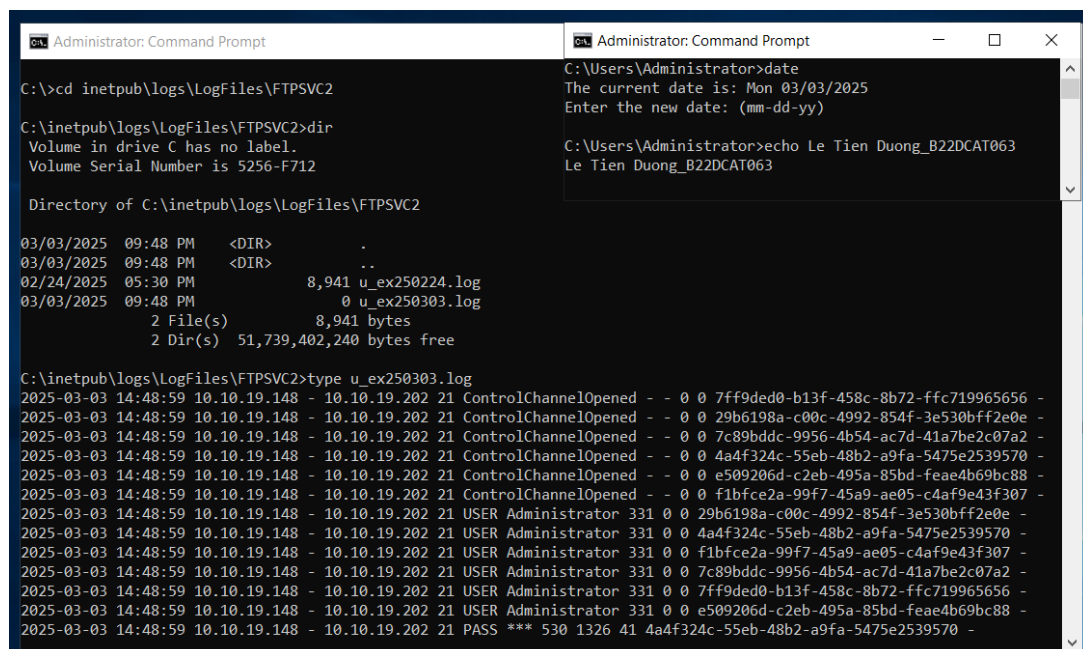
Hình 20 – Nhập Username và chọn đường dẫn đến file password_list

- Chọn Start và chờ xHydra tìm được mật khẩu.



Hình 21 – xHydra tìm được mật khẩu

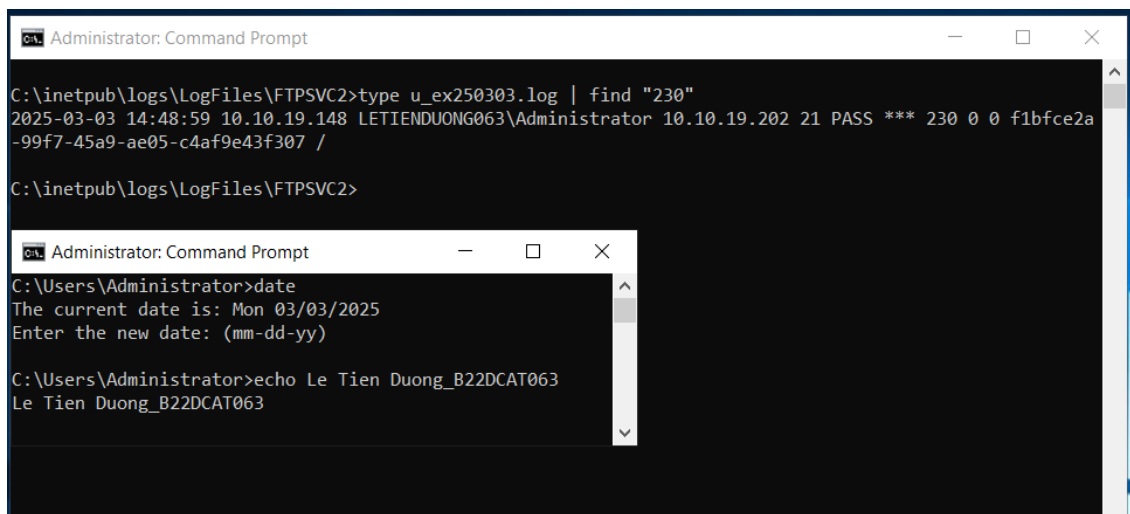
- Trên máy Windows Server 2019 External Victim, thực hiện điều hướng đến FTP Logfile (C:\>cd inetpub\logs\LogFiles\FTPSVC2). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có định dạng yymmdd).



Hình 22 – Điều hướng đến FTP Logfile và mở file log mới nhất

- Gõ lệnh để tìm kiếm kết quả tấn công login thành công.

type u_ex250303.log | find "230"



```
Administrator: Command Prompt
C:\inetpub\logs\LogFiles\FTPSVC2>type u_ex250303.log | find "230"
2025-03-03 14:48:59 10.10.19.148 LETIENDUONG063\Administrator 10.10.19.202 21 PASS *** 230 0 0 f1bfce2a
-99f7-45a9-ae05-c4af9e43f307 /

C:\inetpub\logs\LogFiles\FTPSVC2>

Administrator: Command Prompt
C:\Users\Administrator>date
The current date is: Mon 03/03/2025
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063
```

Hình 23 – Gõ lệnh để tìm kiếm kết quả login thành công

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>