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

**KHOA AN TOÀN THÔNG TIN**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 9: Phân tích log hệ thống.**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

Phân tích log hệ thống

I. Tìm hiểu lý thuyết:

1. grep:

– grep là công cụ tìm kiếm các dòng văn bản trong một tệp văn bản chứa nội dung khớp với cụm từ mà người dùng yêu cầu tìm.

– grep ban đầu được phát triển cho hệ điều hành Unix, nhưng sau đó có sẵn cho tất cả các hệ điều hành họ Unix và một số hệ thống khác như OS-9.

– Trong bài thực hành bên dưới, sinh viên sử dụng lệnh grep <từ khoá> <tên file> để in ra các dòng có chứa từ khoá trong file văn bản.

2. gawk và awk:

– gawk là một phiên bản của ngôn ngữ lập trình Awk, do GNU phát triển.

– AWK (awk) là ngôn ngữ lập trình được thiết kế để xử lý văn bản và thường được sử dụng làm công cụ báo cáo và trích xuất dữ liệu.

– Trong bài thực hành bên dưới, sinh viên sử dụng lệnh awk '/từ khoá/ {print}' <tên file> để in ra màn hình các dòng chứa từ khoá tương ứng trong file văn bản.

3. find:

– find là một lệnh có trong shell hoặc terminal của một số hệ điều hành như DOS, ReactOS, Microsoft Windows, v.v

– Nó được sử dụng để tìm kiếm một chuỗi văn bản cụ thể trong một tệp hoặc các tệp.

– Nếu tìm kiếm thành công, find sẽ in ra các dòng chứa nội dung trùng khớp ra màn hình terminal (cmd).

– Cần lưu ý rằng lệnh find trên Windows và find trên Linux có tác dụng hoàn toàn khác nhau.

– Trong bài thực hành bên dưới, sinh viên dùng lệnh type <tên file> | find "<từ khoá>" để lọc và in ra các dòng có chứa từ khoá trong file văn bản.

4. hydra và xhydra:

– hydra là một trình bẻ khóa đăng nhập mạng được có sẵn trong các hệ điều hành khác nhau như Kali Linux, Parrot và các môi trường thử nghiệm thâm nhập lớn khác.

– hydra hoạt động bằng cách sử dụng các cách tiếp cận khác nhau để thực hiện các cuộc tấn công brute-force nhằm đoán đúng các cặp tên người dùng và mật khẩu.

– hydra hỗ trợ nhiều giao thức đăng nhập phổ biến như biểu mẫu trên trang web, FTP, SMB, POP3, IMAP, MySQL, VNC, SSH, v.v

– xhydra là giao diện đồ hoạ (GUI) của hydra.

II) Cài dặt và chuẩn bị:

Chuẩn bị các máy ảo

Cấu hình địa chỉ IP cho máy Windows Server 2022 mạng Internal(IP 192.168.100.201), và mạng External(IP 10.10.19.202)

|  |  |
| --- | --- |
|  |  |

Cấu hình địa chỉ IP(10.10.19.148) cho Kali Linux External:

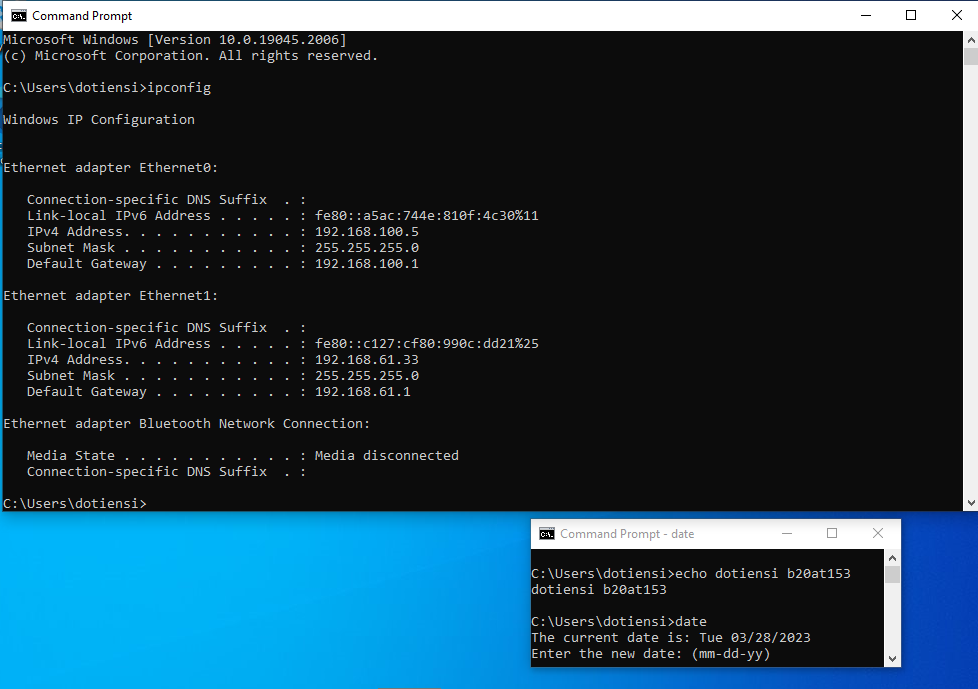
A screenshot of a computer

Description automatically generated

Cấu hình địa chỉ IP(192.168.100.147) cho Ubuntu Linux Internal

Text

Description automatically generated

Windows Internal(192.168.100.5)

2. Các bước thực hiện và kết quả cần đạt

2.1 Phân tích log sử dụng grep trong Linux Khởi chạy zenmap và scan cho địa chỉ 192.168.100.147

Text

Description automatically generated

Text

Description automatically generated

Trên máy Linux Internal Victim(192.168.100.147), để xem thư mục chứa access\_log dùng lệnh

Text

Description automatically generated with low confidence

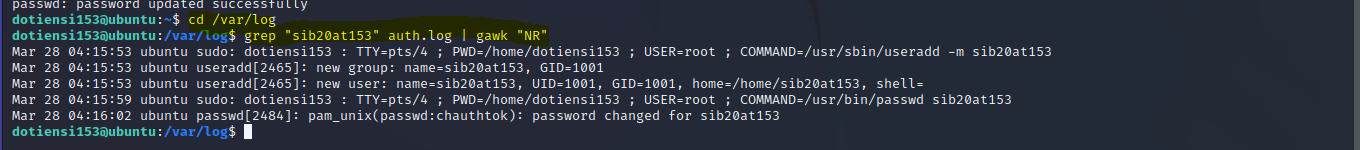
2.2 phân tích log sử dụng gawk trong linux

Trên máy Kali attack remote máy Linux Internal Victim. Tạo một account mới

Graphical user interface, text

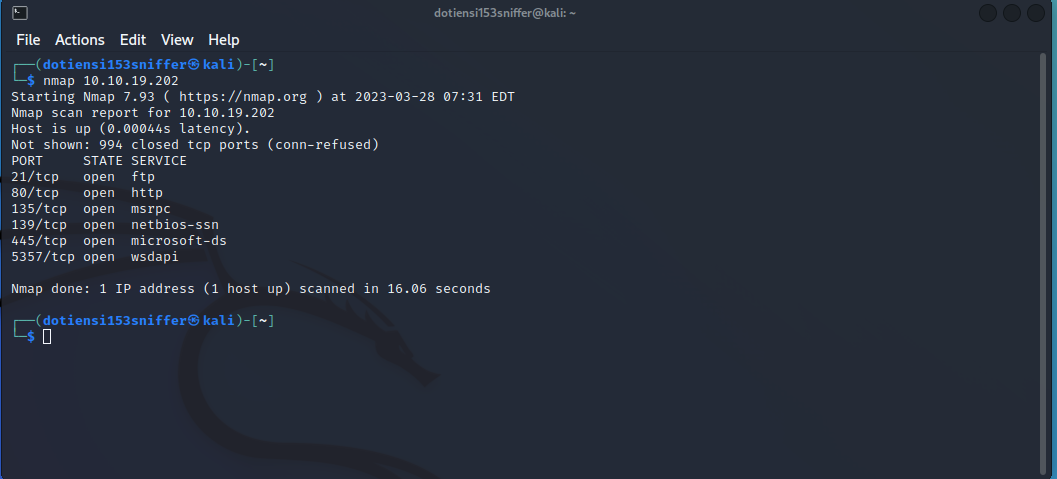
Description automatically generated

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.



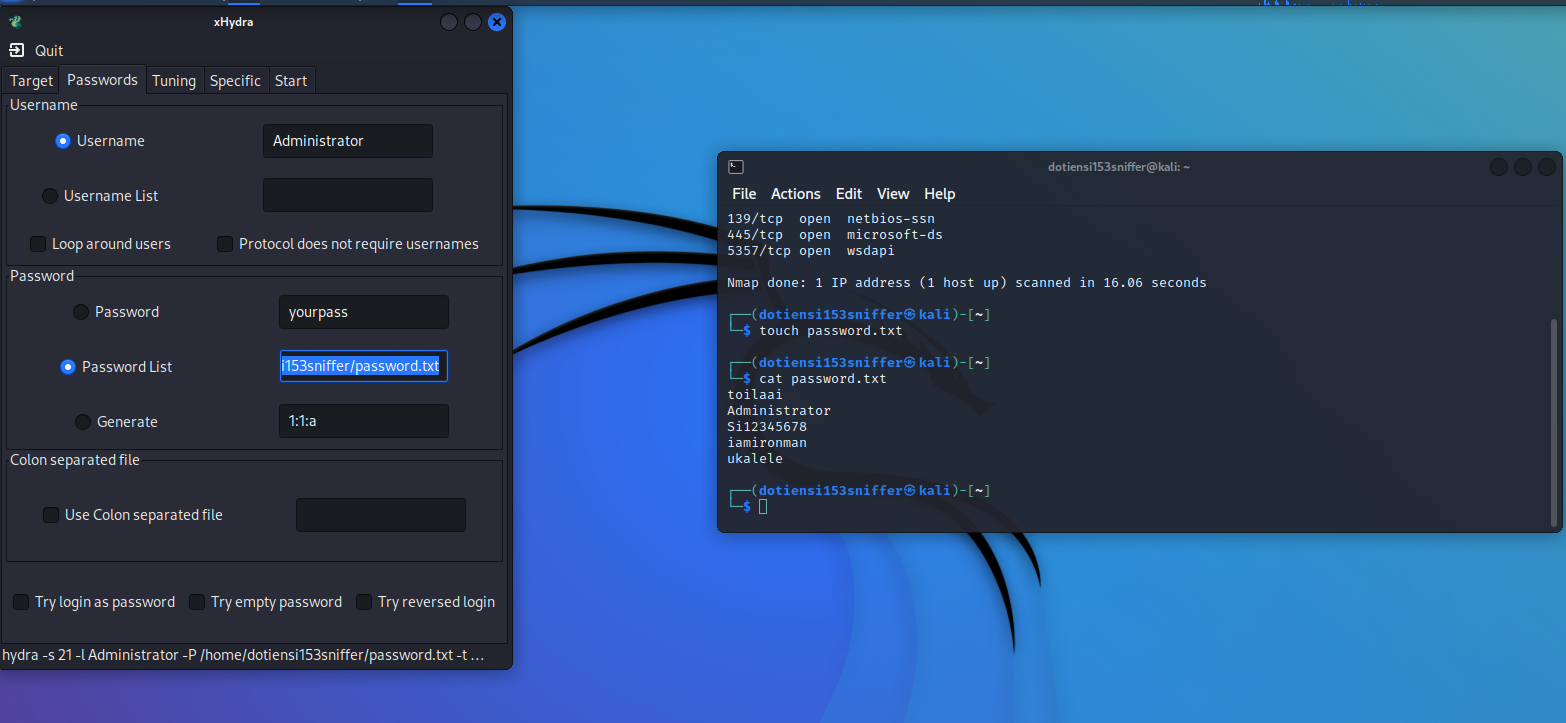
Dùng find

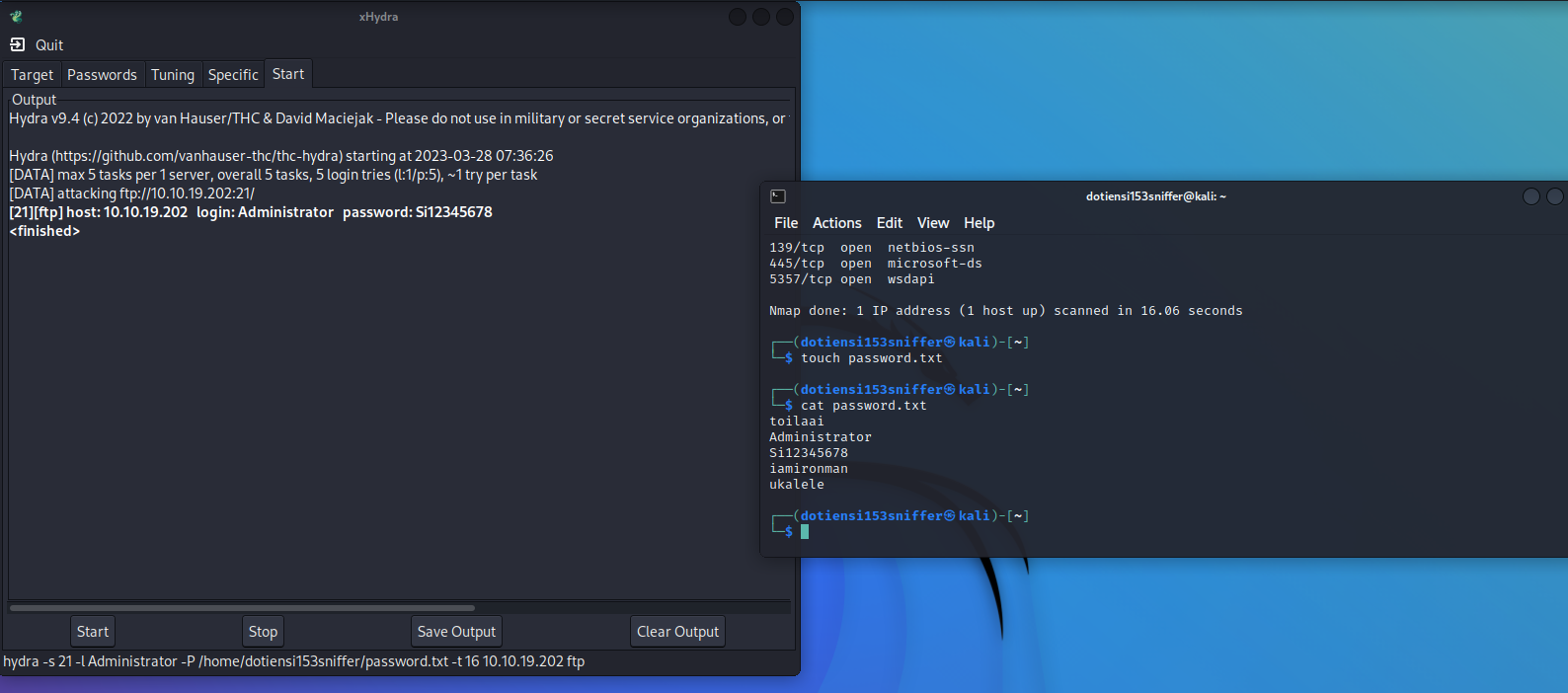
2.3.3 Phân tích log sử dụng find trong Windows



Khởi động xhydra

A screenshot of a computer

Description automatically generated with medium confidenceNhấn Start và chờ xHydra tìm ra mật khẩu

Trên máy Windows 2019 Server External Victim, thực hiện điều hướng đến FTP Logfile(C:\inetpub\log\LogFiles\FTPSVC2>find“230” u\_ex230328.log)

Graphical user interface, text

Description automatically generatedText

Description automatically generated