

# HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**BÁO CÁO THỰC HÀNH MÔN THỰC TẬP CƠ SỞ ATTT**

**Bài 9: Phân tích log hệ thống**

**Họ và tên: Nguyễn Huy Quang**

**Mã sinh viên: B20DCAT144 Hệ: Chính Quy**

**Giảng viên: Nguyễn Hoa Cương**

***Hà Nội – 2023***

# Mục lục

1. [Mục đích 3](#_bookmark0)
2. [Nội dung thực hành 3](#_bookmark1)
   1. [Tìm hiểu lý thuyết 3](#_bookmark2)
   2. [Chuẩn bị môi trường 4](#_bookmark3)
   3. [Các bước thực hiện và kêt quả 5](#_bookmark4)
      1. [Phân tích log sử dụng grep trong Linux 5](#_bookmark5)
      2. [Phân tích log sử dụng gawk trong Linux 7](#_bookmark6)
      3. [Phân tích log sử dụng find trong Windows 10](#_bookmark7)
3. [Tài liệu tham khảo 12](#_bookmark8)

## Mục đích

Bài thực hành này giúp sinh viên nắm được công cụ và cách phân tích log hệ thống, baogồm:

* 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

## 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, …

* + - **grep**

Grep (Global Regular Expression Print) là một công cụ dòng lệnh Linux/Unix đượcsử dụng để tìm kiếm một chuỗi ký tự trong một tệp được chỉ định. Khi tìm thấy kếtquả khớp, nó sẽ in dòng kết quả. Lệnh grep rất tiện lợi khi tìm kiếm log

**Cú pháp:**

grep [OPTION ...] PATTERNS [FILE ...]

grep [OPTION ...] -e PATTERNS ... [FILE ...]

grep [OPTION ...] -f PATTERN\_FILE ... [FILE ...] grep

* + Lựa chọn
    - đối sánh -E, --extended-regexp : Diễn giải MẪU dưới dạng biểu thức chính quymở rộng
    - -F, --fixed-string : Diễn giải MẪU là chuỗi cố định, không phải biểu thức chínhquy.
    - -G, --basic-regexp : Diễn giải MẪU dưới dạng biểu thức chính quy cơ bản
    - -P, --perl-regex: Giải thích MẪU dưới dạng biểu thức chính quy tương thích với Perl (PCRE). Tùy chọn này là thử nghiệm khi được kết hợp với tùy chọn
    - -z (--null-data) và grep -P có thể cảnh báo về các tính năng chưa được thực hiện
      * **gawk**
  + gawk - mô hình quét và xử lý ngôn ngữ
  + Nó có thể được sử dụng như một trình trích xuất trường (như lệnh cắt), một máy tính cơ bản và như một trình so khớp mẫu (như lệnh grep)
* **Find**
  + Đây là một command rất mạnh trong việc tìm kiếm và xác định file đối với thư mục có dạng cây (the directory heirarchy) theo Regex được định nghĩa, ngoài ra còn thực hiện tìm theo các điều kiện chi tiết như thời gian, loại file...
  + Command của Find có dạng như sau:

$ find [Command-Option] [PATH] [Option] [File/Search\_Expresion]

* + Option:

-P Không đọc Symbolic Link-các lối tắt(tương ứng trong window là short- cut).

Đây là cấu hình mặc định

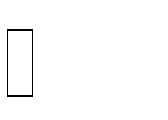
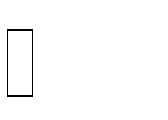
-L Đọc tất cả Symbolic Link

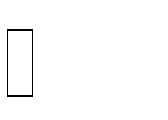
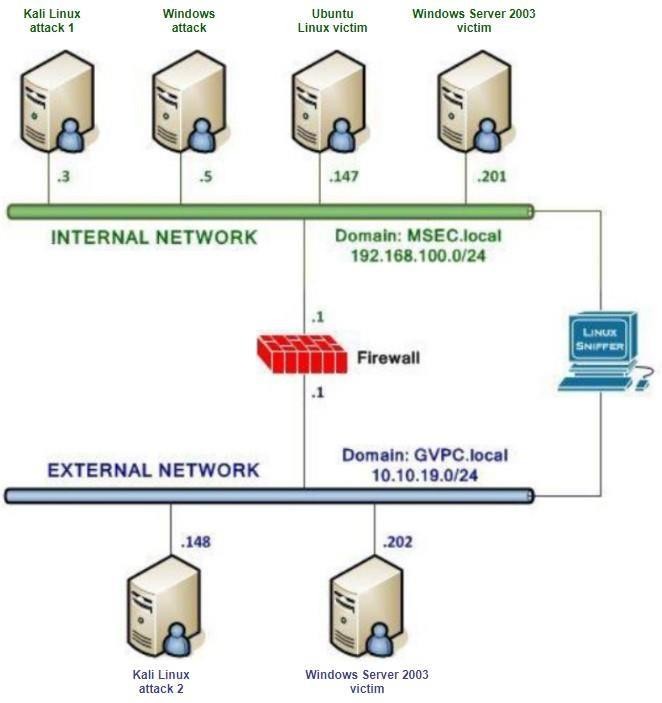
-H Chỉ đọc Symbolic Link được chỉ định

-D <sub\_option> Hiển thị thông tin Debug

-O<level> Cấp tối ưu hóa xử lý. Cấp -O1 là cấp tối ưu hóa được cài đặt mặc định.

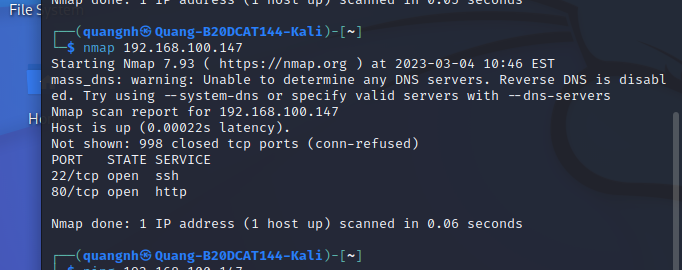
* **Access\_log**
  + Log truy cập (access log) ghi lại các thông tin người dùng truy cập vào website. Log lỗi (error log) ghi lại các cảnh báo các lỗi xảy ra với dịch vụ liên quan web server.
  1. Chuẩn bị môi trường

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: máytrạm, máy Kali Linux, máy chủ Windows và Linux. Chú ý: chỉ cần bật các máy cầnsử dụng trong bài thực hành.

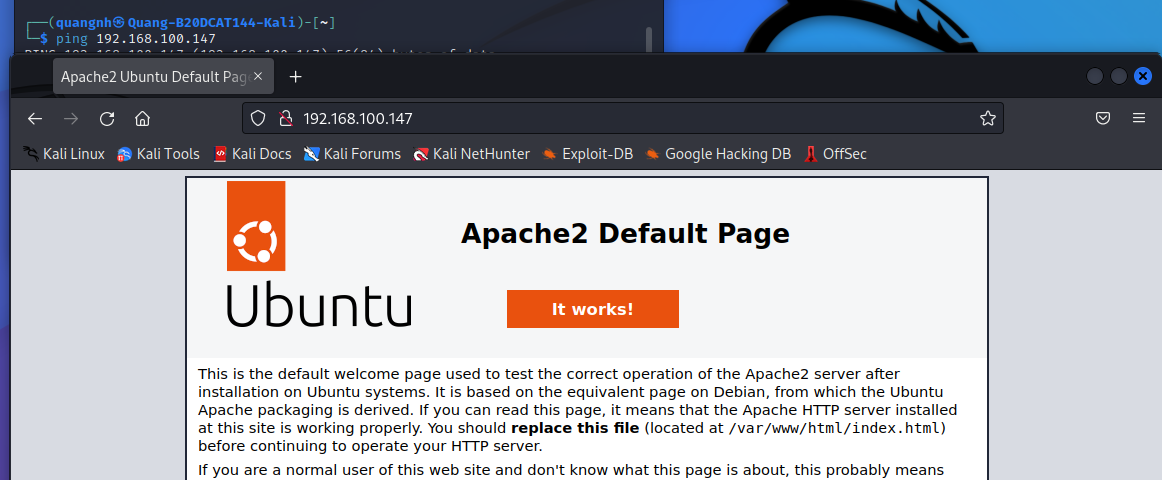
Topo mạng như đã cấu hình trong bài 5

* 1. Các bước thực hiện và kêt quả
     1. Phân tích log sử dụng grep trong Linux

- Trên máy Kali attack trong mạng Internal, khởi chạy nmap và scan cho địa chỉ 192.168.100.147 (Máy Linux Victim Internal) và xem được port 80 đang mở cho Web Server Apache

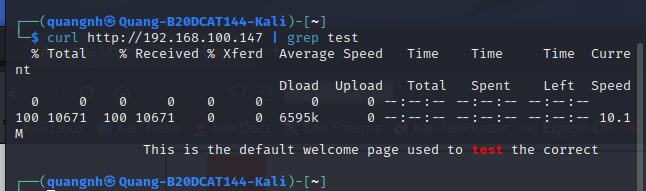


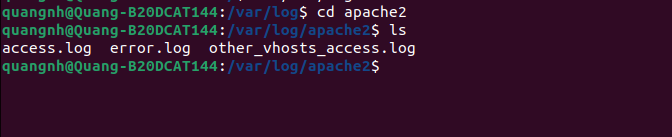
Trên máy Kali attack ở mạng Internal, truy cập vào địa chỉ web



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

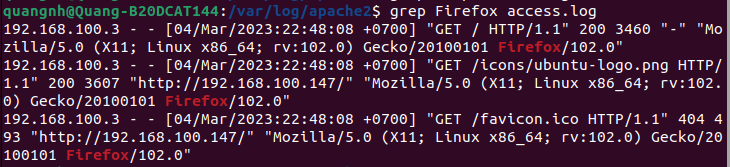
Trên máy Linux Internal Victim, xem thư mục chứa access.log



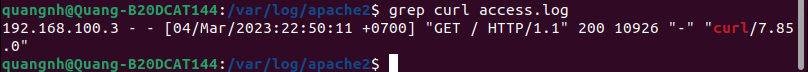


- Khi đã mở được file access.log trên máy Linux Internal Victim, dùng grep để lọc ra kết quả với một số từ khóa tìm kiếm:

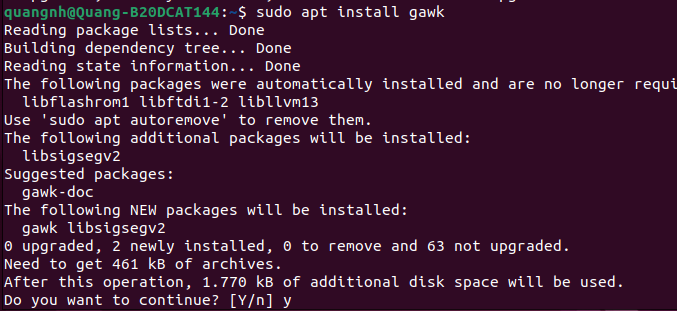
+ Firefox



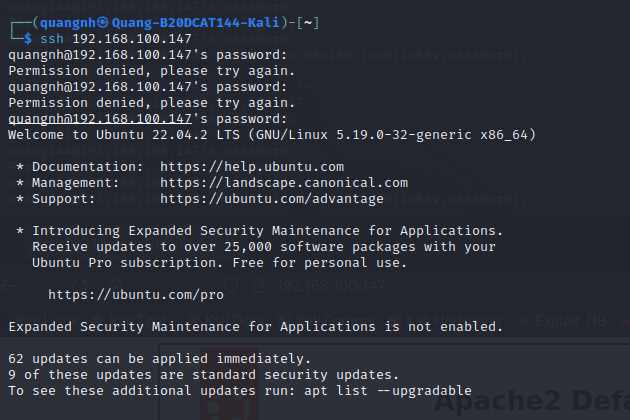
+ Curl



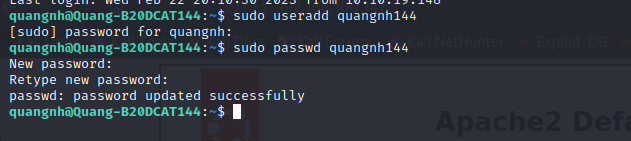
* + 1. Phân tích log sử dụng gawk trong Linux
* Kiểm tra cổng SSH trên địa chỉ 192.168.100.147 (Linux Internal Victim)



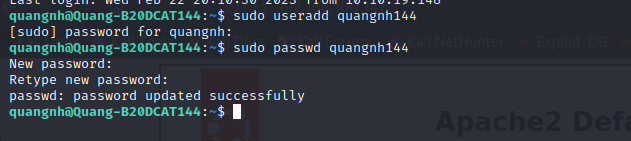
* Trên máy Kali Attack tiến hành remote vào máy Linux Internal Victim

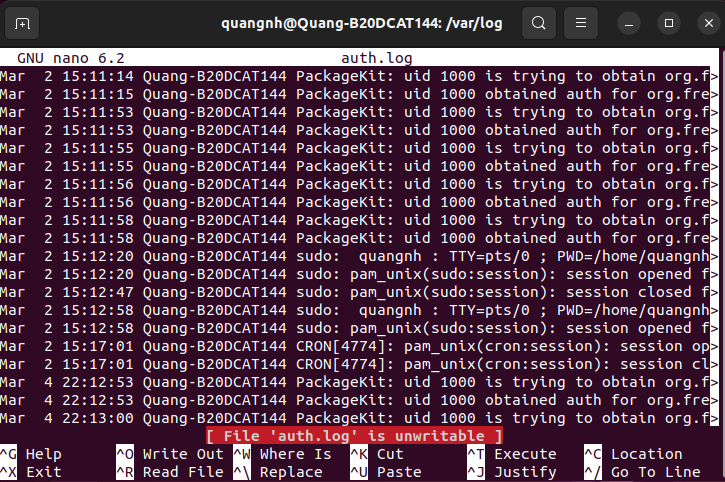


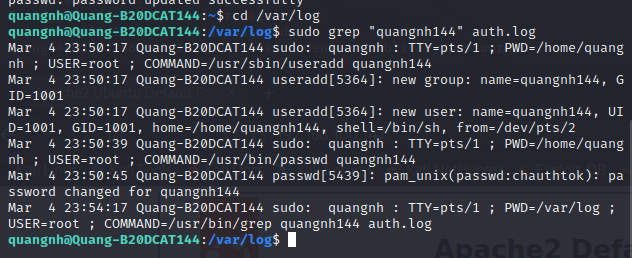
* Tạo một account mới với tên sinh viên và mật khẩu tùy chọn



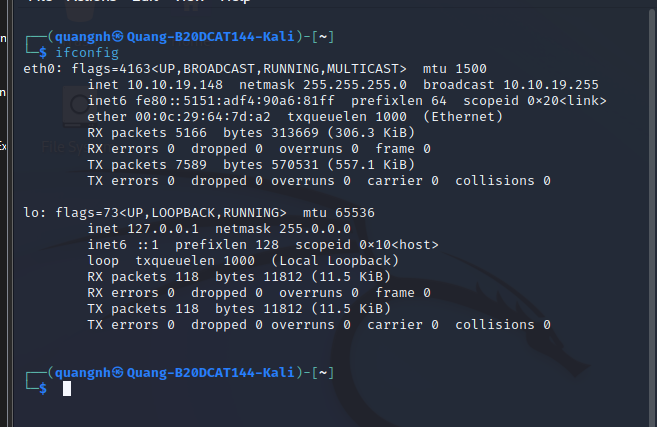
* Sau đó tiến hành thay đổi mật khẩu cho tài khoản vừa tạo

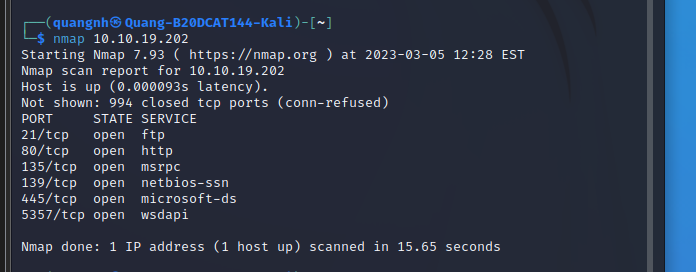


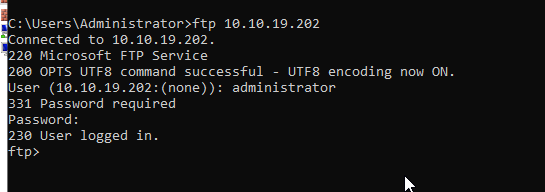
* Trên máy Linux Internal Victim, tiến hành xem file auth.log 
* Trên máy Kali Attack, thông qua chế độ remote tiến hành tìm kiếm những người dùng vừa tạo bằng lệnh grep

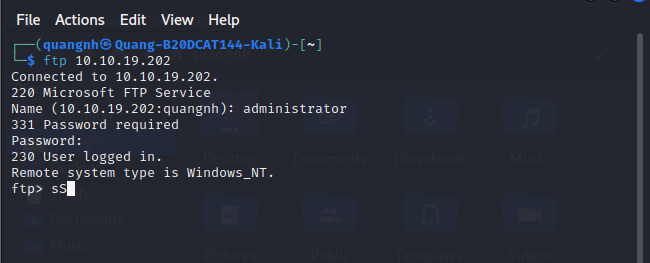


* + 1. Phân tích log sử dụng find trong Windows
* Trên máy Kali External Attack dùng nmap cho địa chỉ 10.10.202 và xem được port 21 đang được mở

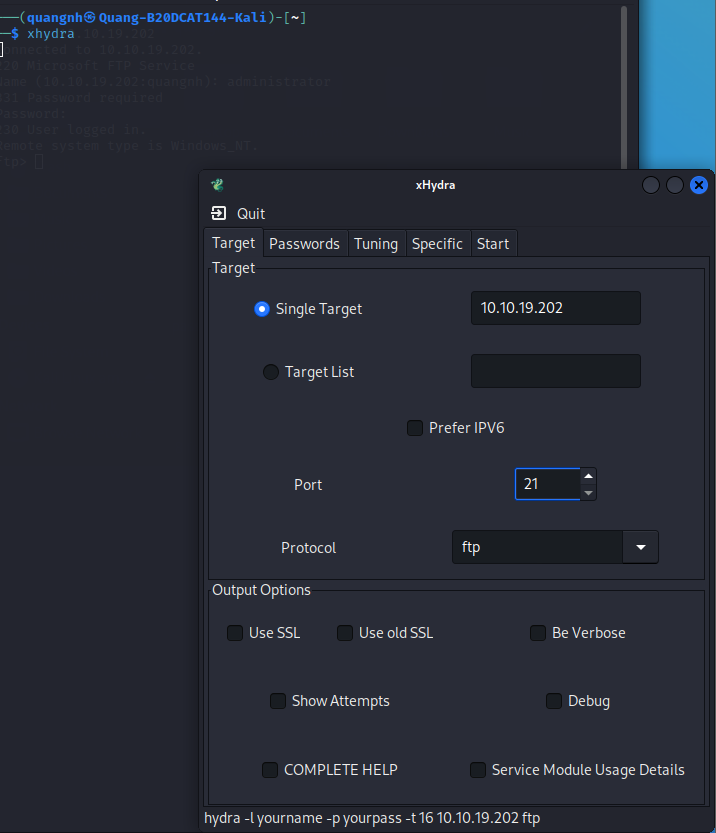




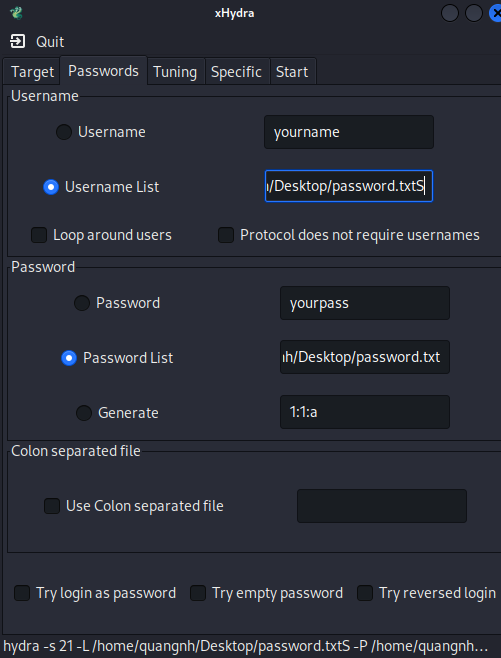


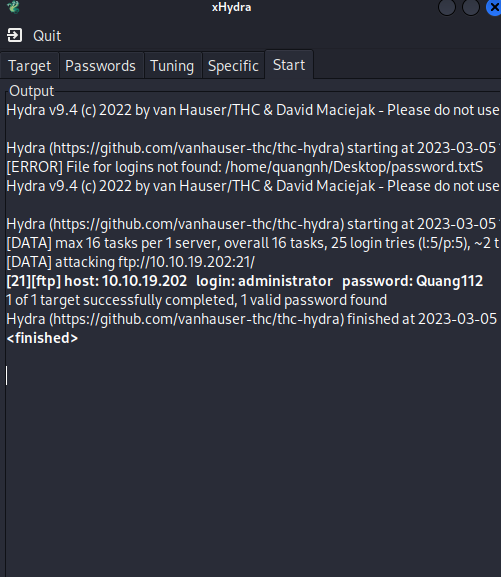


* Trong máy Kali External Attack khởi động #xhydra, chọn target là **10.10.19.202**, giao thức ftp

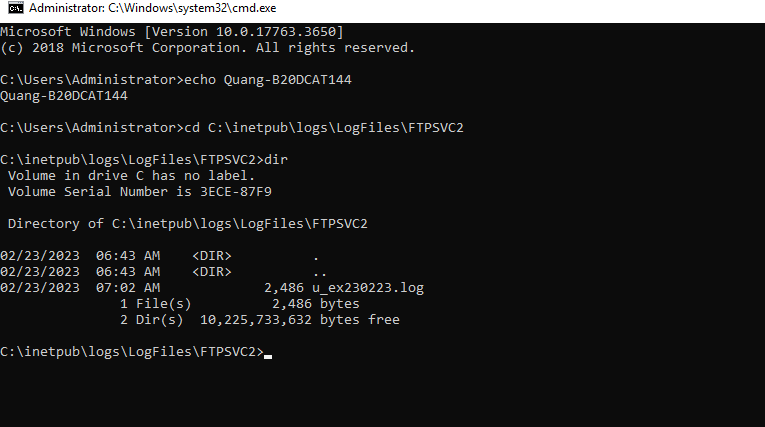


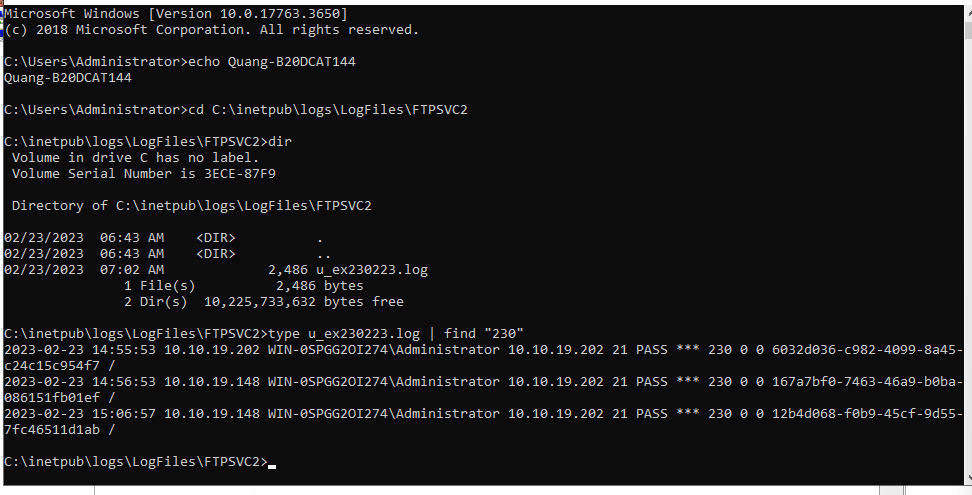
và cài đặt Password list, sau đó nhấn Start và chờ xHydra tìm ra mật khẩu





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



* Tìm kiếm kết quả login thành công
* 

## 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/windowsserver/administration/windows commands/find
* xhydra: <http://manpages.ubuntu.com/manpages/bionic/man1/hydra.1.html>