Bắt dữ liệu mạng

Chuẩn bị các máy

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:

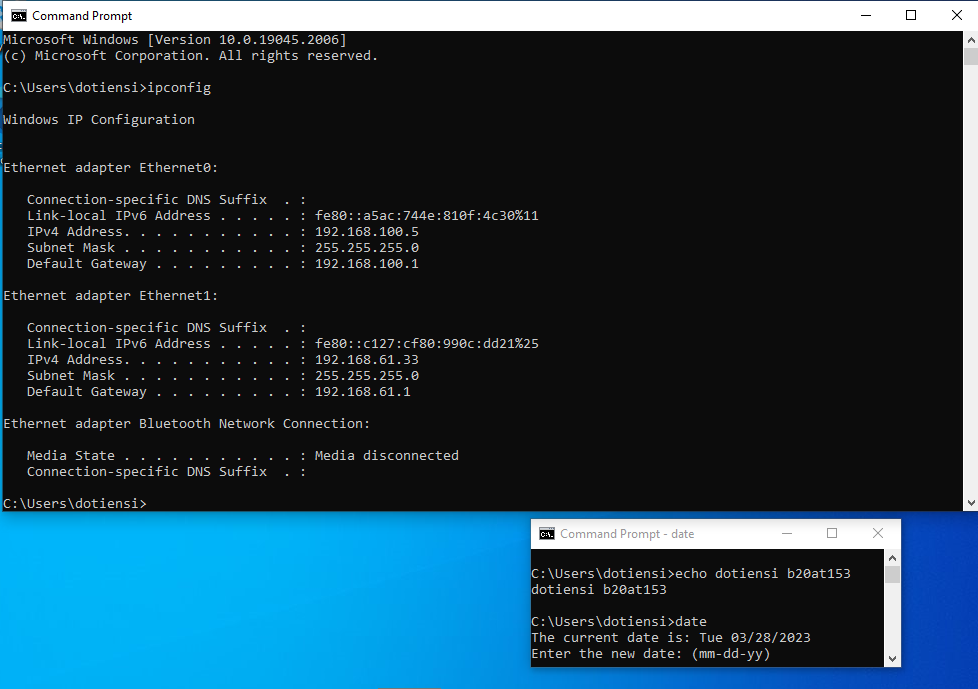
A screenshot of a computer

Description automatically generated

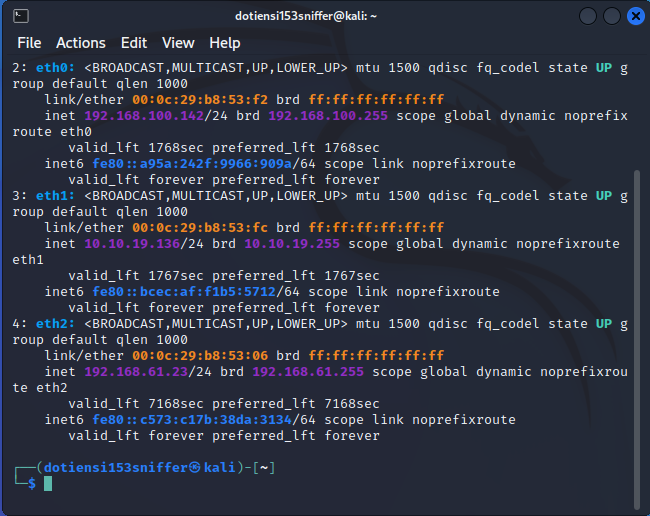
Cấu hình địa chỉ IP(192.168.100.147) cho Ubuntu Linux Internal

Text

Description automatically generated

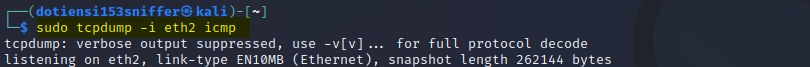
Windows Internal(192.168.100.5)

Trong bài 8 cần thêm 1 máy Linux Sniffer có 2 chân mạng. 1 chân mạng eth0 trong dải 192.168.100.0/24 (Internal), 1 chân mạng eth1 trong dải 10.10.19.0/24 (External).

Kích hoạt các eth1 và eth2 hoạt động ở chế độ hỗn hợp

Text

Description automatically generated

Khởi động tcpdump bắt các gói tin trên interfaces mạng Internal

Và gửi vào 1 file (file được đặt tên là eth0-b20at105.pcap) 

Trên máy Windows Server Internal ping đến dải mạng Interna

A picture containing graphical user interface

Description automatically generated

Từ máy Linux Sniffer bắt được dữ liệu

Text

Description automatically generatedGraphical user interface, text

Description automatically generated Tương tự trên máy Windows Server Victim External ping đến dải mạng External.Khởi động tcpdump trên interfaces eth1.

Graphical user interface

Description automatically generated with medium confidence

Text

Description automatically generated

Khởi động Wireshark chọn Start ở dòng eth0 để bắt các gói tin trên dải mạng 192.168.100.0/24

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated Graphical user interface, text

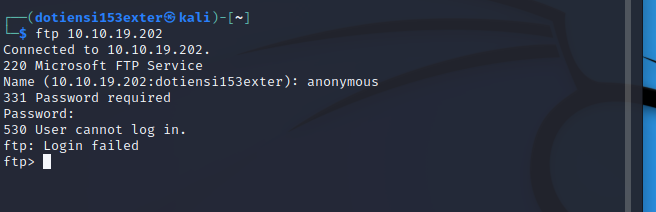
Description automatically generated

Lưu lại file trên

Graphical user interface, application

Description automatically generated

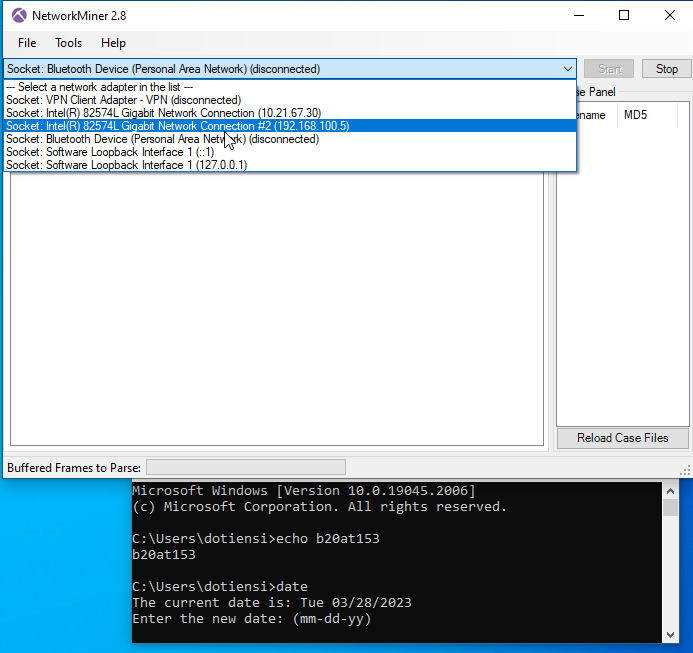
Tương tự với mạng external

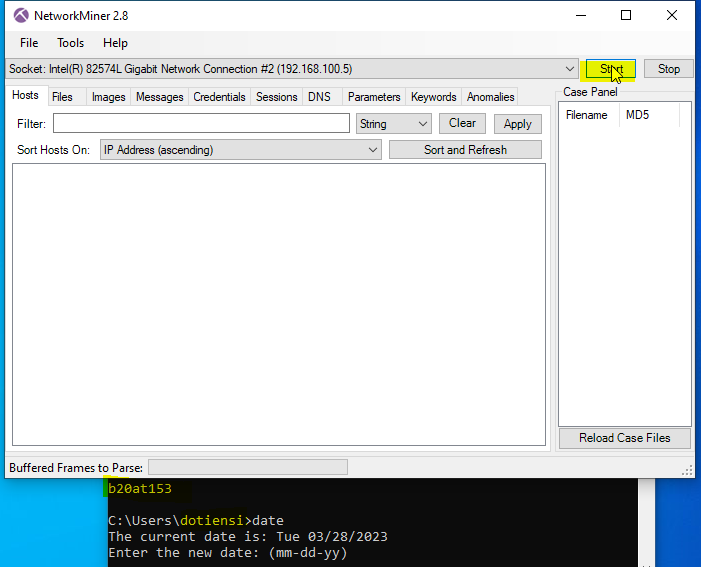
Graphical user interface, text

Description automatically generatedA screenshot of a computer

Description automatically generated

3.3 Sử dụng Network Miner để bắt và phân tích các gói tin Mở NetworkMiner ở máy Windows Internal với quyền Administrator, chọn (192.168.100.5)





Kết nối tới trang web(192.168.100.201) và bắt gói tin

