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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SSH	Secure Shell	Vỏ an toàn
FTP	File Transfer Protocol	Giao thức truyền file
IP	Internet Protocol	Giao thức mạng
HTTP	Hyper Text Transfer Protocol	Giao thức truyền siêu văn bản

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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

1.2 Tìm hiểu lý thuyết

1.2.1 Một số lệnh dùng cho quá trình phân tích log

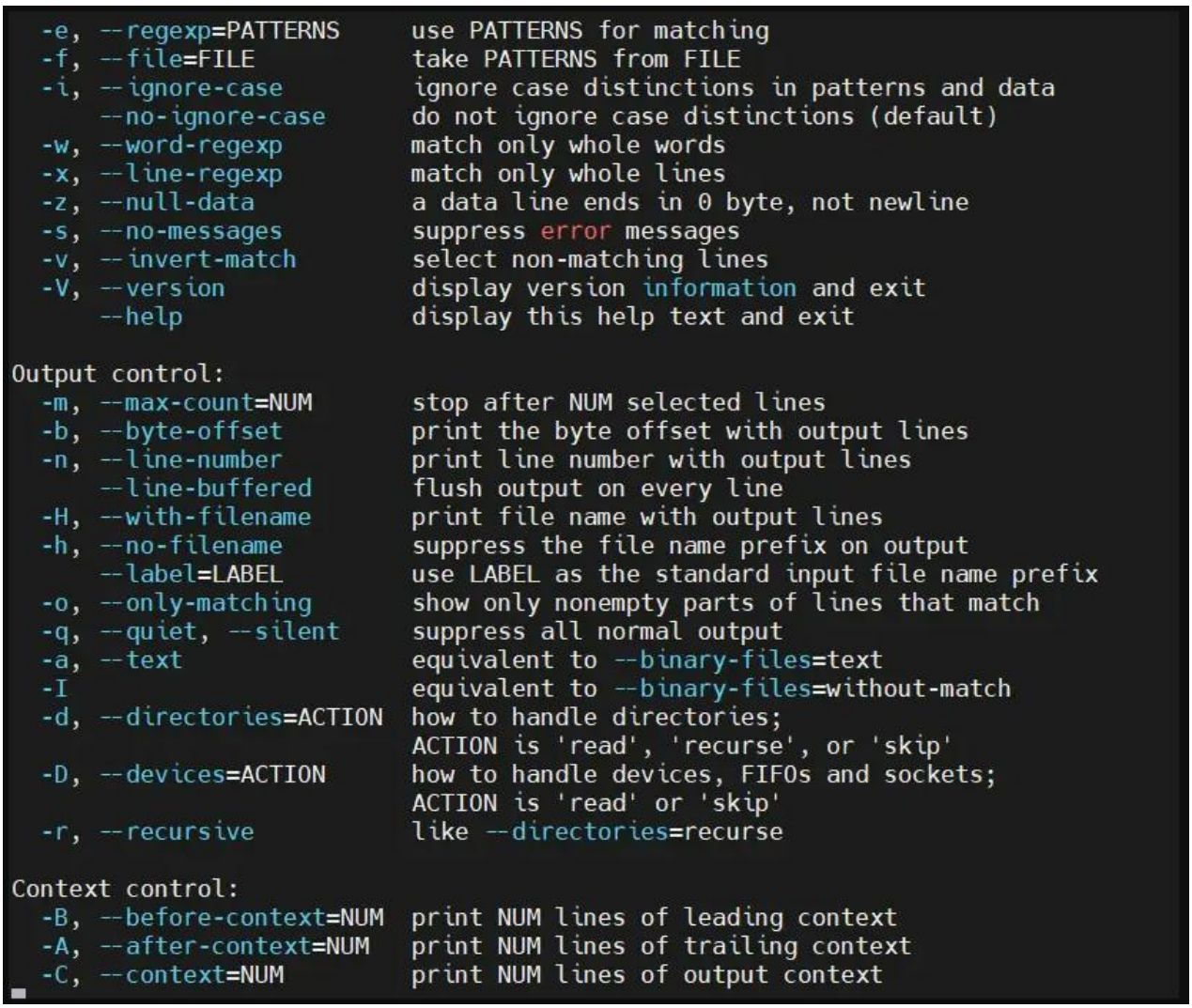
1.2.1.1 Lệnh "grep"

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]

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 (-i)
- Tìm kiếm ngược sử dụng tùy chọn (-v)
- Hiển thị số dòng (-n), số lượng (-c), giới hạn số dòng đầu ra (-m N)
- Tìm kiếm nhiều chuỗi (-e)
- Tìm kiếm trên tệp (-a)
- Hiển thị thêm dòng trước (-B), sau (-A), xung quanh (-C) dòng chứa kết quả cần tìm.



Hình 1 Các tùy chọn của lệnh "grep"

1.2.1.2 Lệnh "gawk"

Lệnh gawk trong Linux là một ngôn ngữ quét mẫu và xử lý văn bản. Không cần biên dịch, và có thể sử dụng các biến cùng với các hàm số học, hàm chuỗi và toán tử logic.

Gawk là một tiện ích cho phép lập trình viên viết các chương trình ngắn gọn nhưng hiệu quả bằng cách xác định các mẫu văn bản cần tìm trong một tài liệu, cũng như hành động cần thực hiện mỗi khi tìm thấy một dòng khớp với mẫu đó.

Gawk có thể được sử dụng để:

- Quét tệp từng dòng một
- Chia nhỏ mỗi dòng đầu vào thành các trường
- So sánh dòng/trường đầu vào với mẫu xác định
- Thực hiện hành động trên các dòng khớp với mẫu
- Chuyển đổi tệp dữ liệu

- Tạo báo cáo định dạng
- Định dạng dòng đầu ra
- Thực hiện các phép toán số học và xử lý chuỗi
- Thực thi câu lệnh điều kiện và vòng lặp

1.2.1.3 Lệnh "find"

Lệnh find trong Linux là một công cụ mạnh mẽ để tìm kiếm tệp và thư mục theo nhiều tiêu chí khác nhau, chẳng hạn như tên, kích thước, kiểu tệp, thời gian chỉnh sửa, quyền truy cập, và nhiều yếu tố khác.

Cú pháp chung: find [đường_dẫn] [tùy_chọn] [biểu_thức_điều_kiện] [hành_động]

- đường_dẫn: Vị trí bắt đầu tìm kiếm (ví dụ: /home, . cho thư mục hiện tại, / cho toàn bộ hệ thống).
- tùy_chọn: Các tùy chọn như theo tên, kích thước, thời gian, quyền, v.v.
- biểu_thức_điều_kiện: Điều kiện lọc tệp hoặc thư mục cần tìm.
- hành_động: Thao tác thực hiện với các tệp tìm được (xóa, di chuyển, thực thi lệnh,...).

Các tùy chọn phổ biến của find:

- Tìm theo tên tệp hoặc thư mục (-name)
- Tìm theo loại tệp (-type)
- Tìm theo kích thước tệp (-size)
- Tìm theo thời gian chỉnh sửa (-mtime, -atime, -ctime)
- Tìm theo quyền (-perm)
- Tìm và thực hiện hành động (-exec, -delete)

1.2.1.4 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 ra 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.

1.2.1.5 Tệp "access_log"

Access_log là tệp 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.

1.2.1.6 Công cụ 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:

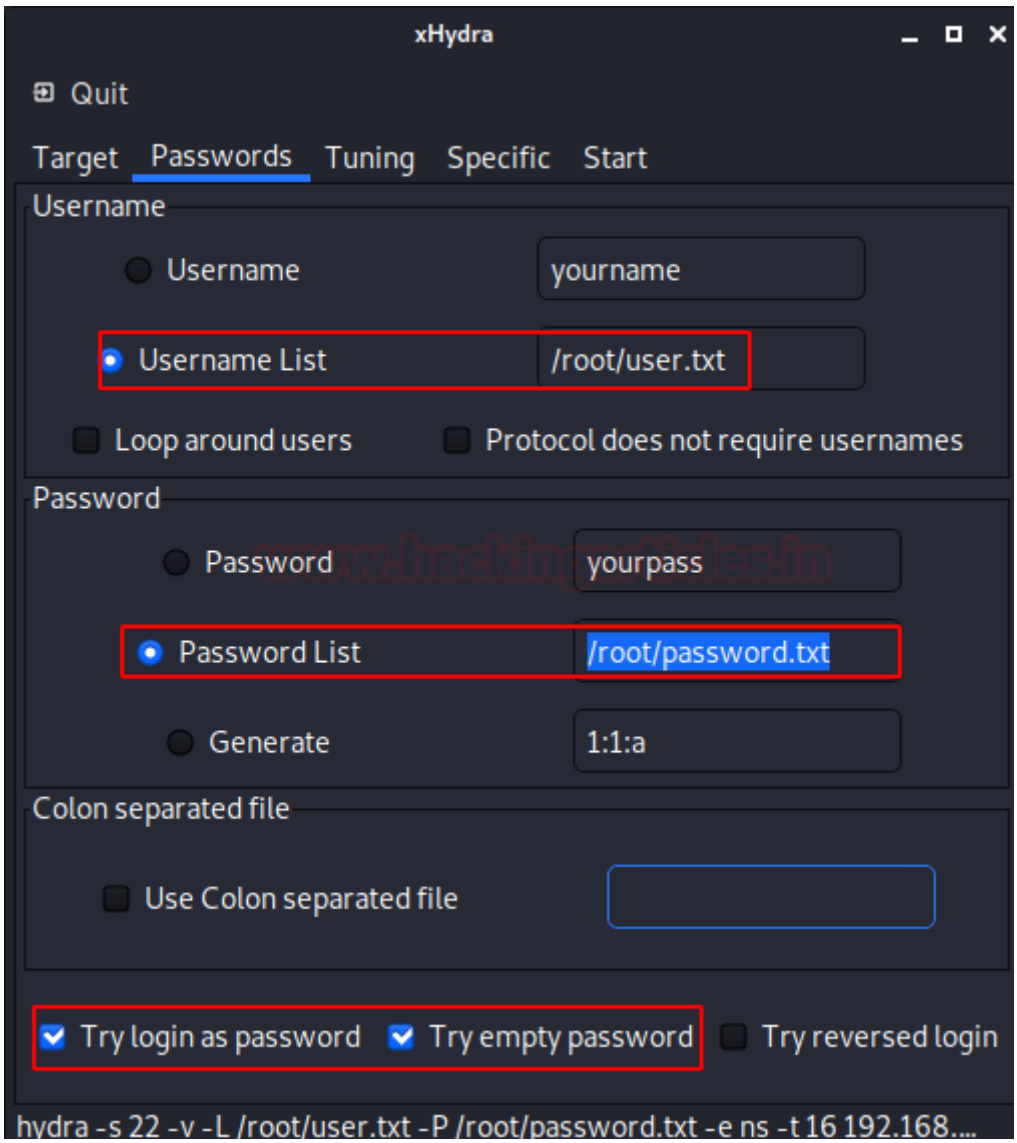
- Tấn công từ điển đa giao thức: xhydra cho phép thực hiện các cuộc tấn công từ điển trên nhiều giao thức như SSH, FTP, Telnet, MySQL, SMB,…

- 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.

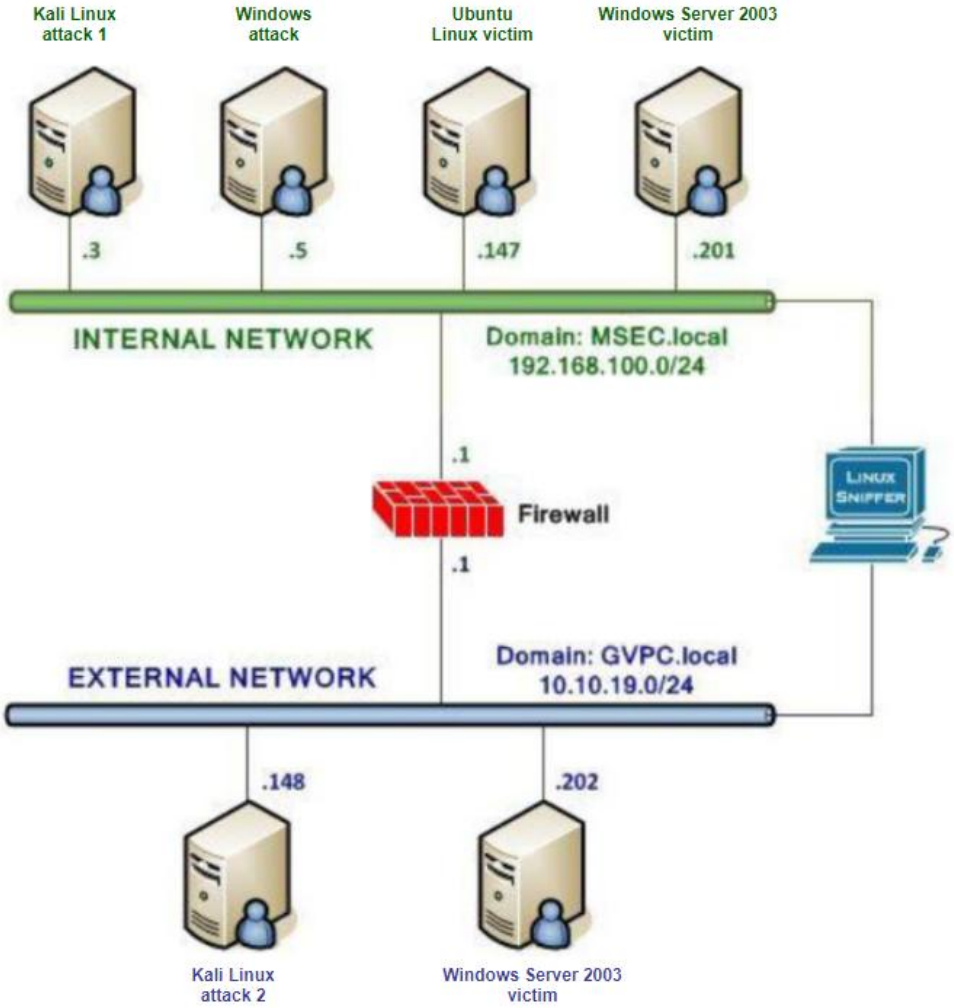


Hình 2 Giao diện làm việc của xhydra

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- File iso máy ảo Windows Server 2019, Ubuntu 20.04, Kali Linux.
- Phần mềm ảo hóa VMWare Workstation.



- Topo mạng cấu hình như trên. Trong bài này sẽ sử dụng máy Kali Linux attack 1 và Ubuntu victim ở mạng Internal; máy Kali Linux attack 2 và Windows Server ở mạng External.

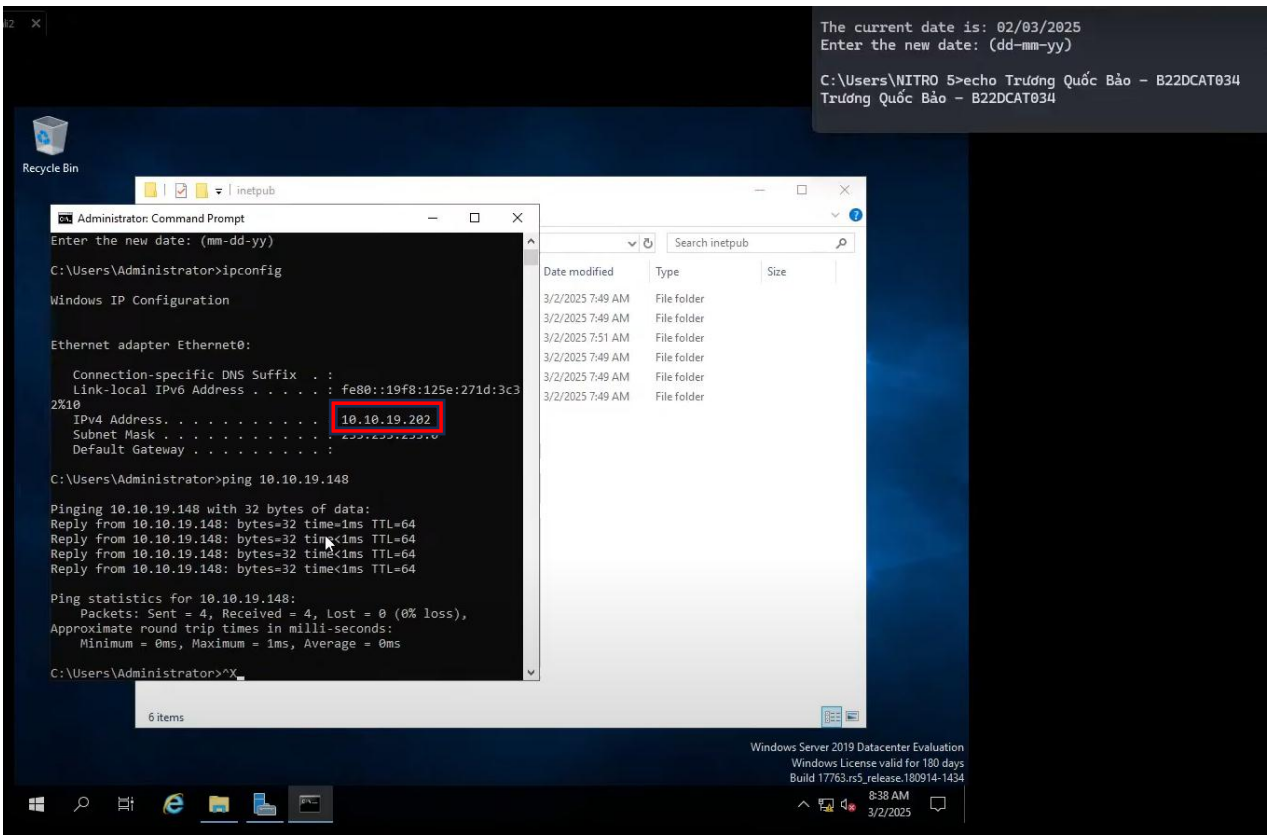
2.2 Các bước thực hiện

2.2.1 Chuẩn bị máy ảo

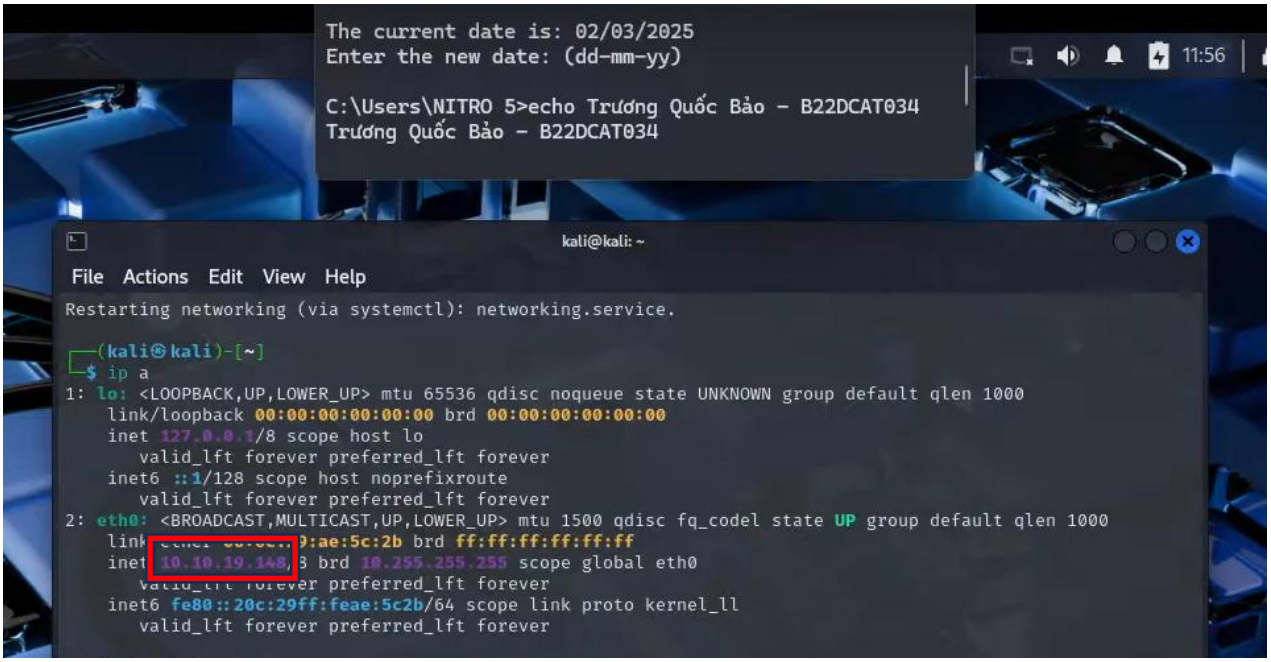
Ta cài đặt các máy ảo sử dụng file iso đã chuẩn bị như các bài trước đó.

Các máy trong mạng Internal cấu hình địa chỉ IP tĩnh như đã làm trong bài số 5.

Các máy trong mạng External cấu hình địa chỉ IP tĩnh như sau:



Hình 3 Địa chỉ IP của máy Windows Server

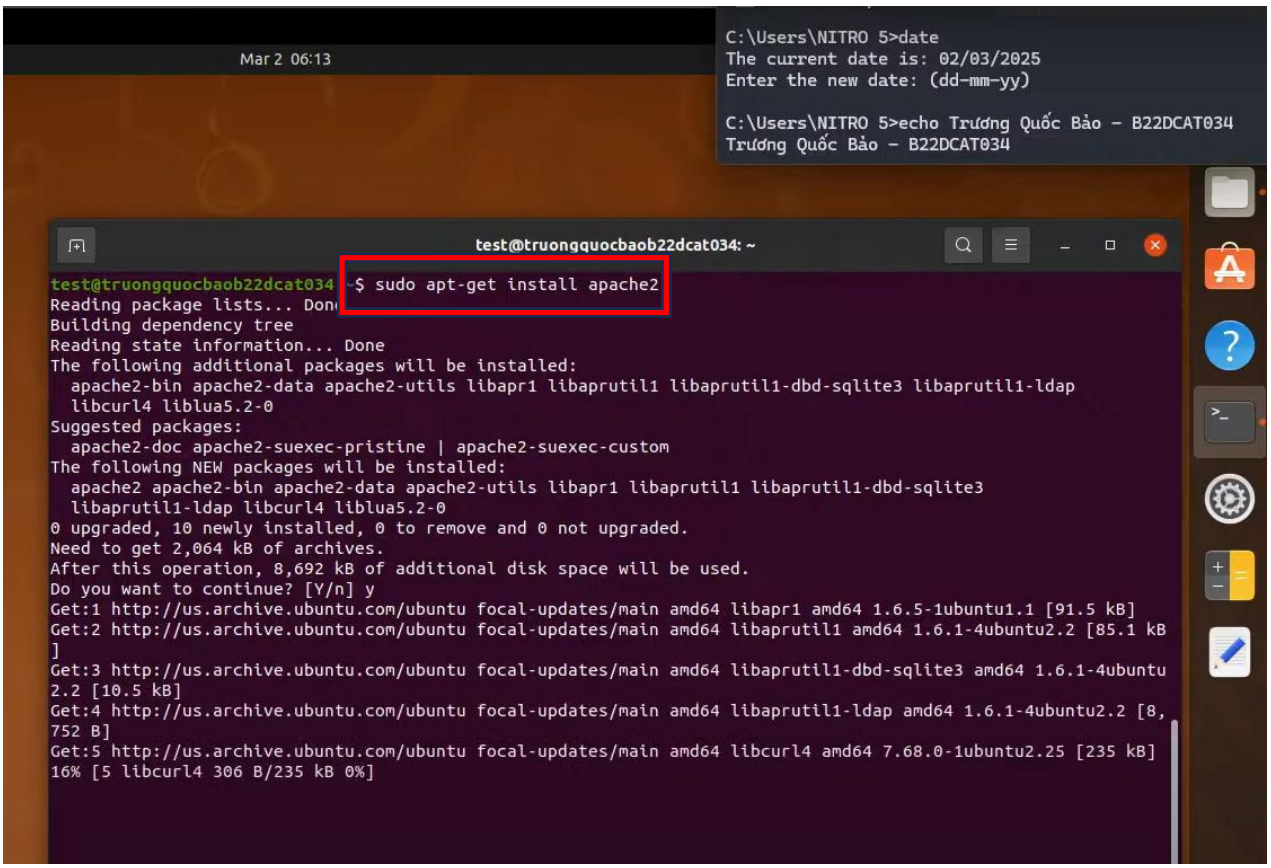


Hình 4 Địa chỉ IP của máy Kali Linux

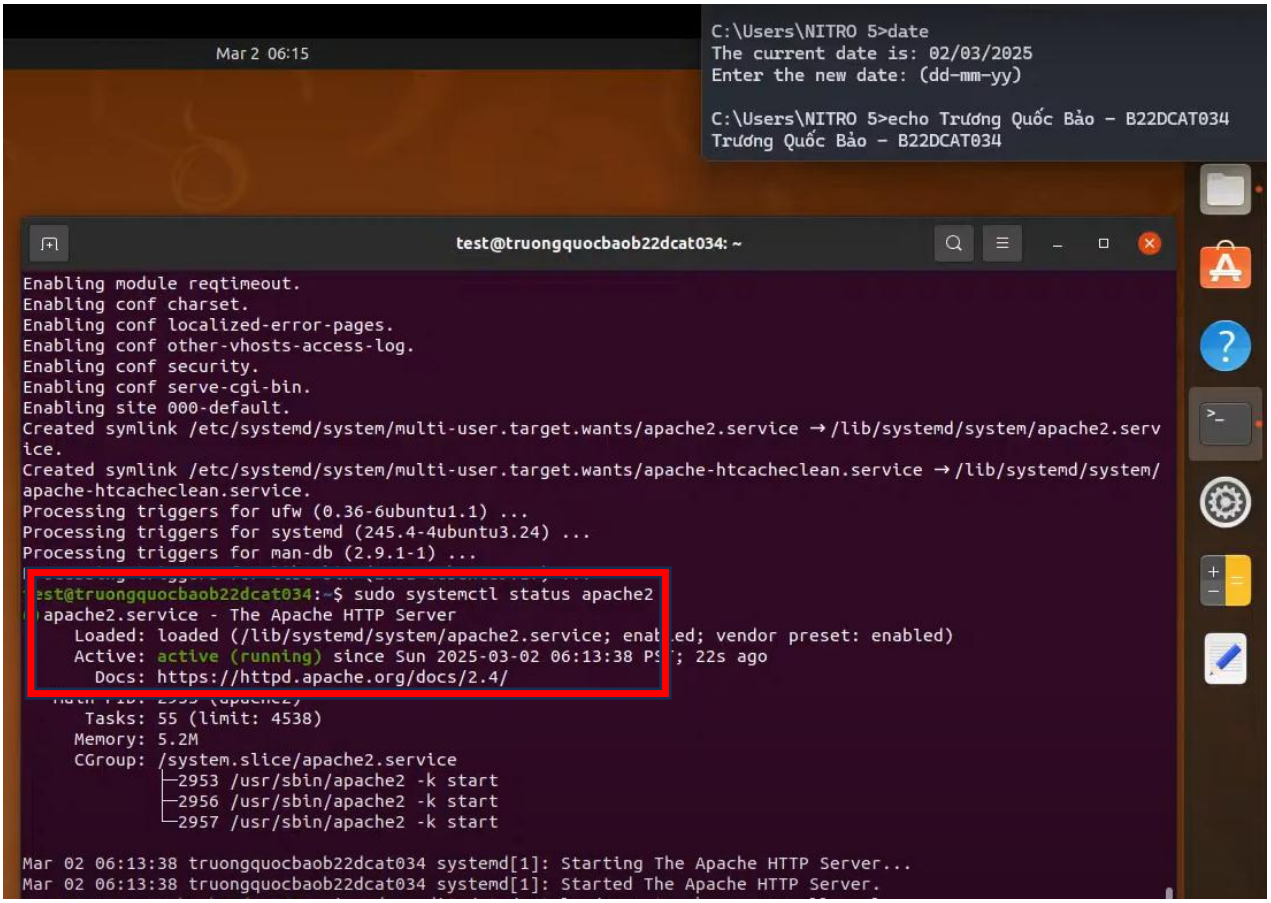
2.2.2 Phân tích log sử dụng grep trong Linux

Trên máy Ubuntu, cài đặt dịch vụ Web Apache bằng lệnh "sudo apt-get install apache2"

Và kiểm tra hoạt động của dịch vụ bằng lệnh "sudo systemctl status apache2", nếu hiện chữ màu xanh active (running) nghĩa là đã khởi động dịch vụ thành công.

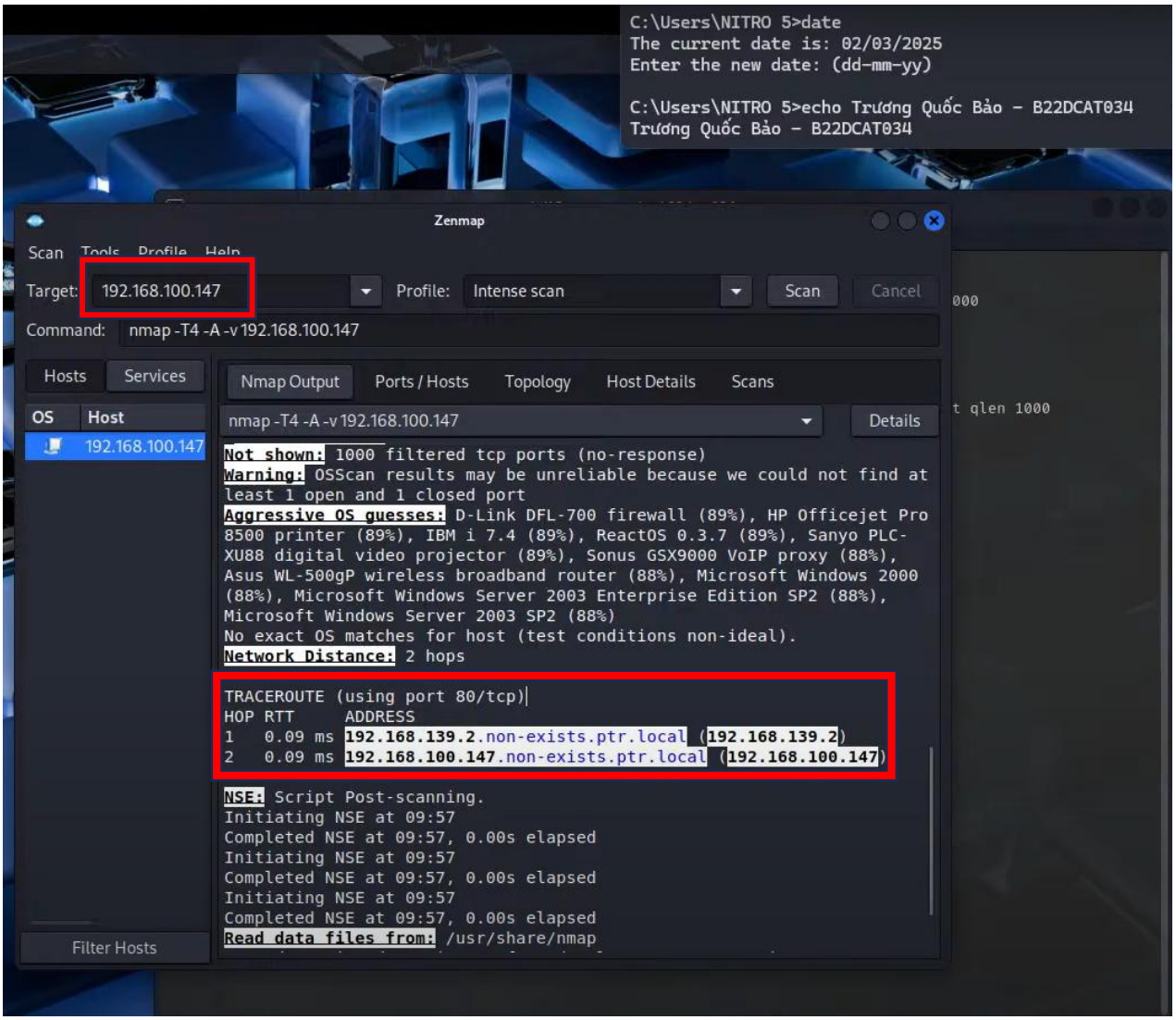


Hình 5 Cài đặt dịch vụ web apache trên máy Ubuntu



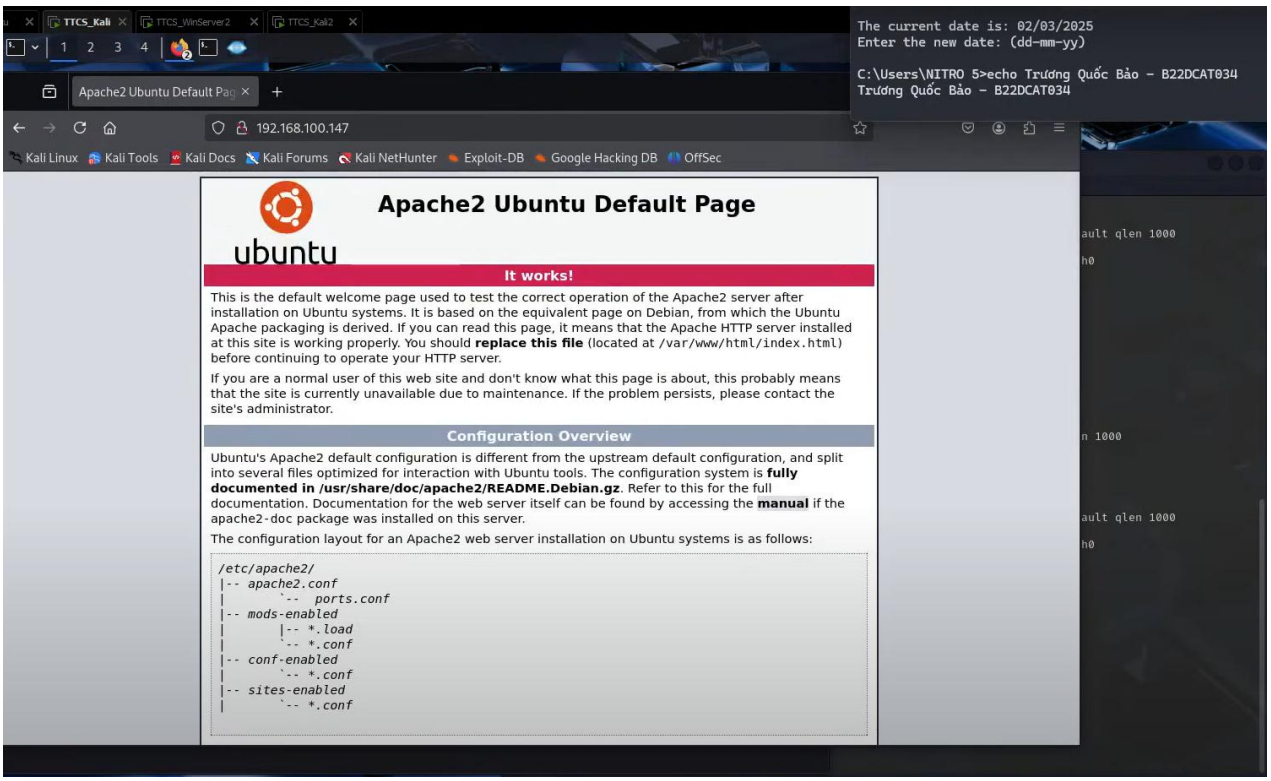
Hình 6 Kiểm tra trạng thái hoạt động của dịch vụ

Trên máy Kali attack, khởi chạy zenmap và scan cho địa chỉ 192.168.100.147 (địa chỉ IP của máy Ubuntu) và xem được port 80 đang mở cho Web Server Apache.



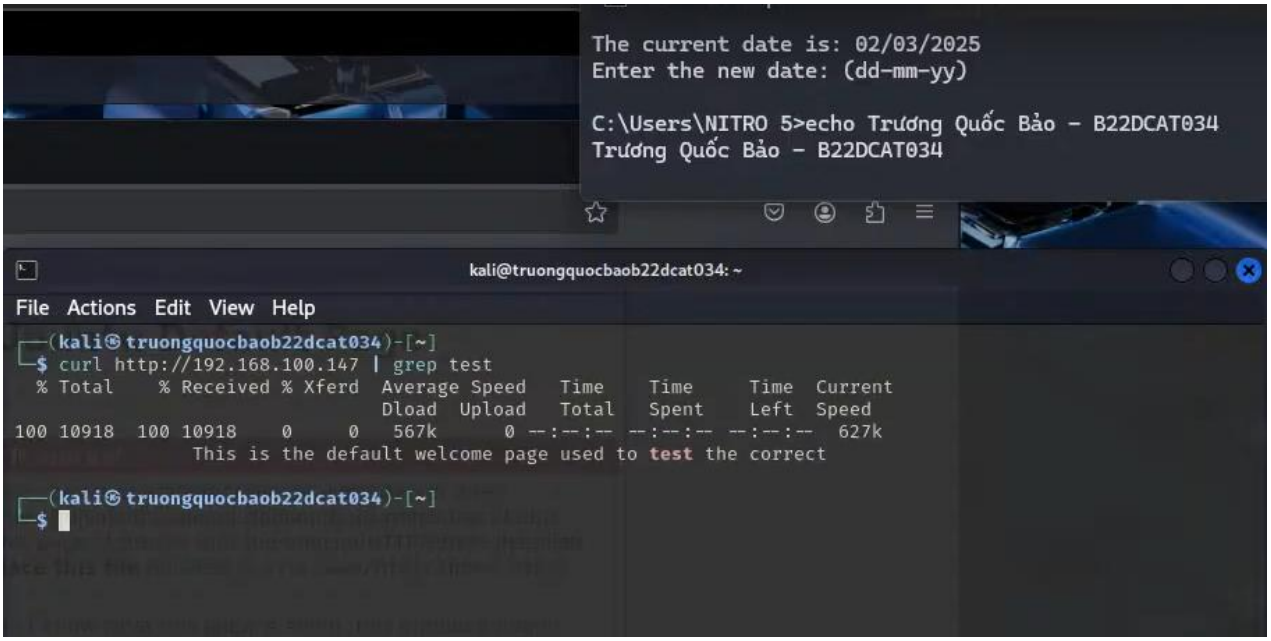
Hình 7 Sử dụng công cụ Zenmap để quét cổng dịch vụ

Trên máy Kali attack, truy cập địa chỉ web http://192.168.100.147, ta sẽ thấy giao diện web server apache giống của máy Ubuntu.



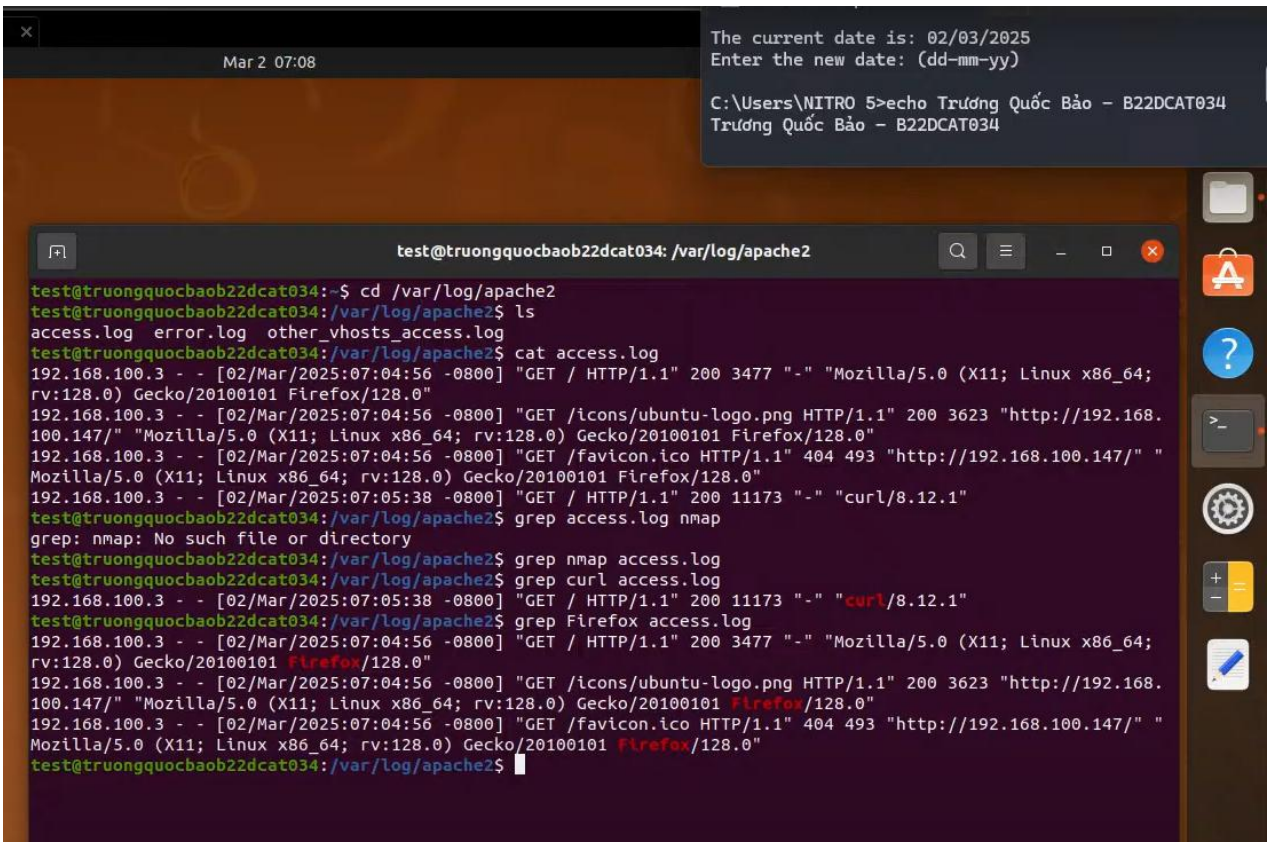
Hình 8 Truy cập vào dịch vụ web của máy Ubuntu

Trên máy Kali, gõ lệnh "curl http://192.168.100.147 | grep test" để tìm kiếm từ khóa "test" trên website vừa rồi.



Hình 9 Tìm kiếm từ khóa "test" thông qua lệnh "grep"

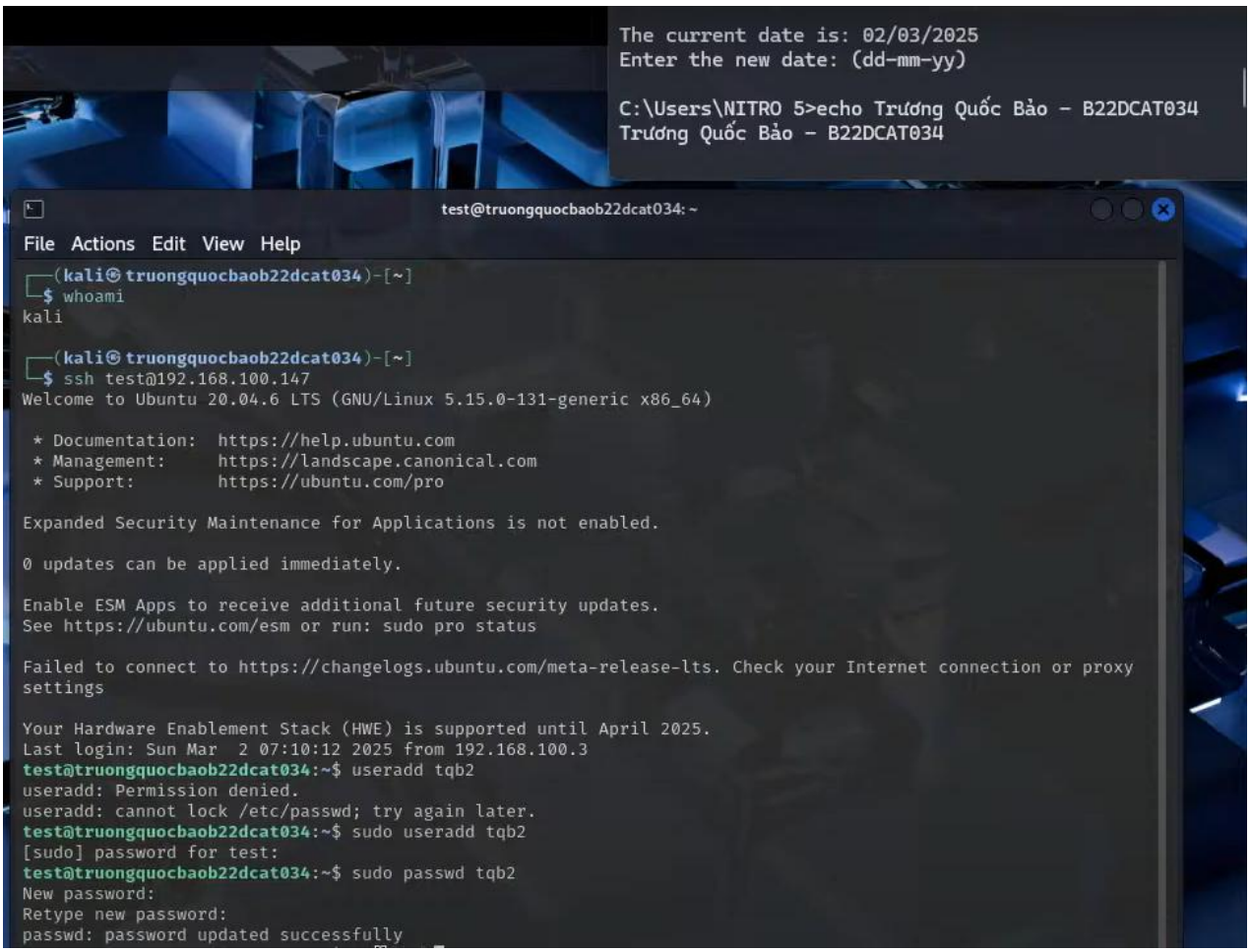
Thư mục chứa access_log nằm ở đường dẫn /var/log/httpd, tiến hành đọc file với lệnh cat và sử dụng lệnh grep để tìm kiếm các từ khóa "nmap", "firefox", "curl".



Hình 10 Tìm kiếm các log trong file access.log

2.2.3 Phân tích log sử dụng gawk trong Linux

Trên máy Kali attack tiến hành remote vào máy Ubuntu victim bằng lệnh “ssh <tên máy>@<địa chỉ IP>”. Tạo user mới là “tqb2” và đặt mật khẩu.

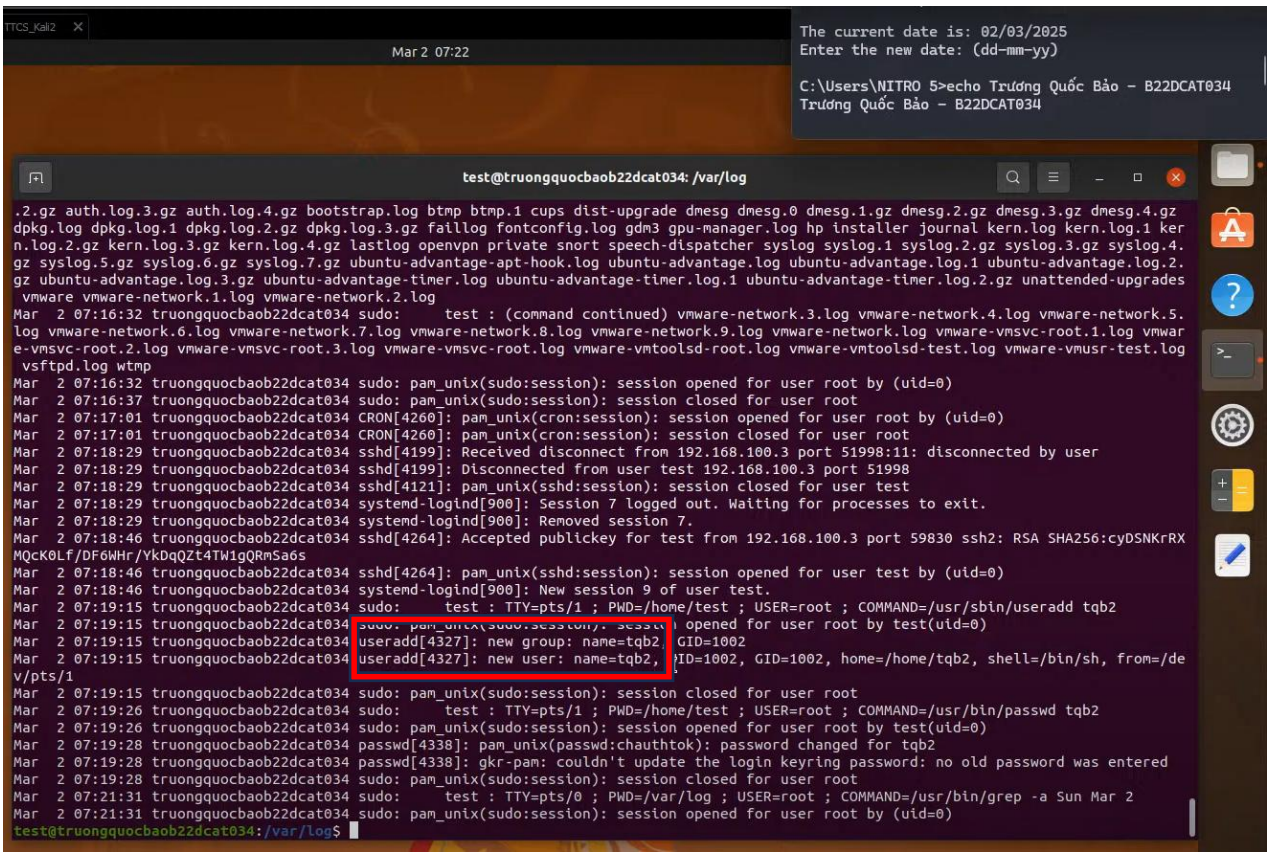


Hình 11 SSH đến máy Ubuntu và tạo user mới

Đọc file auth.log ở trên máy Ubuntu bằng lệnh cat.

Hình 12 Đọc file auth.log

Ta thấy được một số log được lưu sau khi tạo user.

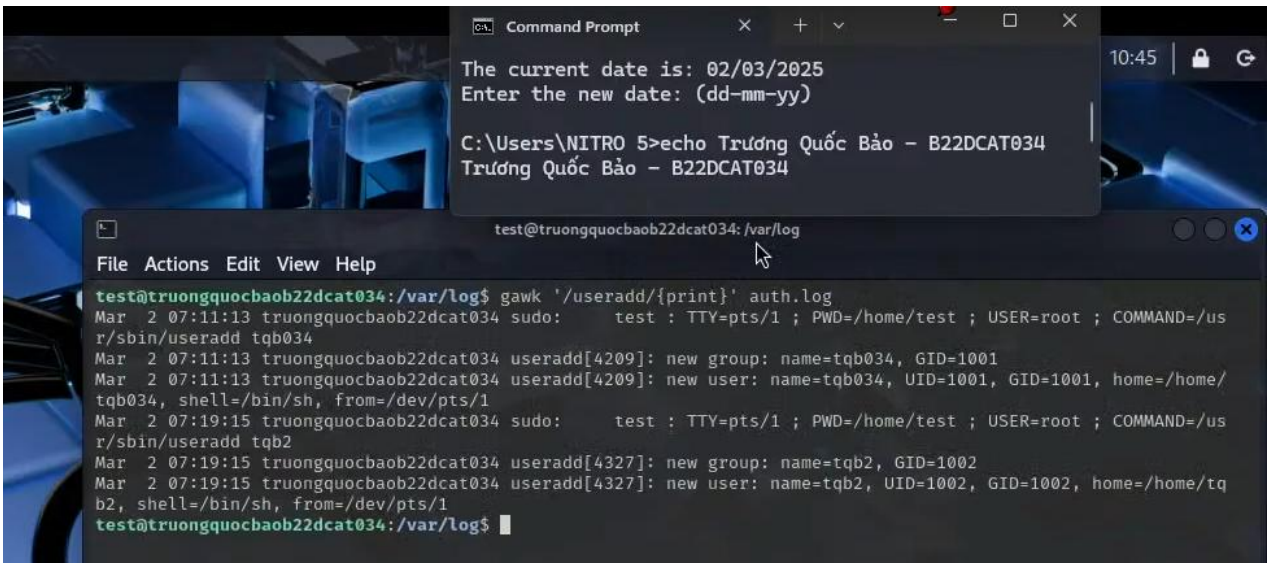


Hình 13 File access.log

Có thể tìm kiếm tương tự ở trên máy Kali với lệnh cat.

Hình 14 Tìm kiếm user vừa tạo bằng lệnh "grep"

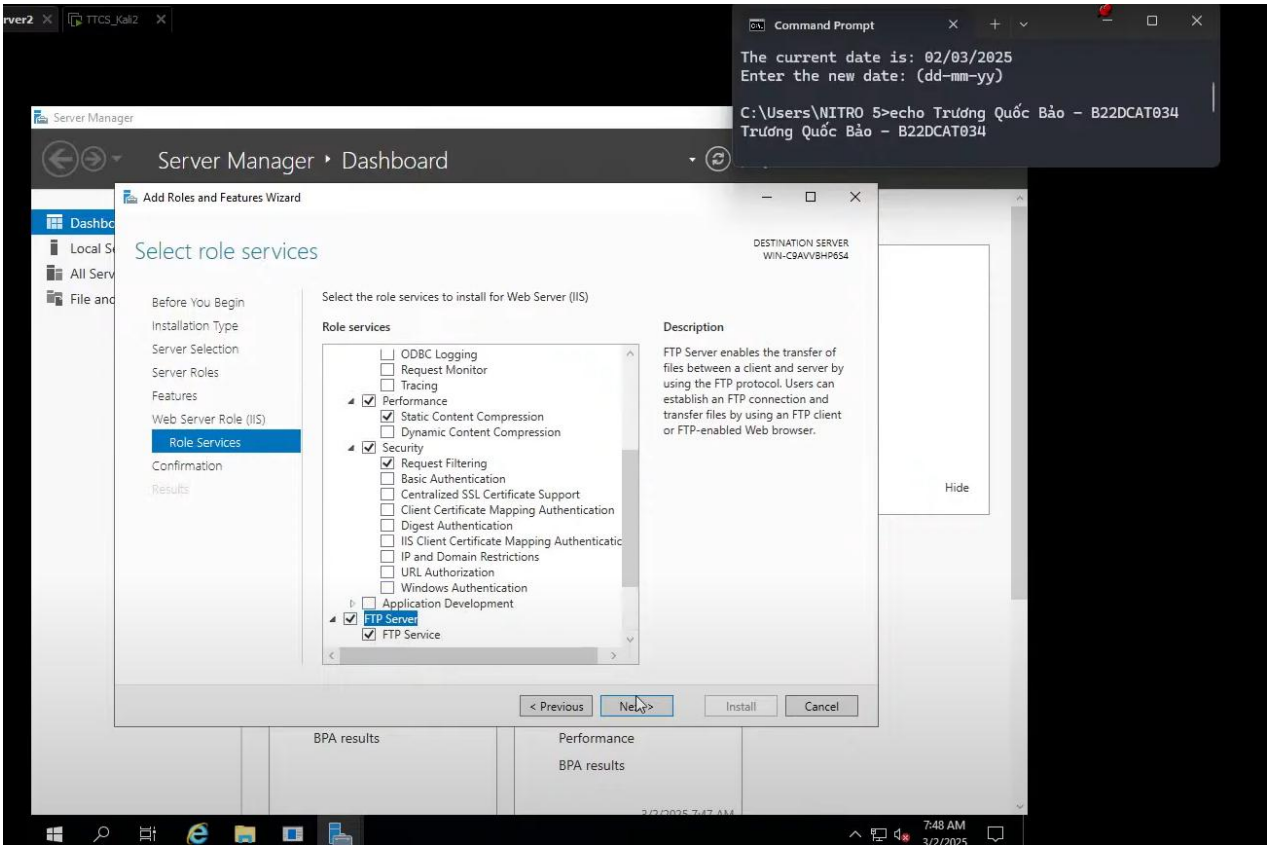
Sử dụng lệnh "gawk" để tìm kiếm dữ liệu tương tự.



Hình 15 Sử dụng lệnh "gawk"

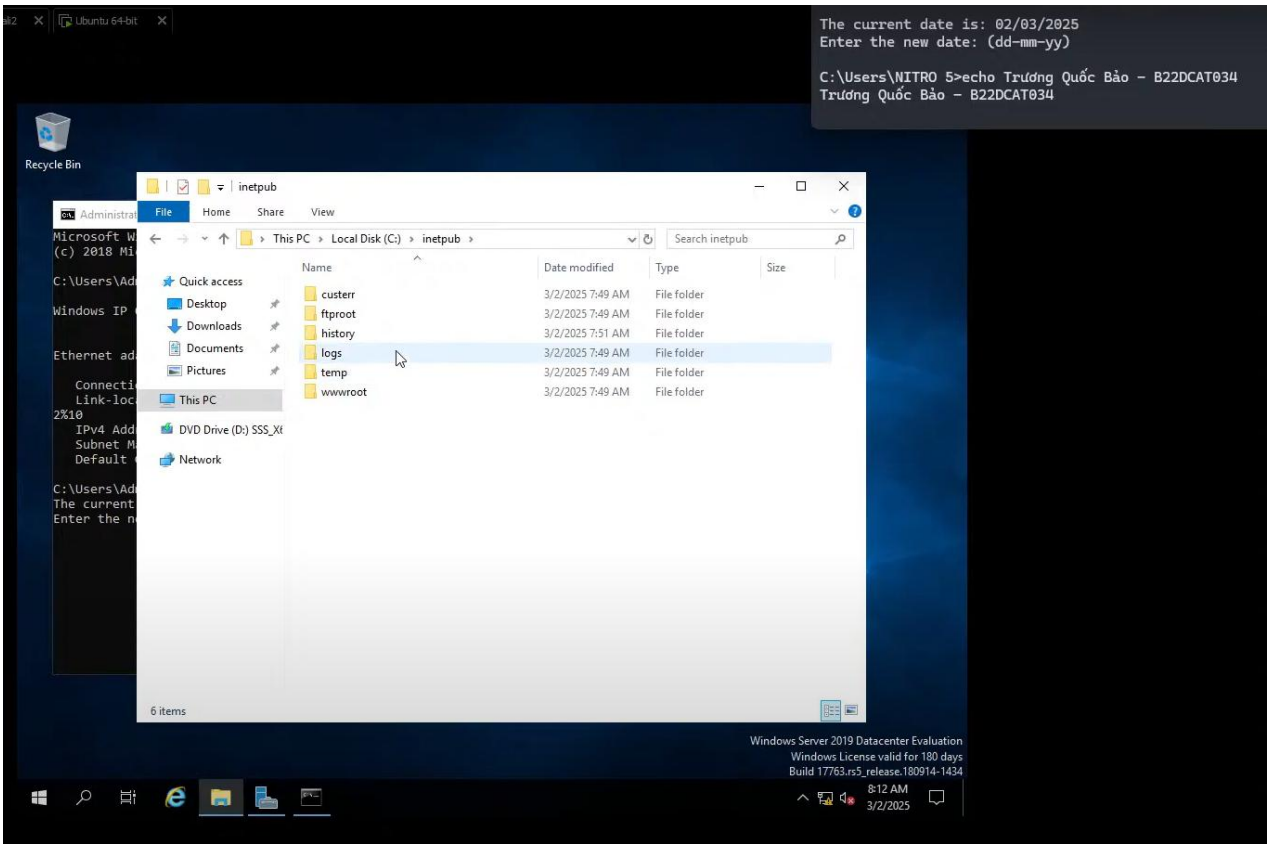
2.2.4 Phân tích log sử dụng find trong Windows

Cài đặt dịch vụ FTP Server trên máy Windows Server như các bài trước.



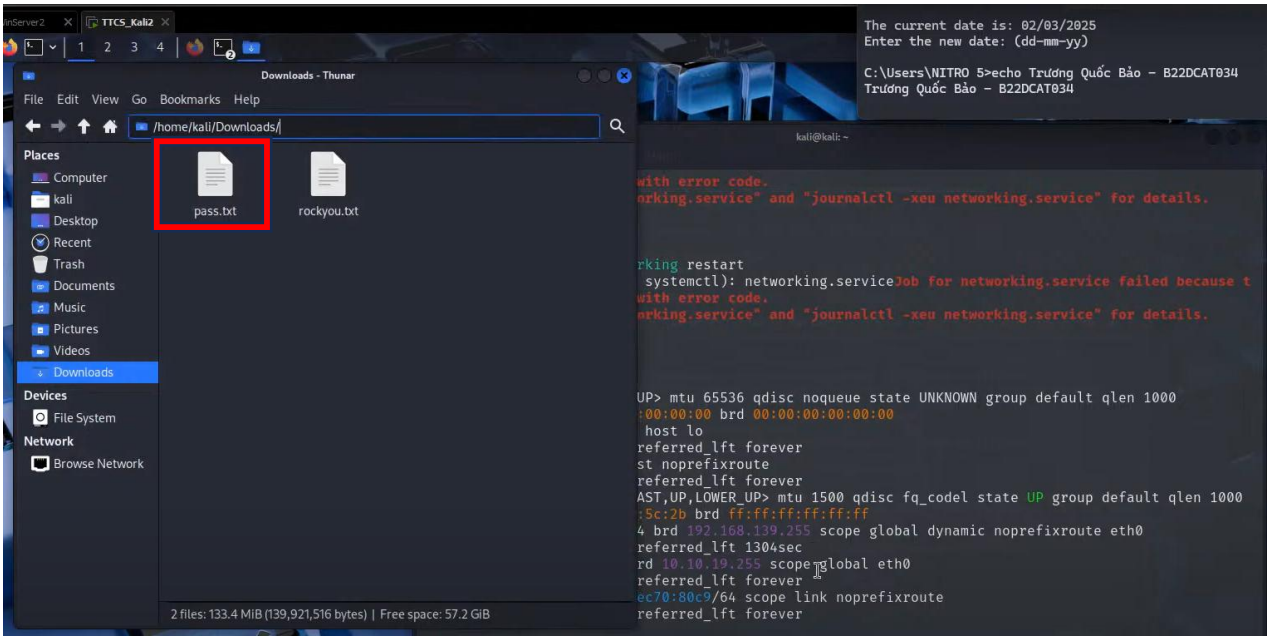
Hình 16 Cài đặt dịch vụ FTP trên máy Windows Server

Kiểm tra đường dẫn đến file ftp log để lưu file log của kết quả tấn công.



Hình 17 Kiểm tra đường dẫn tới thu mục logs

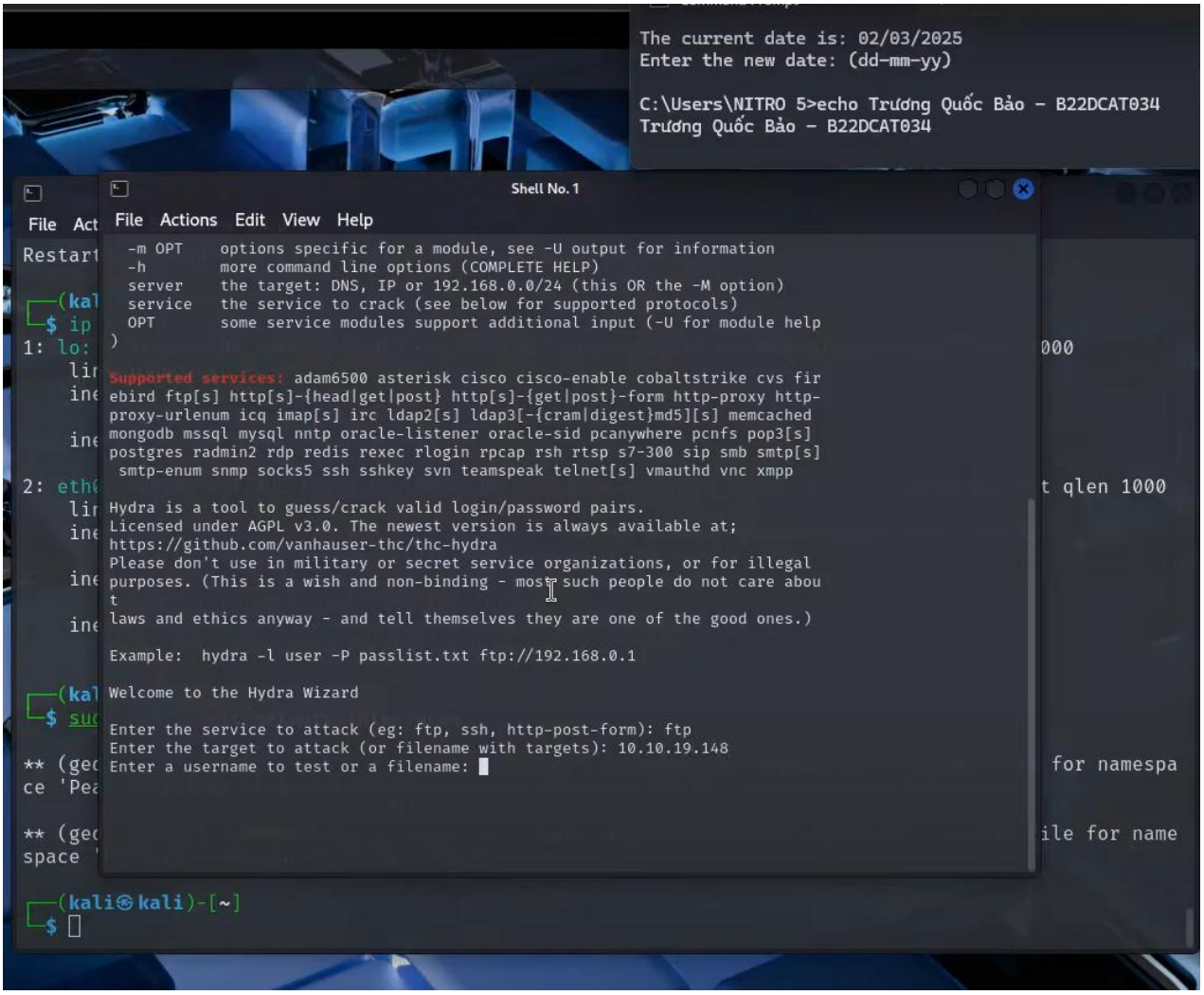
Trên máy Kali, tạo file pass.txt để lưu một số mật khẩu để dò, phải đảm bảo có mật khẩu chính xác để tiến hành tấn công dò quét.



Hình 18 Tạo password list

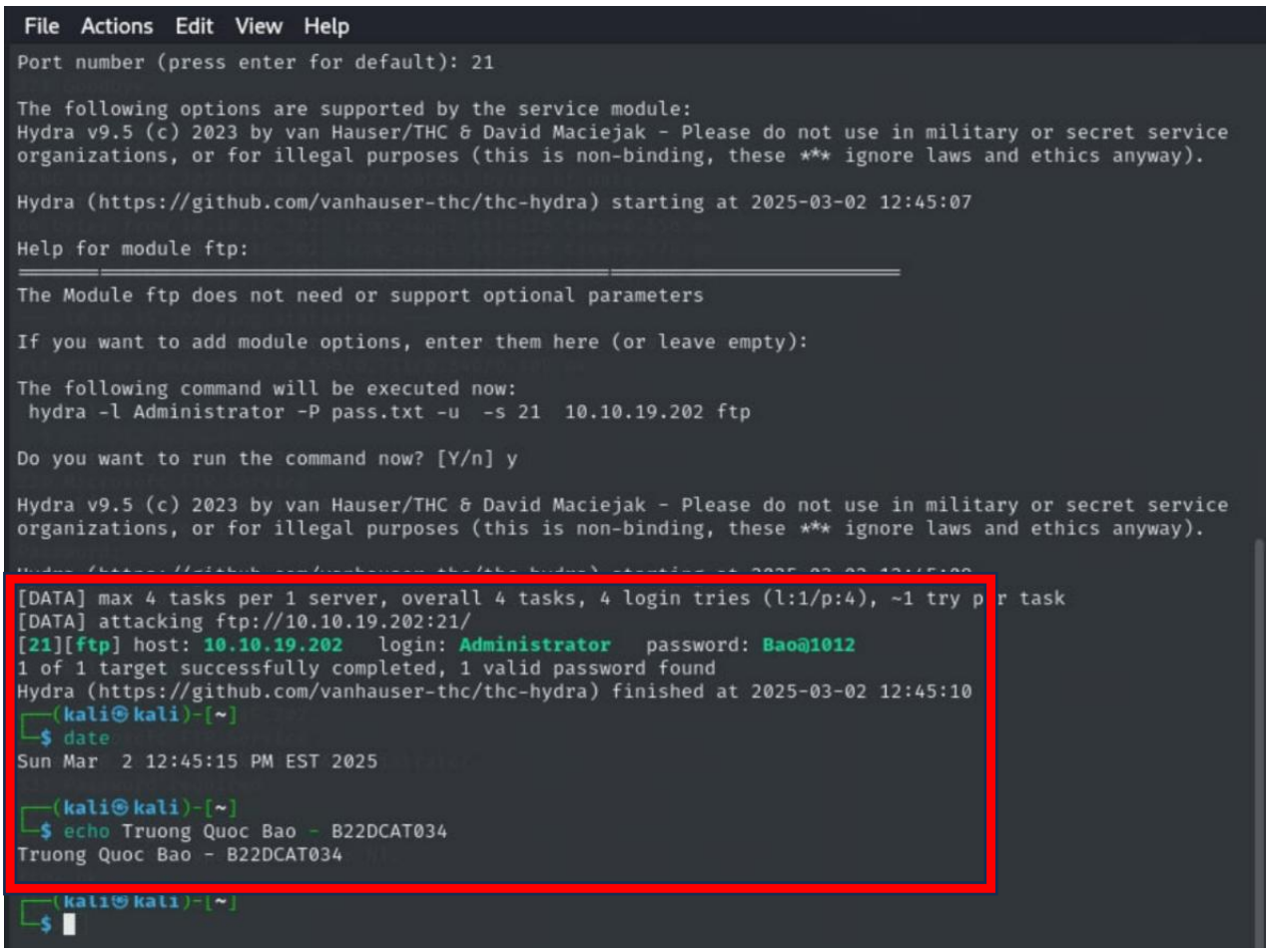
Nếu không có công cụ xhydra, ta có thể dùng công cụ hydra để thay thế, công cụ này làm việc trên giao diện dòng lệnh. Các thông tin yêu cầu gồm: dịch vụ để tấn công (ftp),

mục tiêu tấn công (địa chỉ IP của máy Windows – 10.10.19.202), tên đăng nhập (Administrator), danh sách mật khẩu (pass.txt), cổng tấn công (21) và một số tùy chọn cấu hình khác.



Hình 19 Sử dụng công cụ hydra

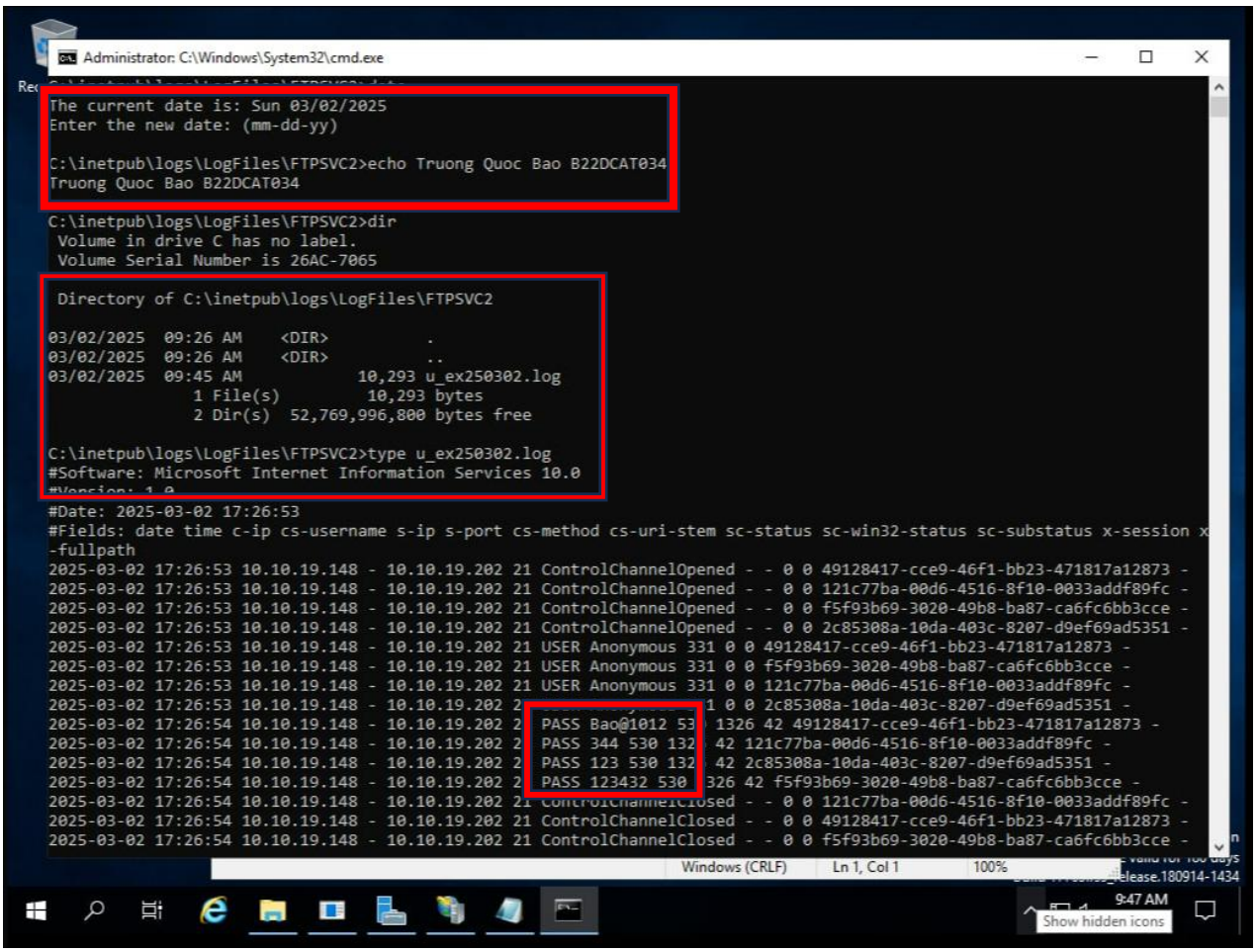
Thông báo dò mật khẩu thành công, mật khẩu này là chính xác so với máy Windows Server.



Hình 20 Công cụ hydra dò mật khẩu thành công

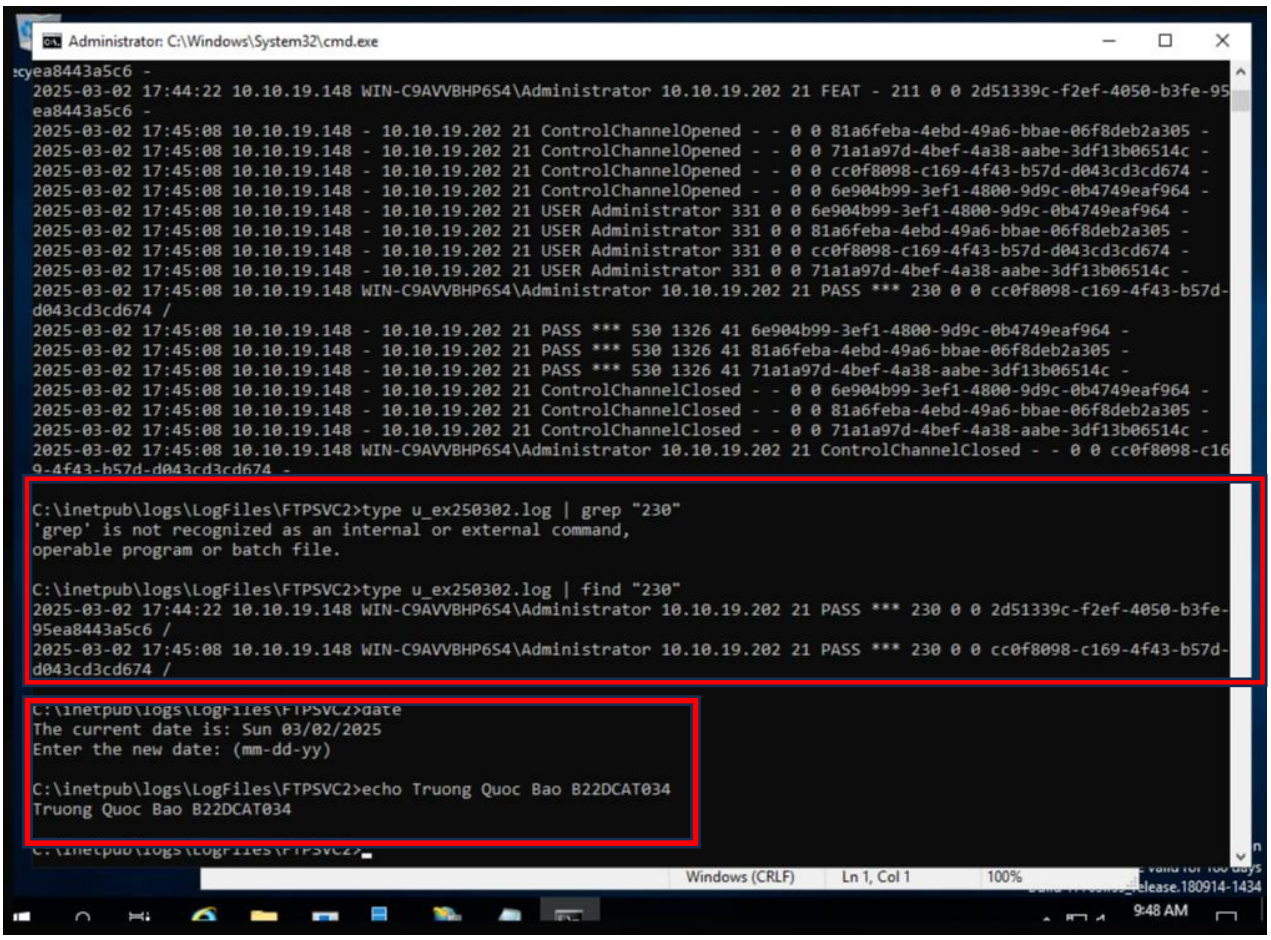
Trên máy Windows Server, thực hiện điều hướng đến FTP Logfile(C:\cd c:\Windows\System32\Logfiles\msftpsvc1). Chọn hiển thị tất cả các file log đang có và chọn 1 file mới nhất để mở ra (ngày tháng có dạng yymmdd).

Có thể thấy, công cụ hydra đã dò hết tất cả các mật khẩu đã lưu trong file pass.txt với tên đăng nhập là Anonymous.



Hình 21 Đọc file log trên máy Windows

Gõ lệnh để tìm kiếm kết quả tấn công login thành công (C:\WINDOWS\system32\LogFiles\MSFTPSVC1>type exyymmdd.log | find “230”). Ta đã thành công phân tích log sử dụng find trong Windows.



Hình 22 Tìm kiếm kết quả tấn công

TÀI LIỆU THAM KHẢO

[1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.

[2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.

[3] https://linuxcommand.org/lc3_man_pages/grep1.html

[4] http://www.gnu.org/software/gawk/manual/gawk.html

[5] https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/find

[6] http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html