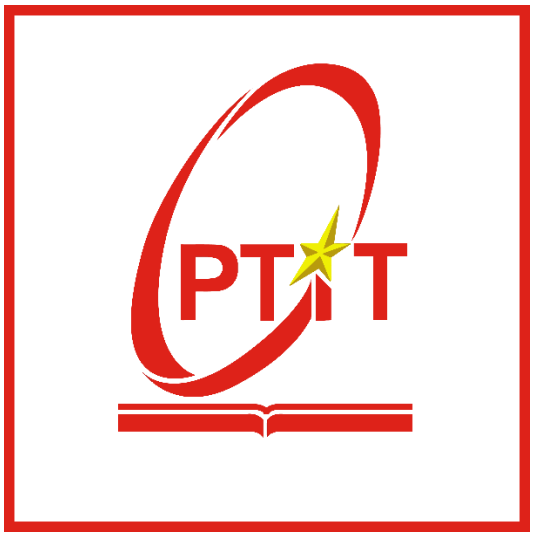
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 8

BẮT DỮ LIỆU MẠNG

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 3/2024 ~

Mục Lục

Bài 8: Bắt dữ liệu mạng

1 Mục đích

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

- Sử dụng tcpdump để bắt gói tin mạng
- Sử dụng được Wireshark để bắt và phân tích gói tin mạng (HTTP/HTTPS/FTP / TCP/IP)
- Sử dụng Network Miner để bắt và phân tích gói tin mạng

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

a) Tcpdump

Tcpdump là gì ?

TCPdump là một tiện ích dòng lệnh mạnh mẽ được sử dụng trong hệ thống Unix và Linux để theo dõi và phân tích gói tin truyền qua một mạng. Được thiết kế để cung cấp thông tin chi tiết về giao thức truyền tải lớp transport, TCPdump là một công cụ không thể thiếu cho các chuyên gia mạng, quản trị viên hệ thống và những người quan tâm đến việc giám sát và phân tích giao tiếp mạng.

- Sử dụng TCPdump, người dùng có khả năng theo dõi và ghi lại các gói tin đi và đến từ một hay nhiều giao diện mạng. Điều này cho phép họ xem xét nhanh chóng thông tin như địa chỉ IP nguồn và đích, cổng nguồn và đích, cũng như các trường quan trọng khác trong tiêu đề gói tin. Đồng thời, TCPdump hỗ trợ lọc dữ liệu để người dùng có thể tập trung vào các gói tin quan trọng hoặc cụ thể.

- Một tính năng mạnh mẽ khác của TCPdump là khả năng đọc các tệp pcap, nơi mà thông tin gói tin đã được ghi lại từ trước. Điều này rất hữu ích để phân tích các vấn đề mạng hoặc xem xét lưu lượng truyền qua mạng trong quá khứ.

- Tính linh hoạt và khả năng tùy chỉnh của TCPdump giúp nó trở thành công cụ ưa thích trong cộng đồng mạng, cung cấp một cách hiệu quả để giải quyết vấn đề, theo dõi lưu lượng mạng, và nhanh chóng xác định nguyên nhân của các vấn đề kỹ thuật.

Các hình thức của tcpdump

Để lựa chọn gói tin phù hợp với biểu thức logic mà khách hàng nhập vào, tcmpdump sẽ xuất ra màn hình một gói tin chạy trên card mạng mà máy chủ đang lắng nghe.

Tùy vào các lựa chọn khác nhau khách hàng có thể xuất mô tả này ra một gói tin thành một file “pcap” để phân tích và có thể đọc nội dung “pcap” đó với option – r của lệnh tcpdump, hoặc sử dụng các phần mềm khác như là : Wireshark.

Đối với những trường hợp không có tùy chọn, lệnh tcpdump sẽ được chạy cho đến khi nhận được một tín hiệu ngắt từ 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.

Lợi ích sử dụng tcpmdump

Tcpdump sẽ giúp phân các gói dữ liệu phù hợp với dòng lệnh mang theo, cụ thể:

- Bắt bản tin và lưu bằng định dạng PCAP (có thể đọc bởi wireshark).
- Nhìn thấy trực tiếp các bản tin điều khiển hệ thống Linux sử dụng wireshark, xem chi tiết remote packet capture using Wireshark và tcmpdump.
- Có thể nhìn thấy các bản tin trên DUMP trên terminal.
- Tạo các bộ lọc Filter để bắt bản tin cần thiết như: http, ssh, fpt...
- Ngoài ra tcmpdump còn sử dụng nhiều option khác nhau nữa.

b) Wireshark

Wireshark là gì ?

- Wireshark là một ứng dụng phần mềm mạng mạnh mẽ, sử dụng để phân tích và giám sát lưu lượng giao tiếp trên mạng. Với giao diện đồ họa thân thiện và khả năng hỗ trợ nhiều loại giao thức, Wireshark trở thành một công cụ quan trọng cho các chuyên gia mạng, quản trị viên hệ thống, và những người nghiên cứu về bảo mật mạng.

- Wireshark có khả năng bắt, hiển thị và phân tích các gói tin truyền qua một hoặc nhiều giao diện mạng. Với khả năng lọc mạnh mẽ, người dùng có thể tập trung vào các gói tin cụ thể, giúp họ nhanh chóng định rõ vấn đề mạng hay kiểm tra các giao thức cụ thể. Công cụ này hỗ trợ một loạt các giao thức như TCP, UDP, IP, HTTP, DNS và nhiều loại khác, giúp người dùng theo dõi và hiểu rõ lưu lượng mạng.

- Wireshark cũng cho phép lưu trữ và đọc các tệp tin thu thập được, ví dụ như các tệp pcap, để phân tích chi tiết hơn hoặc chia sẻthông tin với các đồng nghiệp. Ngoài ra, tính năng đồng bộ hóa đồ thị giúp hiển thị tương quan giữa các sự kiện mạng, giúp người dùng nhanh chóng phát hiện và giải quyết vấn đề.

- Wireshark không chỉ là một công cụ quan sát mạng, mà còn là một nguồn thông tin quan trọng giúp cải thiện hiệu suất, bảo mật và quản lý mạng trong môi trường công nghiệp và doanh nghiệp.

Mục đích sử dụng của wireshark

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.

Tính năng

- Có sẵn cho UNIX và Windows.
- Chụp dữ liệu gói trực tiếp từ giao diện mạng.
- Mở các tệp có chứa dữ liệu gói được bắt bằng tcpdump/ WinDump,
- Wireshark và một số chương trình packet capture khác.
- Nhập các gói từ các tệp văn bản có chứa các hex dumps của packet data.
- Hiển thị các gói với thông tin giao thức rất chi tiết.
- Lưu dữ liệu gói bị bắt.
- Xuất một số hoặc tất cả các gói trong một số định dạng capture file.
- Lọc các gói tin trên nhiều tiêu chí.
- Tìm kiếm các gói trên nhiều tiêu chí.
- Colorize gói hiển thị dựa trên bộ lọc.
- Tạo các số liệu thống kê khác nhau.

c) Network Miner

NetworkMiner là một công cụ phân tích pháp y mạng (NFAT) mã nguồn mở dành cho Windows (nhưng cũng hoạt động trong Linux /Mac OS X/FreeBSD). NetworkMiner có thể được sử dụng như một công cụ thu thập gói / dò tìm 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 cũng có thể phân tích cú pháp tệp PCAP để phân tích ngoại tuyến và tái tạo / tập hợp lại các tệp và chứng chỉ đã truyền từ tệp PCAP.

NetworkMiner giúp dễ dàng thực hiện Phân tích lưu lượng mạng nâng cao (NTA) bằng cách cung cấp các tạo tác được trích xuất trong giao diện người dùng trực quan. Cách dữ liệu được trình bày không chỉ làm cho việc phân tích đơn giản hơn mà còn tiết kiệm thời gian quý báu cho nhà phân tích hoặc điều tra viên pháp y.

Cách sử dụng Network Miner

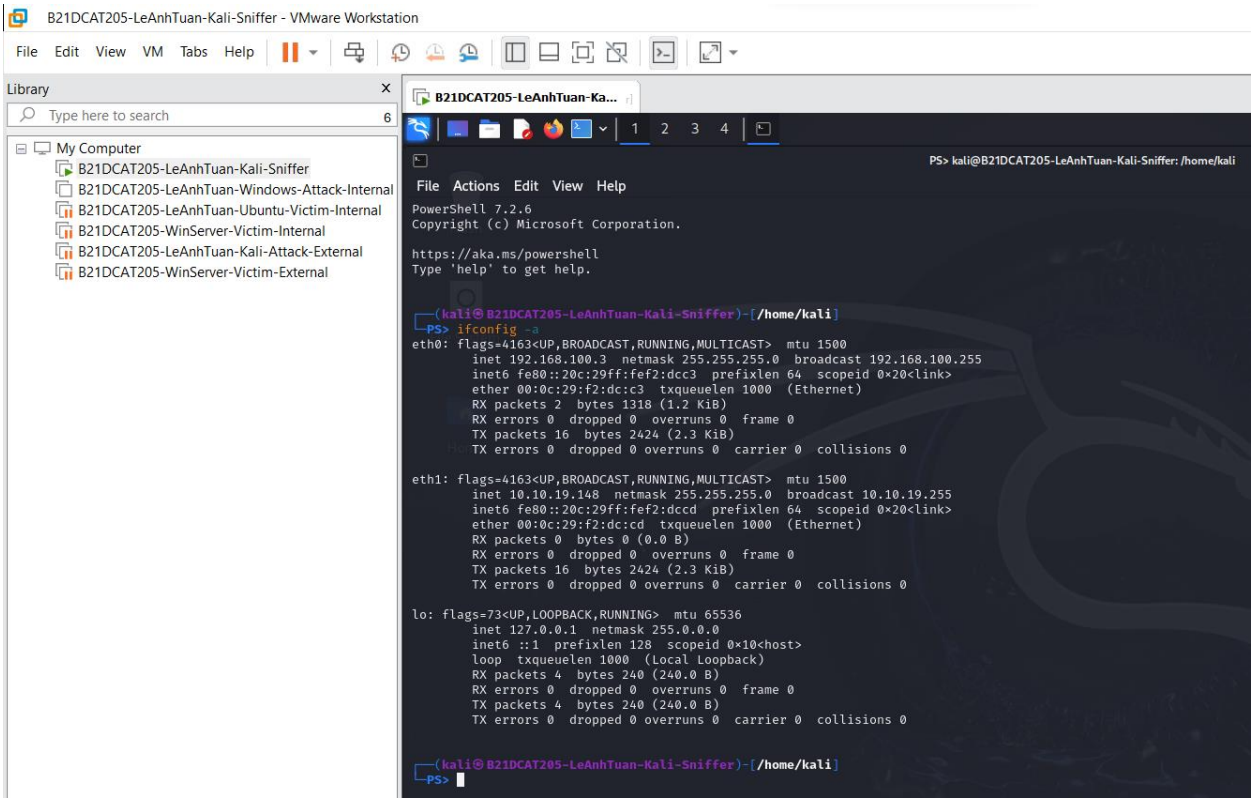
- Tải và Cài Đặt NetworkMiner: Trước hết, cần tải và cài đặt NetworkMiner từ trang web chính thức của nó. NetworkMiner hỗ trợ cả phiên bản Windows và Linux.
- Khởi động NetworkMiner: Sau khi cài đặt xong, mở ứng dụng NetworkMiner.

- Chọn Giao Diện Mạng: Chọn giao diện mạng muốn theo dõi từ danh sách. Điều này sẽ bắt đầu thu thập dữ liệu từ giao diện mạng đó.
- Quan sát Dữ Liệu: NetworkMiner sẽ bắt đầu hiển thị thông tin chi tiết về các máy chủ, máy khách, giao thức, và các tệp tin truyền qua mạng. có thể theo dõi các kết nối mạng và xem thông tin chi tiết về từng máy tính.
- Lưu Dữ Liệu Thu Thập Được: NetworkMiner cung cấp khả năng lưu trữ dữ liệu đã thu thập được. có thể lưu lại các tệp tin pcap và cả dữ liệu thu thập từ các kết nối HTTP.
- Phân Tích Dữ Liệu: NetworkMiner hỗ trợ phân tích nhanh chóng thông qua việc hiển thị các yếu tố quan trọng như địa chỉ IP, cổng, giao thức, và các tệp tin đang được truyền qua mạng.
- Xem Giao Diện Đồ Họa: NetworkMiner cung cấp giao diện đồ họa giúp người dùng xem các thông tin mạng một cách trực quan. có thể xem các biểu đồ và sơ đồ tương tác giữa các máy tính trên mạng.

2.2 Các bước thực hiện

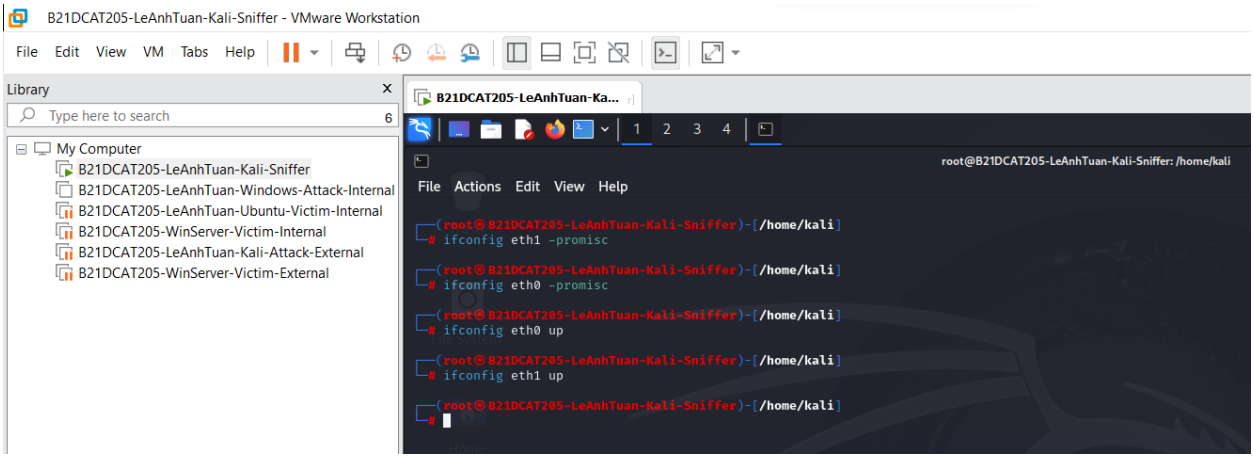
2.2.1 Sử dụng tcpdump

Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống



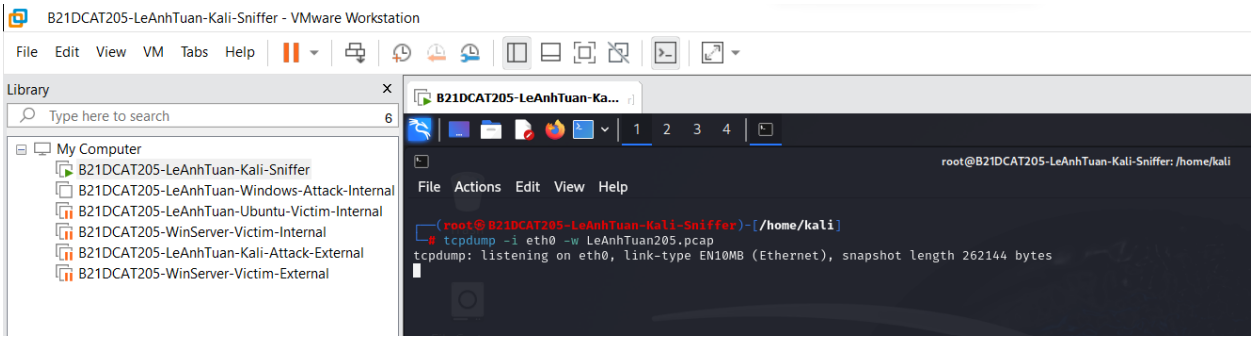
Hình 1: Hai interfaces eth0 và eth1.

Kích hoạt các interfaces (eth0, eth1) hoạt động ở chế độ hỗn hợp



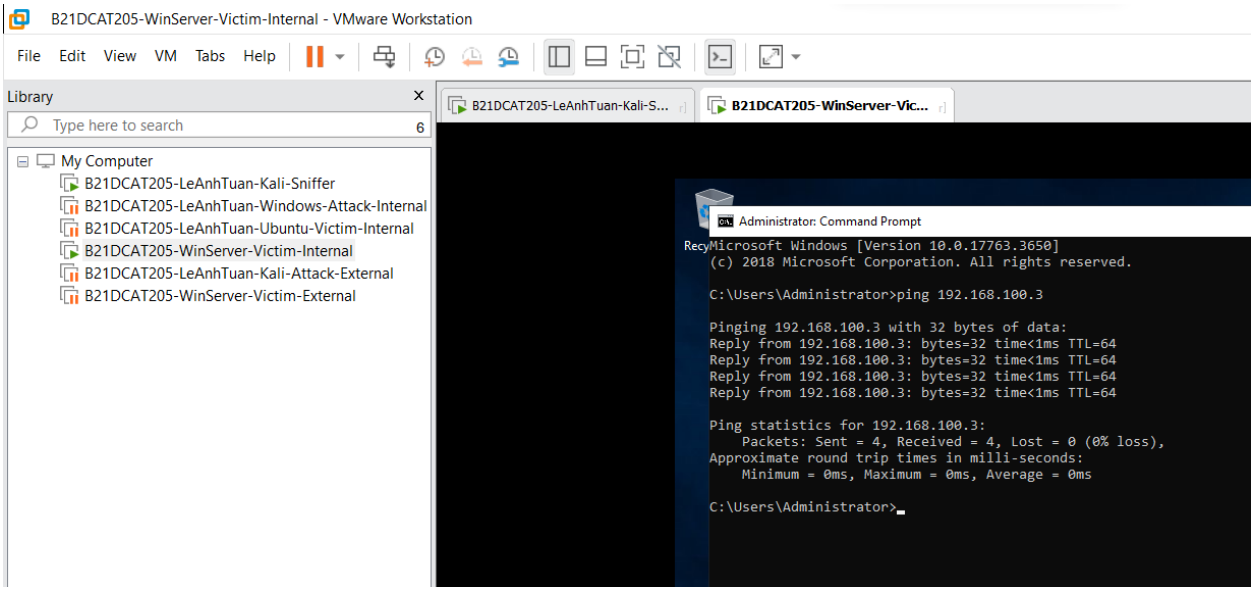
Hình 2: Kích hoạt 2 interfaces

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

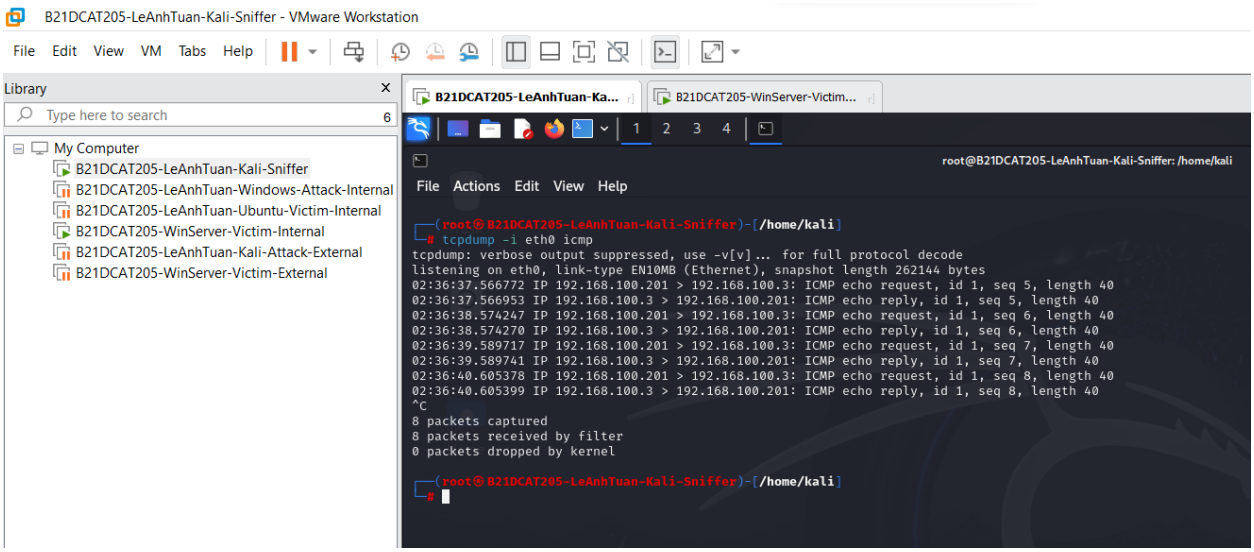


Hình 3: Bắt gói tin trên tcpdump và lưu vào file LeAnhTuan205.

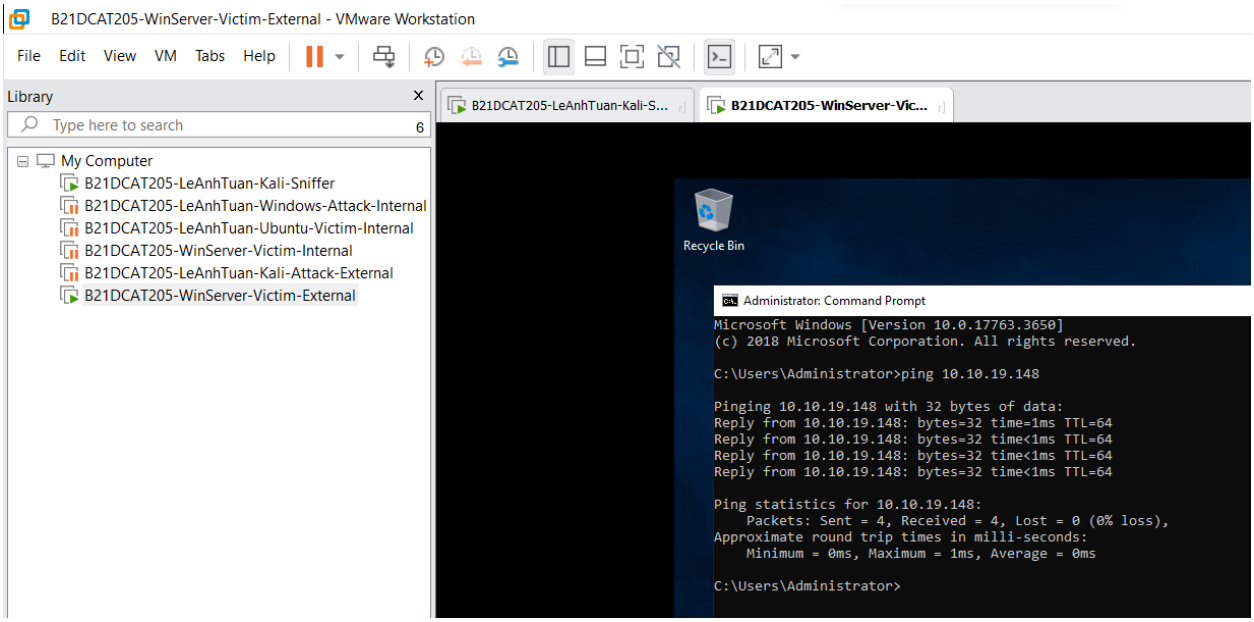
Đăng nhập Window Server 2019 và tiến hành ping đến dải mạng internal và dải mạng external.



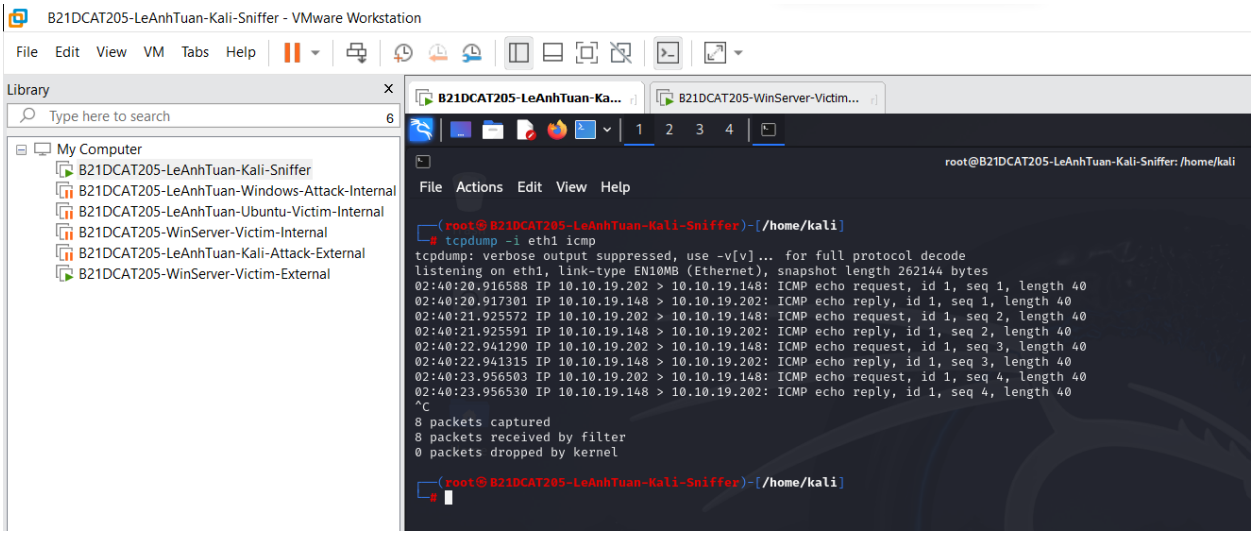
Hình 4: Ping từ máy Windows Server 2019 Victim Internal tới máy Kali Sniffer



Hình 5: Sử dụng tcpdump bắt các gói tin ping tới từ máy WinServer-Victim-Internal

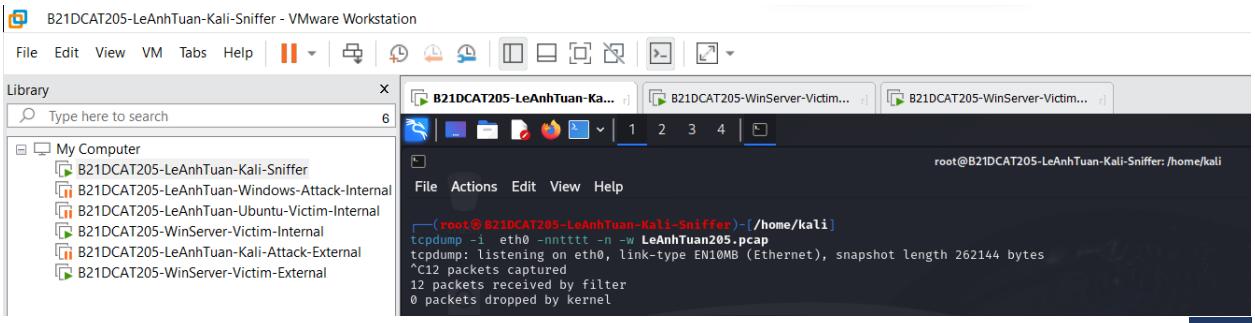


Hình 6: Ping từ máy Windows Server 2019 Victim External tới máy Kali Sniffer

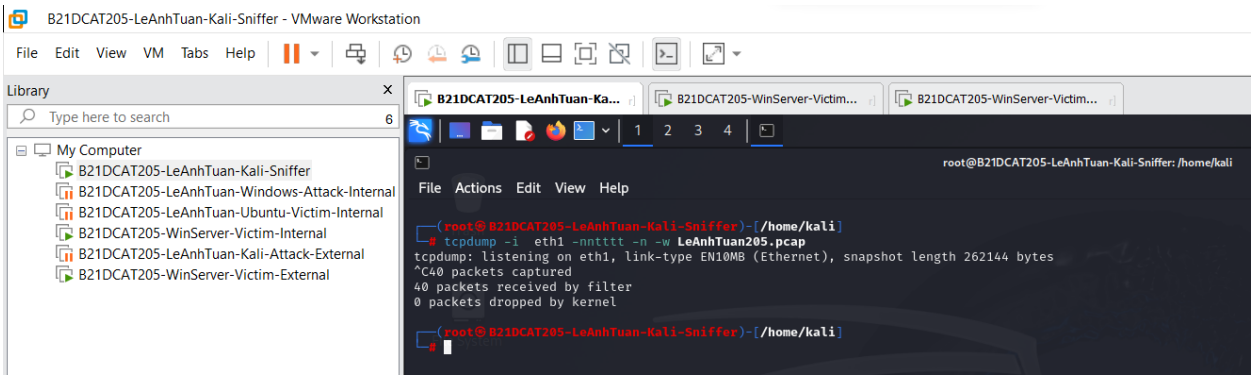


Hình 7: Sử dụng tcpdump bắt các gói tin ping tới từ máy WinServer-Victim-External

Trên máy Linux Sniffer, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.



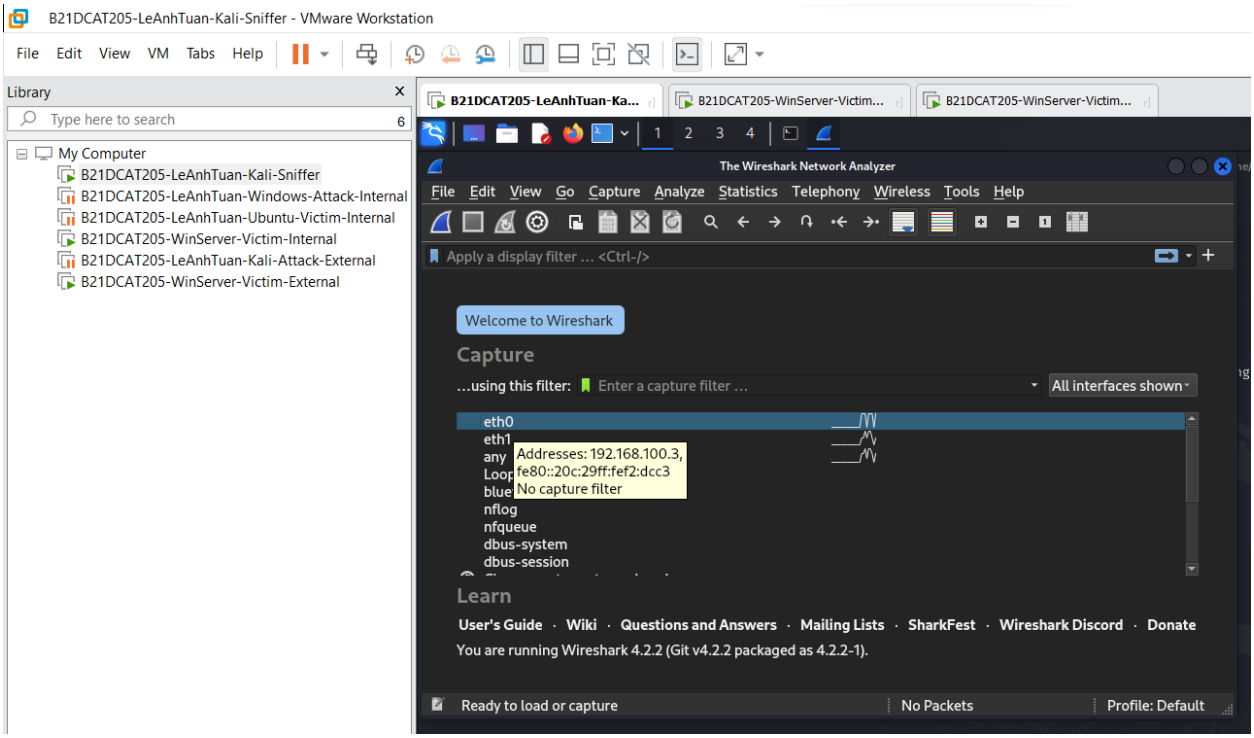
Hình 8: Lưu dữ liệu vào file LeAnhTuan205.pcap từ eth0



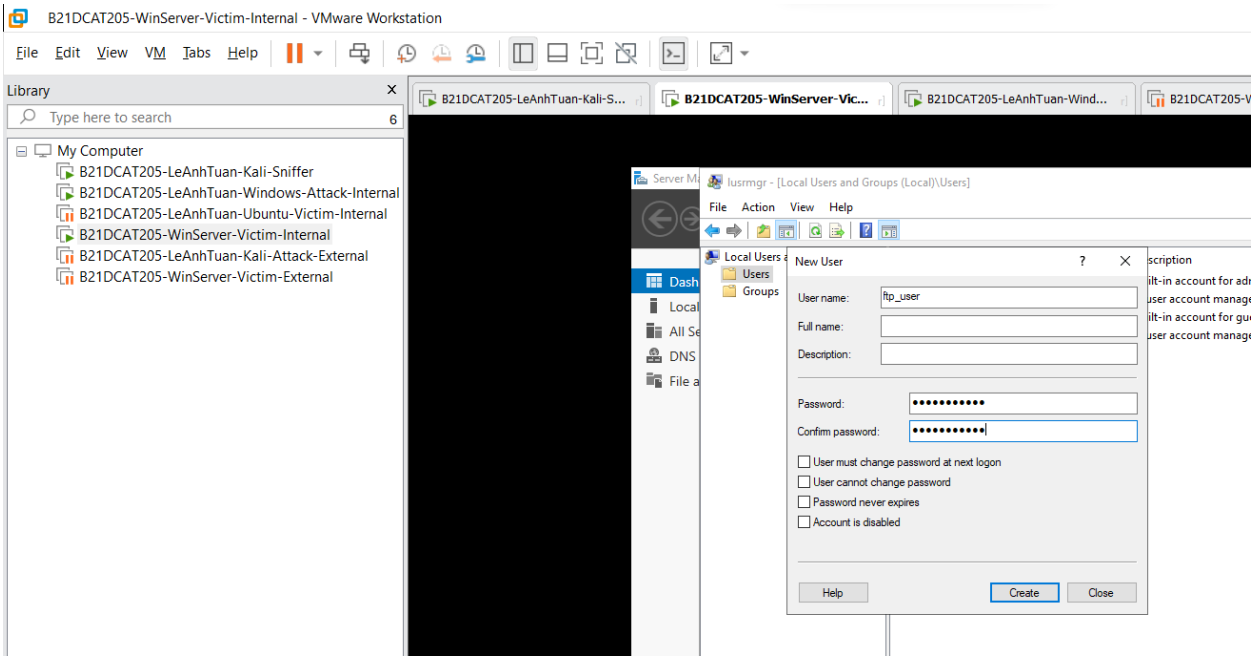
Hình 9: Lưu dữ liệu vào file LeAnhTuan205.pcap từ eth1

2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin

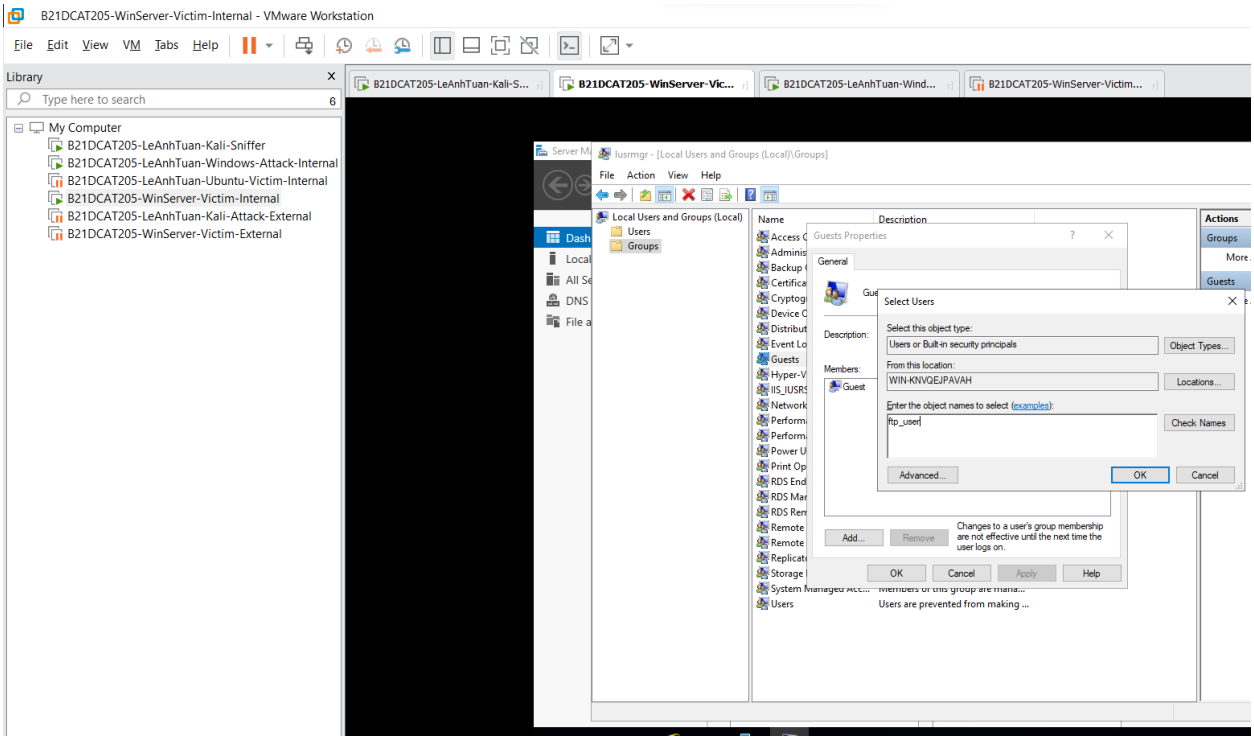
Trên máy **Linux Sniffer**, bật các **interfaces eth0, eth1** và khởi động Wireshark. Trong **Capture Interfaces** chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0.



Hình 10: Chọn eth0 với dải mạng để bắt gói tin trên dải mạng 192.168.100.0

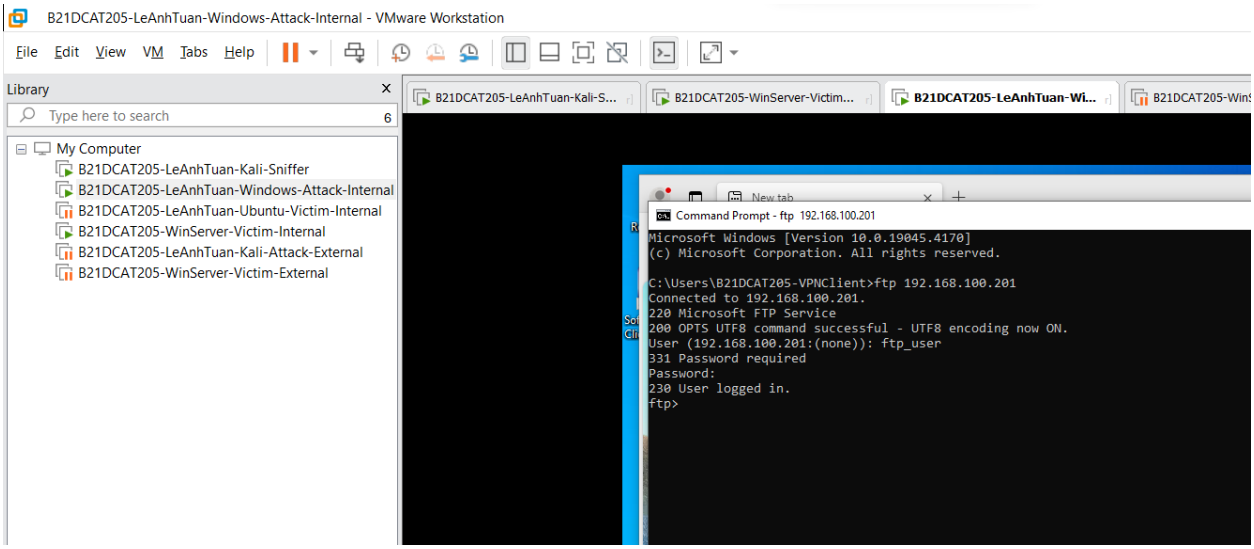


Hình 11: Tạo username ftp_user cho phép ftp



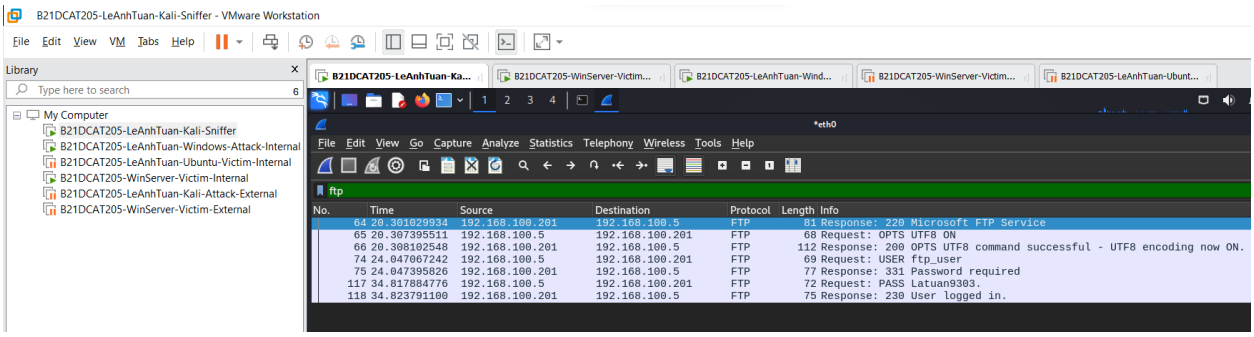
Hình 12: Thêm user ftp_user vào group Guest

Trên máy Windows-Attack-Internal kết nối tới ftp server (C:\ftp 192.168.100.201) trên máy WinServer-Victim-Internal (tắt tường lửa cả 2 máy)

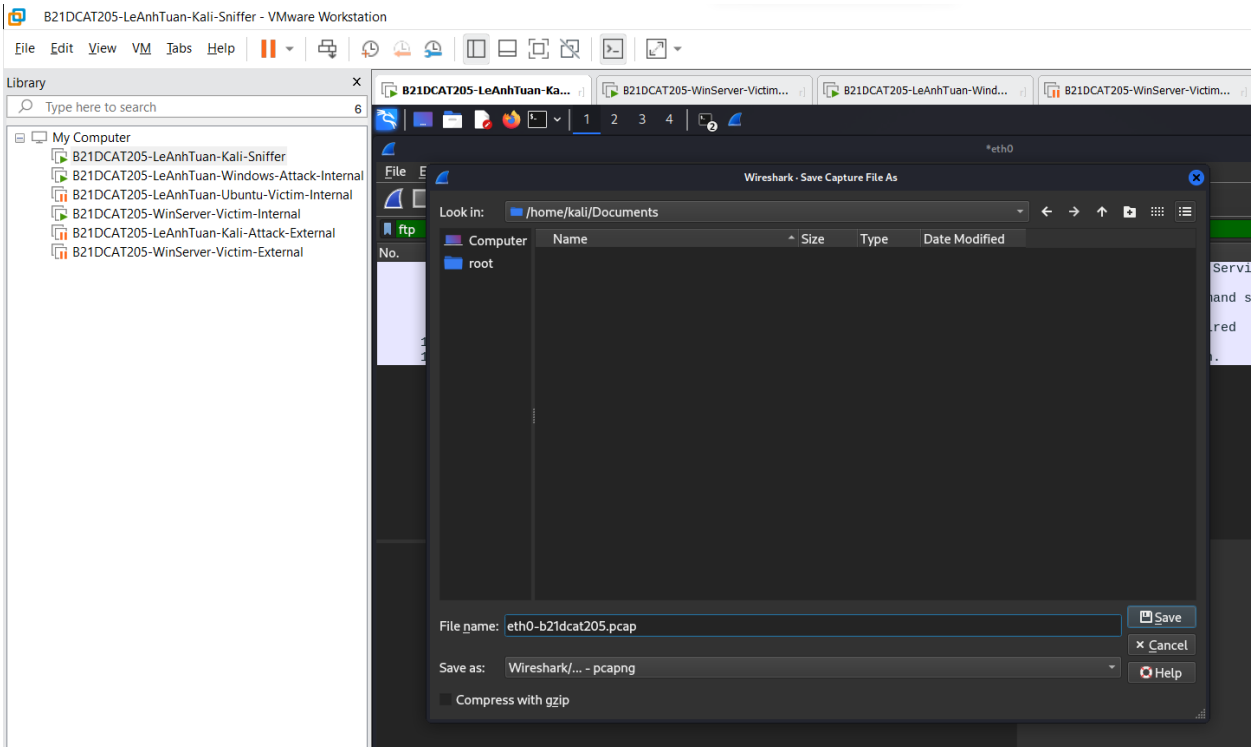


Hình 13: ftp thành công

Trên linux sniffer dừng bắt gói tin và lọc các gói ftp

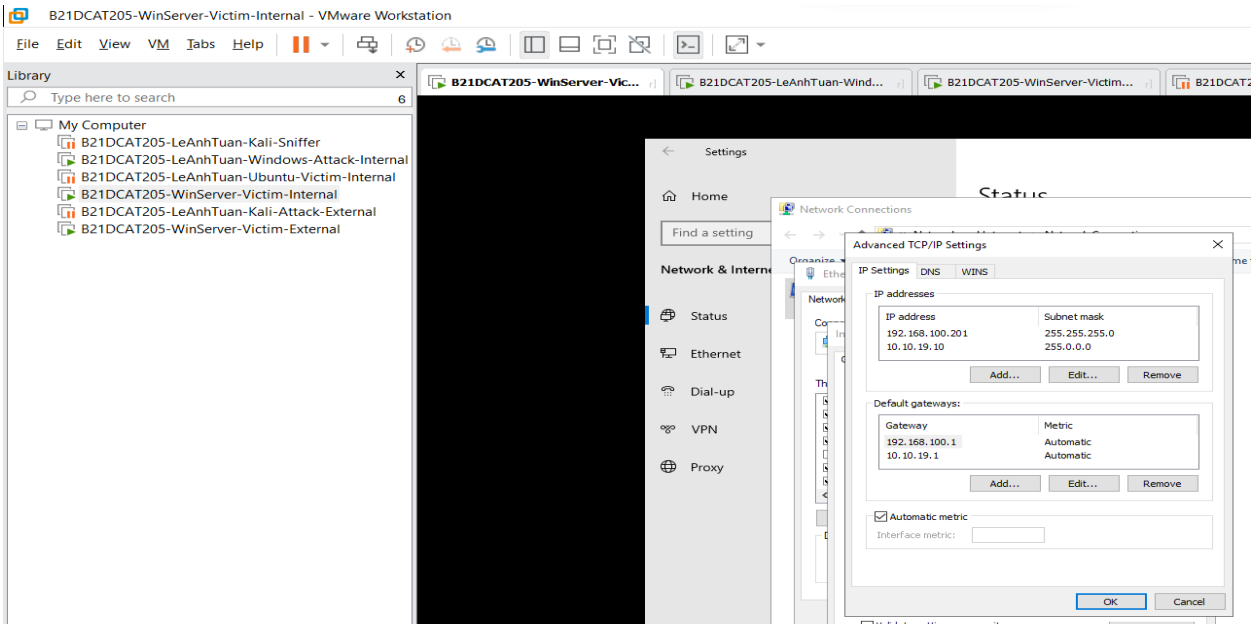


Hình 14: Các gói tin được bắt bởi wireshark từ máy Kali-Sniffer



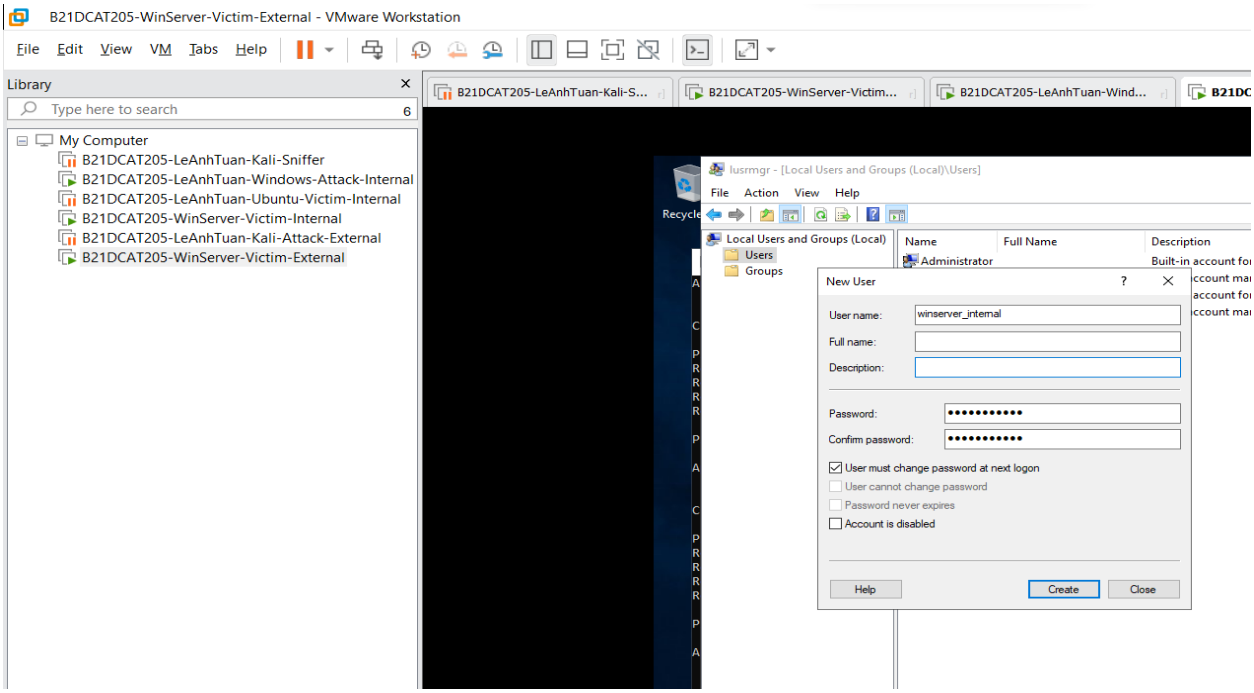
Hình 15: Lưu file eth0-b21dcat205.pcap

Tương tự với việc **ftp 192.168.100.201,** ta sẽ sử dụng **ftp 10.10.19.202** từ máy **WinServer-Victim-Internal với ip 192.168.100.201.**Ta thấy rằng do dải mạng khác nhau nên trên máy **WinServer-Victim-Internal** ta sẽ thêm 1 ipv4 **10.10.19.10.**

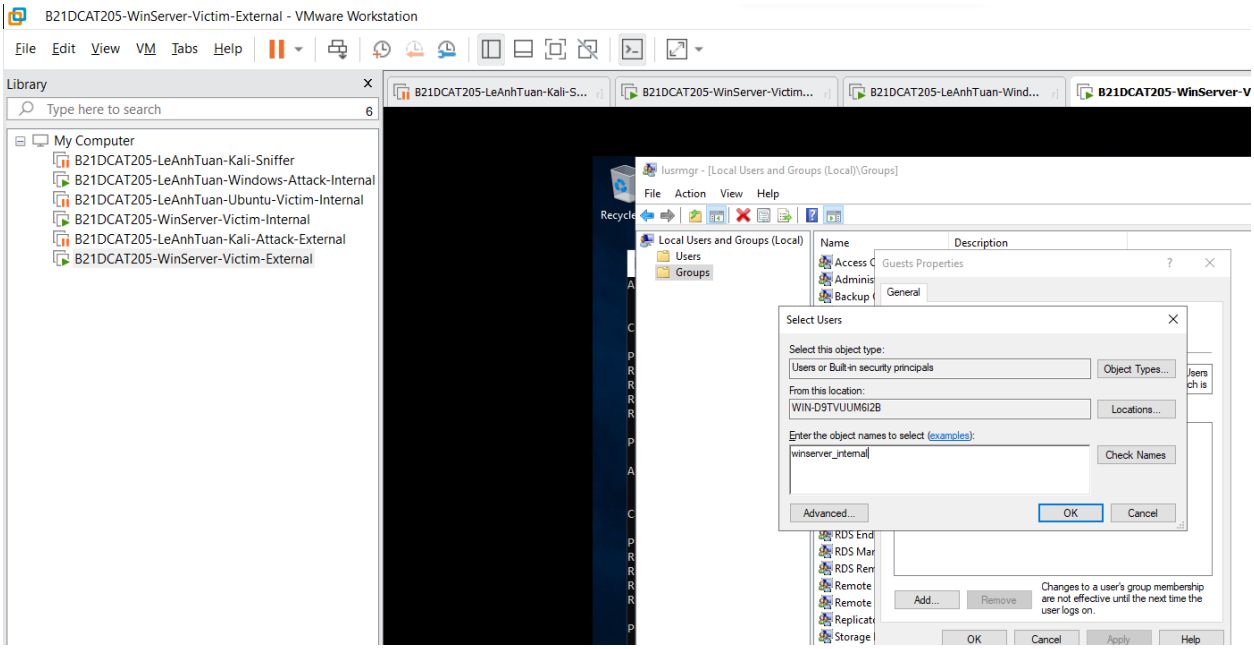


Hình 16: Thêm vào máy WinServer-Victim-Internal với ip 10.10.19.10

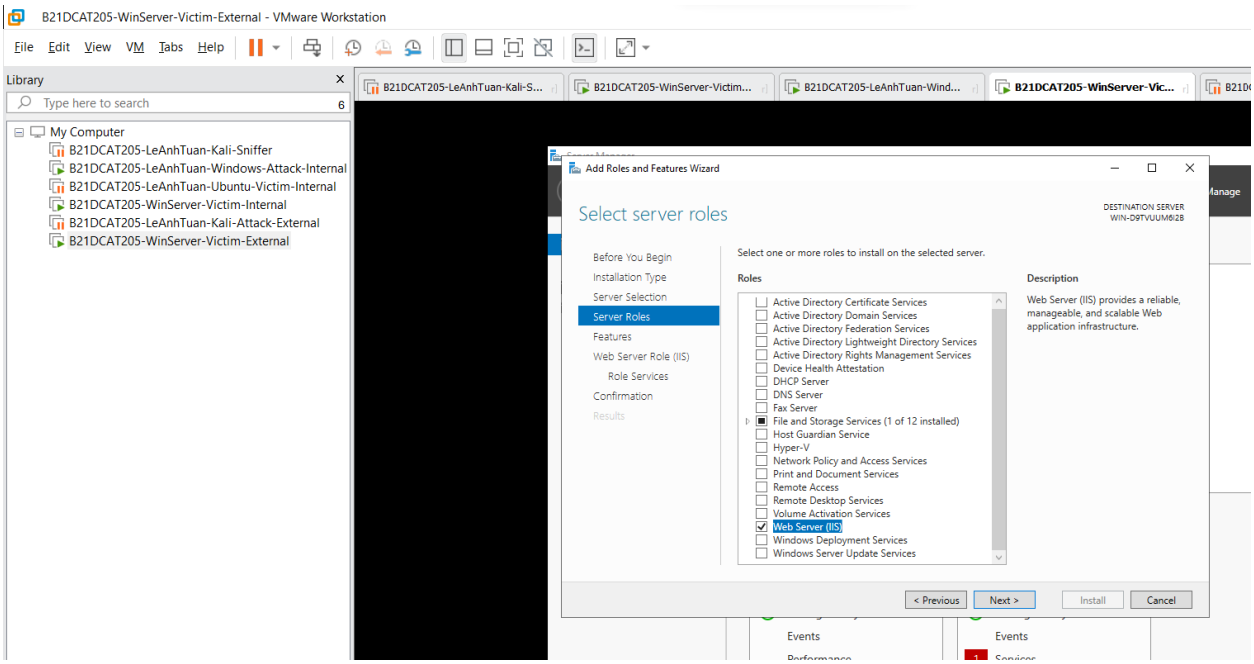
Tại máy **WinServer-Victim-External (10.10.19.202)** thêm user **winserver_external**



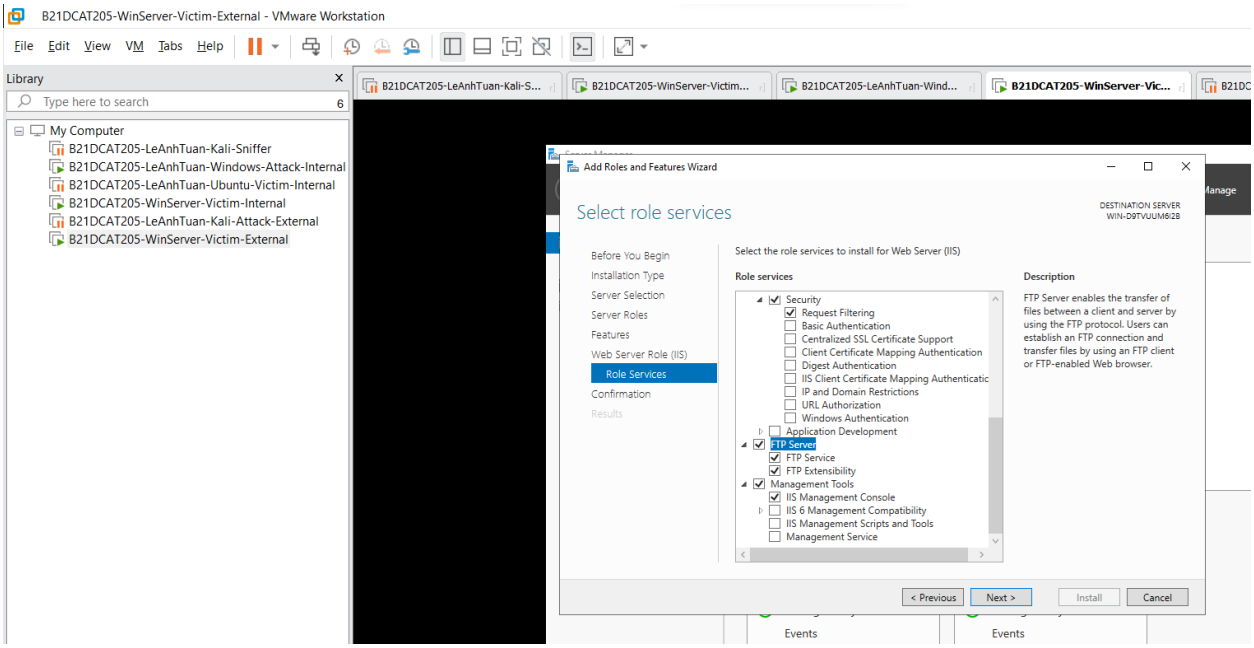
Hình 17: Tại máy WinServer-Victim-External (10.10.19.202)



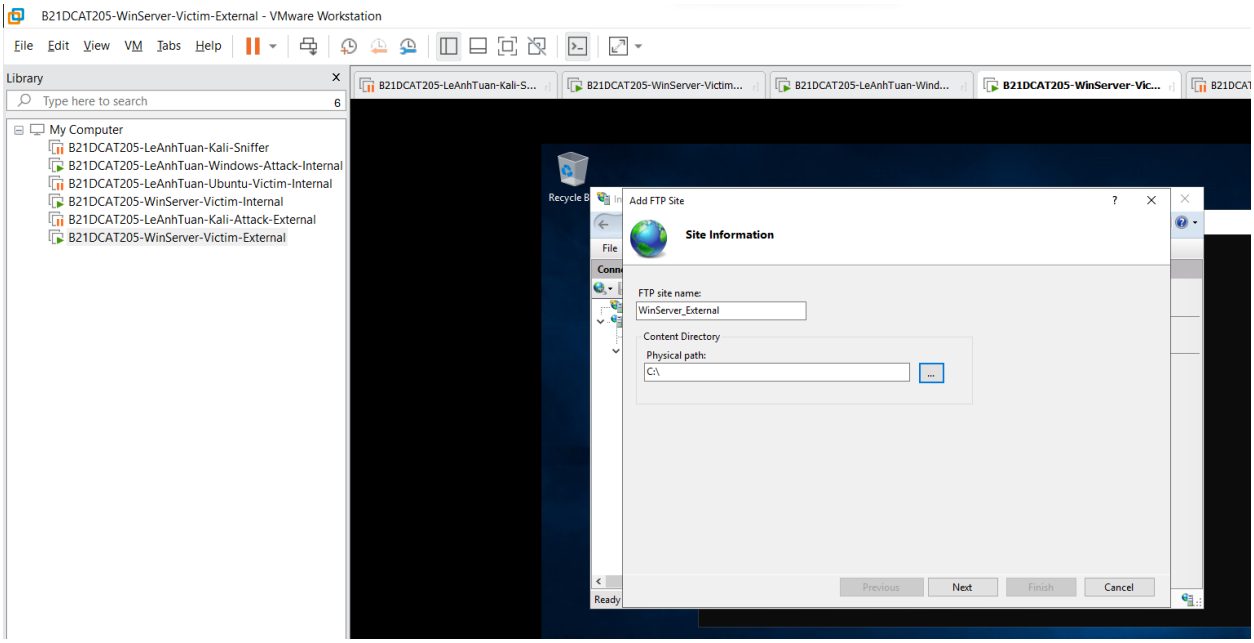
Hình 18: Thêm user winserver_internal vào group Guest



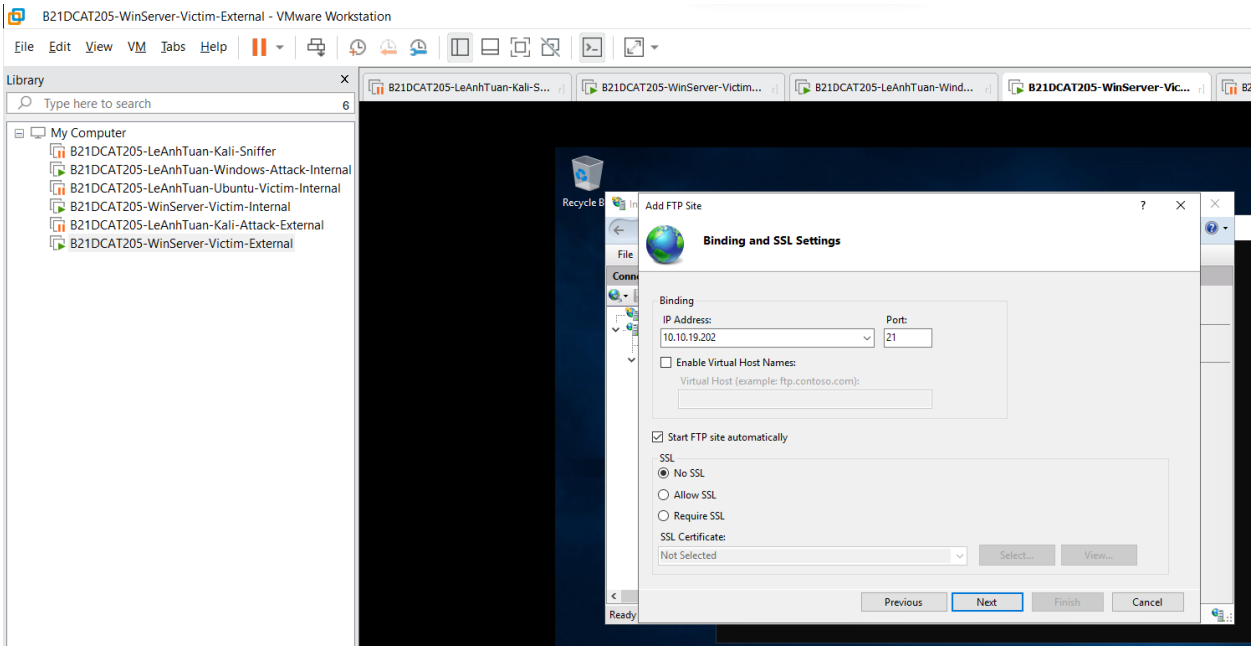
Hình 19: Cài đặt IIS tại WinServer-Victim-External



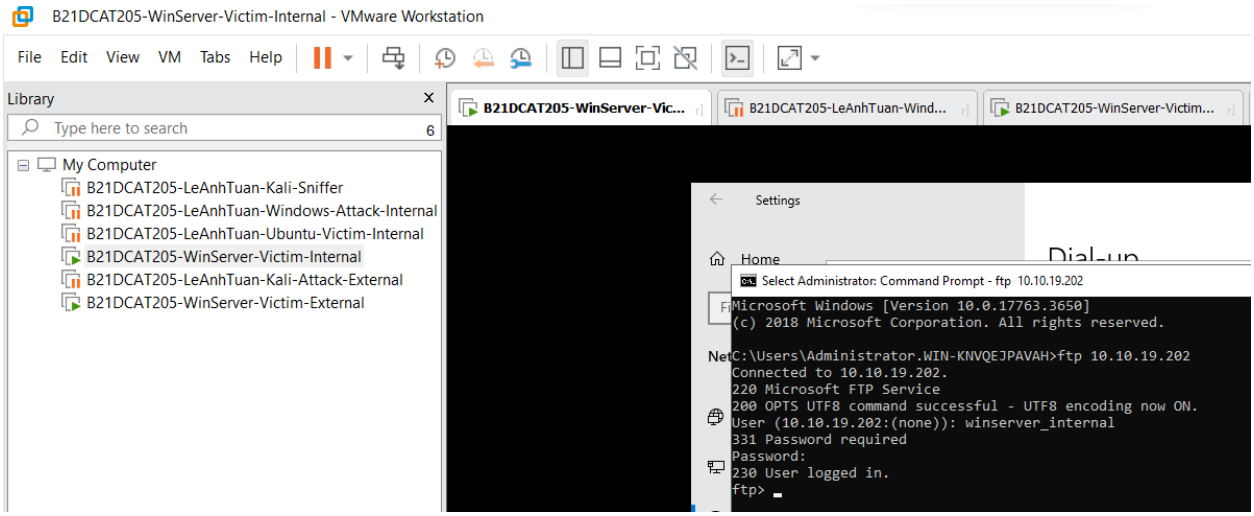
Hình 20: Tại Role Services chọn FTP Server



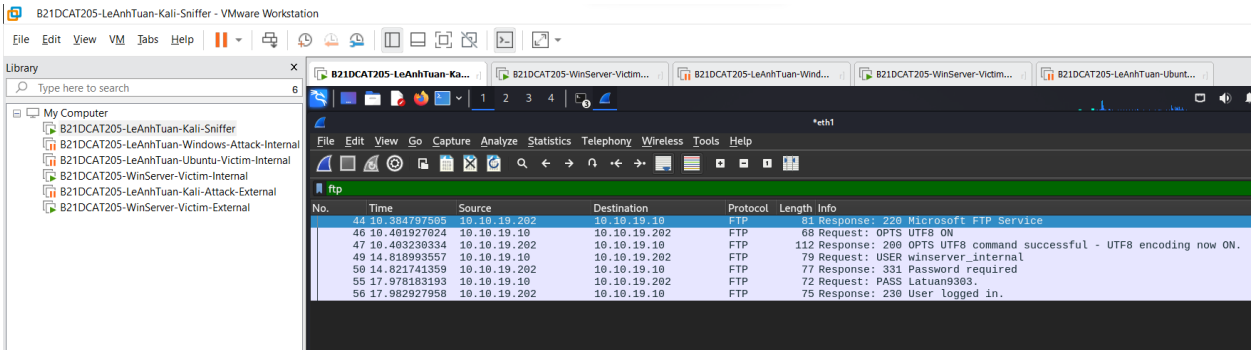
Hình 21: Add FTP Site tại IIS



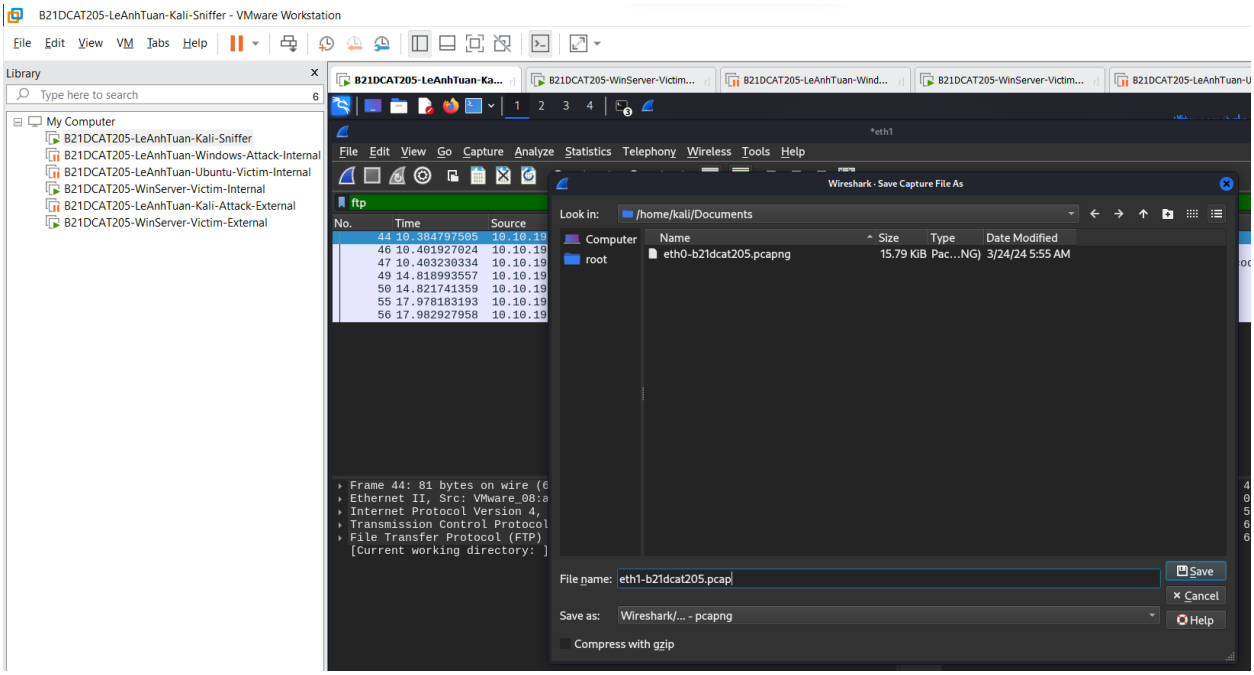
Hình 22: Cấu hình cho phép ftp tới 10.10.19.202



Hình 23: ftp thành công tới máy WinServer-Victim-External



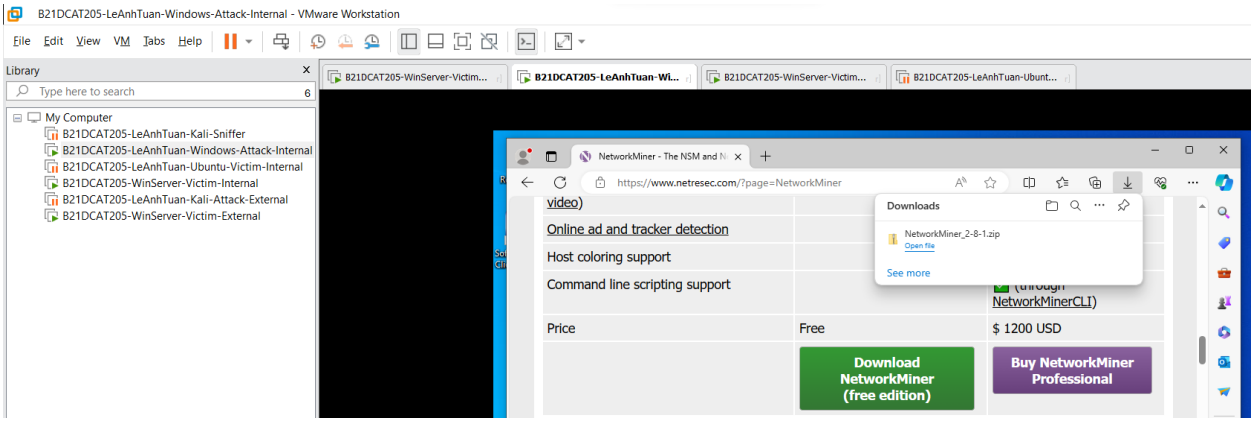
Hình 24: Tại máy Kali-Sniffer bắt được các gói tin.



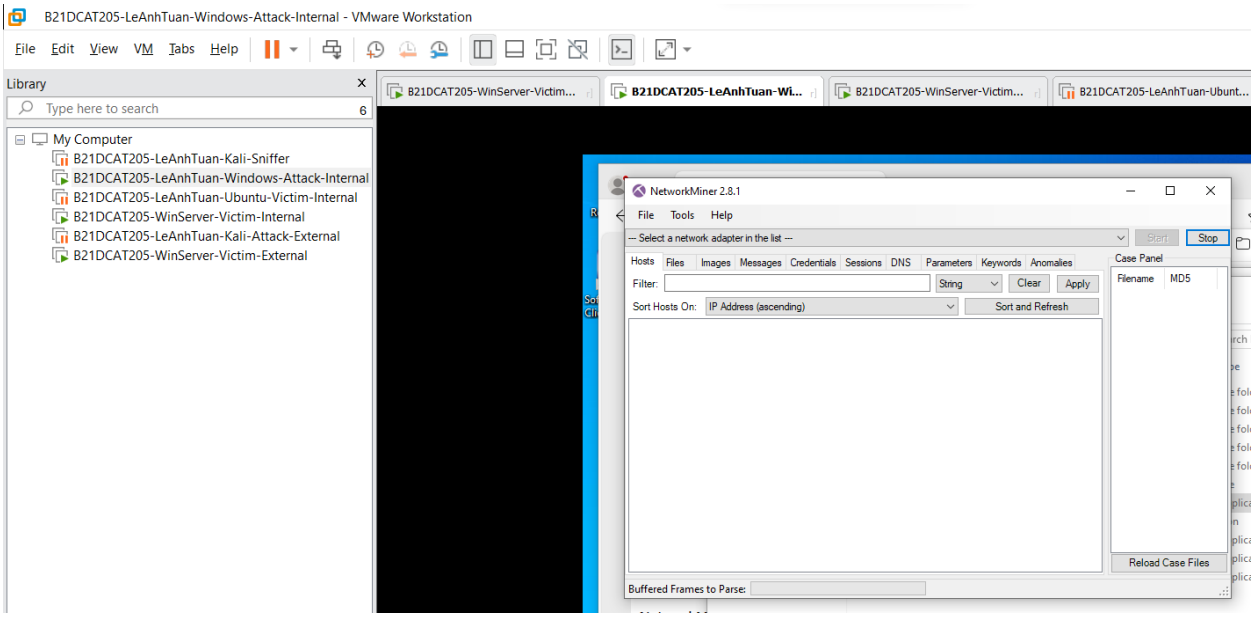
Hình 25: Lưu file eth1-b21dcat205.pcap

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

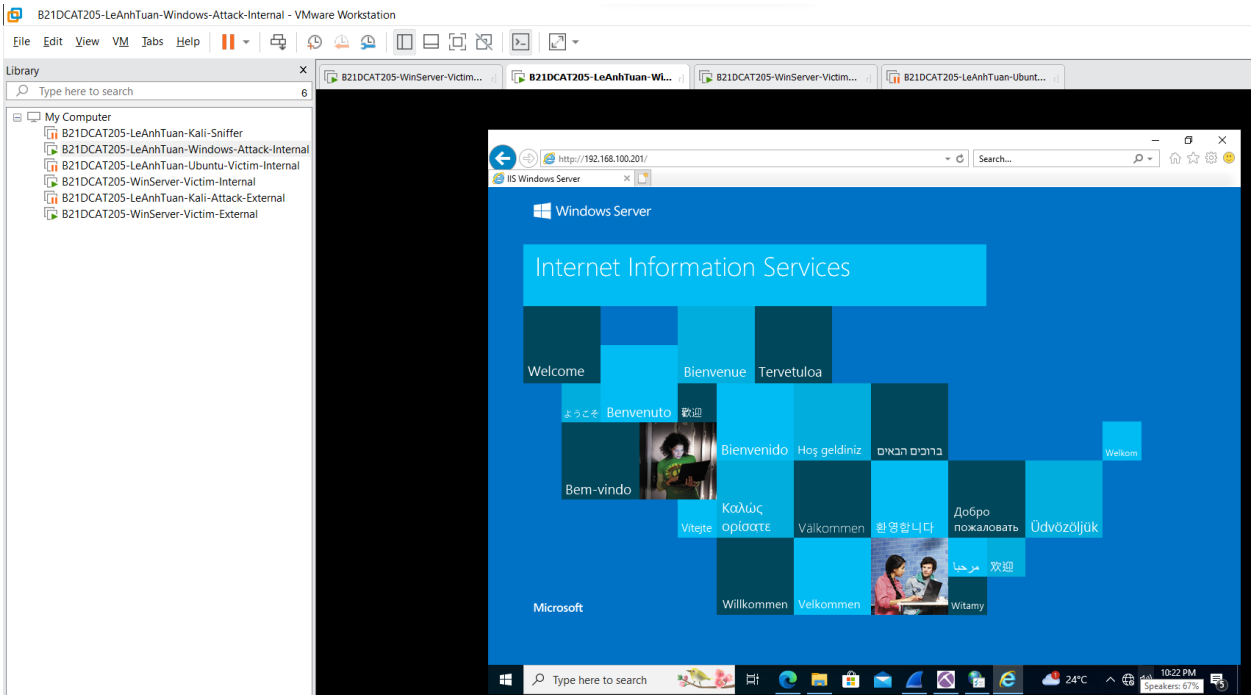
Trên máy **Windows-Attack-Internal** khởi động **Network Miner** và chọn **Socket: Intel® PRO/1000MT Network Connection(192.168.100.5)** và bắt đầu bắt gói tin.



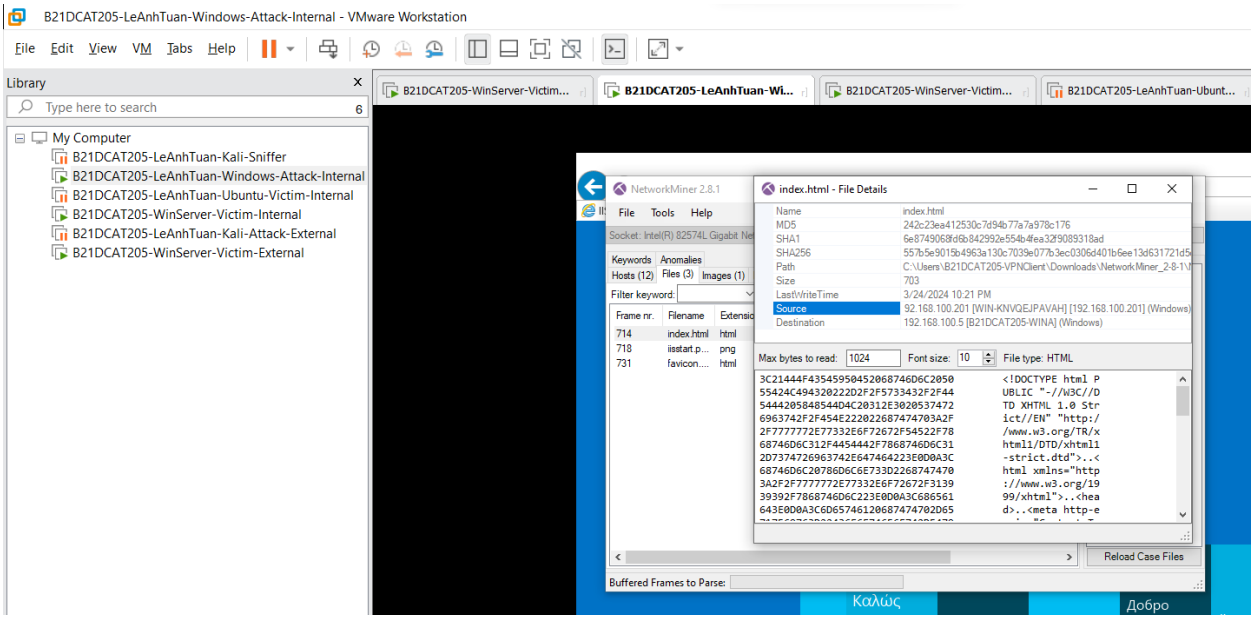
Hình 26: Tải Network Miner



Hình 27: Giao diện Network Miner sau khi cài đặt và giải nén thành công



Hình 28: Kết nối đến trang web của WinServer-Internal-Victim



Hình 29: Nội dung File index.html.

3 Kết luận

- Bắt gói tin và các file pcap thông qua tcpdump thành công
- Sử dụng Wireshark để bắt và lọc ra được các gói tin ftp, các file pcap tương ứng thành công
- Bắt được các dữ liệu trong file index.html thành công.

4 Tài liệu tham khảo

- Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021
- https://www.tcpdump.org/index.html#documentation
- https://www.wireshark.org/docs/wsug_html/
- https://docs.securityonion.net/en/2.3/networkminer.html#