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

BÁO CÁO
Bài 9: Phân tích log hệ thống

Giảng viên hướng dẫn: Vũ Minh Mạnh
Sinh viên thực hiện: Nguyễn Quốc Vượng
Mã sinh viên: B21DCAT227
Lớp: D21CQAT03-B

HÀ NỘI, 2024

Môn học Thực tập cơ sở

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:

1. Phân tích log sử dụng grep/gawk trong Linux
2. Phân tích log sử dụng find trong Windows
3. Tìm hiểu về Windows Event Viewer và auditing
4. Phân tích event log trong Windows

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

- Tìm hiểu về Windows Event Viewer và auditing:

Windows Event Viewer: Là một công cụ trên hệ điều hành Windows cho phép người dùng xem và quản lý các sự kiện được ghi lại trong hệ thống. Event Viewer cho phép bạn xem các loại sự kiện khác nhau, bao gồm thông tin về hệ thống, bảo mật, ứng dụng và nhiều hơn nữa. Bằng cách sử dụng Event Viewer, người quản trị hệ thống có thể giám sát và chẩn đoán sự kiện và vấn đề trong hệ thống Windows.

Auditing (Kiểm toán): Là quá trình theo dõi và ghi lại các hoạt động trong hệ thống hoặc mạng máy tính. Trong ngữ cảnh của hệ điều hành Windows, auditing thường được sử dụng để giám sát và ghi lại các hoạt động liên quan đến bảo mật, như đăng nhập, truy cập vào tập tin và thư mục, thay đổi cấu hình và nhiều hoạt động khác.

- Tìm hiểu về ý nghĩa của một số lệnh dùng cho quá trình phân tích log: grep, gawk, find, secure, access_log, …

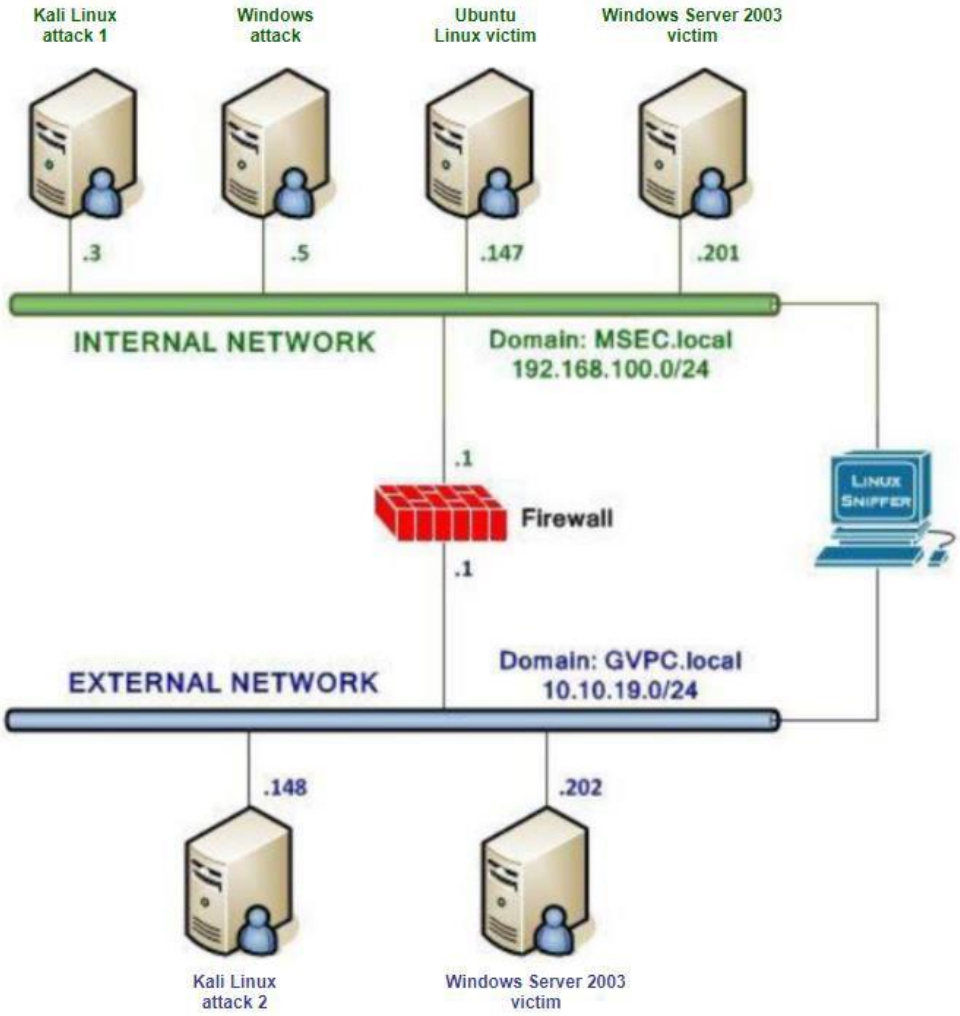
grep: Là một công cụ dòng lệnh được sử dụng để tìm kiếm các dòng trong văn bản hoặc tập tin và trả về các dòng chứa các chuỗi phù hợp với mẫu tìm kiếm được chỉ định.
gawk: Là một triển khai GNU của lệnh awk, một ngôn ngữ lập trình dòng lệnh và một công cụ xử lý văn bản mạnh mẽ. Gawk cung cấp nhiều tính năng mạnh mẽ để phân tích và xử lý văn bản, bao gồm việc tìm kiếm, xử lý và trích xuất dữ liệu từ các tệp văn bản.

find: Là một công cụ dòng lệnh được sử dụng để tìm kiếm và liệt kê các tệp và thư mục trong hệ thống tệp dựa trên các tiêu chí tìm kiếm được cung cấp.
secure: Trong ngữ cảnh của các hệ thống Unix và Linux, "secure" thường là một thư mục hoặc một tập tin log chứa các thông tin về các hoạt động bảo mật trên hệ thống, bao gồm đăng nhập và các sự kiện bảo mật khác.
access_log: Là một tệp log thường được sử dụng trong máy chủ web để ghi lại các yêu cầu truy cập đến các tài nguyên web. Tập tin log này chứa thông tin về IP của máy khách, thời gian truy cập, URL được truy cập và nhiều thông tin khác liên quan đến việc truy cập vào các tài nguyên web.

- Event log trong Windows là một cơ chế quan trọng để ghi lại các sự kiện quan trọng xảy ra trong hệ thống như đăng nhập, lỗi ứng dụng, và hoạt động bảo mật. Các loại sự kiện chính bao gồm Application, Security, System, và Setup. Dữ liệu trong event log cung cấp thông tin quan trọng để giám sát và phân tích hoạt động của hệ thống, giúp người quản trị hệ thống phát hiện và giải quyết các vấn đề một cách hiệu quả. Event log có thể được truy cập và quản lý thông qua Event Viewer, một công cụ tích hợp trong Windows.
  - Tài liệu tham khảo:
    - grep: https://linuxcommand.org/lc3_man_pages/grep1.html
    - gawk: http://www.gnu.org/software/gawk/manual/gawk.html
    - find:https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find
    - xhydra: http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html

2.2 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.

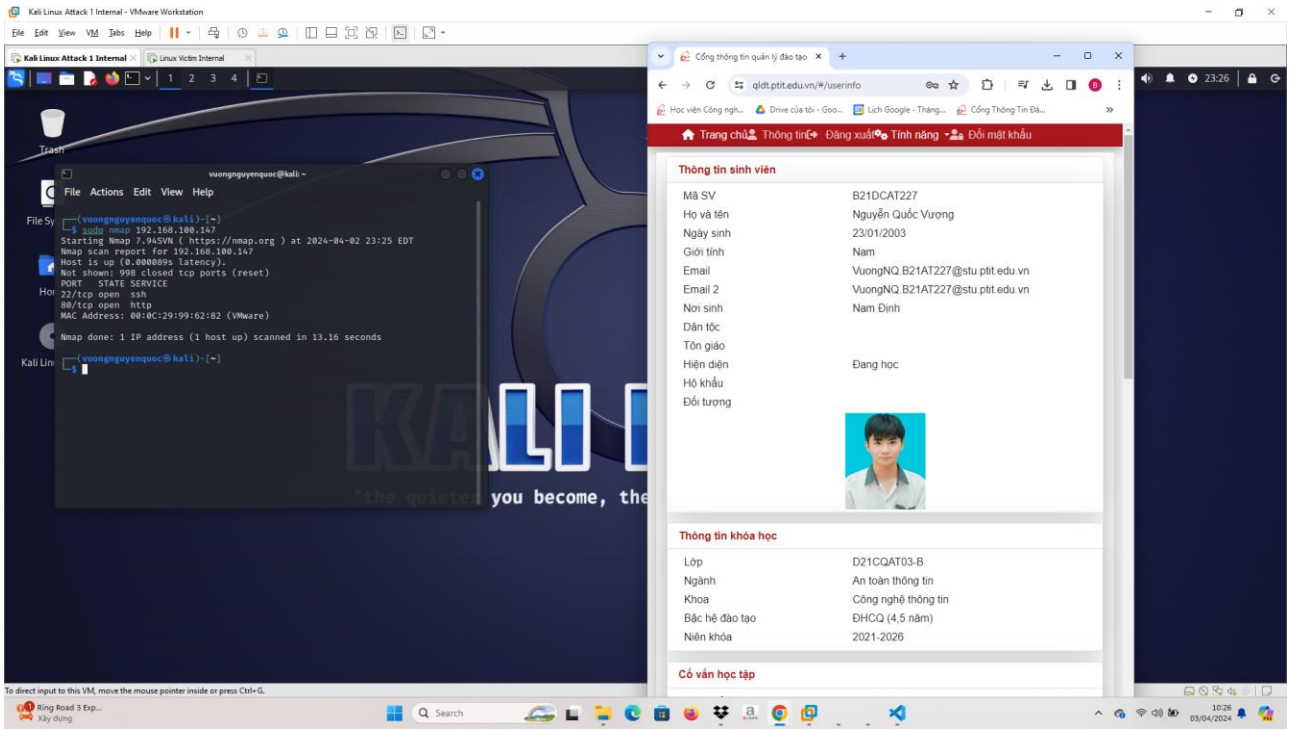


2.3 Các bước thực hiện và kết quả cần đạt

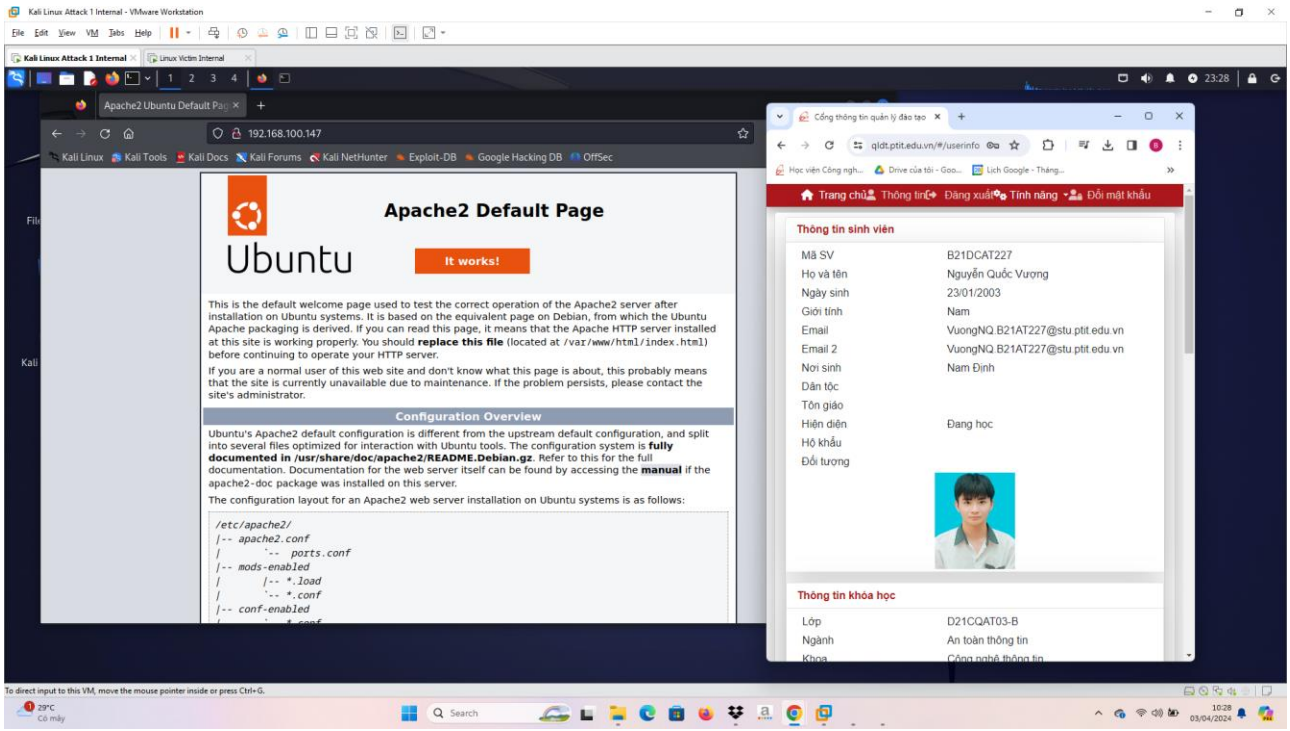
2.3.1 Phân tích log sử dụng grep trong Linux

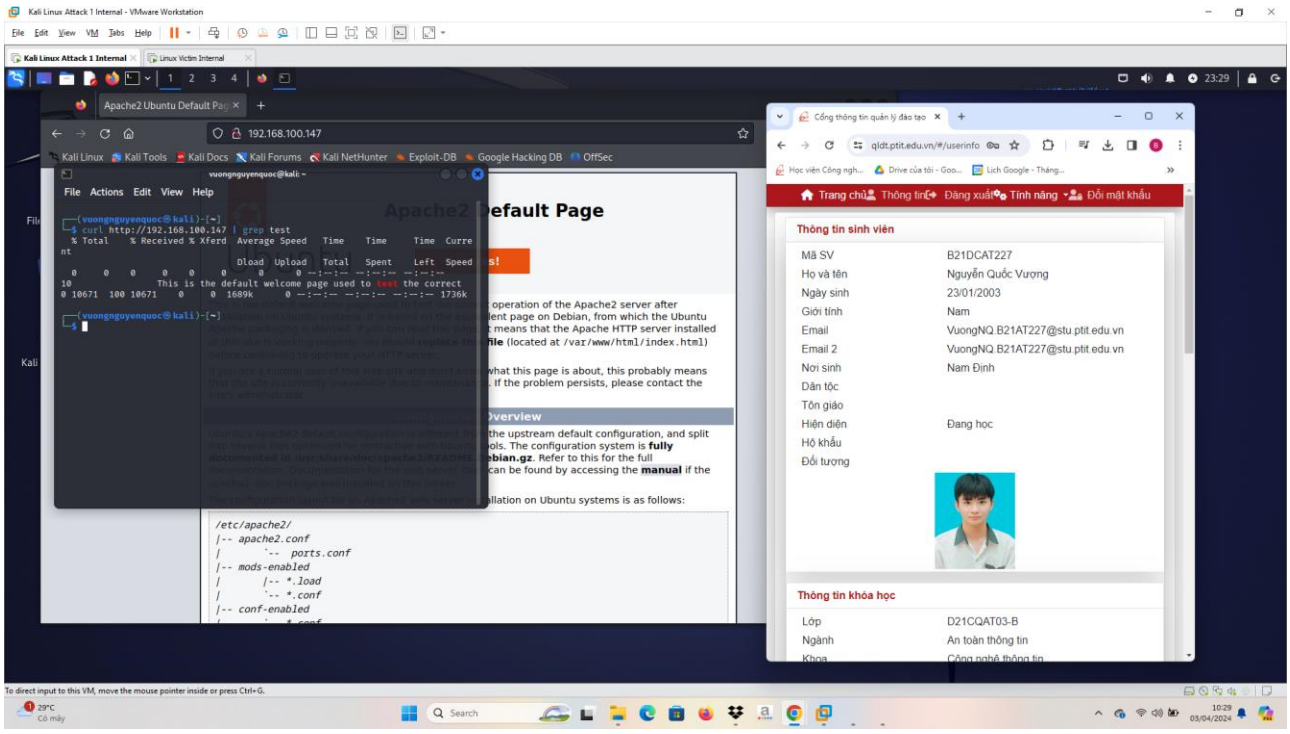
a) Các bước thực hiện

- Trên máy Kali attack trong mạng Internal, khởi chạy nmap 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



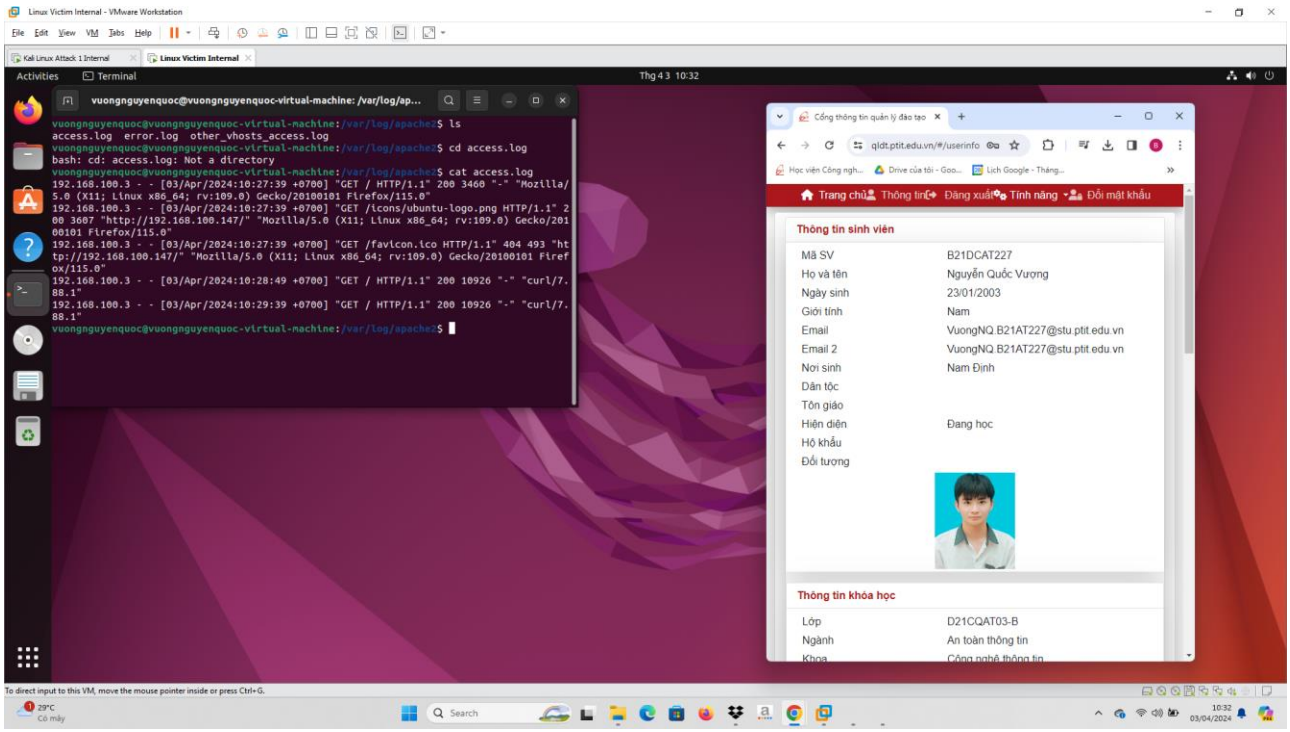
- Trên máy Kali attack ở mạng Internal, truy cập địa chỉ web http://192.168.100.147. Trên terminal tiến hành sao chép website và tìm kiếm từ khóa "test"(root@bt:~#**curl http://192.168.100.147 grep test)**





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

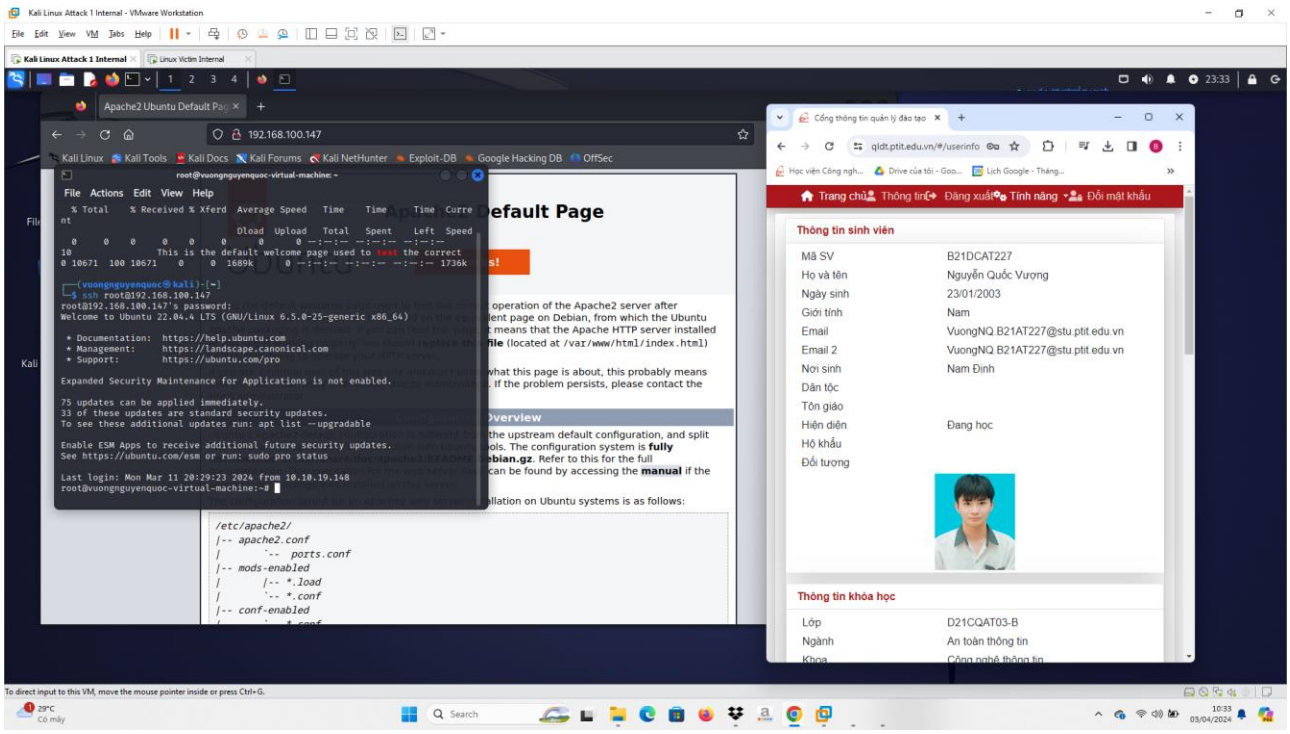
  [root@rhel ~]# **cd /var/log/apache2**

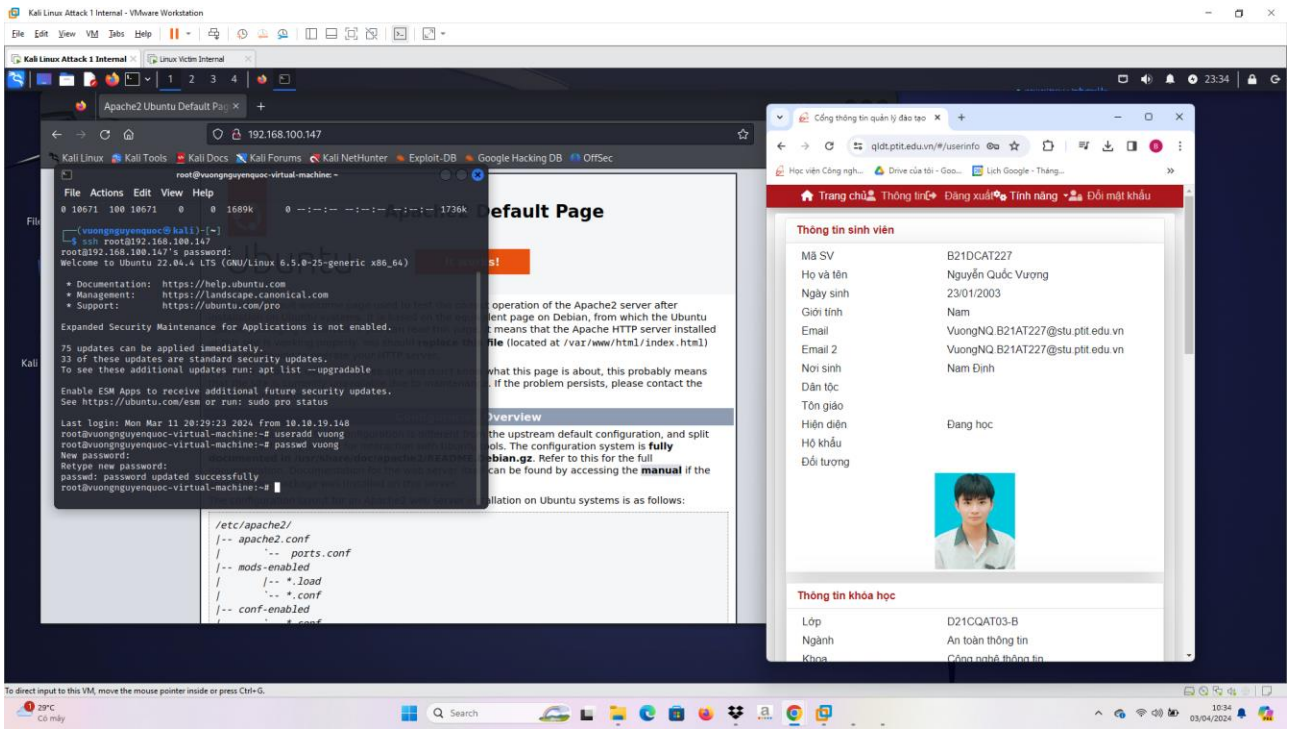


2.3.2 Phân tích log sử dụng gawk trong Linux

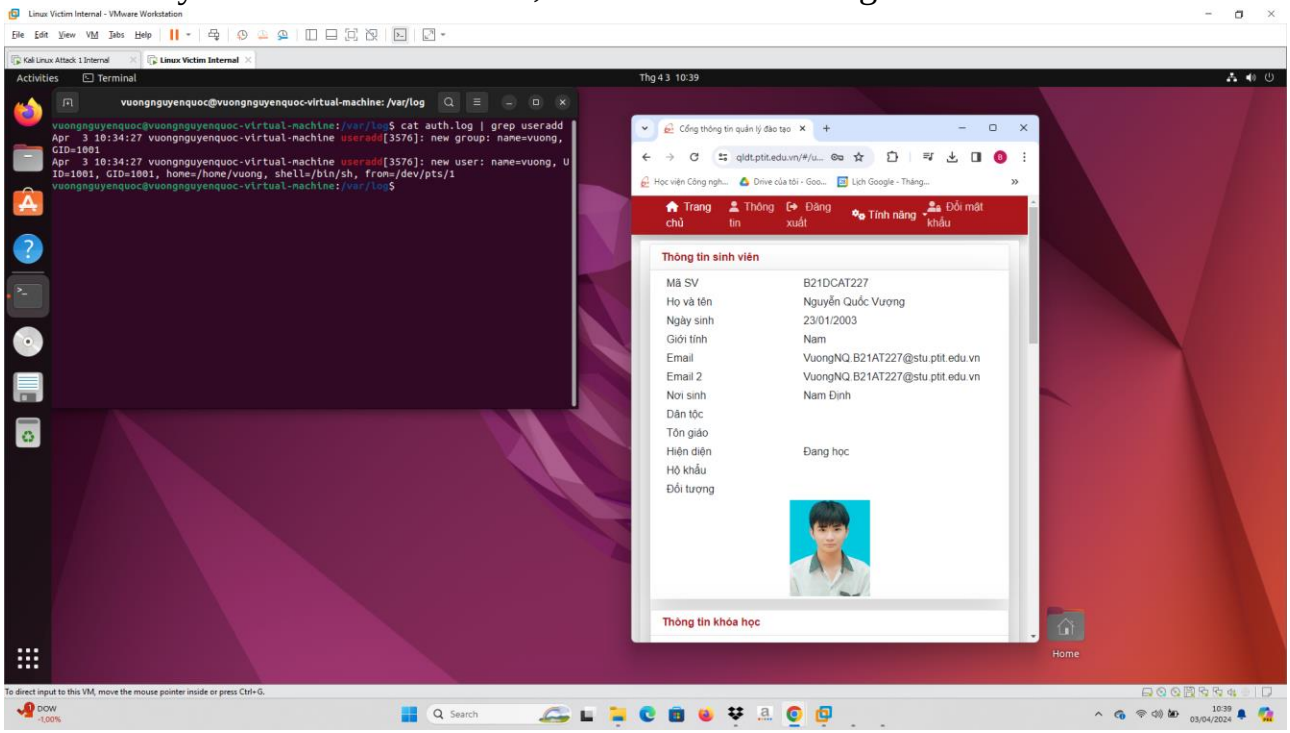
a) Các bước thực hiện

- 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.

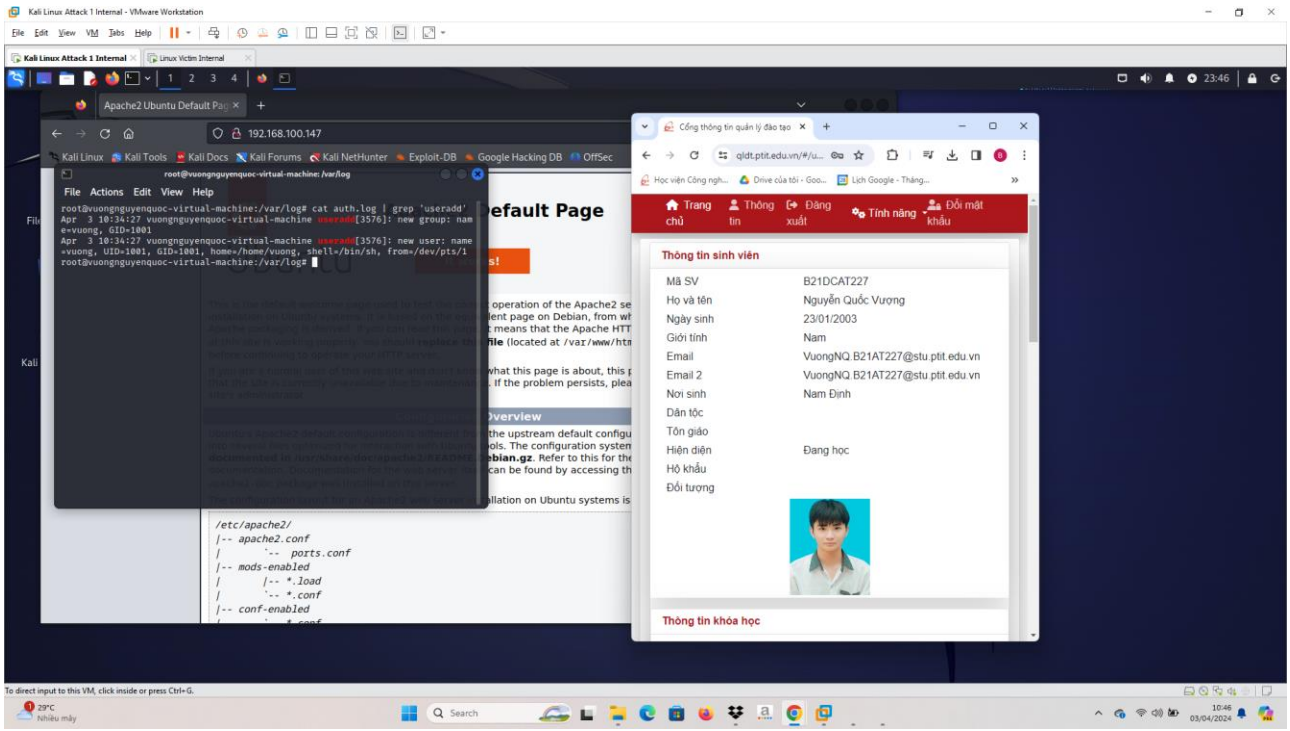


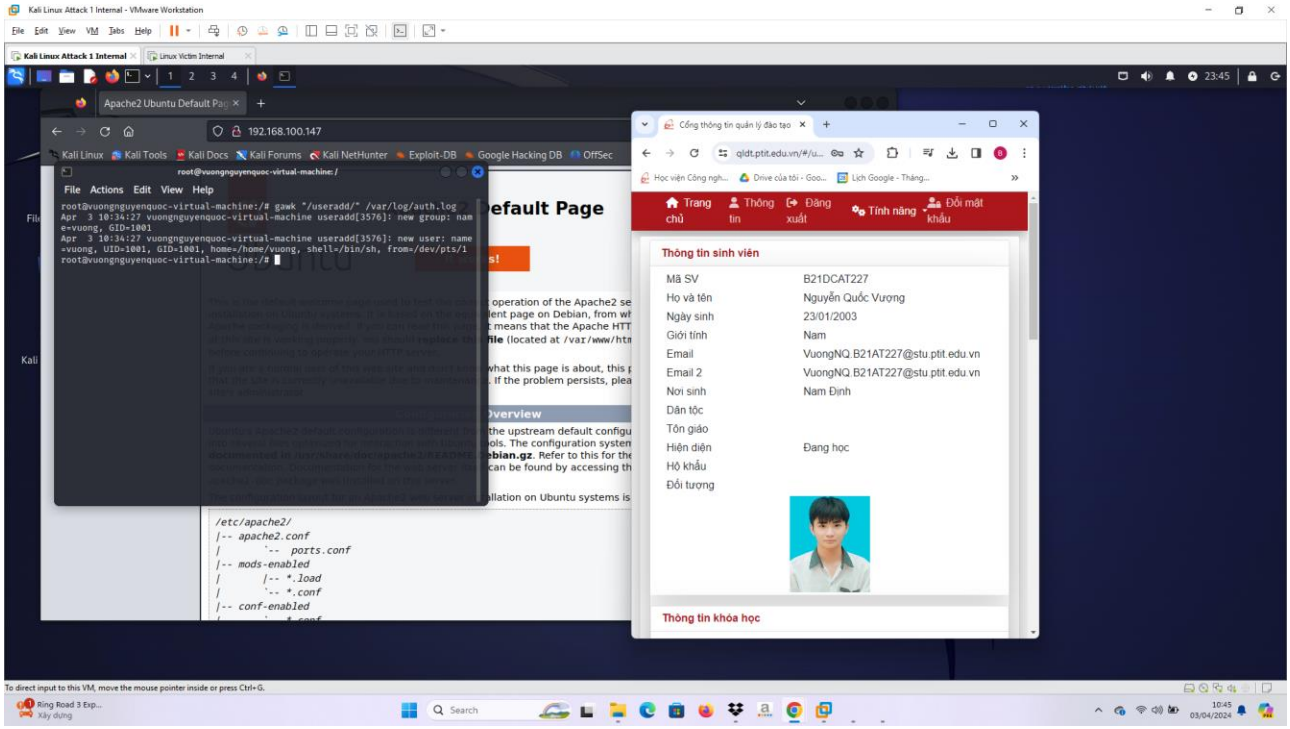


- Trên máy Linux Internal Victim, tiến hành xem file log



- 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.

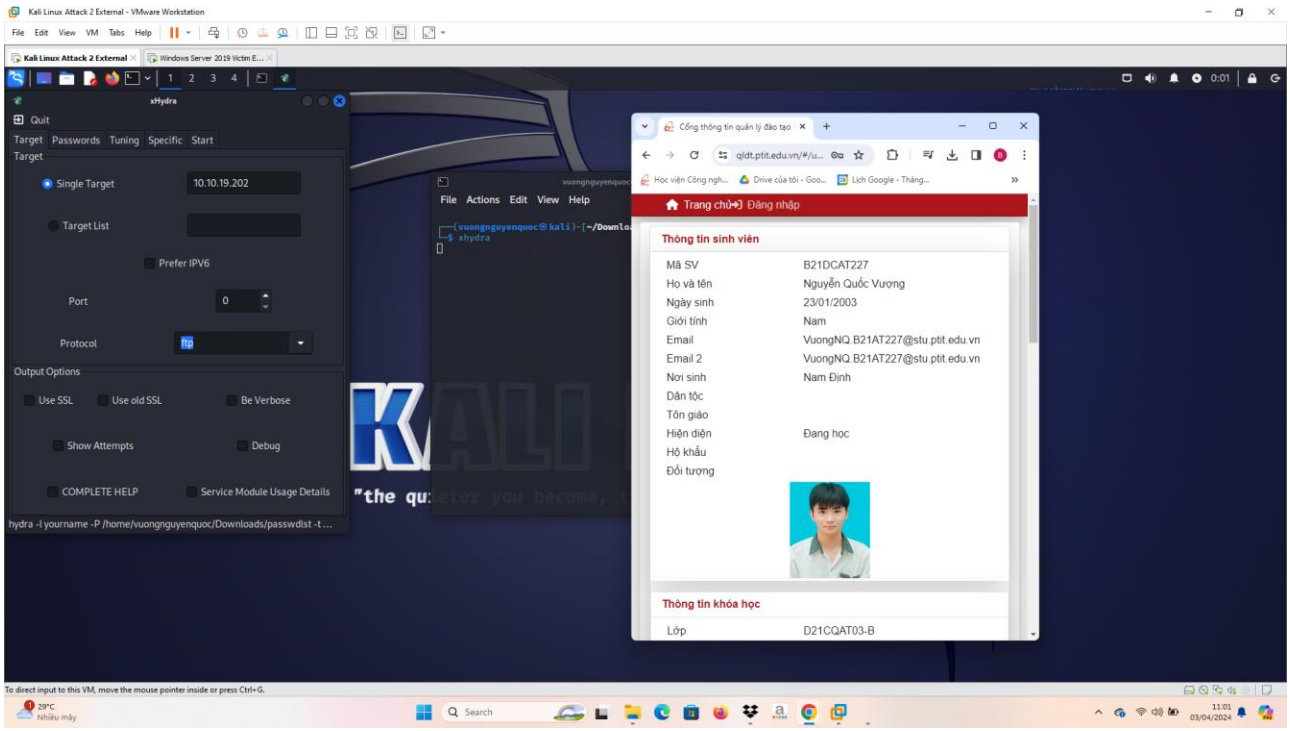


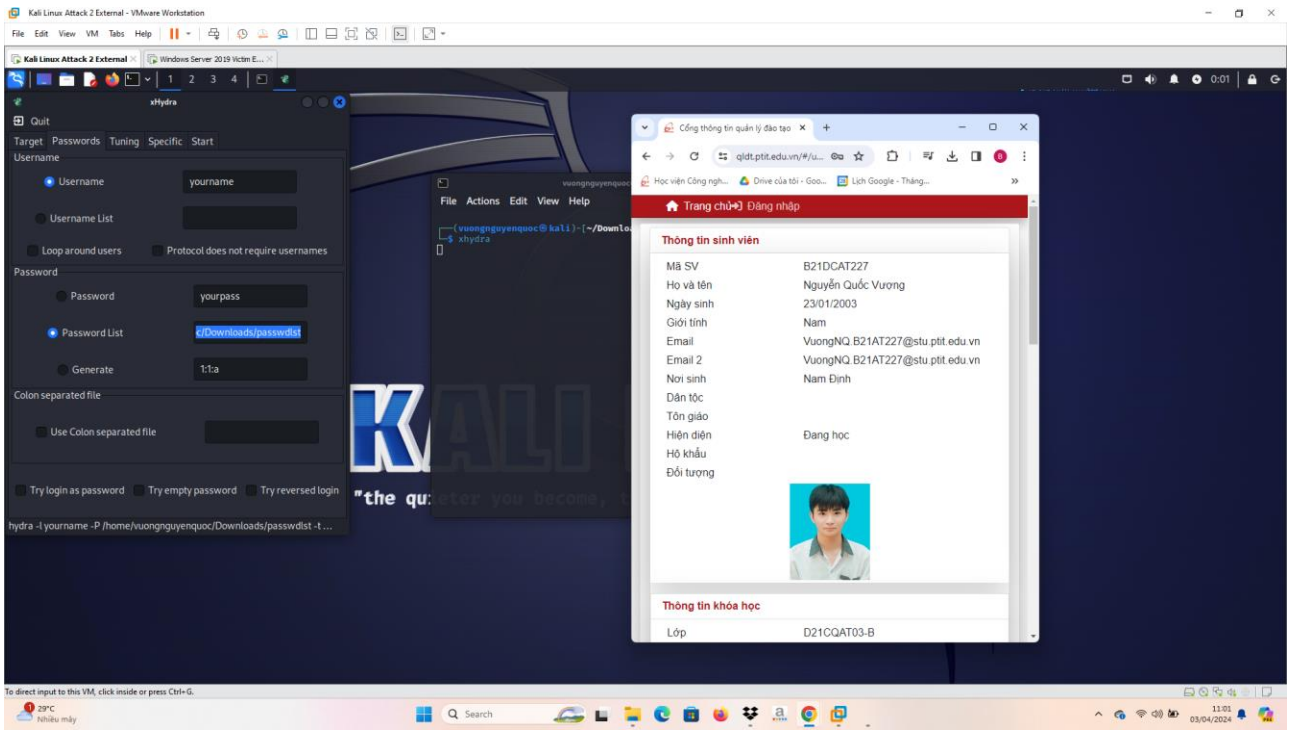


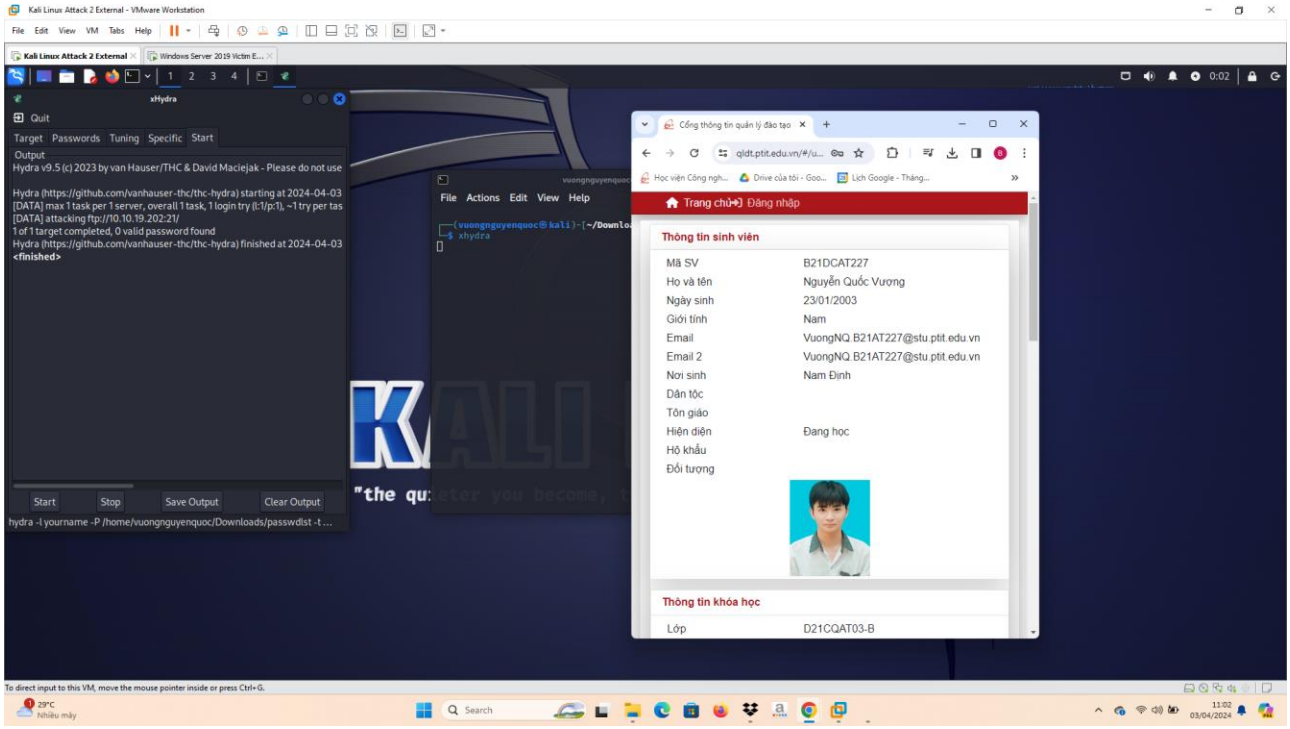
2.3.3 Phân tích log sử dụng find trong Windows

a) Các bước thực hiện

- 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







- Trên máy Windows 2003 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