

**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:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH.....	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
1.2.1 Windows Event Viewer và Auditing	4
1.2.2 Lệnh grep.....	5
1.2.3 Lệnh gawp	5
1.2.4 Lệnh find	5
1.2.5 Secure và Access_log.....	5
1.3 Kết chương	6
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	7
2.1 Chuẩn bị môi trường	7
2.2 Các bước thực hiện.....	7
2.2.1 Phân tích log sử dụng grep trong Linux	7
2.2.2 Phân tích log sử dụng gawk trong Linux	11
2.2.3 Phân tích log sử dụng find trong Windows.....	15
2.3 Kết luận	17
KẾT LUẬN	18
TÀI LIỆU THAM KHẢO.....	19

DANH MỤC CÁC HÌNH VẼ

Hình 1 Cài đặt web server apache2	7
Hình 2 Cài đặt thành công web server apache2	8
Hình 3 Cổng 80 đang mở cho Web Server Apache 2	9
Hình 4 Truy cập vào địa chỉ web http://192.168.100.147	9
Hình 5 Tiến hành sao chép website và tìm kiếm từ khóa “test”	10
Hình 6 Xem thư mục chứa cccess_log	10
Hình 7 Remote vào máy Linux Internal	11
Hình 8 Tạo tài khoản mới và đổi mật khẩu	12
Hình 9 Xem file log trên máy Linux Internal Victim	13
Hình 10 Dùng lệnh grep	14
Hình 11 Sử dụng gawk	14
Hình 12 Cài đặt để xHydra tìm mật khẩu	15
Hình 13 xHydra đã thành công tìm được mật khẩu của tài khoản administrator	16
Hình 14 Kết quả việc tấn công thành công	17

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Nắm được công cụ và các phân tích log hệ thống:

- 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 Windows Event Viewer và Auditing

Windows Event Viewer là công cụ tích hợp trong Windows, giúp theo dõi và quản lý các sự kiện (logs) liên quan đến hệ thống, bảo mật, ứng dụng và các hoạt động khác. Nó cung cấp thông tin chi tiết về những gì đang diễn ra trong máy tính. Ví dụ như:

- Cảnh báo và lỗi.
- Đăng nhập/ Đăng xuất.
- Cài đặt, cập nhật phần mềm.
- Thay đổi cấu hình và chính sách bảo mật.

Các thành phần chính của Windows Event Viewer:

- Event Viewer: Cửa sổ chính quản lý sự kiện.
- Windows Logs: Nhật ký hệ thống.
- Applications and Services Logs: Nhật ký từ ứng dụng và dịch vụ cụ thể.

Auditing trong Windows là quá trình theo dõi, ghi lại các hoạt động liên quan đến bảo mật như:

- Đăng nhập/Đăng xuất.
- Truy cập file, thư mục.
- Thay đổi cài đặt bảo mật.
- Khởi chạy ứng dụng.

Việc kích hoạt Auditing giúp các quản trị viên theo dõi hành vi đáng ngờ hoặc các sự cố bảo mật.

1.2.2 Lệnh *grep*

grep là lệnh dùng để tìm kiếm các dòng khớp với một mẫu trong tập tin hoặc đầu ra của lệnh khác. Lệnh hỗ trợ biểu thức chính quy giúp tìm kiếm linh hoạt và mạnh mẽ.

Cách dùng: *grep* [tùy chọn] “mẫu tìm kiếm” tên_file.

Ví dụ: câu lệnh *grep* “error” /var/log/syslog có nghĩa là tìm tất cả dòng chứa từ “error” trong file /var/log/syslog.

1.2.3 Lệnh *gawk*

gawk là một phần mở rộng của lệnh *awk*, chuyên xử lý và phân tích dữ liệu dạng văn bản. Hữu ích khi cần trích xuất, lọc, xử lý và tính toán từ các tệp log có cấu trúc.

Cách dùng: *gawk* ‘pattern {action}’ tên_file.

Cách hoạt động:

- Biến \$1, \$2,..., \$n: Đại diện cho cột thứ nhất, thứ hai,...
- {action}: Hành động cần thực hiện với dòng khớp mẫu.

Ví dụ: câu lệnh *gawk* '{print \$1}' /var/log/nginx/access.log dùng để in địa chỉ IP (cột đầu tiên) từ file access.log.

1.2.4 Lệnh *find*

find là lệnh dùng để tìm kiếm file, thư mục dựa trên nhiều tiêu chí: tên, kích thước, ngày sửa đổi, quyền hạn,... Nó hỗ trợ tìm kiếm trong cả hệ thống tập tin (file system).

Cách dùng: *find* [thư mục] [tùy chọn] [điều kiện].

Ví dụ : câu lệnh *find* /var/log -name “*.log” là tìm tất cả các file .log trong /var/log.

1.2.5 *Secure và Access_log*

secure là file log chứa thông tin bảo mật quan trọng:

- Đăng nhập thành công/ thất bại.
- Hoạt động sudo.
- Các kết nối SSH

access_log là file log ghi nhận các yêu cầu HTTP tới máy chủ web (như Apache hoặc Nginx). Mỗi dòng log thường bao gồm:

- Địa chỉ IP.
- Dấu thời gian.
- Yêu cầu (GET, POST,...)
- Mã trạng thái (200, 400, 500,...)

1.3 Kết chương

Ở chương này giới thiệu về Windows Event Viewer và Auditing. Bên cạnh đó còn giới thiệu về một số câu lệnh dùng cho quá trình phân tích log như grep, gawk, find, secure, access_log,..

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

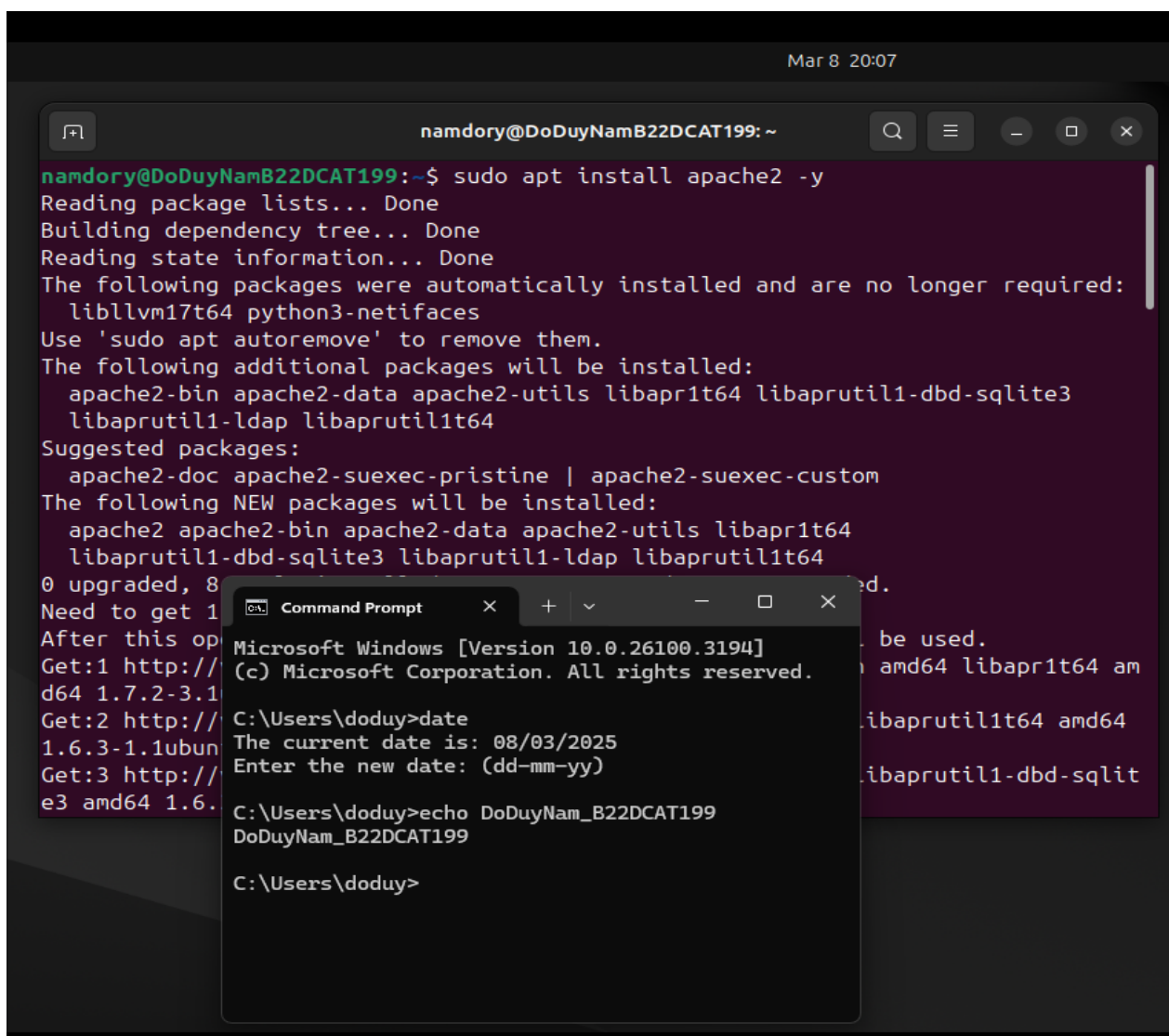
2.1 Chuẩn bị môi trường

- Chuẩn bị các máy trong mạng Internal:
 - Máy Kali Linux Attack: IP: 192.168.100.3
 - Máy Linux Victim: IP: 192.168.100.147
- Chuẩn bị các máy trong mạng External:
 - Máy Kali Linux Attack: IP: 10.10.19.148
 - Máy Windows Server 2019 victim: IP: 10.10.19.202

2.2 Các bước thực hiện

2.2.1 Phân tích log sử dụng grep trong Linux

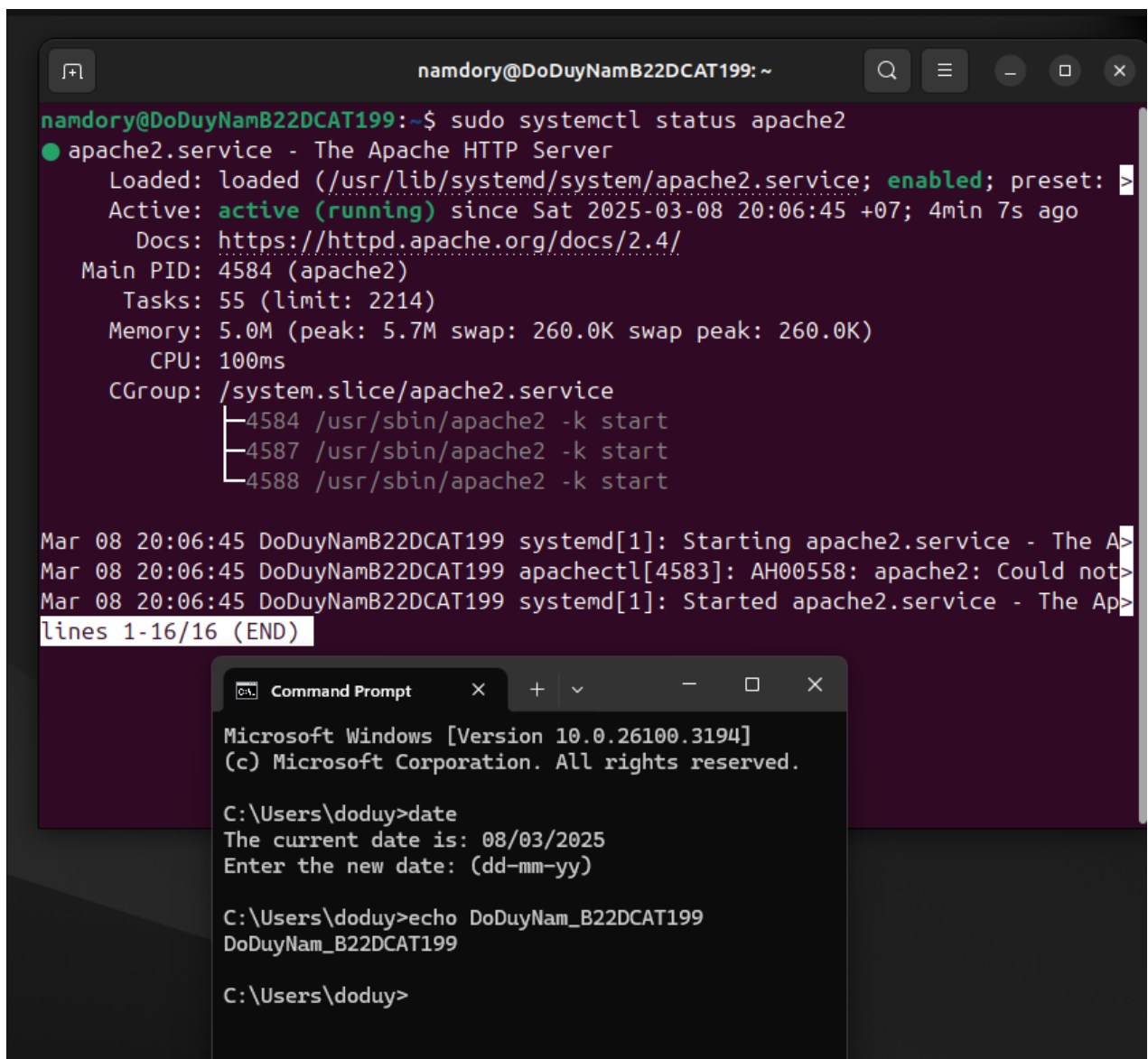
- Ở trên máy Linux Internal Victim sử dụng câu lệnh **sudo apt install apache2 -y** để cài đặt web server apache2



```
Mar 8 20:07
namdory@DoDuyNamB22DCAT199: ~
namdory@DoDuyNamB22DCAT199:~$ sudo apt install apache2 -y
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
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 11.6 MB of archives.
After this operation, 42.5 MB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 libapr1t64 amd64 1.7.2-3.1
Get:2 http://deb.debian.org/debian bullseye/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu1
Get:3 http://deb.debian.org/debian bullseye/main amd64 libaprutil1-dbd-sqlit
e3 amd64 1.6.3-1.1ubuntu1
C:\Users\doduy>date
The current date is: 08/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199
C:\Users\doduy>
```

Hình 1 Cài đặt web server apache2

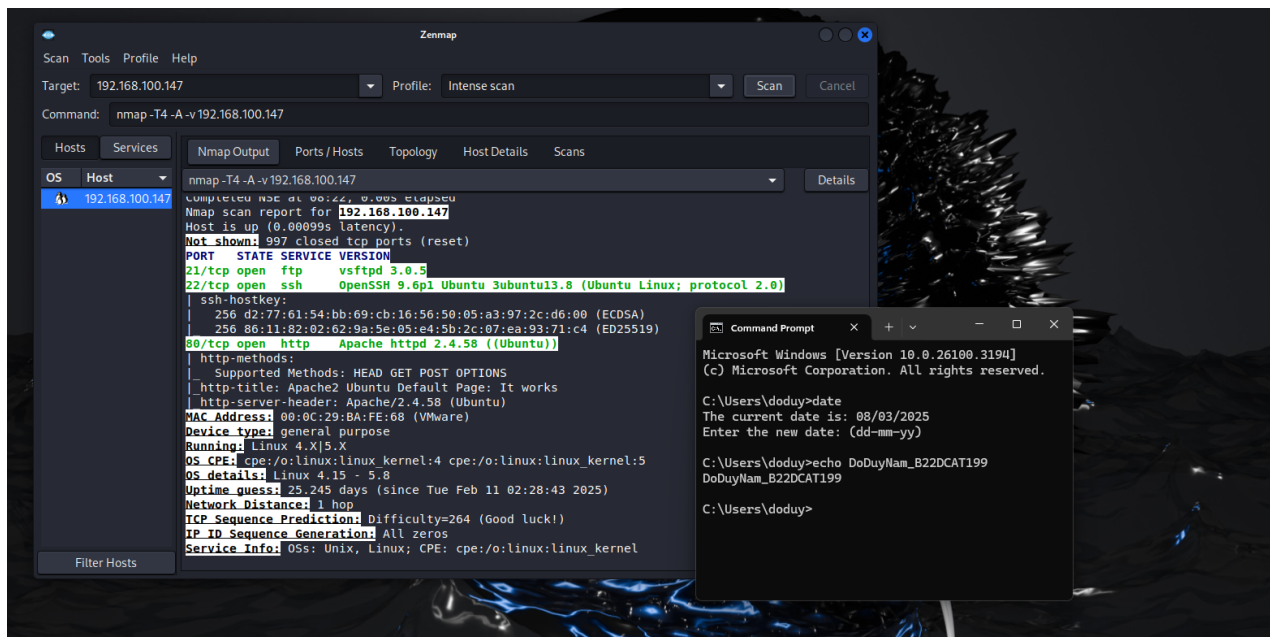
- Sau khi cài đặt xong sử dụng câu lệnh **sudo systemctl status apache2** để kiểm tra -
> hiển thị active -> thành công



```
namdory@DoDuyNamB22DCAT199: ~  
namdory@DoDuyNamB22DCAT199:~$ sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: >  
   Active: active (running) since Sat 2025-03-08 20:06:45 +07; 4min 7s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
  Main PID: 4584 (apache2)  
    Tasks: 55 (limit: 2214)  
  Memory: 5.0M (peak: 5.7M swap: 260.0K swap peak: 260.0K)  
    CPU: 100ms  
   CGroup: /system.slice/apache2.service  
           └─4584 /usr/sbin/apache2 -k start  
             └─4587 /usr/sbin/apache2 -k start  
               └─4588 /usr/sbin/apache2 -k start  
  
Mar 08 20:06:45 DoDuyNamB22DCAT199 systemd[1]: Starting apache2.service - The A>  
Mar 08 20:06:45 DoDuyNamB22DCAT199 apachectl[4583]: AH00558: apache2: Could not>  
Mar 08 20:06:45 DoDuyNamB22DCAT199 systemd[1]: Started apache2.service - The Ap>  
lines 1-16/16 (END)  
  
Microsoft Windows [Version 10.0.26100.3194]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\doduy>date  
The current date is: 08/03/2025  
Enter the new date: (dd-mm-yy)  
  
C:\Users\doduy>echo DoDuyNam_B22DCAT199  
DoDuyNam_B22DCAT199  
  
C:\Users\doduy>
```

Hình 2 Cài đặt thành công web server 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 2.2.3



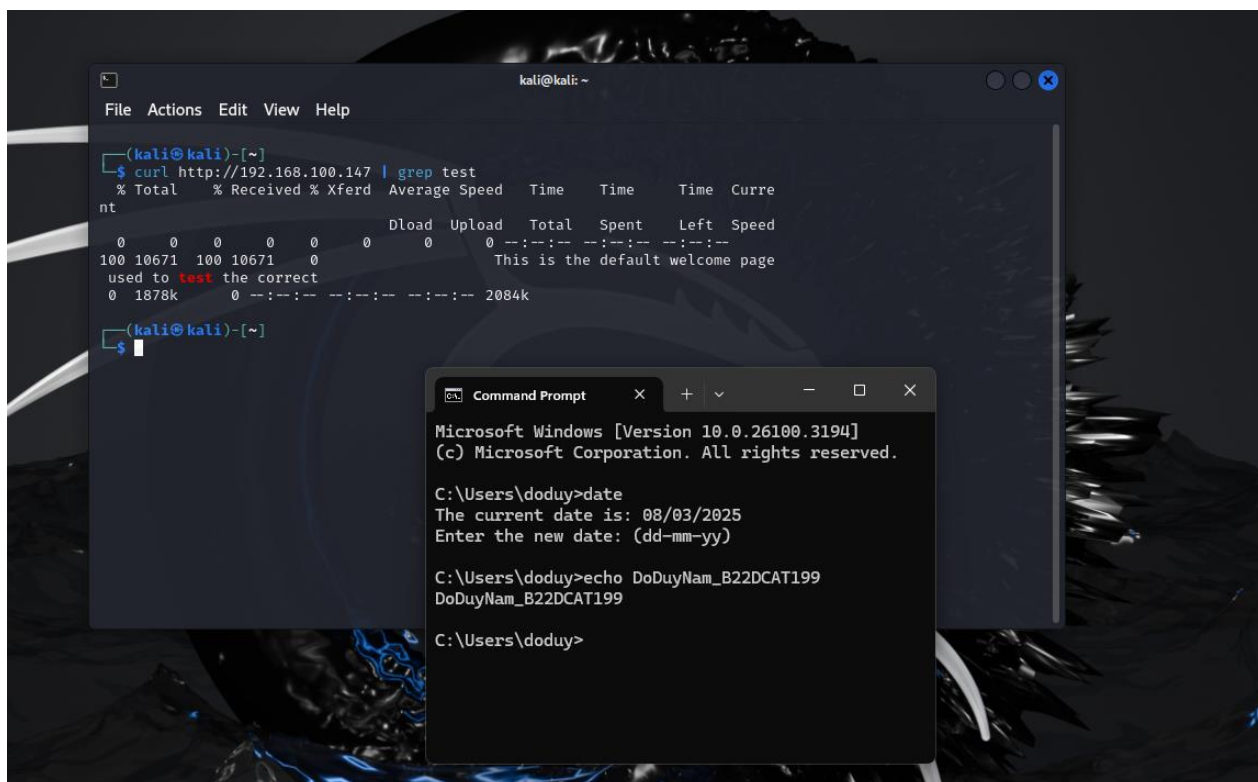
Hình 3 Cổng 80 đang mở cho Web Server Apache 2

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



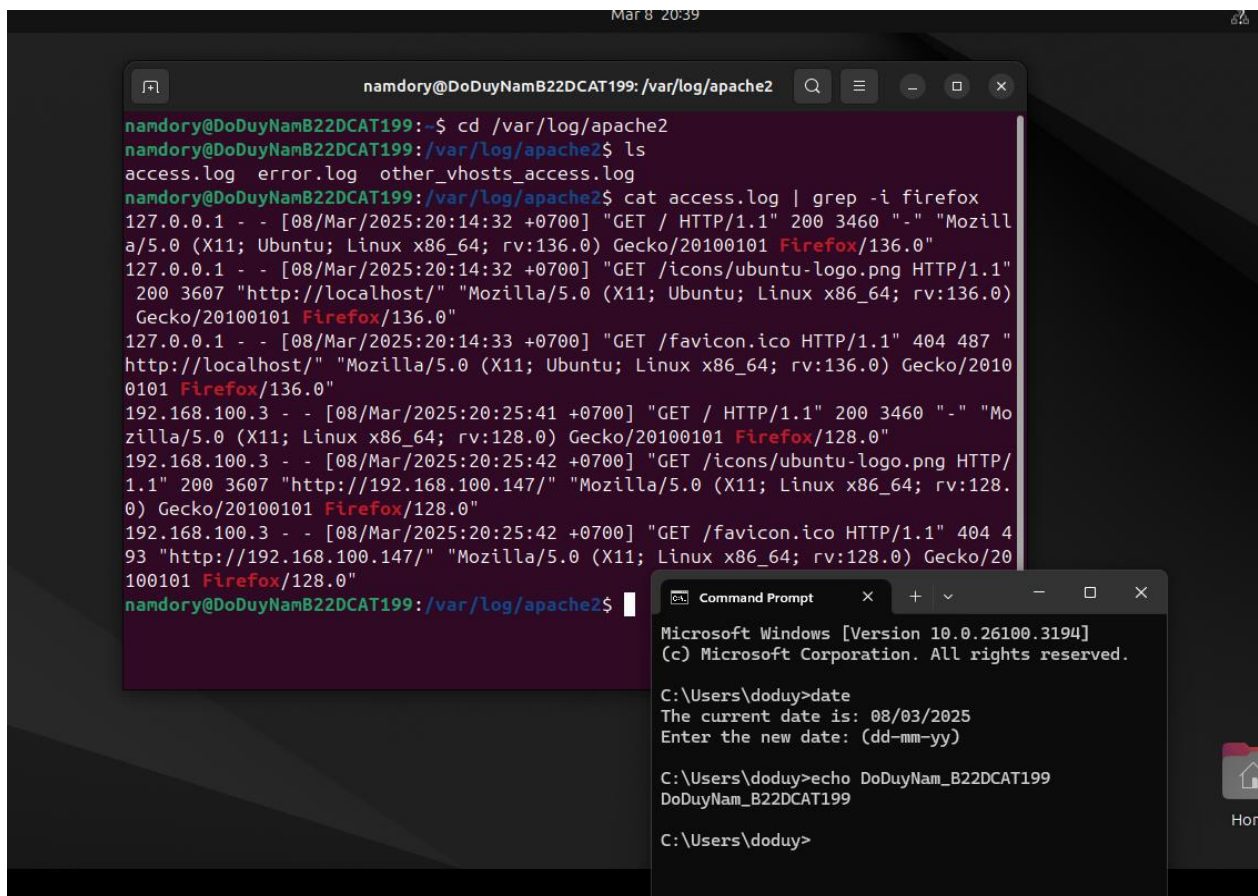
Hình 4 Truy cập vào địa chỉ web <http://192.168.100.147>

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



Hình 5 Tiến hành sao chép website và tìm kiếm từ khóa “test”

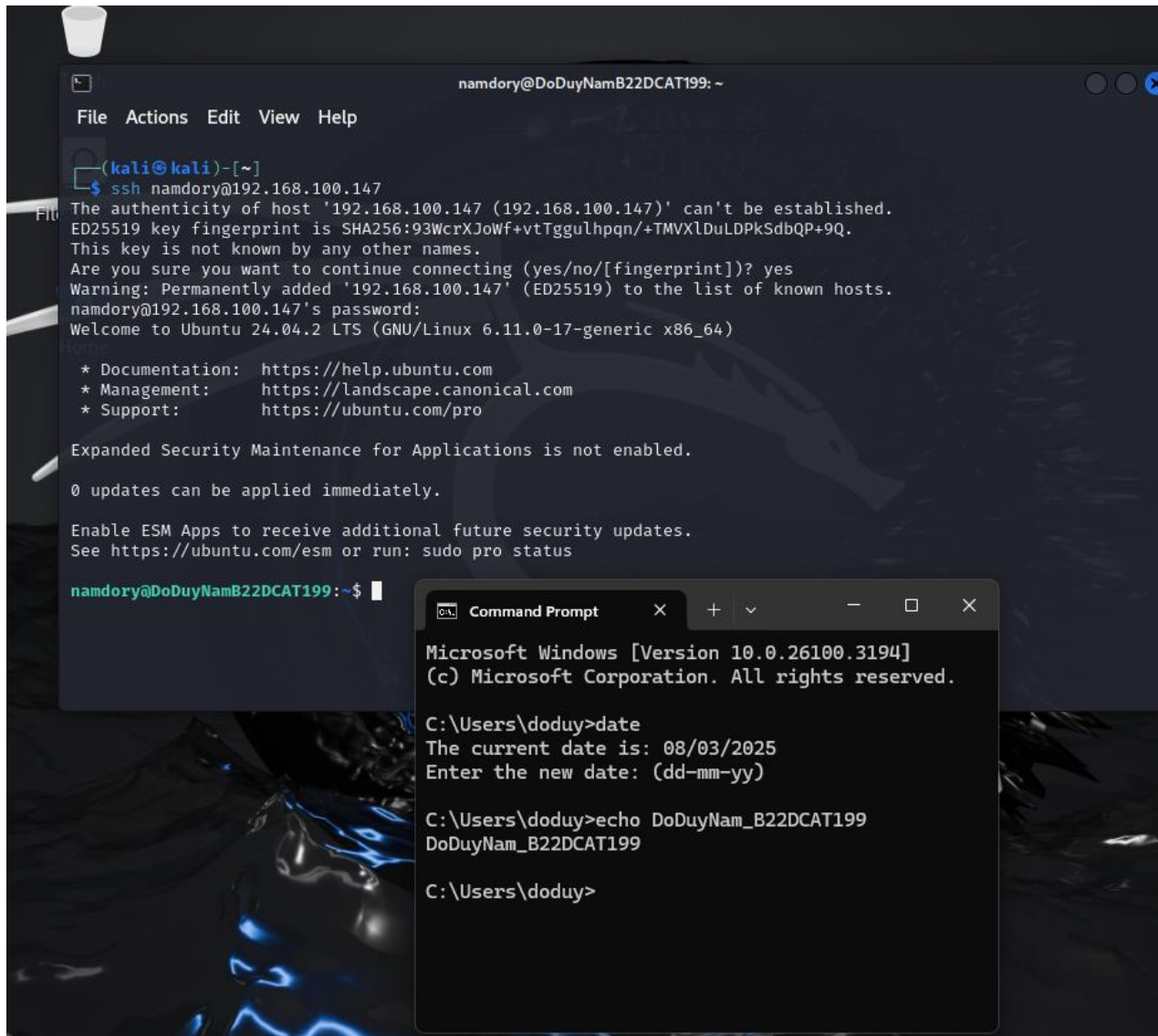
- Trên máy Linux Internal Victim, để xem thư mục chứa **access_log** dùng lệnh: **cd /var/log/apache2**



Hình 6 Xem thư mục chứa access_log

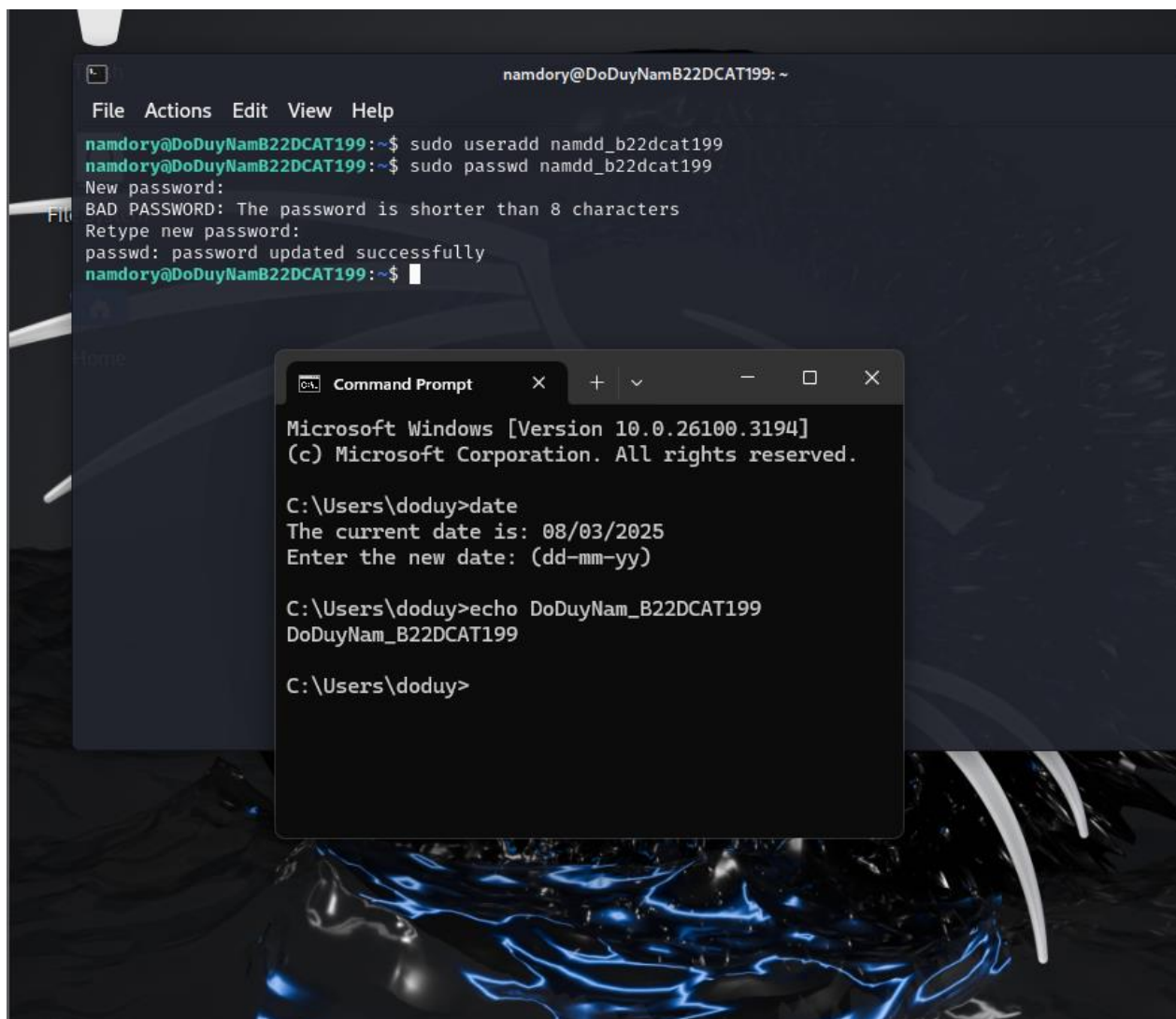
2.2.2 Phân tích log sử dụng gawk trong Linux

- Trên máy Kali attack tiến hành remote vào máy Linux Internal Victim bằng cách sử dụng SSH



Hình 7 Remote vào máy Linux Internal

- 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 8 Tạo tài khoản mới và đổi mật khẩu

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

The image shows a Linux terminal window with the title bar 'namdory@DoDuyNamB22DCAT199: /var/log'. The terminal output shows the user navigating to /var/log and using 'grep' to search for 'namdd_b22dcat199' in 'auth.log'. The results show several log entries related to user creation and password changes for 'namdd_b22dcat199'. An inset window titled 'Command Prompt' shows a Windows command prompt with the following text: 'Microsoft Windows [Version 10.0.26100.3194] (c) Microsoft Corporation. All rights reserved. C:\Users\doduy>date The current date is: 08/03/2025 Enter the new date: (dd-mm-yy) C:\Users\doduy>echo DoDuyNam_B22DCAT199 DoDuyNam_B22DCAT199 C:\Users\doduy>'.

```
namdory@DoDuyNamB22DCAT199:~$ cd /var/log
namdory@DoDuyNamB22DCAT199:/var/log$ grep namdd_b22dcat199 auth.log
2025-03-08T20:59:17.082807+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ;
  PWD=/home/namdory ; USER=root ; COMMAND=/usr/sbin/useradd namdd_b22dcat199
2025-03-08T20:59:17.115661+07:00 DoDuyNamB22DCAT199 useradd[5275]: new group: na
me=namdd_b22dcat199, GID=1004
2025-03-08T20:59:17.116231+07:00 DoDuyNamB22DCAT199 useradd[5275]: new user: nam
e=namdd_b22dcat199, UID=1004, GID=1004, home=/home/namdd_b22dcat199, shell=/bin/
sh, from=/dev/pts/3
2025-03-08T20:59:32.489628+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ;
  PWD=/home/namdory ; USER=root ; COMMAND=/usr/bin/passwd namdd_b22dcat199
2025-03-08T20:59:36.355910+07:00 DoDuyNamB22DCAT199 passwd[5291]: pam_unix(passw
d:chauthtok): password changed for namdd_b22dcat199
namdory@DoDuyNamB22DCAT199:/var/log$
```

```
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\doduy>date
The current date is: 08/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\doduy>echo DoDuyNam_B22DCAT199
DoDuyNam_B22DCAT199

C:\Users\doduy>
```

Hình 9 Xem file log trên máy Linux Internal Victim

- 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.

```
namdory@DoDuyNamB22DCAT199: ~  
File Actions Edit View Help  
namdory@DoDuyNamB22DCAT199:~$ cat /var/log/auth.log | grep useradd  
2025-03-06T23:39:36.467875+07:00 DoDuyNamB22DCAT199 useradd[5275]: new user: name=ftp, UID=122, GID=124, home=/srv/ftp, shell=/usr/sbin/nologin, from=none  
2025-03-07T12:46:23.745039+07:00 DoDuyNamB22DCAT199 useradd[3669]: new user: name=sshd, UID=123, GID=65534, home=/run/ssh, shell=/usr/sbin/nologin, from=none  
2025-03-08T20:58:33.033815+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ; PWD=/home/namdory ; USER=root ; COMMAND=/usr/sbin/useradd doduynam_b22dcat199  
2025-03-08T20:58:33.067308+07:00 DoDuyNamB22DCAT199 useradd[5268]: failed adding user 'doduynam_b22dcat199', exit code: 9  
2025-03-08T20:59:17.082807+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ; PWD=/home/namdory ; USER=root ; COMMAND=/usr/sbin/useradd namdd_b22dcat199  
2025-03-08T20:59:17.115661+07:00 DoDuyNamB22DCAT199 useradd[5275]: new group: name=namdd_b22dcat199, GID=1004  
2025-03-08T20:59:17.116231+07:00 DoDuyNamB22DCAT199 useradd[5275]: new user: name=namdd_b22dcat199, UID=1004, GID=1004, home=/home/namdd_b22dcat199, shell=/bin/sh, from=/dev/pts/3  
namdory@DoDuyNamB22DCAT199:~$  
  
Microsoft Windows [Version 10.0.26100.3194]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\doduy>date  
The current date is: 08/03/2025  
Enter the new date: (dd-mm-yy)  
  
C:\Users\doduy>echo DoDuyNam_B22DCAT199  
DoDuyNam_B22DCAT199  
  
C:\Users\doduy>
```

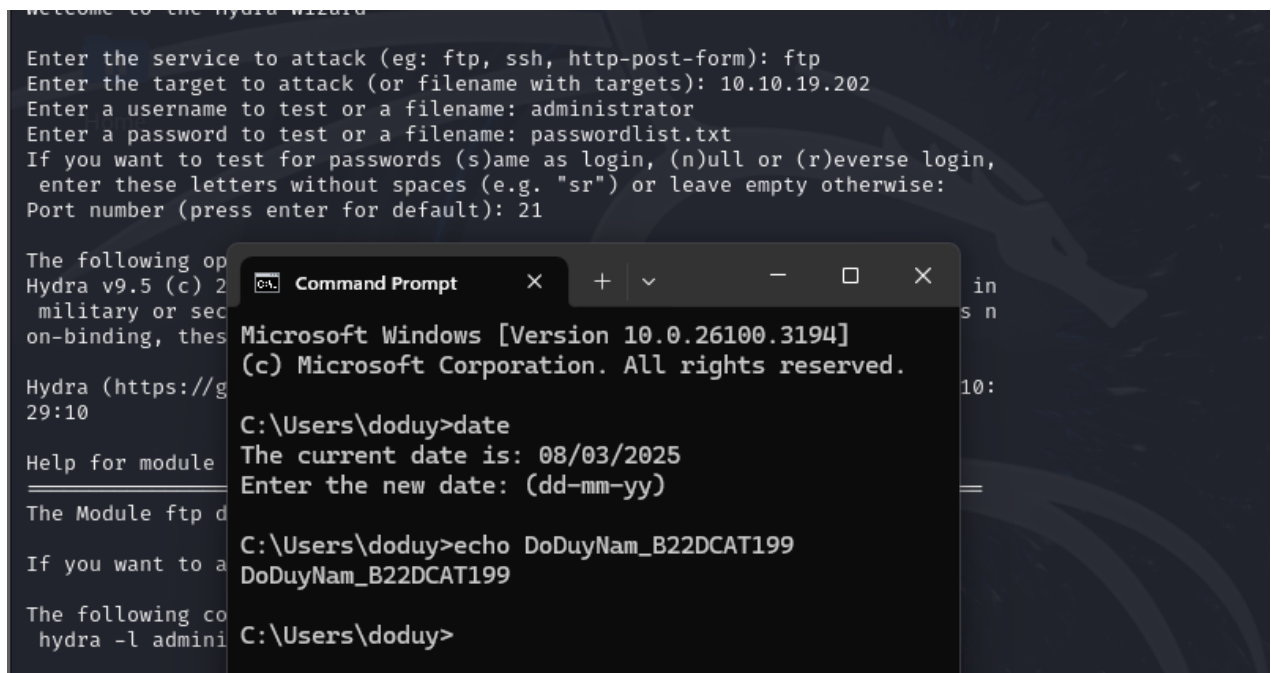
Hình 10 Dùng lệnh grep

```
namdory@DoDuyNamB22DCAT199: ~  
File Actions Edit View Help  
namdory@DoDuyNamB22DCAT199:~$ awk '/useradd/ {print}' /var/log/auth.log  
2025-03-06T23:39:36.467875+07:00 DoDuyNamB22DCAT199 useradd[5275]: new user: name=ftp, UID=122, GID=124, home=/srv/ftp, shell=/usr/sbin/nologin, from=none  
2025-03-07T12:46:23.745039+07:00 DoDuyNamB22DCAT199 useradd[3669]: new user: name=sshd, UID=123, GID=65534, home=/run/ssh, shell=/usr/sbin/nologin, from=none  
2025-03-08T20:58:33.033815+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ; PWD=/home/namdory ; USER=root ; COMMAND=/usr/sbin/useradd doduynam_b22dcat199  
2025-03-08T20:58:33.067308+07:00 DoDuyNamB22DCAT199 useradd[5268]: failed adding user 'doduynam_b22dcat199', exit code: 9  
2025-03-08T20:59:17.082807+07:00 DoDuyNamB22DCAT199 sudo: namdory : TTY=pts/2 ; PWD=/home/namdory ; USER=root ; COMMAND=/usr/sbin/useradd namdd_b22dcat199  
2025-03-08T20:59:17.115661+07:00 DoDuyNamB22DCAT199 useradd[5275]: new group: name=namdd_b22dcat199, GID=1004  
2025-03-08T20:59:17.116231+07:00 DoDuyNamB22DCAT199 useradd[5275]: new user: name=namdd_b22dcat199, UID=1004, GID=1004, home=/home/namdd_b22dcat199, shell=/bin/sh, from=/dev/pts/3  
namdory@DoDuyNamB22DCAT199:~$  
  
Microsoft Windows [Version 10.0.26100.3194]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\doduy>date  
The current date is: 08/03/2025  
Enter the new date: (dd-mm-yy)  
  
C:\Users\doduy>echo DoDuyNam_B22DCAT199  
DoDuyNam_B22DCAT199  
  
C:\Users\doduy>
```

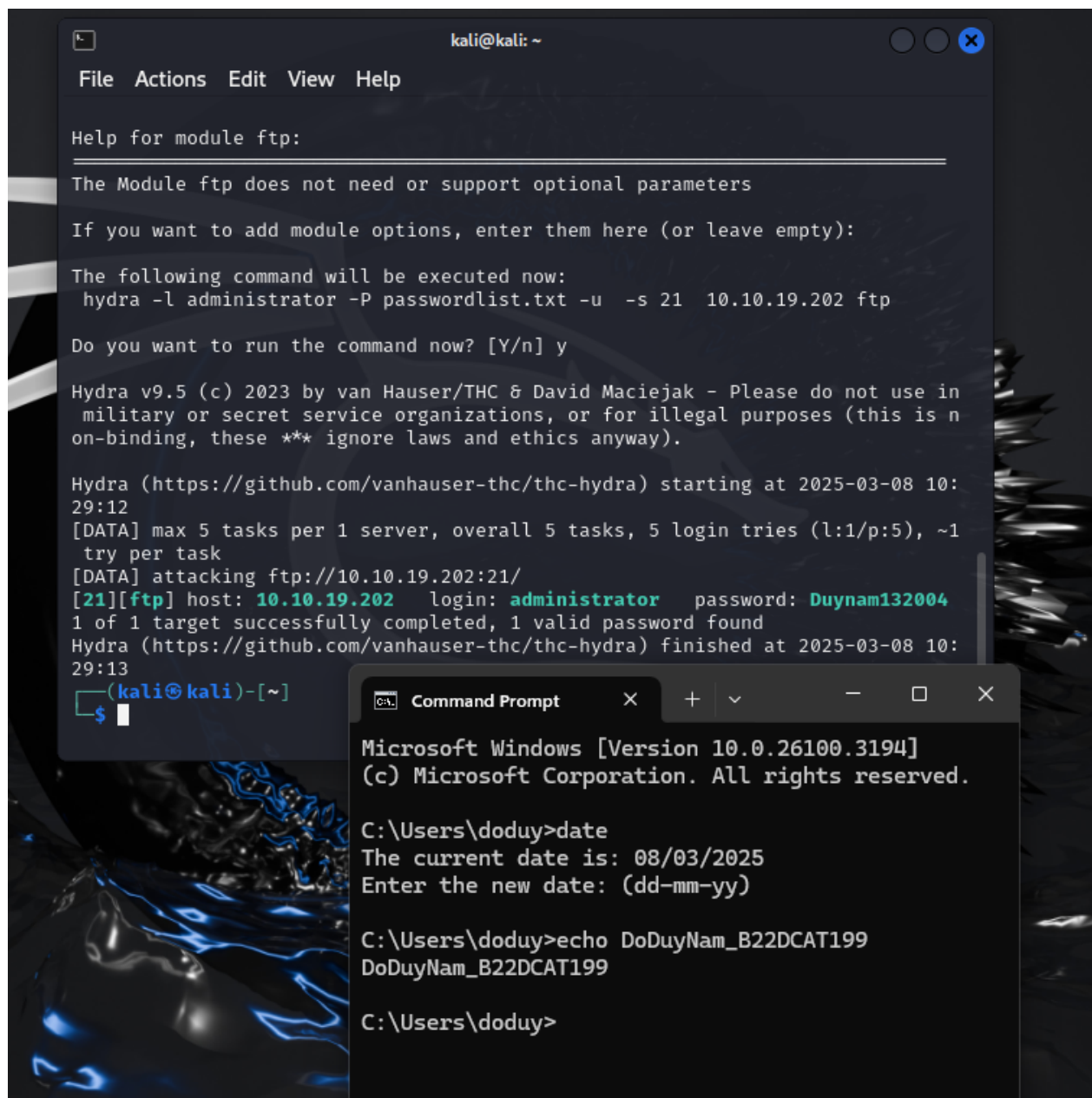
Hình 11 Sử dụng gawk

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, username là administrator, chọn file test password, chọn cổng 21 sau đó nhấn Start và chờ xHydra tìm ra mật khẩu

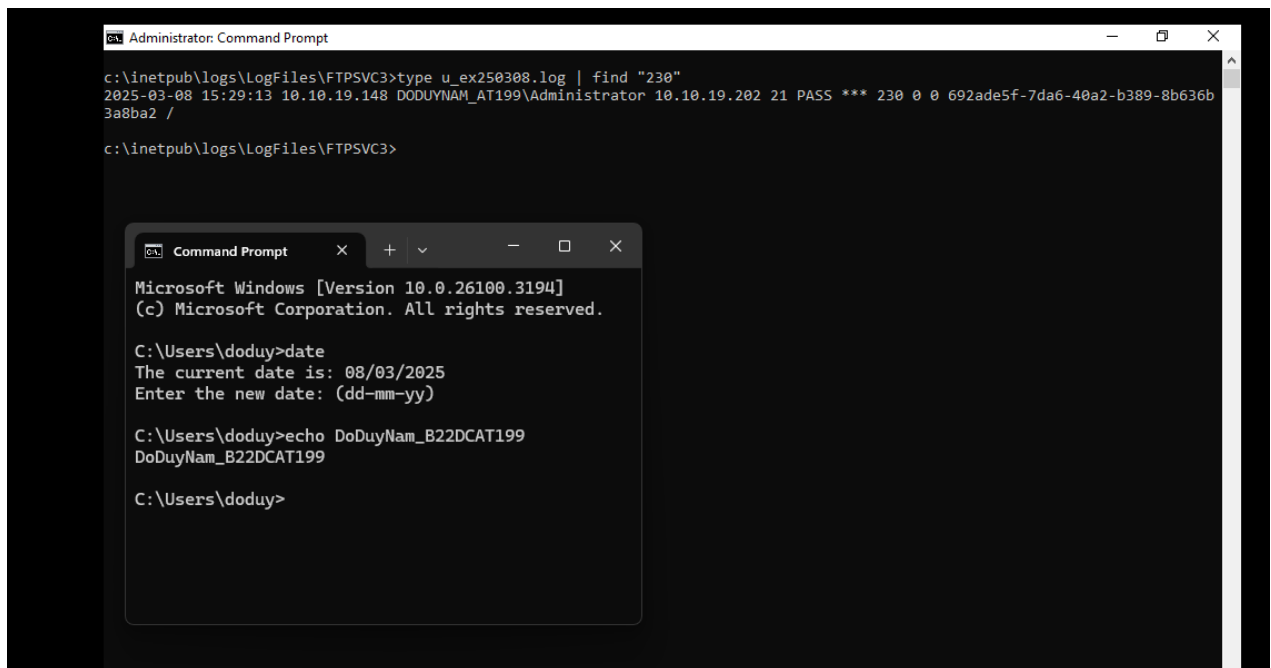


Hình 12 Cài đặt để xHydra tìm mật khẩu



Hình 13 xHydra đã thành công tìm được mật khẩu của tài khoản administrator

- Trên máy Windows 2019 Server External Victim, thực hiện điều hướng đến FTP Logfile bằng câu lệnh `cd c:\inetpub\logs\LogFiles\FTPSVC3`
- Gõ lệnh `type u_exyymmdd.log | find "230"` để tìm kiếm kết quả tấn công login thành công



Hình 14 Kết quả việc tấn công thành công

2.3 Kết luận

Ở chương này đã thực hiện phân tích log sử dụng grep và gawk trong linux và phân tích log sử dụng find trong Windows

KẾT LUẬN

- Tìm hiểu về Windows Event Viewer và Auditing
- Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk, find, secure, access_log,...
- Phân tích log thành công khi sử dụng grep/gawk trong Linux
- Phân tích log thành công khi sử dụng find trong Windows

-

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>