Phân tích log hệ thống

1Chuẩn 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:

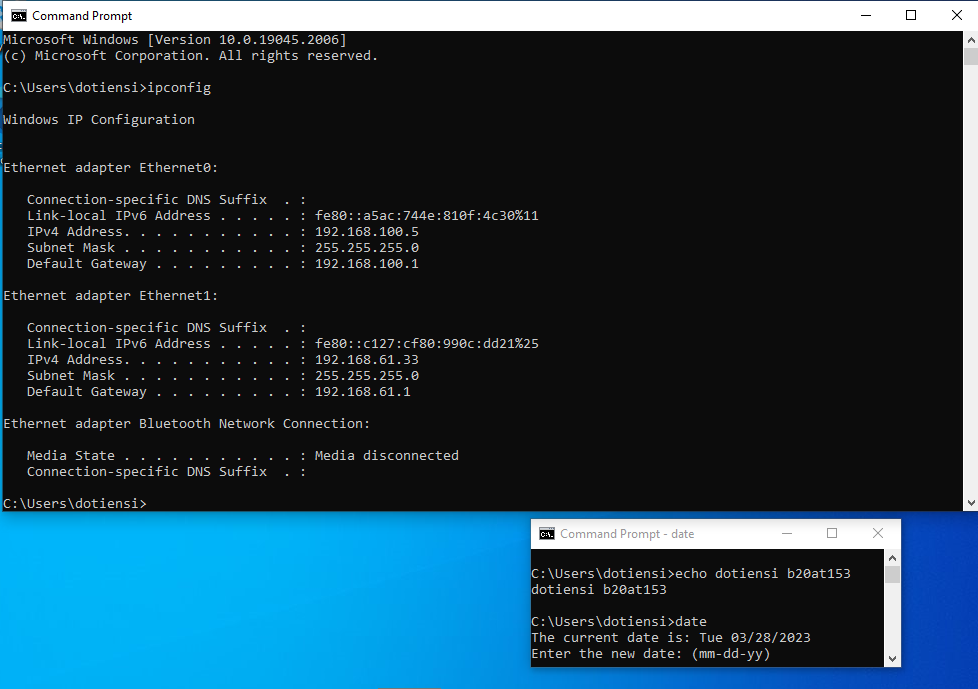
A screenshot of a computer

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 generatedText

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

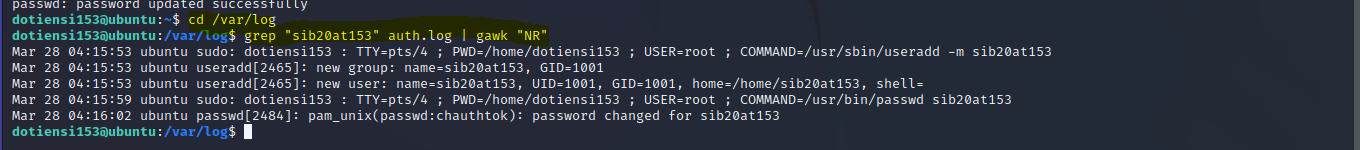
2.2 phân tích log sử dụng gawk trong linux

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

Graphical user interface, text

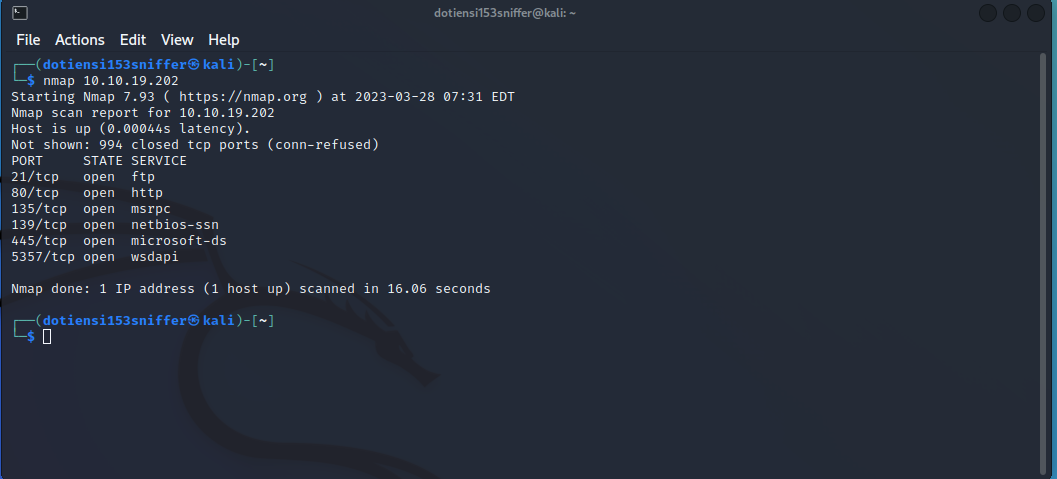
Description automatically generated

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.



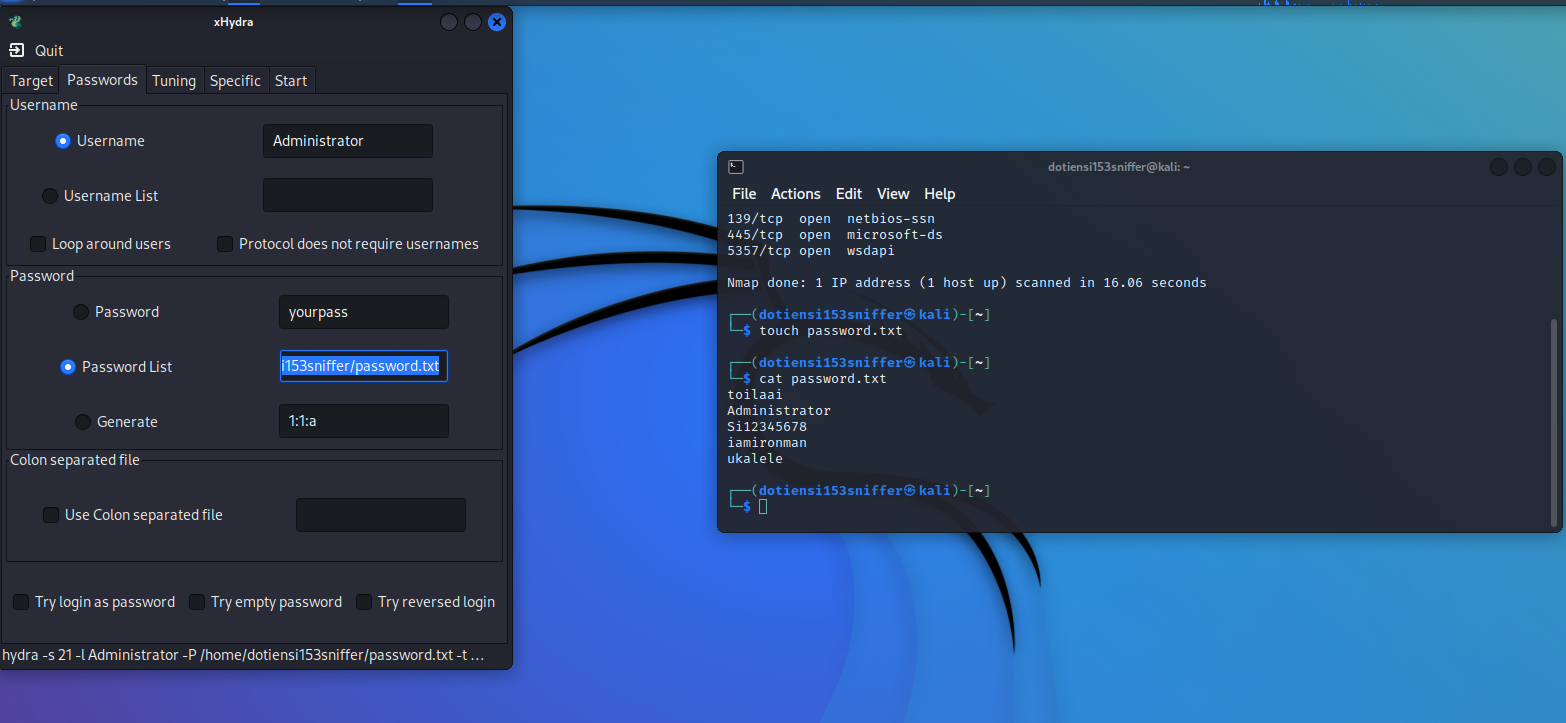
Dùng find

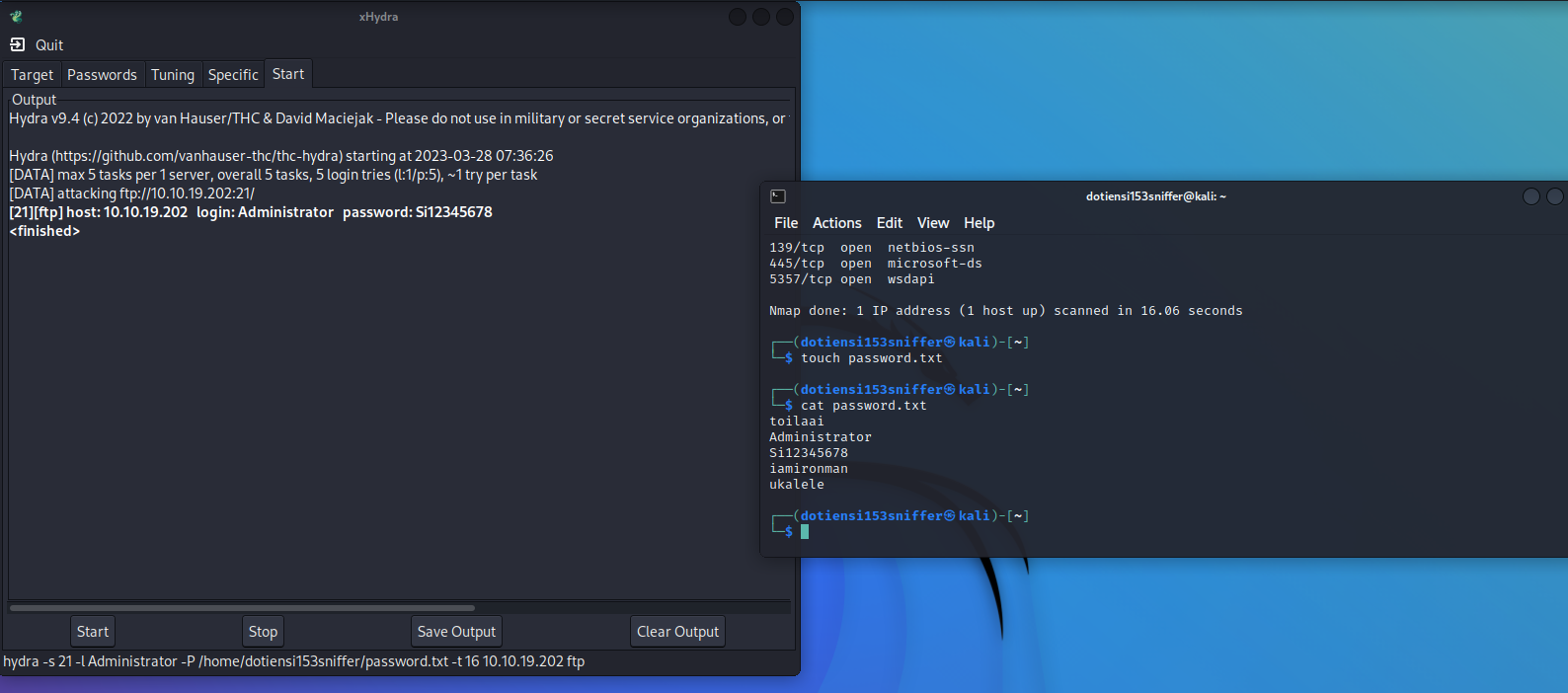
2.3.3 Phân tích log sử dụng find trong Windows



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