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

**KHOA AN TOÀN THÔNG TIN**

****

**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 11**

**Bắt và phân tích gói tin trong mạng**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 2/2023

**I. Mục đích Bài thực hành này giúp sinh viên nắm được công cụ và cách thức bắt dữ** **liệu mạng, bao gồm:**

1. Sử dụng tcpdump để bắt gói tin mạng

2. Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)

3. Sử dụng Network Miner để bắt và phân tích gói tin mạng

**II. Tìm hiểu lý thuyết**

-TCPDUMP thực chất là công cụ được phát triển nhằm mục đích nhận diện và phân tích các gói dữ liệu mạng theo dòng lệnh.

-TCPDUMP cho phép khách hàng chặn và hiển thị các gói tin được truyền đi hoặc được nhận trên một mạng có sự tham gia của máy tính.

-TCPDUMP xuất ra màn hình nội dung các gói tin (chạy trên card mạng mà máy chủ đang lắng nghe) phù hợp với biểu thức logic chọn lọc mà khách hàng nhập vào. Với từng loại tùy chọn khác nhau khách hàng có thể xuất những mô tả về gói tin này ra một file “pcap” để phân tích sau, và có thể đọc nội dung của file “pcap” đó với option –r của lệnh TCPDUMP, hoặc sử dụng các phần mềm khác như là : Wireshark.

-Trong trường hợp không có tùy chọn, lệnh TCPDUMP sẽ tiếp tục chạy cho đến khi nào nó nhận được một tín hiệu ngắt từ phía khách hàng. Sau khi kết thúc việc bắt các gói tin, TCPDUMP sẽ báo cáo các cột sau:

+Packet capture: số lượng gói tin bắt được và xử lý.

+Packet received by filter: số lượng gói tin được nhận bởi bộ lọc.

+Packet dropped by kernel: số lượng packet đã bị dropped bởi cơ chế bắt gói tin của hệ điều hành.

-Wireshark là một bộ phân tích gói mạng (network packet analyzer). Một network packet analyzer sẽ cố gắng nắm bắt các network packets và cố gắng hiển thị dữ liệu gói đó càng chi tiết càng tốt.

Sử dụng Wireshark nhằm các mục đích sau:

+Network administrators sử dụng Wireshark để khắc phục sự cố mạng.

+Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.

+Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.

+Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.

+Mọi người sử dụng Wireshark để học internals giao thức mạng.

-Cách hoạt động của Wireshark:

1. Bắt gói – Packet Capture

2. Lọc – Filtering

3. Hiển thị trực quan – Visualization

-Network Miner là một công cụ phân tích bảo mật mạng Nguồn Mở di động có thể giám sát lưu lượng của bộ điều hợp mạng được kết nối trong hệ điều hành Windows.

Nó sử dụng một công cụ thu thập gói / dò tìm mạng thụ động có thể phát hiện IP, tên máy chủ, hệ điều hành, cổng và nhiều thông tin khác của bất kỳ kết nối nào. Công cụ bảo mật mạng yêu cầu cài đặt - riêng biệt - của WinPcap để hoạt động đúng và đáng tin cậy.

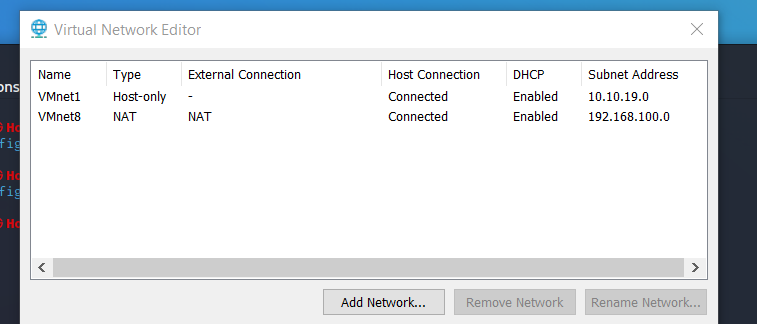
-Mục đích chính của Network Miner là thu thập dữ liệu để phân tích trong tương lai (chẳng hạn như phân tích bằng chứng pháp y) hơn là thu thập dữ liệu liên quan đến lưu lượng trên mạng. Thông tin được nhóm theo máy chủ chứ không phải theo gói hoặc khung mặc dù có thể chuyển đổi chế độ xem dễ dàng trong giao diện phần mềm.

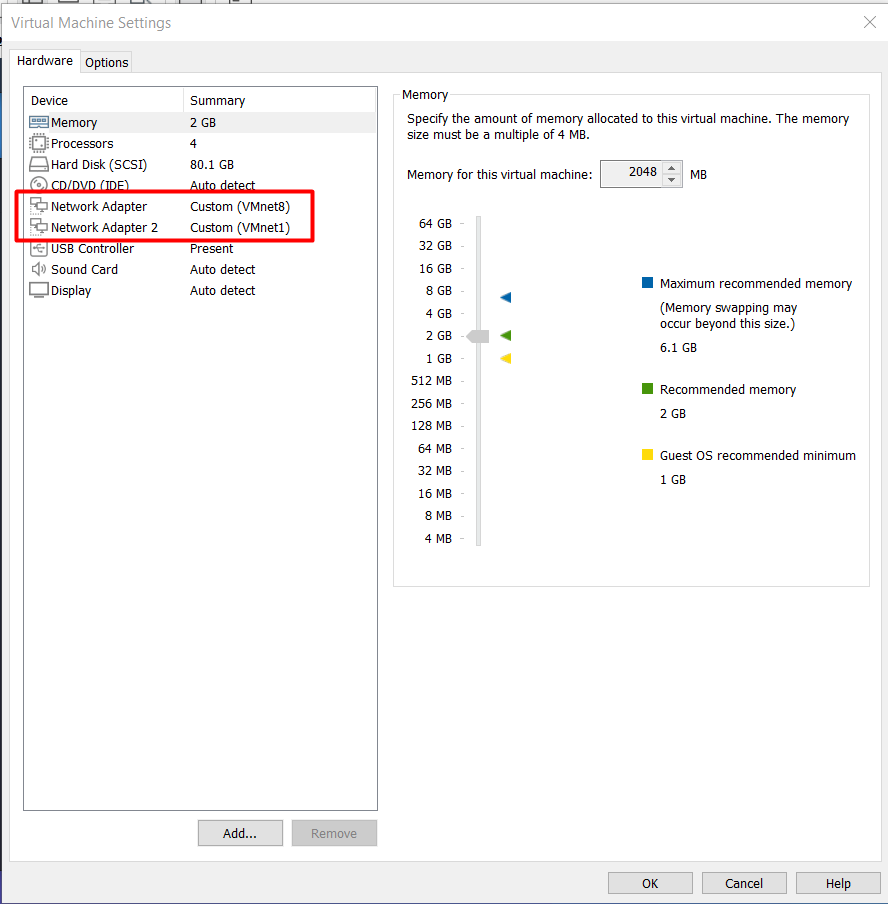
**III.Thực hành**

1. Sử dụng tcpdump

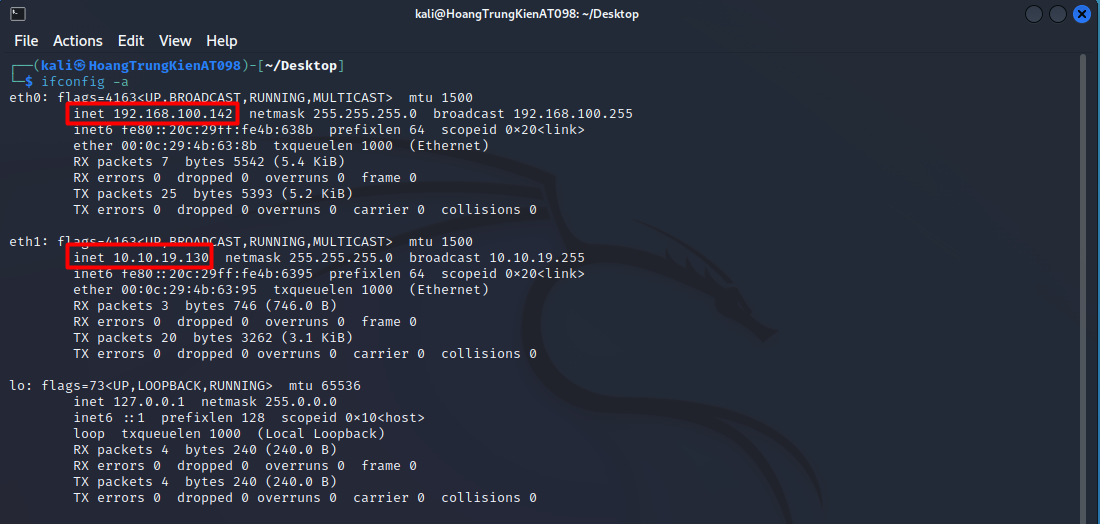
-Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống (root@bt:~#ifconfig -a), kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp, sau đó khởi động tcpdump. Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file

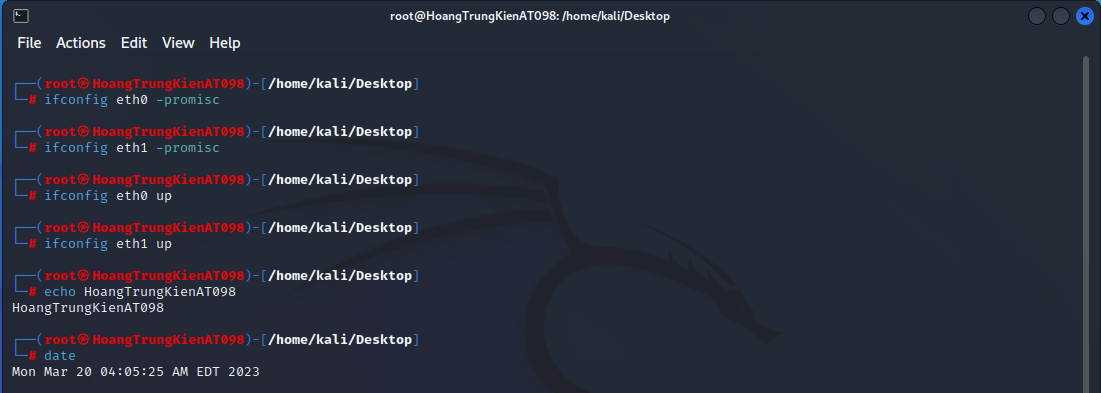
-Thêm dải mạng 10.10.19.0 vào máy kali Internal



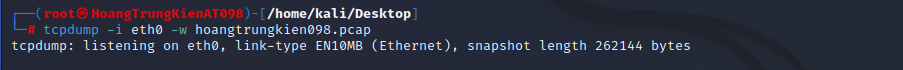


Gõ lệnh ifconfig -a để xem địa chỉ ip

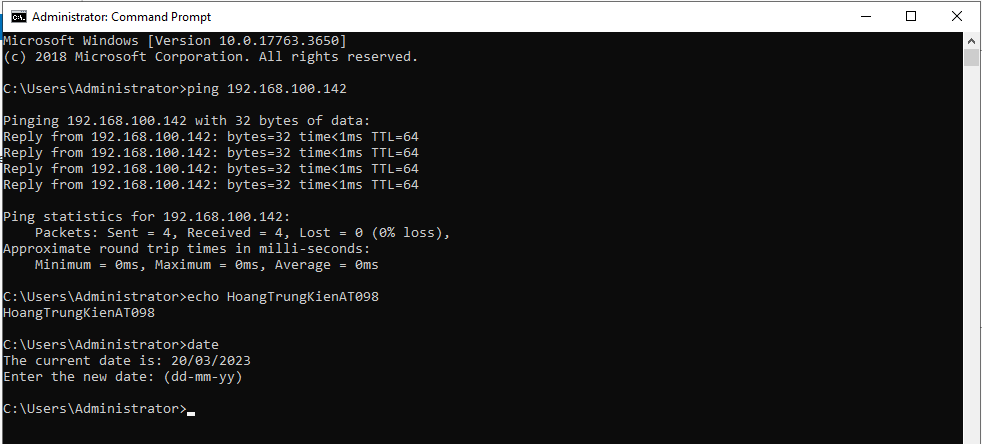




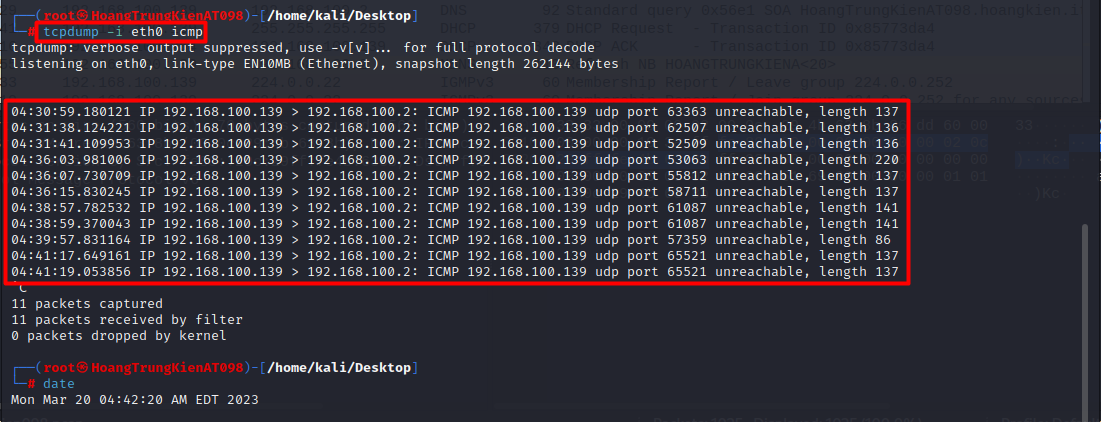
Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file



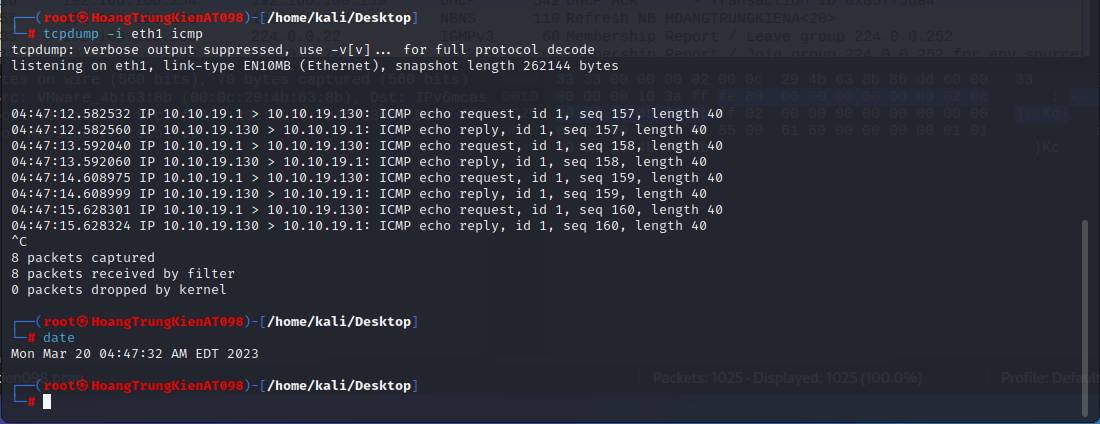
Đăng nhập vào windows server internal và ping đến giải mạng internal và external



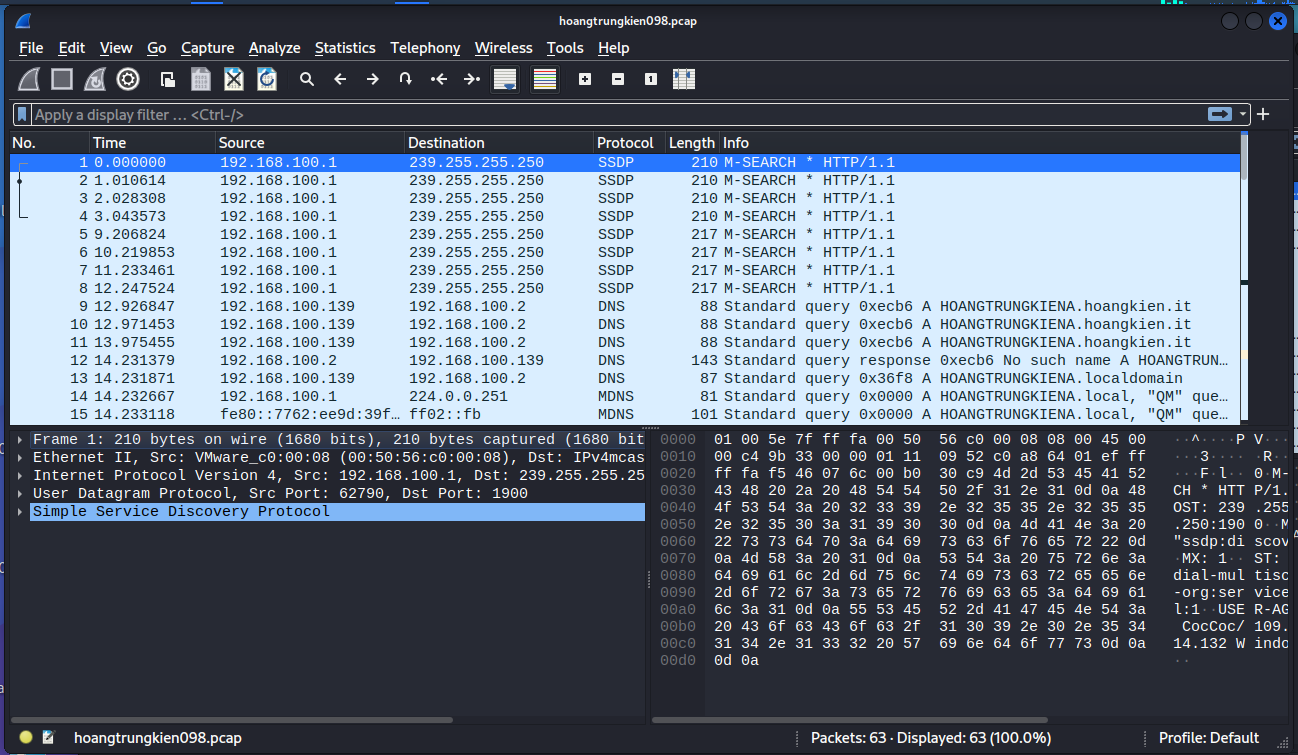
Gõ lệnh: tcpdump -i eth0 icmp để xem thông tin

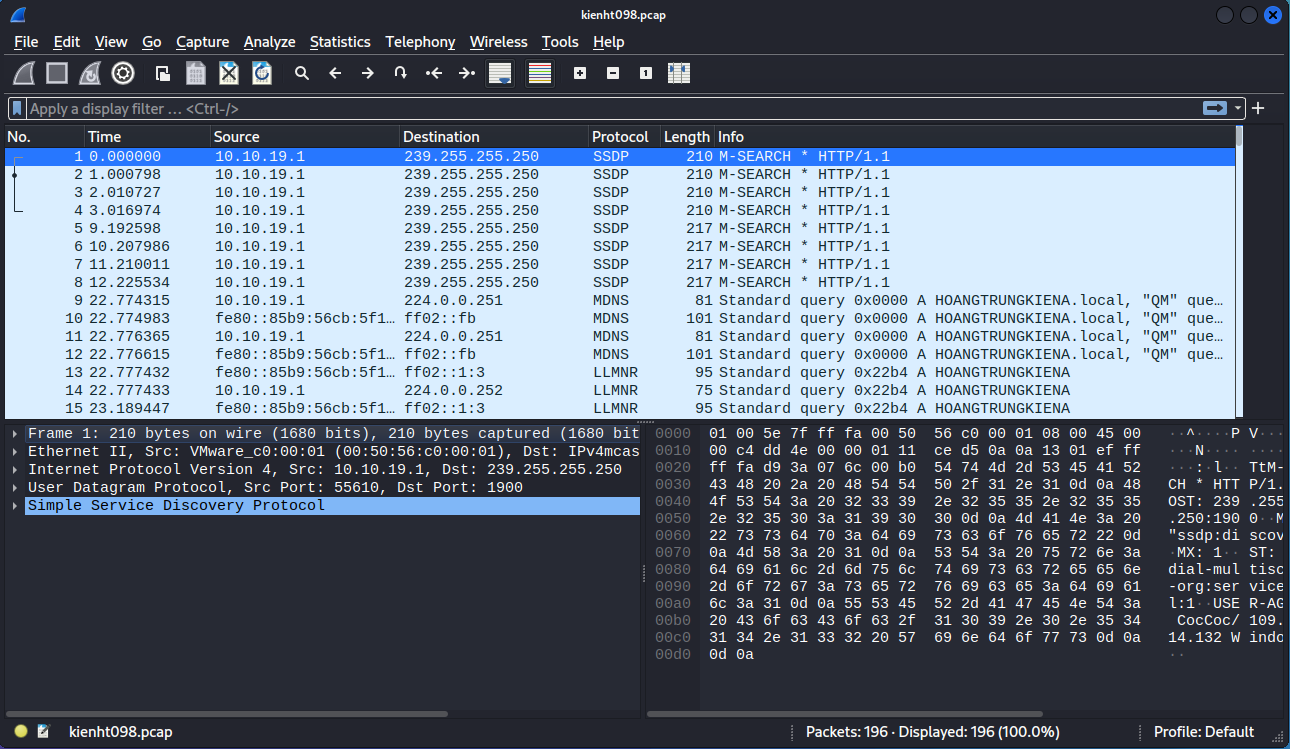


Gõ lệnh: tcpdump -i eth1 icmp để xem thông tin



Lưu dữ liệu ra 2 file pcap là: eth0-hoangtrungkien098.pcap và eth1-kienht098.pcap

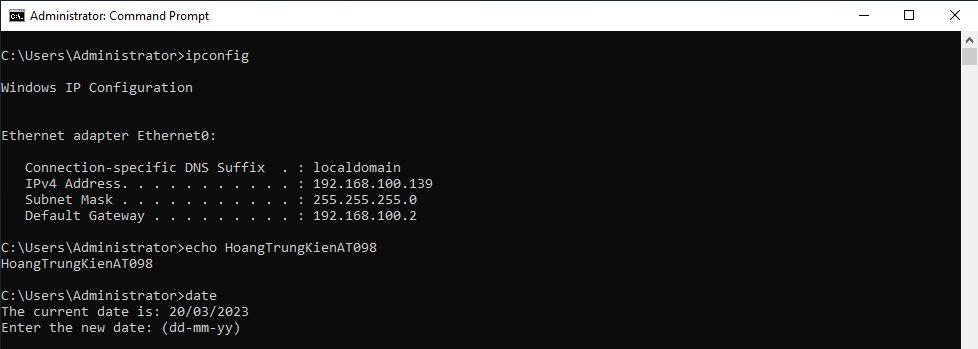




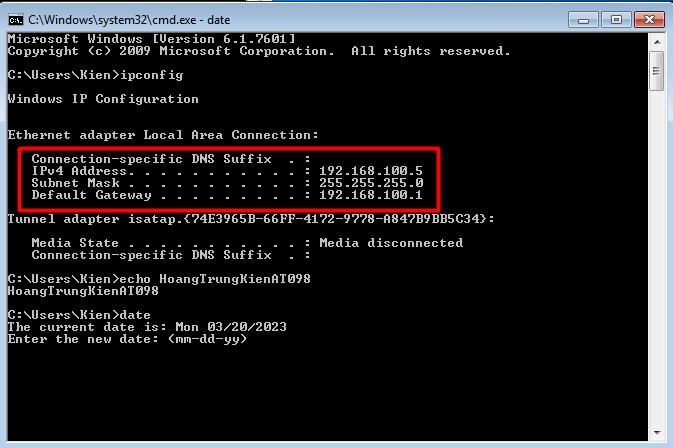
2. Sử dụng Wireshark để bắt và phân tích gói tin

Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0

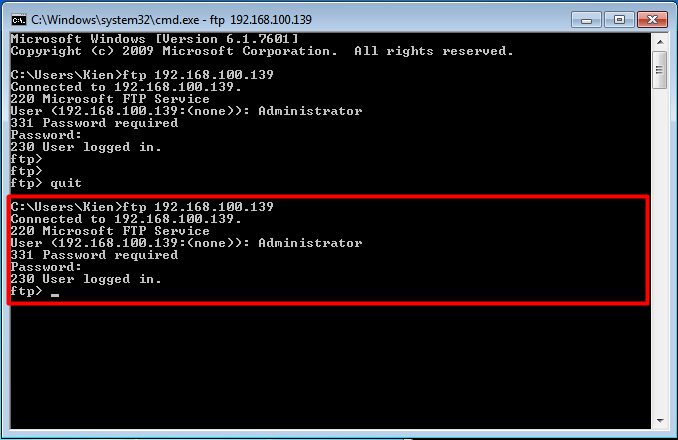
Địa chỉ ip máy windows server



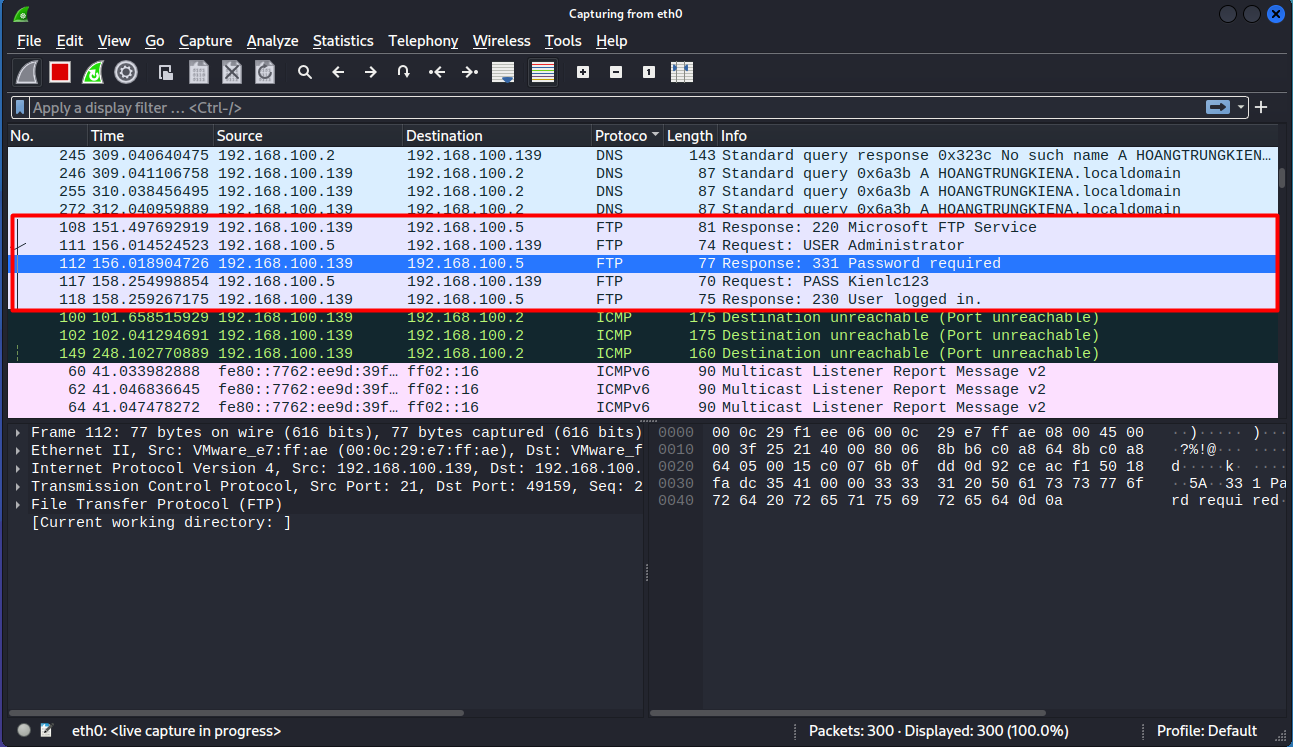
Địa chỉ ip máy Windows 7



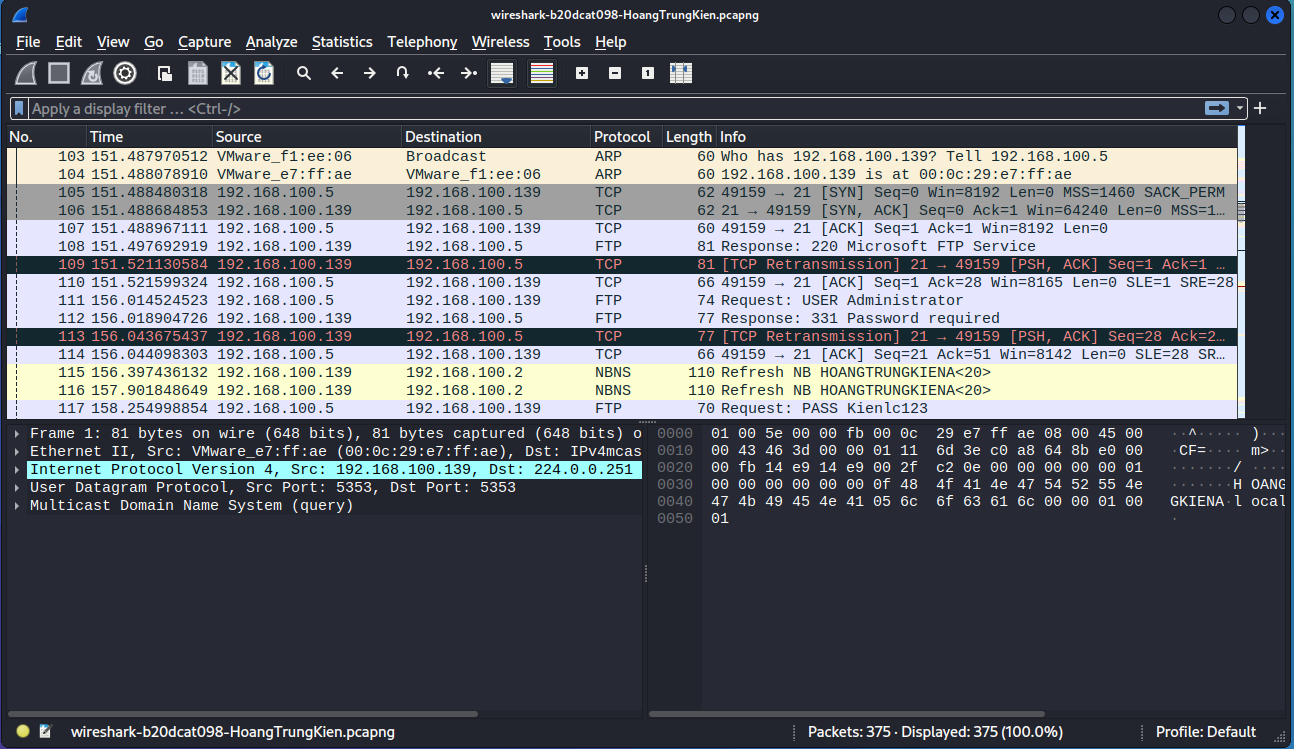
Trên máy windows 7 kết nối ftp server (192.168.100.139)



Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



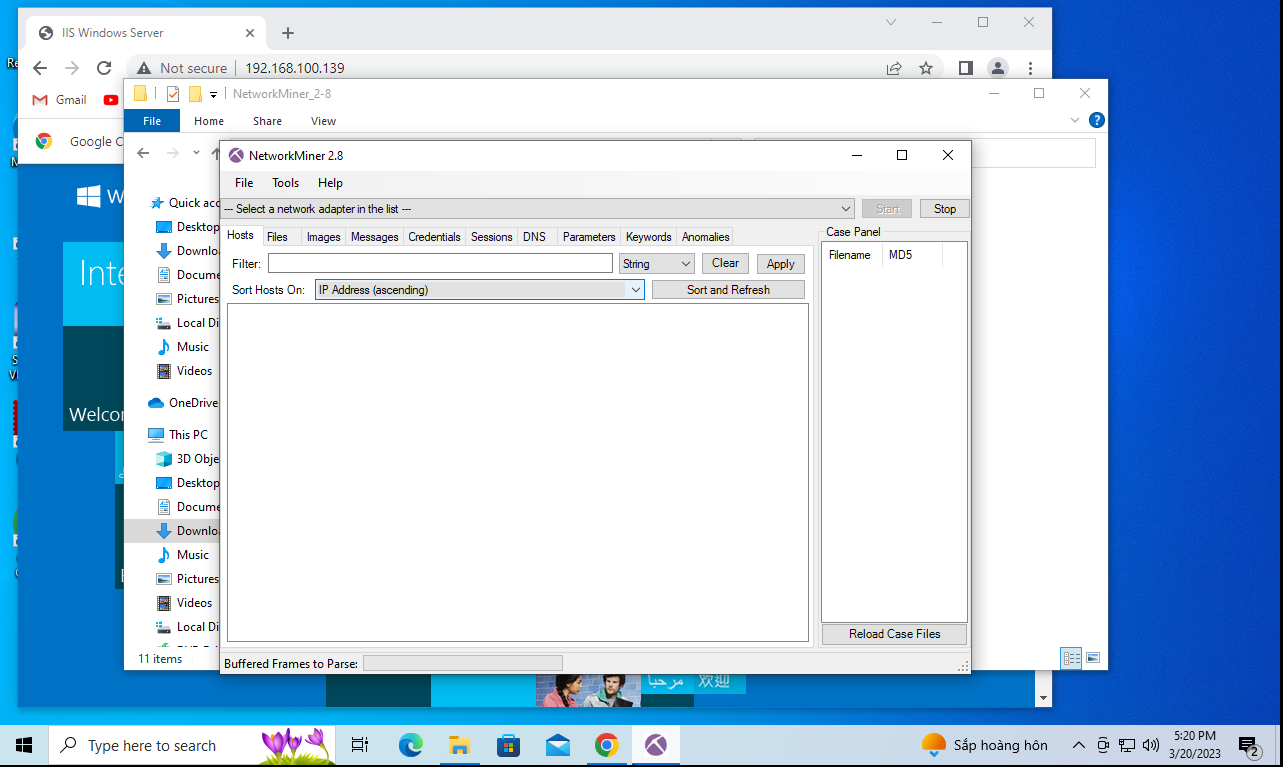
File wireshark đã lưu

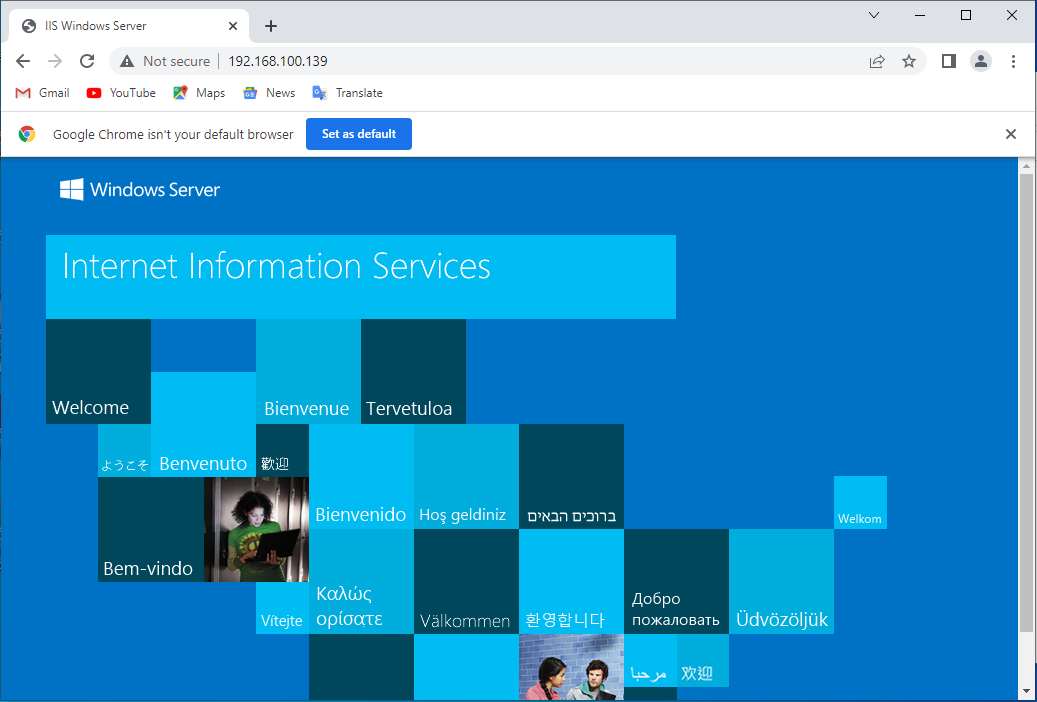


Bắt gói tin ở dải mạng eth1 làm tương tự

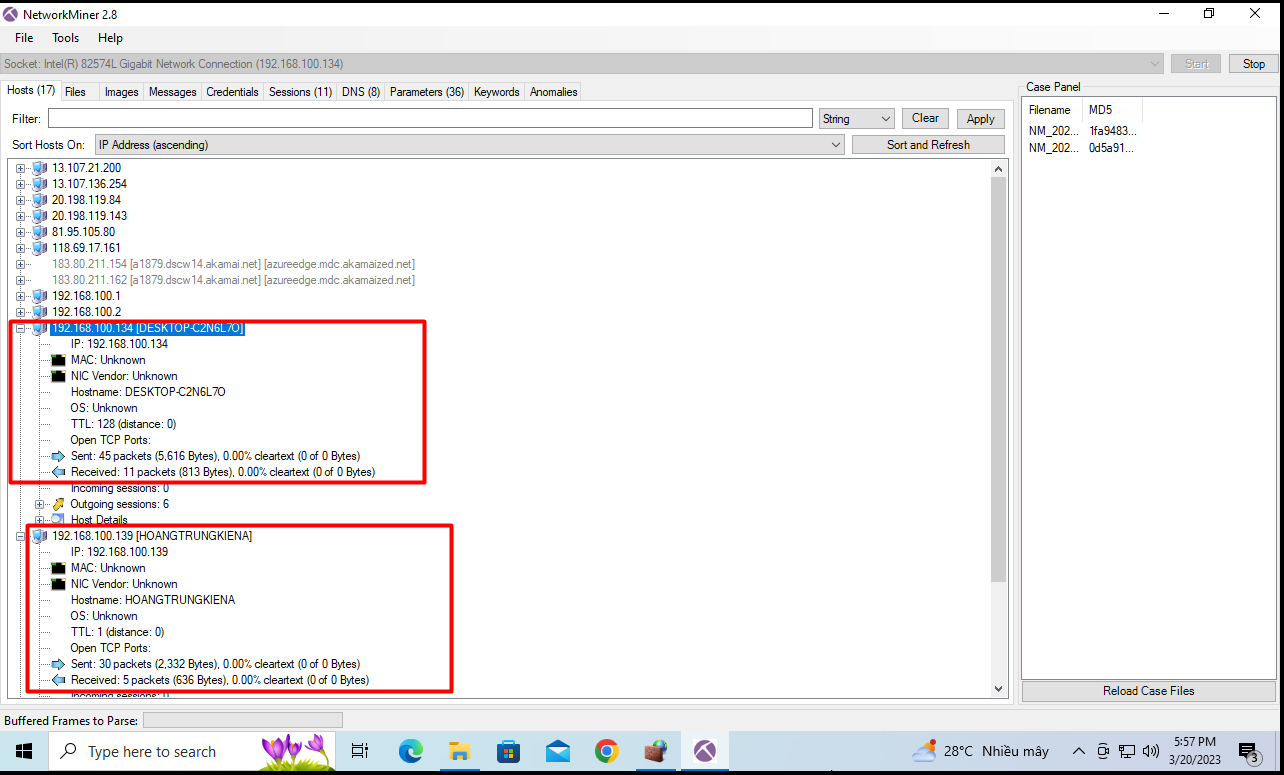
3. Sử dụng Network Miner để bắt và phân tích các gói tin

Trên máy windows 10 internal attack khởi động network miner





Bắt được gói tin của máy Windows 10 và Windows server



Mở file để xem thông tin

