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

**KHOA AN TOÀN THÔNG TIN**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 8**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 8: Bắt dữ liệu mạng**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

Bắt dữ liệu mạng.

I. Tìm hiểu lý thuyết:

1. tcpdump:

– tcpdump là một công cụ phân tích gói tin mạng chạy dưới giao diện dòng lệnh (CLI). Nó cho phép người dùng hiển thị các gói tin TCP/IP đang được truyền hoặc nhận qua mạng mà máy tính chạy tcpdump kết nối tới.

– tcpdump có mặt trên Windows và các hệ điều hành họ Unix như Linux, BSD, MacOS, OpenWRT, v.v

– Một số tác dụng của tcpdump (và các công cụ bắt gói tin nói chung) trên thực tế:

* Giám sát hạ tầng mạng để phát hiện các kết nối bất thường.
* Tấn công ăn trộm tên tài khoản, mật khẩu và các thông tin nhạy cảm khác nếu dữ liệu được truyền qua HTTP không mã hoá.
* Kiểm tra lỗi trên hạ tầng mạng (định tuyến sai, cổng đóng, v.v).

– tcpdump có thể lưu kết quả bắt gói tin vào tệp pcap.

2. Wireshark:

– Wireshark là một công cụ phân tích gói tin mạng mã nguồn mở và miễn phí, được sử dụng rộng rãi trên thế giới. Wireshark có mặt trên Windows và các hệ điều hành họ Unix.

– Khác với tcpdump, Wireshark có giao diện đồ hoạ (GUI) giúp người dùng dễ tương tác hơn.

– Wireshark khá giống với tcpdump. Một số tính năng của Wireshark liệt kê dưới đây cũng có mặt trên tcpdump:

* Hỗ trợ nhiều giao thức mạng khác nhau.
* Giám sát hạ tầng mạng trên thời gian thực.
* Bắt các gói tin trên thời gian thực, có thể lưu lại và kiểm tra sau.
* Hỗ trợ đọc ghi nhiều loại tệp dữ liệu: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, v.v
* Hỗ trợ phân tích VoIP.
* Có thể xuất dữ liệu dưới dạng XML, PostScript, CSV hoặc plain text.

3. NetworkMiner:

– NetworkMiner là một công cụ phân tích mạng (NFAT) mã nguồn mở dành cho Windows.

– Tương tự như tcpdump và Wireshark, NetworkMiner có thể được sử dụng như một công cụ bắt / dò tìm gói tin mạng thụ động để phát hiện hệ điều hành, phiên, tên máy chủ, cổng đang mở, v.v. mà không đặt bất kỳ lưu lượng nào trên mạng.

– NetworkMiner có thể lưu kết quả bắt gói tin vào tệp pcap.

II) mô tả cài đặt kết quả.

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:

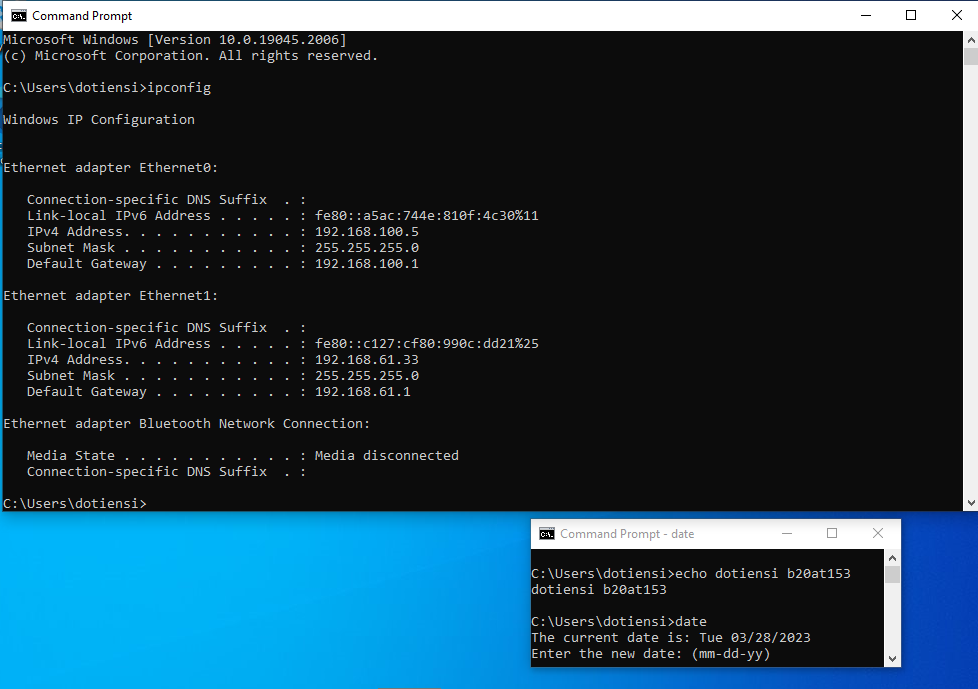
A screenshot of a computer

Description automatically generated

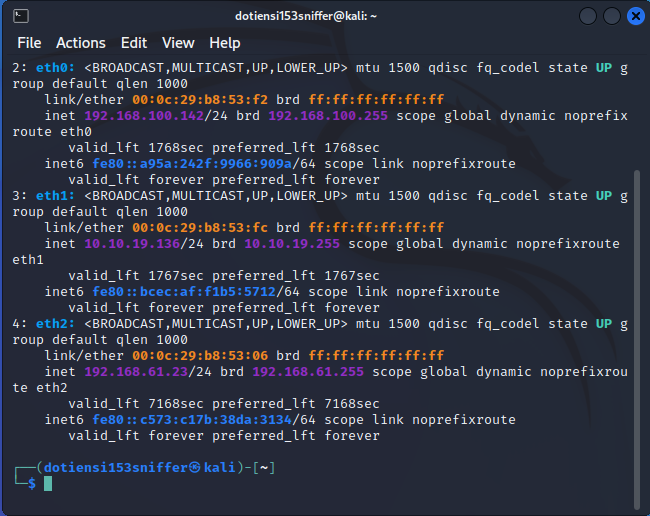
Cấu hình địa chỉ IP(192.168.100.147) cho Ubuntu Linux Internal

Text

Description automatically generated

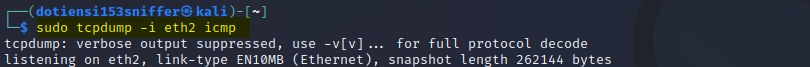
Windows Internal(192.168.100.5)

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

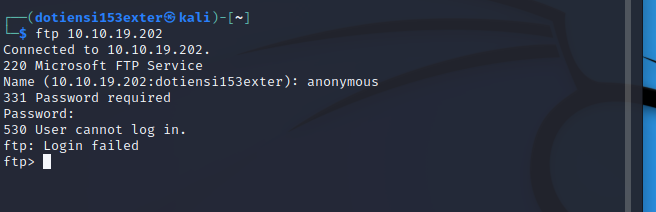
Description automatically generated

Lưu lại file trên

Graphical user interface, application

Description automatically generated

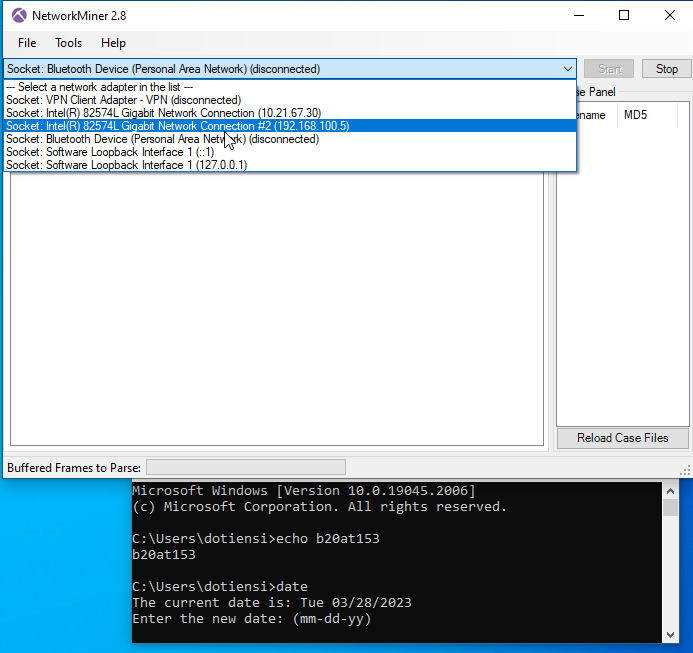
Tương tự với mạng external

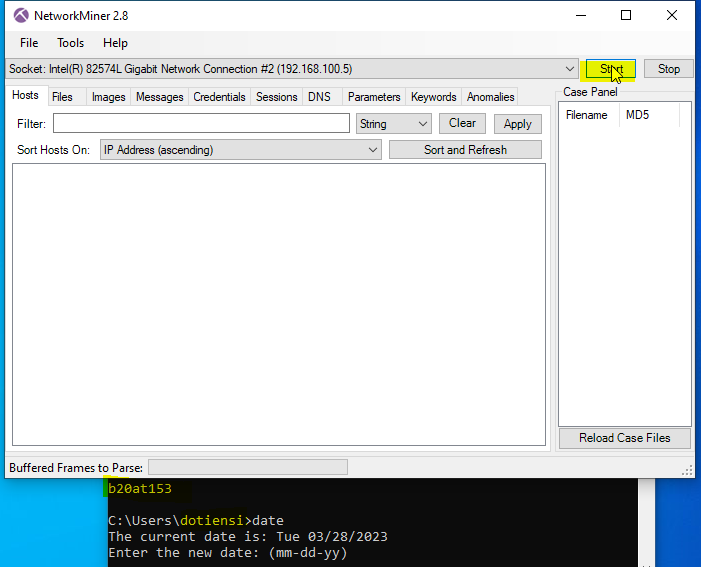
Graphical user interface, text

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

