**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 10**

**Phân tích log hệ thống**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 2/2023

I. Mục đích Bài thực hành này giúp sinh viên nắm 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. Nội dung thực hành

1. Tìm hiểu lý thuyết

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

2. Chuẩn bị môi trường o 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.

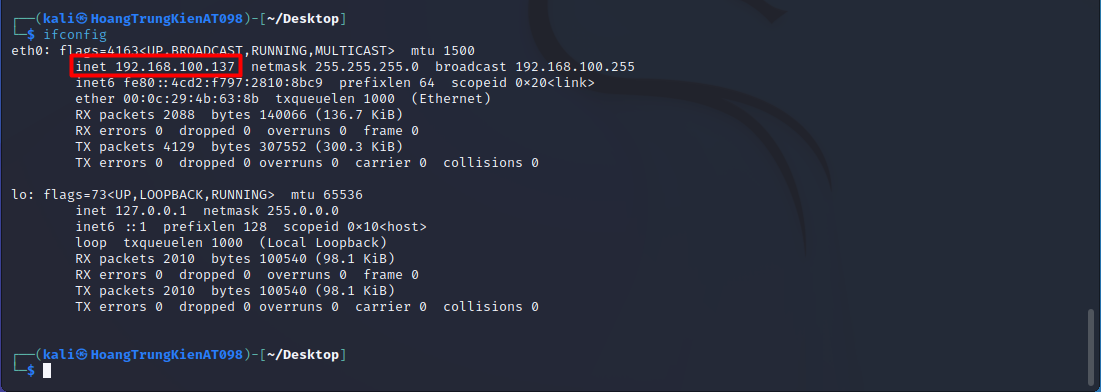
Chú ý: chỉ cần bật các máy cần sử dụng trong bài thực hành.

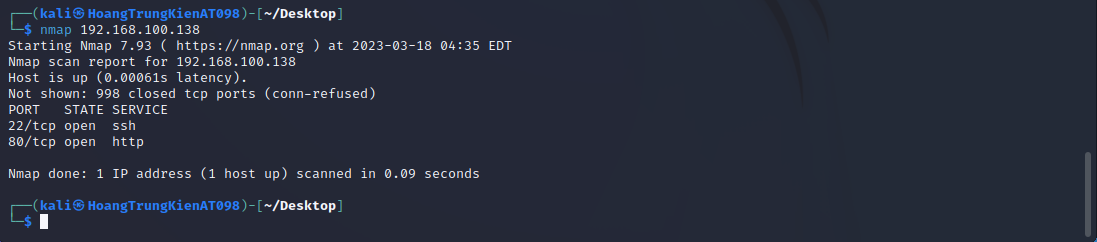
- Topo mạng như đã cấu hình trong bài 5.

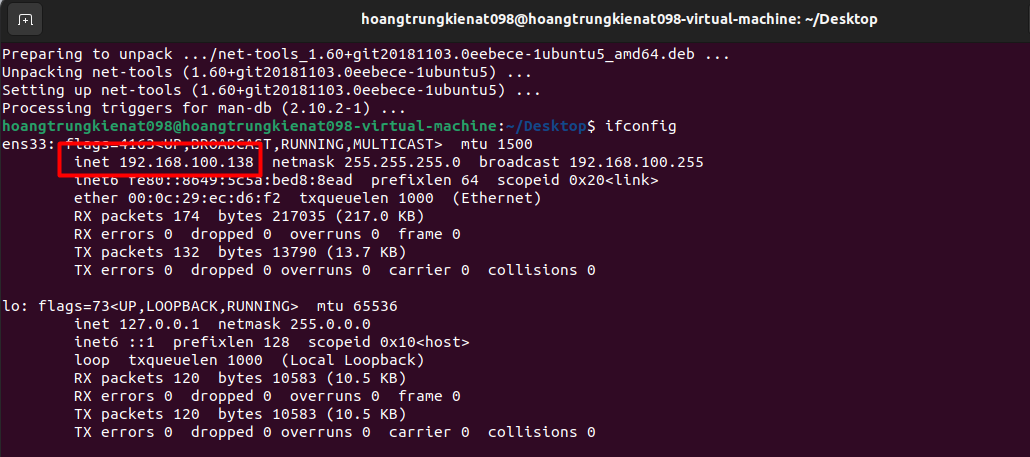
III. Các bước thực hiện

- Phân tích log sử dụng grep trong Linux

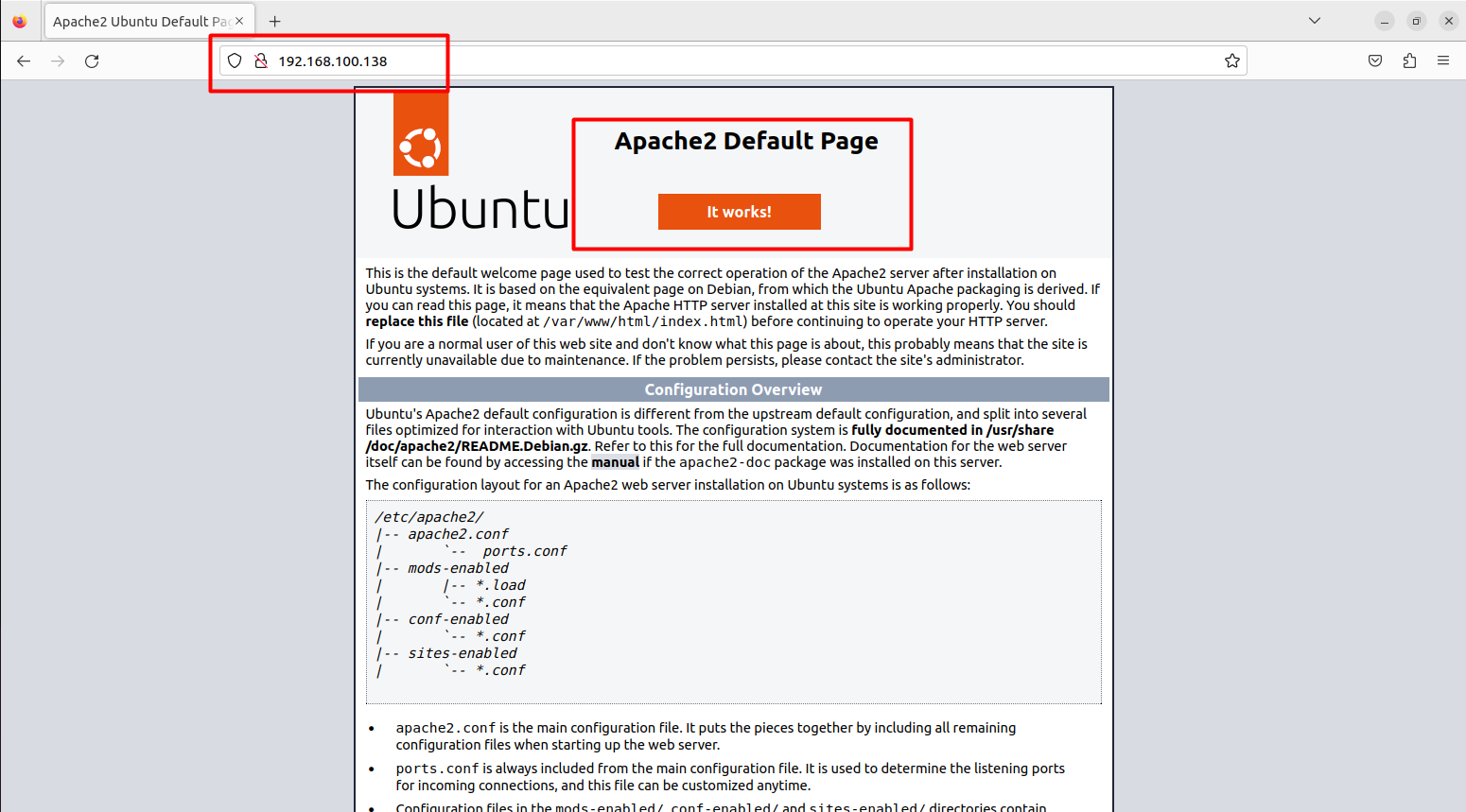
Trên máy Kali attack trong mạng Internal, khởi chạy nmap và scan cho địa chỉ 192.168.100.138(Máy Linux victim) và xem được port 80 đang mở cho Web Server Apache 2.2.3





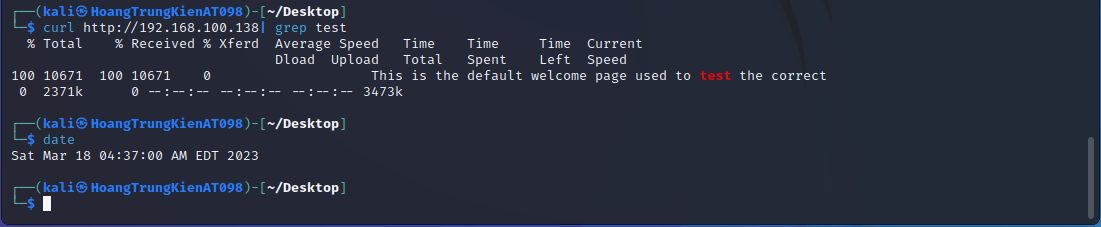


Cai đặt thành công dịch vụ apache trên linux

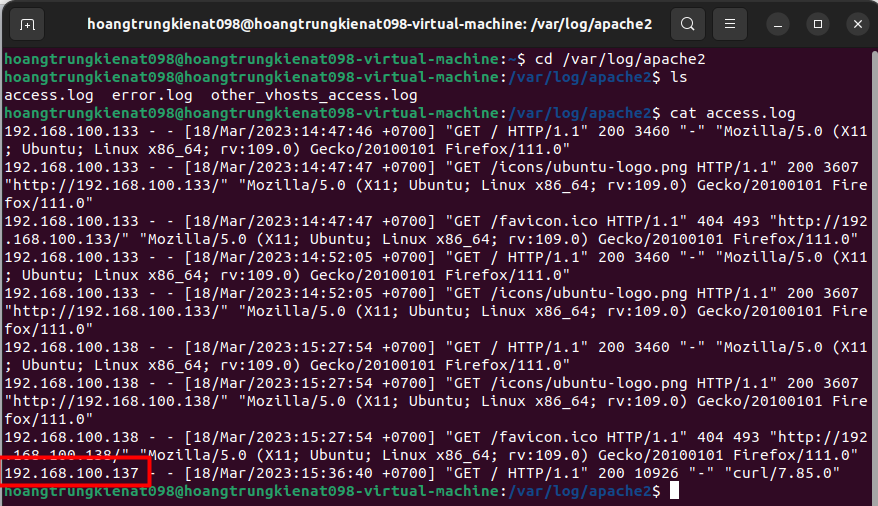


Trên máy kali truy nhập vào địa chỉ web

Trên terminal tiến hành sao chép website và tìm kiếm từ khóa “test”

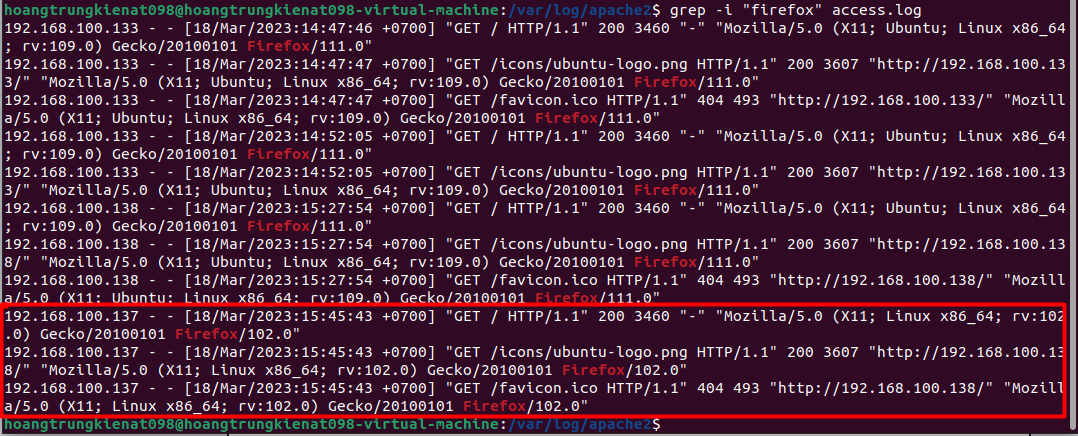


Trên máy Linux , xem thư mục chứa access.log



Khi đã mở được file access.log trên máy Linux , dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm

+Firefox

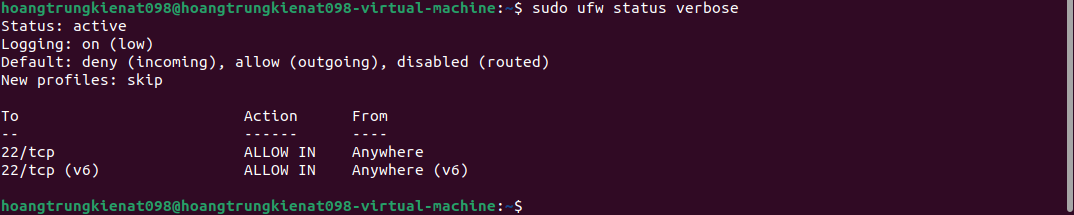


+Curl

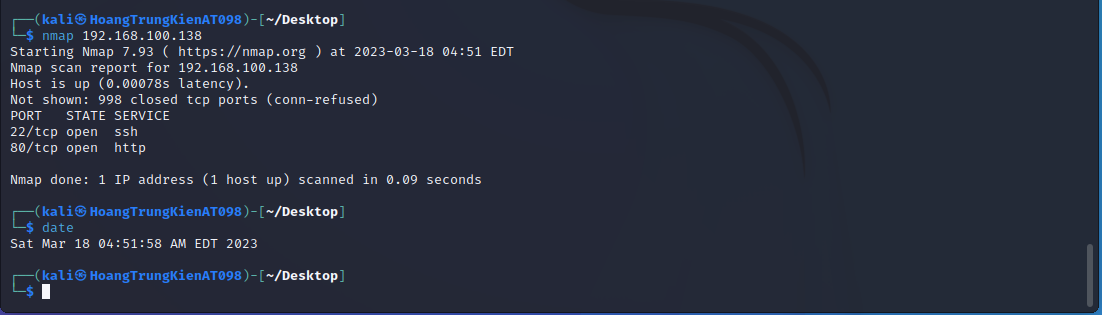


2.3.2.Phân tích log sử dụng gawk trong Linux

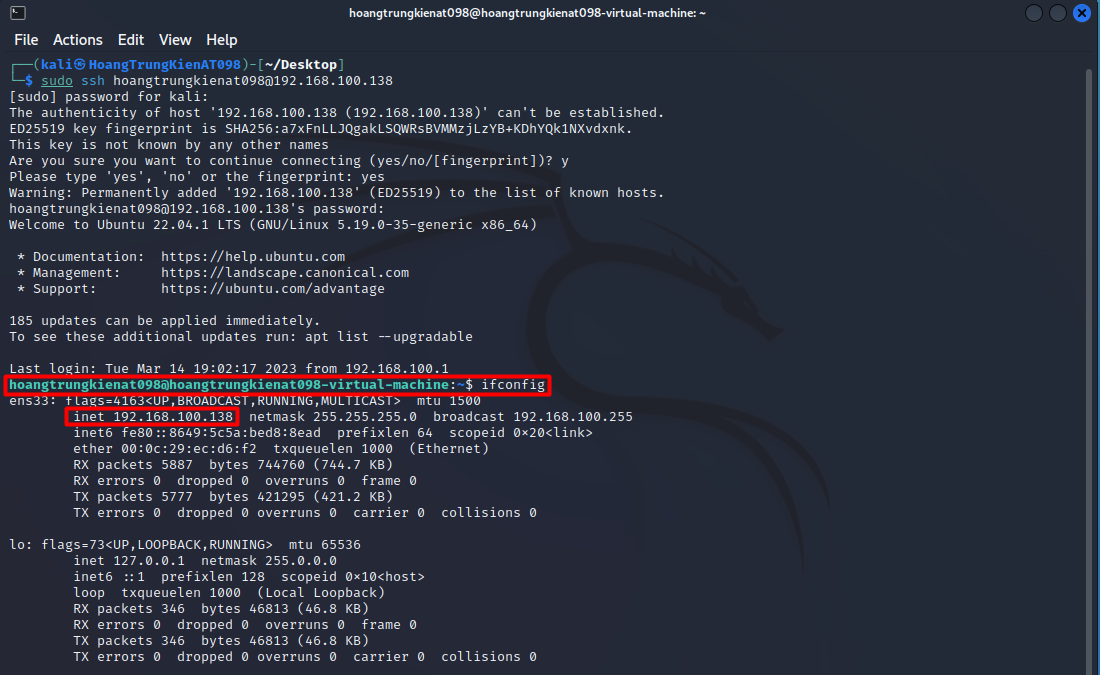
Mở cổng 22 ssh trên Linux



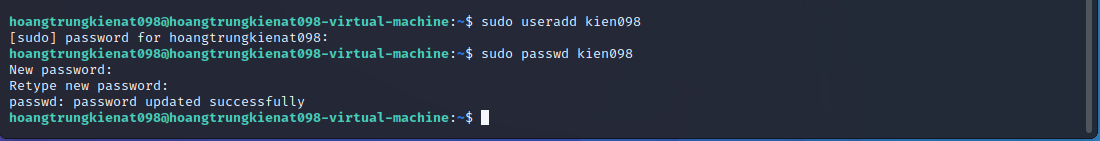
- Kiểm tra cổng SSH trên địa chỉ 192.168.100.129 (Linux)



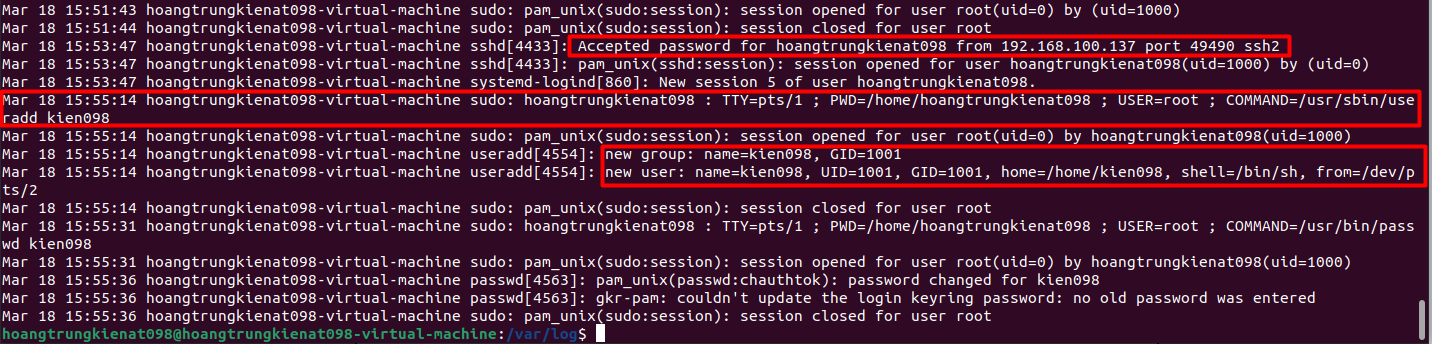
-Trên máy Kali tiến hành remote vào máy Linux :



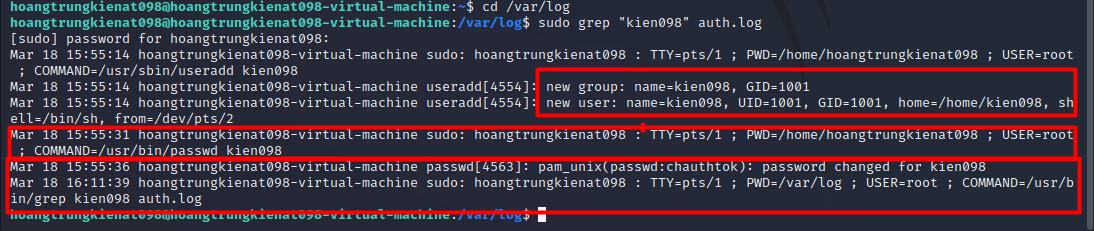
Tạo một account mới với tên sinh viên và mật khẩu tùy chọn



Trên máy Linux, tiến hành xem file auth.log



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

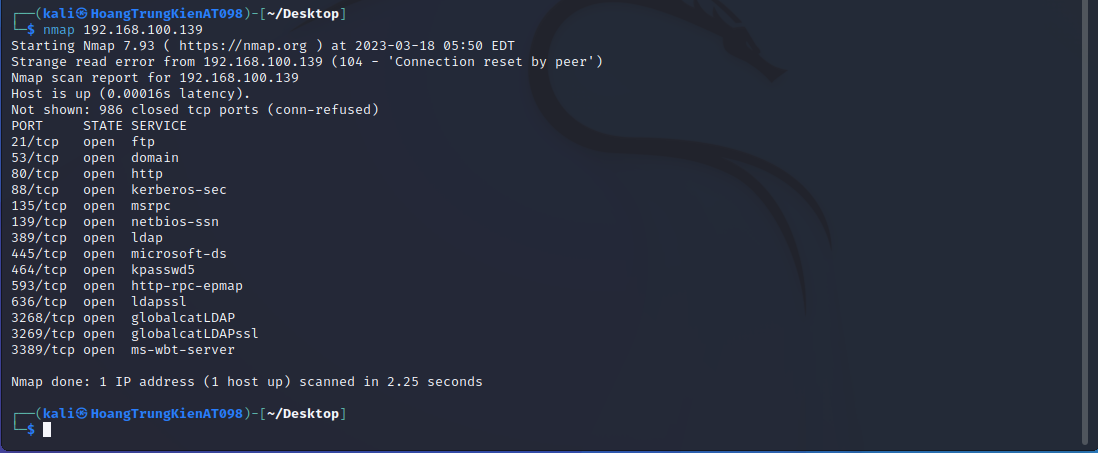


2.3.3.Phân tích log sử dụng find trong Windows

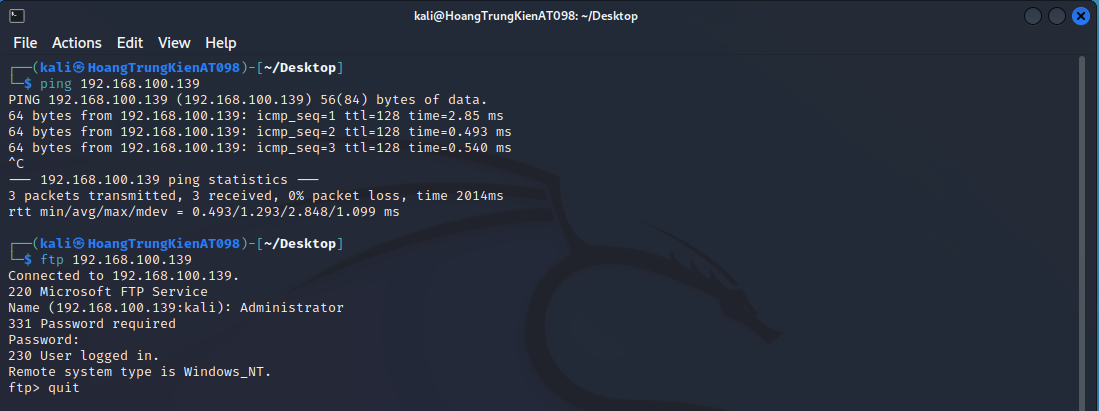
Chuẩn bị 2 máy kali IP: 192.168.100.137

                  máy win server 2019 IP: 192.168.100.139

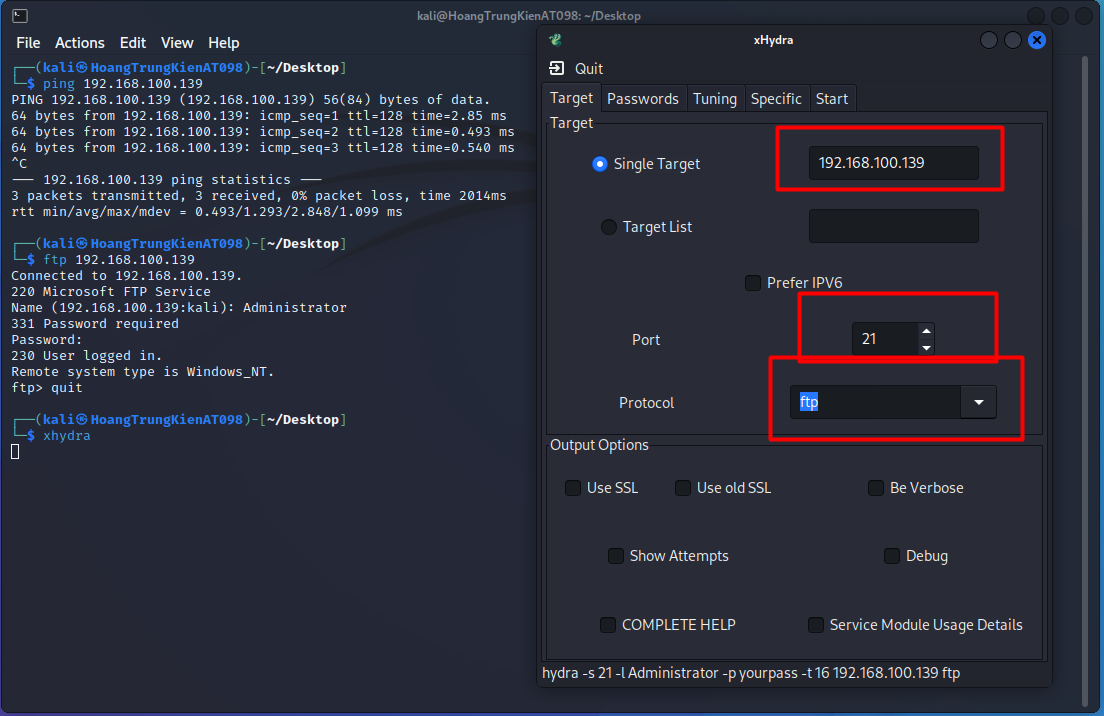
Trên máy Kali External Attack dùng nmap cho địa chỉ 192.168.100.139 và xem được port 21 đang được mở

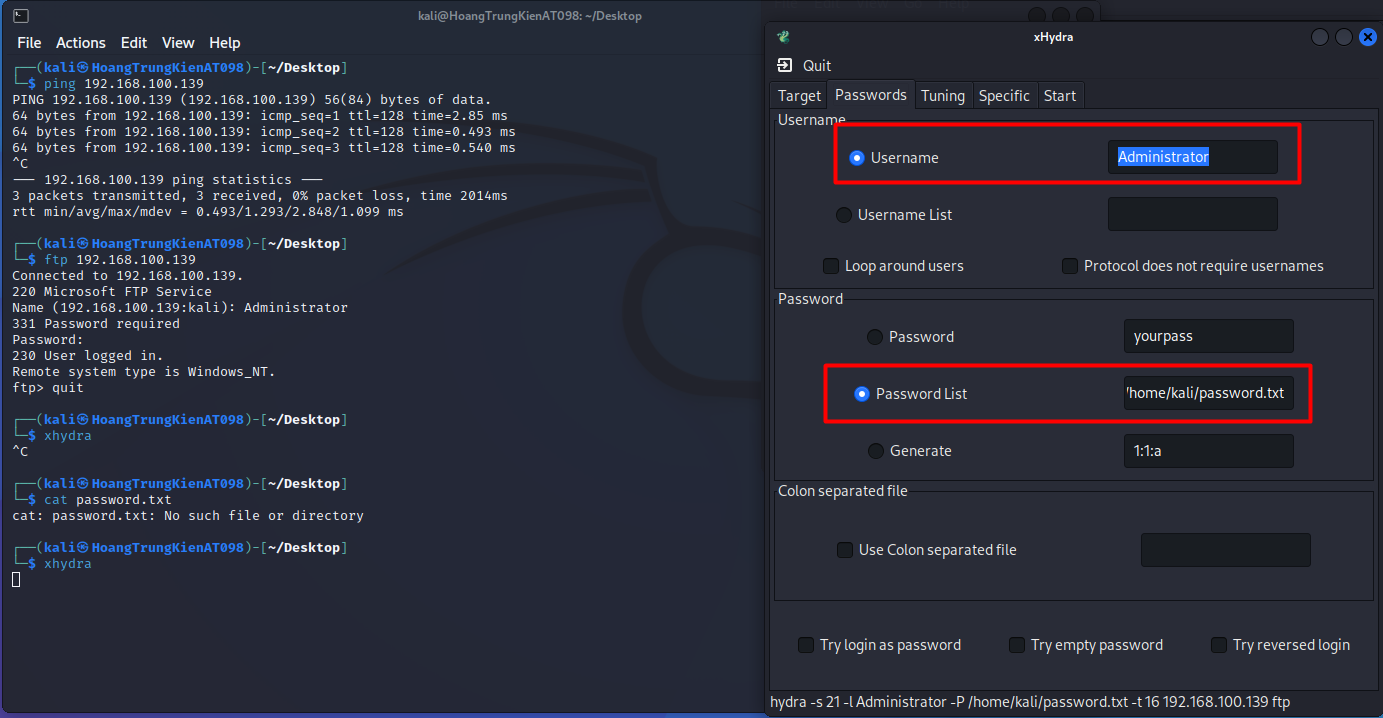


- Trong máy Kali khởi động #xhydra, chọn target là 192.168.100.139, giao thức ftp

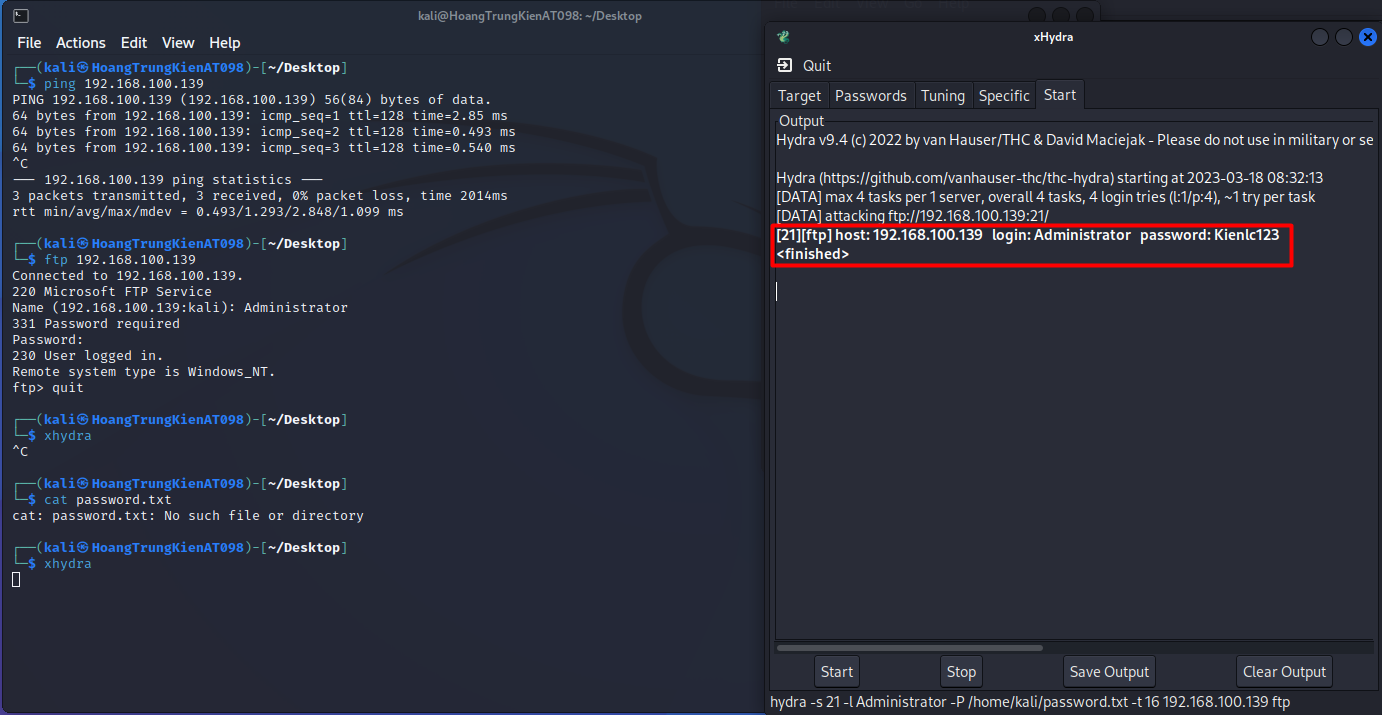


- Trong máy Kali khởi động #xhydra, chọn target là 192.168.100.139, giao thức ftp

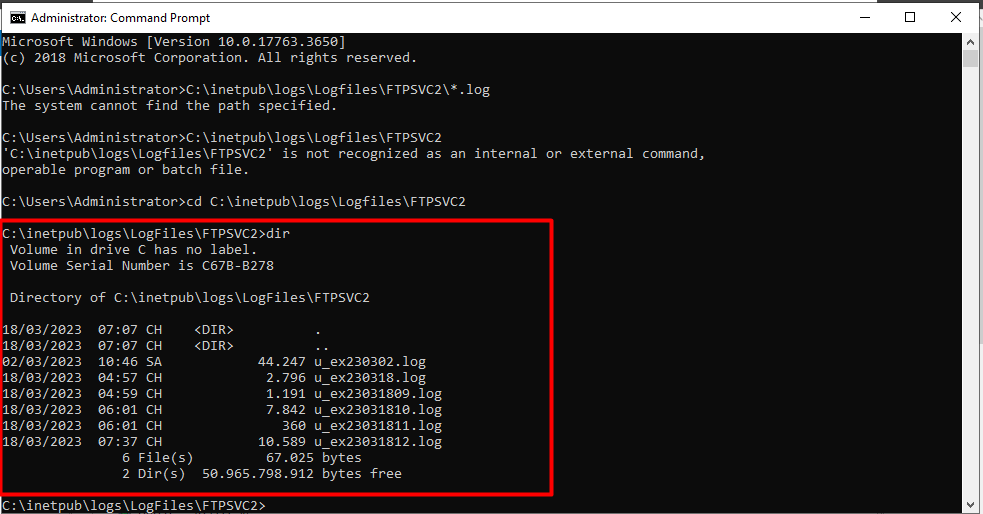




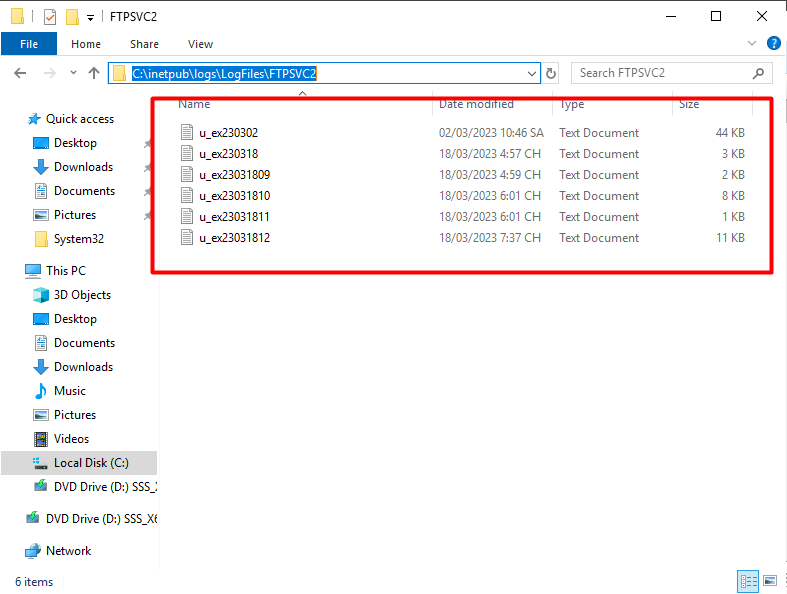
Vét cạn ta tìm được mật khẩu

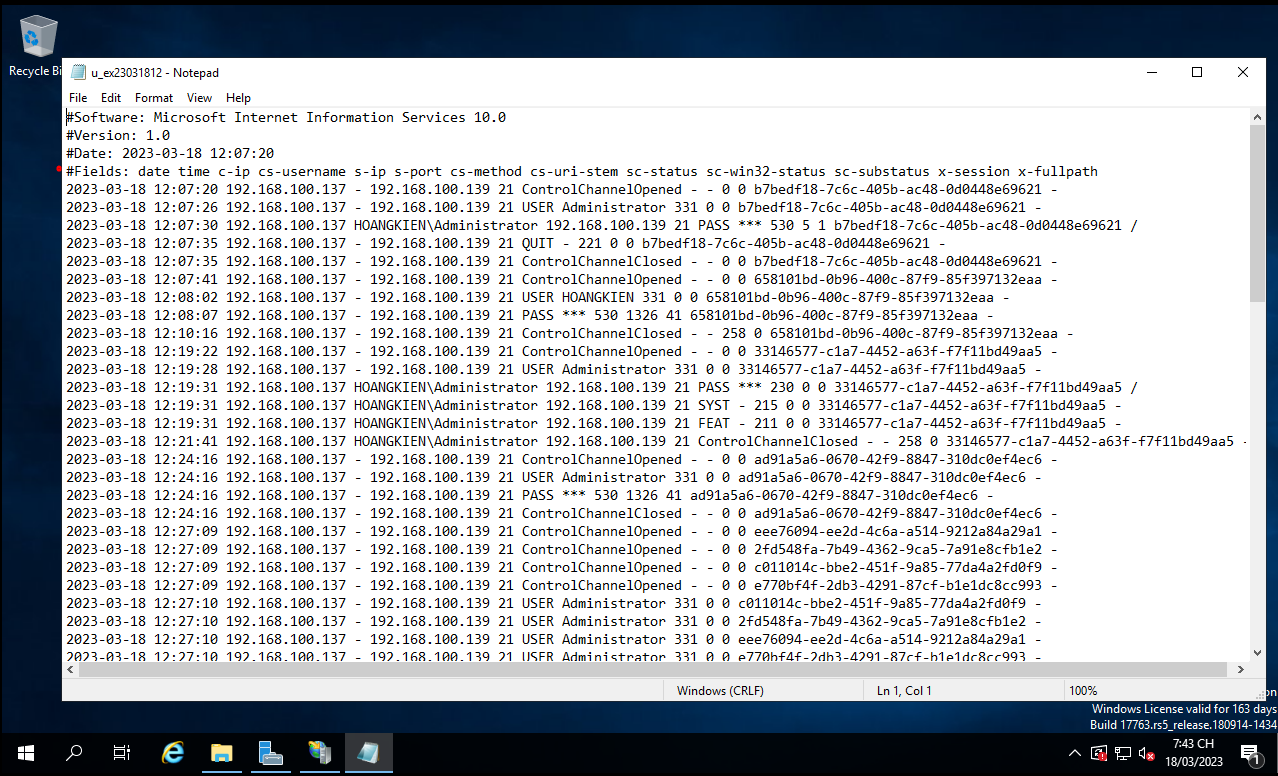


Trên máy Windows Server, thực hiện điều hướng đến FPT Logfile: C:\inetpub\logs\Logfiles\FTPSVC2\\*.log



Chọn 1 file mới nhất để mở ra





Tìm kiếm kết quả login thành công

