HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 3.1:
Bắt và phân tích gói tin trong mạng

Tên sinh viên: Nguyễn Văn Hùng

Mã sinh viên: B22DCAT136

Nhóm lớp: 09

Giảng viên: TS. Quản Trọng Thế

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 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

1.2 Tìm hiểu lý thuyết

1.2.1 Tổng quan về các công cụ bắt gói tin mạng

Các công cụ bắt gói tin mạng (packet sniffers) là phần mềm cho phép ghi lại và phân tích lưu lượng mạng đi qua một giao diện mạng cụ thể. Chúng thường được sử dụng để:

- Phân tích sự cố mạng
- Gỡ lỗi ứng dụng mạng
- Phát hiện các hoạt động đáng ngờ
- Học tập và nghiên cứu giao thức mạng

Tuy nhiên, các công cụ này cũng thường xuyên bị lạm dụng bởi hacker cho mục đích sai trái như theo dõi, nghe trộm, đánh cắp thông tin bảo mật người dùng.

Có 3 loại Sniffer chính:

- Sniffer mạng: Quan sát tất cả hoạt động trên một mạng cục bộ hoặc kết nối internet. Giúp phân tích lưu lượng, lưu trữ dữ liệu, xác định vấn đề về hiệu suất và bảo mật mạng.
- Sniffer giao thức: Theo dõi các giao thức cụ thể như HTTP, FTP, SMTP để phát hiện sự cố kết nối, lỗi ứng dụng.
- Sniffer TCP/IP: Bắt và phân tích các gói tin TCP/IP để xử lý sự cố mạng và bảo mật.

1.2.2 Công cụ tcpdump

TCPDump cho phép người dùng bắt gói tin từ mạng bằng cách lắng nghe trên một giao diện mạng cụ thể.

Các tính năng chính:

- Khi bắt được gói tin, TCPDump hiển thị chúng trực tiếp trên màn hình dòng lệnh. Gói tin được hiển thị theo định dạng đọc được, cho phép người sử dụng xem thông tin như địa chỉ nguồn/đích, loại giao thức, dữ liệu, và nhiều thông số khác.

- TCPDump hỗ trợ nhiều loại giao thức mạng, có thể lọc gói tin theo nhiều tiêu chí khác nhau, đồng thời nó cũng nhẹ và hiệu quả, có thể chạy được trên các hệ thống tài nguyên thấp.

Cách hoạt động:

- TCPDump hoạt động bằng cách đặt card mạng vào chế độ promiscuous mode để bắt tất cả lưu lượng mạng
- Nó phân tích các gói tin ở lớp liên kết dữ liệu (Data Link Layer)
- Có thể lưu kết quả bắt được vào file pcap để phân tích sau

Cú pháp cơ bản của tcpdump: *tcpdump [options] [filter expression]*

1.2.3 Công cụ Wireshark

Wireshark được phát triển dưới dạng phần mềm mã nguồn mở, cung cấp khả năng theo dõi, ghi lại, và phân tích gói tin dữ liệu truyền qua mạng. Đây là một công cụ quan trọng trong lĩnh vực mạng máy tính, được sử dụng rộng rãi cho nhiều mục đích như kiểm thử bảo mật, giám sát mạng, và phân tích giao thức.

Các tính năng chính:

- Wireshark hỗ trợ giao diện đồ họa (GUI) thân thiện với người dùng
- Wireshark có khả năng theo dõi và hiển thị gói tin mạng trong thời gian thực
- Sở hữu khả năng lọc và tìm kiếm gói tin mạnh mẽ
- Cung cấp khả năng phân tích sâu nhiều loại giao thức mạng khác nhau và khả năng phân tích chi tiết giao thức của từng gói tin
- Có khả năng phân tích thống kê lưu lượng mạng hiệu quả

Cách hoạt động:

- Wireshark sử dụng thư viện pcap để bắt gói tin
- Phân tích gói tin từ lớp liên kết dữ liệu lên đến lớp ứng dụng
- Cung cấp khả năng giải mã nhiều giao thức mã hóa (nếu có key)
- Cho phép lưu và mở lại các file bắt gói để phân tích sau

Ngoài ra, Wireshark sở hữu một số tính năng nổi bật khác như: hiển thị phân cấp các lớp giao thức của từng gói tin, khả năng theo dõi các luồng (stream) TCP, UDP, ...

1.2.4 Công cụ Network Miner

NetworkMiner là công cụ giám sát mạng, mã nguồn mở dành cho hệ điều hành Window. Công cụ này cũng được hỗ trợ để cài đặt trên Linux, Mac OS X và FreeBSD.

Các tính năng chính:

- Network Miner là công cụ phân tích mạng thụ động (passive) , tập trung vào trích xuất file và dữ liệu từ lưu lượng mạng.

- Phát hiện host, hệ điều hành và session
- Hỗ trợ tái tạo lại các file được truyền qua mạng
- Sử dụng giao diện GUI dễ sử dụng

Cách hoạt động:

- Phân loại và trích xuất file từ lưu lượng mạng
- Hiển thị thông tin credentials (nếu có) từ các phiên đăng nhập
- Phát hiện hệ điều hành của các host trong mạng
- Tổng hợp thông tin về các host và dịch vụ đang chạy

1.3 Kết chương

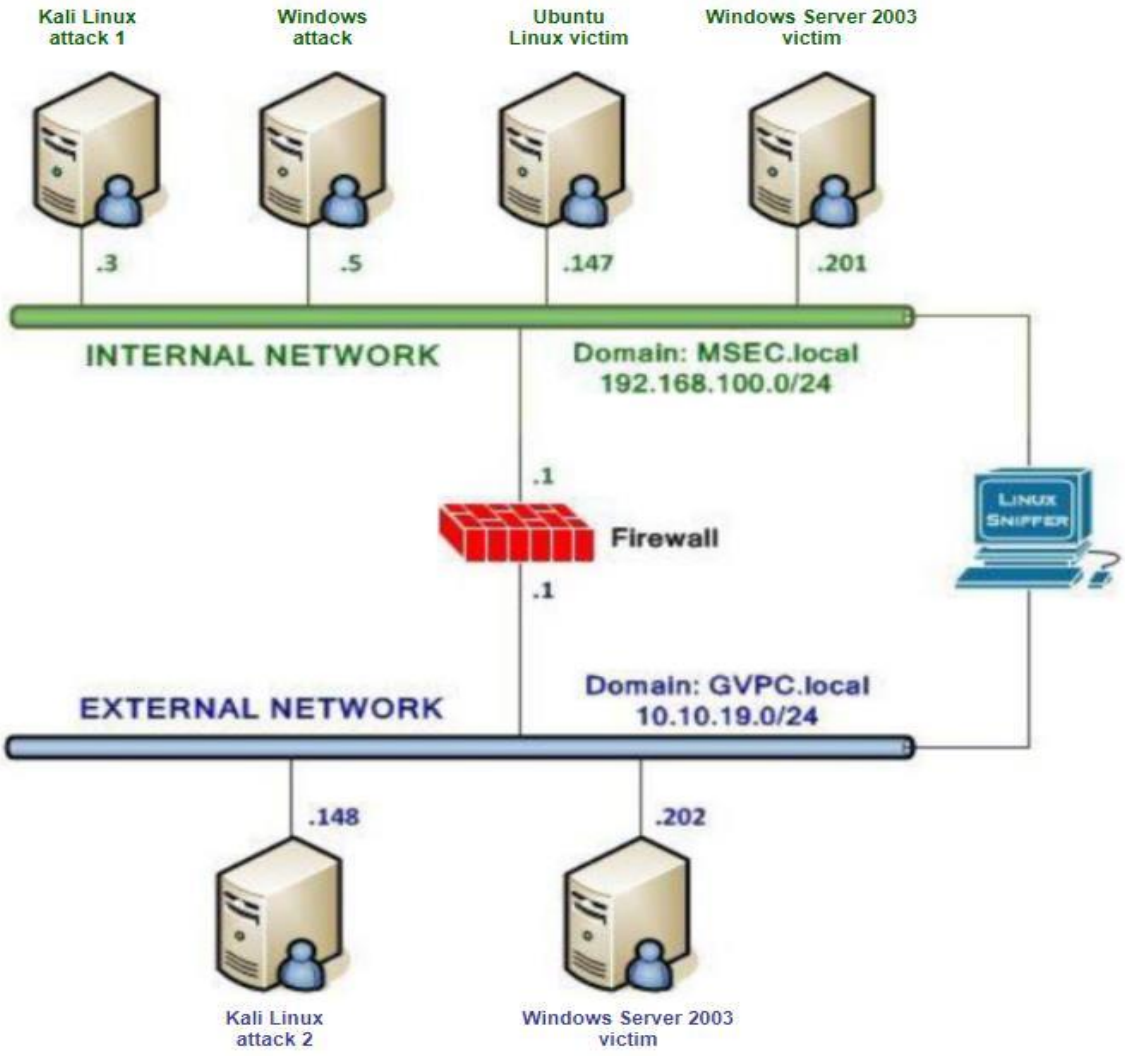
Các công cụ theo dõi và phân tích lưu lượng mạng được sử dụng để phát hiện ra lỗi về hệ thống mạng máy tính hoặc các vấn đề liên quan. Tuy nhiên, nó cũng thường xuyên bị lạm dụng bởi hacker cho các mục đích sai trái như theo dõi, nghe trộm và đánh cắp thông tin bảo mật trái phép. Việc hiểu rõ nguyên lý hoạt động và cách sử dụng các công cụ này là nền tảng quan trọng cho sinh viên tìm hiểu về an toàn thông tin.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation(hoặc các phần mềm hỗ trợ ảo hóa khác).
- Các file máy ảo VMware và hệ thống mạng đã cài đặt trong bài thực hành 5 trước đó: máy trạm, máy Kali Linux, máy chủ Windows và Linux.

  Chú ý: chỉ cần bật các máy cần sử dụng trong bài lab.
- Topo mạng như đã cấu hình:



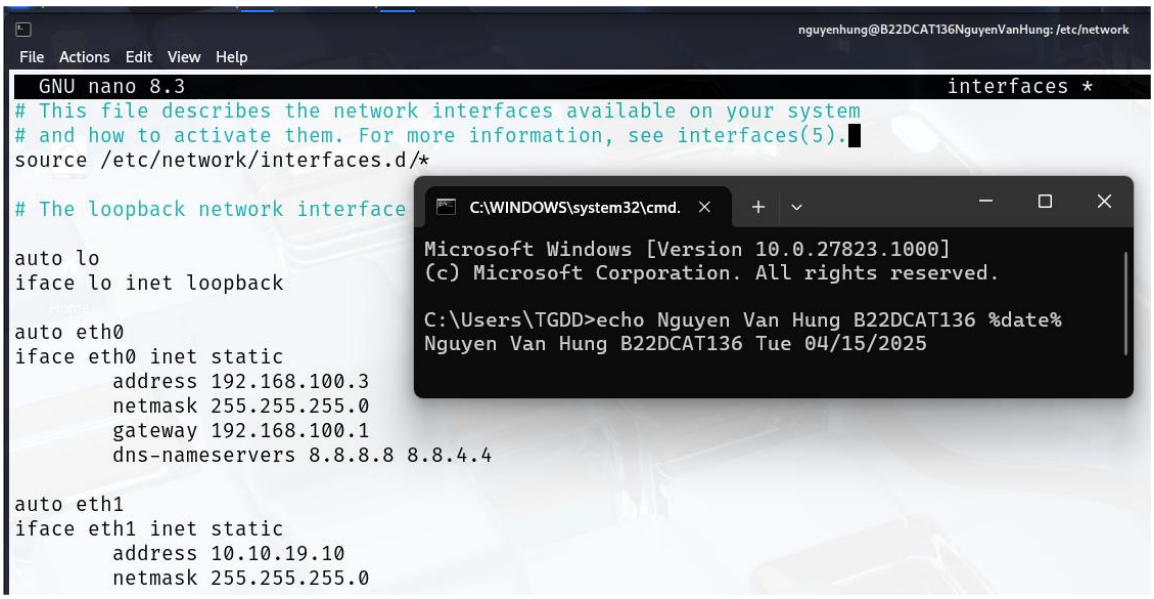
Hình 1. Topo mạng cần chuẩn bị

2.2 Các bước thực hiện

2.2.1 Sử dụng tcpdump

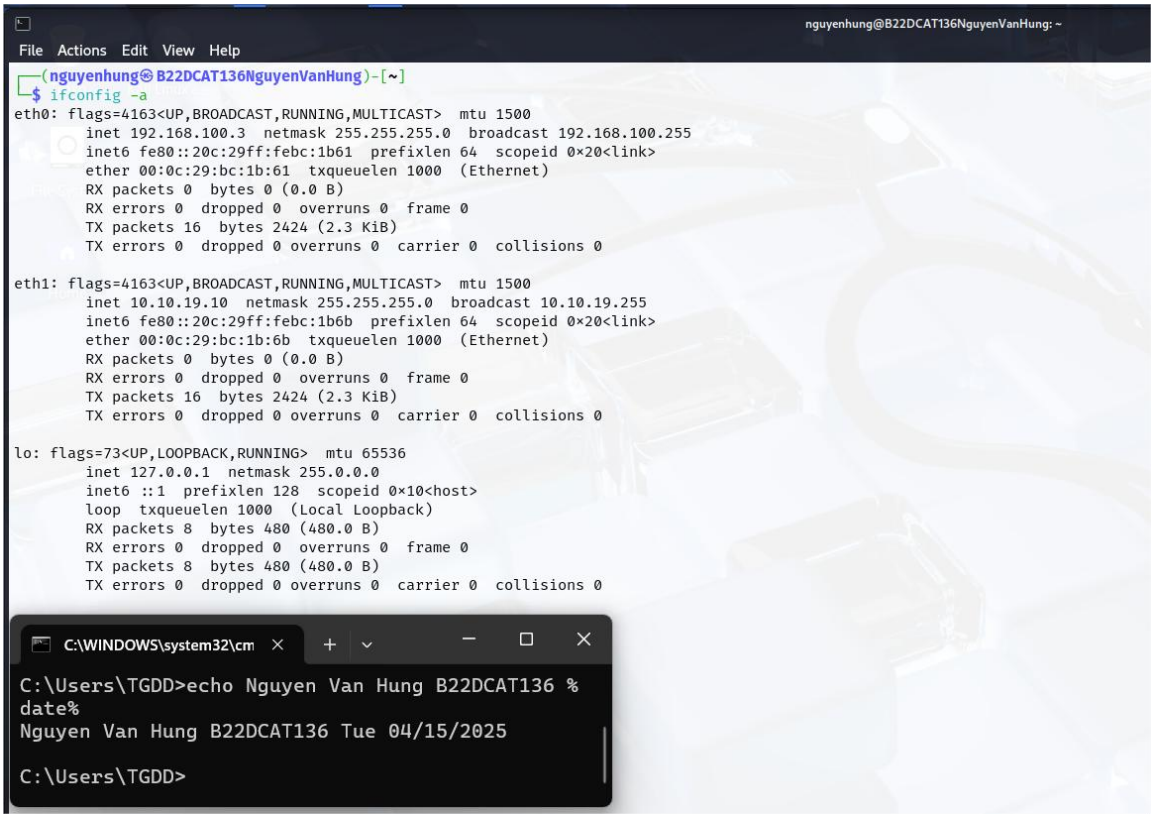
Sử dụng máy Kali Linux Attack Internal để làm máy Linux Sniffer, thêm card mạng External và cấu hình IP External để máy có hai card mạng Internal và External trong file /etc/network/interfaces:

sudo nano /etc/network/interfaces



Hình 2. Cấu hình IP máy Linux Sniffer

Trong máy Linux Sniffer, xem tất cả các interfaces trong hệ thống: *ifconfig -a*

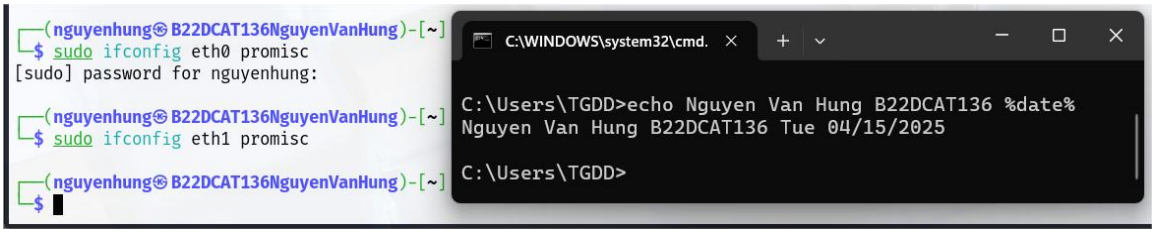


Hình 3. Xem Interfaces trong hệ thống

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

sudo ifconfig eth0 promisc

sudo ifconfig eth1 promisc

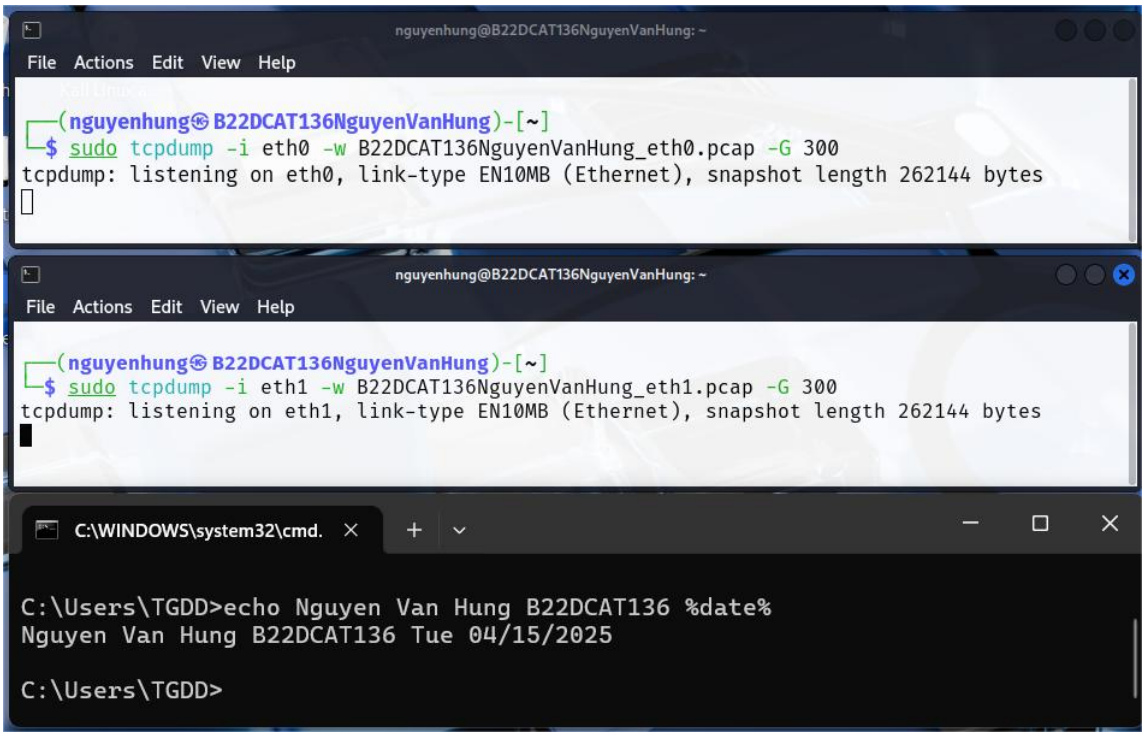


Hình 4. Kích hoạt các interfaces hoạt động ở chế độ hỗn hợp

Khởi động tcpdump, bắt gói tin trên dải mạng 192.168.100.0/24 và 10.10.19.0/24 sau đó gửi vào một file (thời gian chờ dữ liệu trong khoảng 5 phút):

sudo tcpdump -i eth0 -w B22DCAT136NguyenVanHung_eth0.pcap -G 300

sudo tcpdump -i eth0 -w B22DCAT136NguyenVanHung_eth1.pcap -G 300



Hình 5. Bắt gói tin trong dải mạng

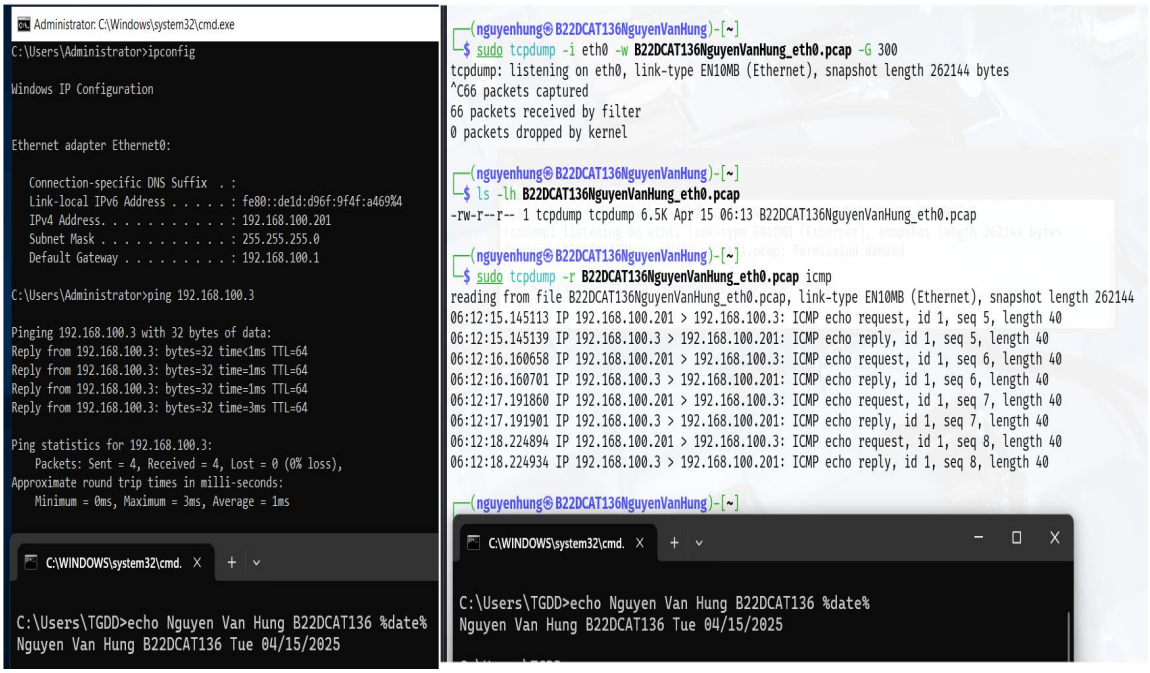
Từ máy Windows Server 2019 ping đến dải mạng Internal: *ping 192.168.100.201*

Từ máy Kali Linux Sniffer tiến hành bắt gói tin bằng tcpdump và lưu dữ liệu vào file pcap. Dừng tcpdump (Ctrl+C) và kiểm tra file B22DCAT136NguyenVanHung_eth0.pcap:

ls -lh B22DCAT136NguyenVanHung_eth0.pcap

Lọc gói tin ICMP:

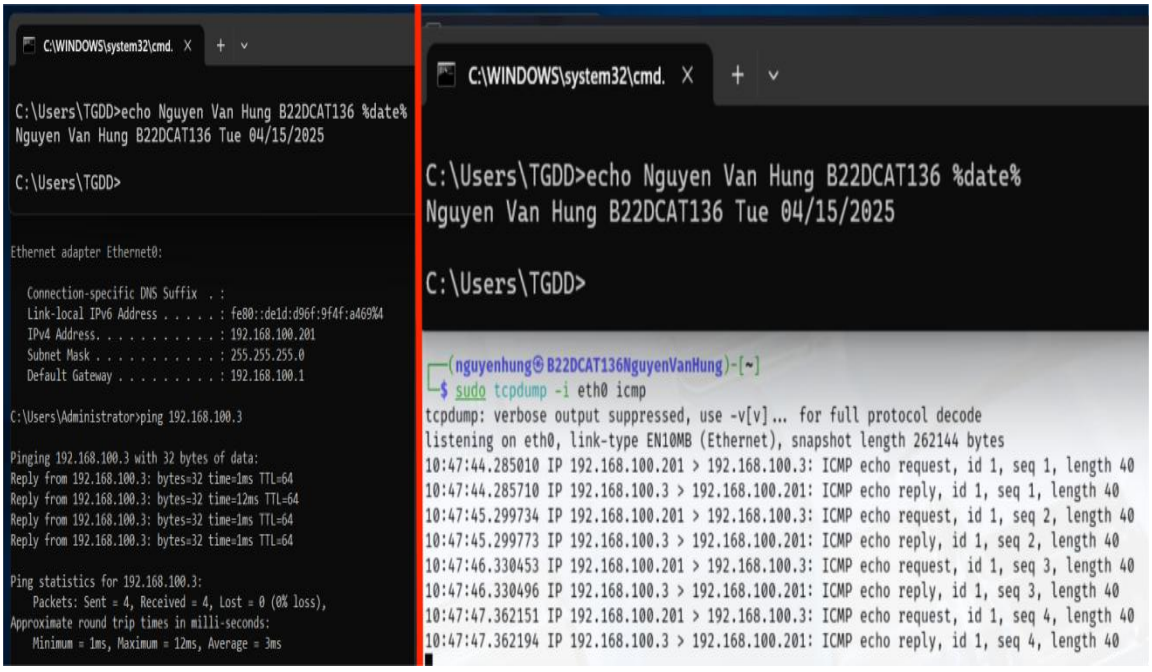
sudo tcpdump -r B22DCAT136NguyenVanHung_eth0.pcap icmp



Hình 6. Ping đến dải mạng Internal, bắt gói tin bằng tcpdump và lưu vào file pcap

Bắt các gói tin trên giao diện mạng eth0:

sudo tcpdump -i eth0 icmp



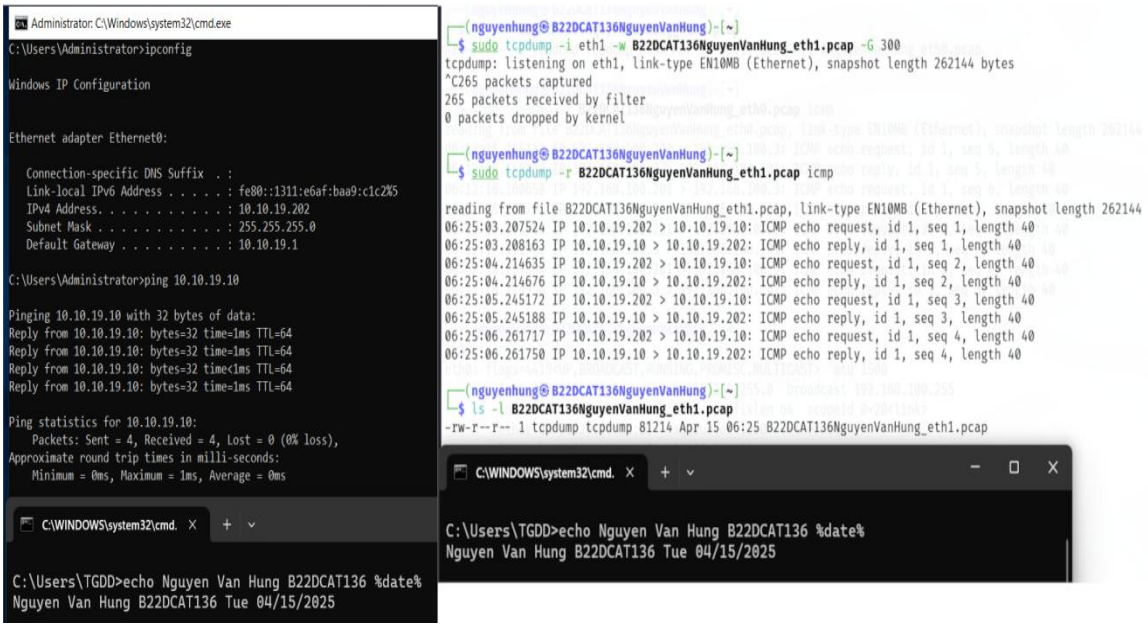
Hình 7. Bắt và hiển thị các gói tin icmp trên giao diện mạng eth0

Tương tự với dải mạng External:

ping 10.10.19.10

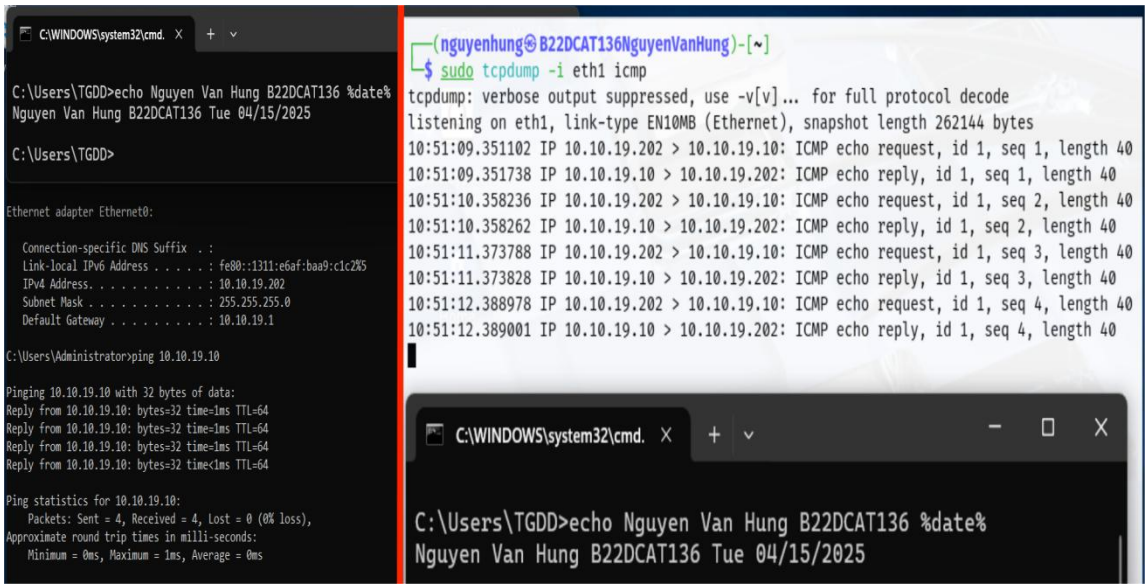
ls -l B22DCAT136NguyenVanHung_eth1.pcap

sudo tcpdump -r B22DCAT136NguyenVanHung_eth1.pcap icmp



Hình 8.Ping đến dải mạng External, bắt gói tin bằng tcpdump và lưu vào file pcap

sudo tcpdump -i eth0 icmp

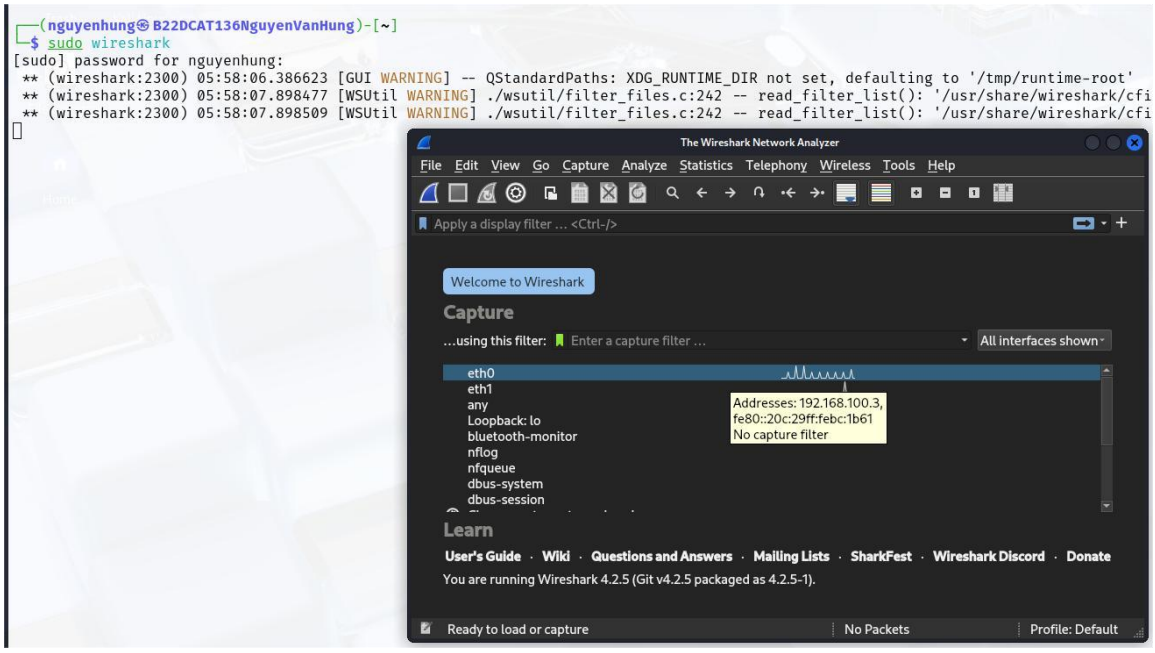


Hình 9. Bắt và hiển thị các gói tin icmp trên giao diện mạng eth1

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

Đăng nhập Linux Sniffer và khởi động Wireshark dưới quyền Administrator:

sudo wireshark

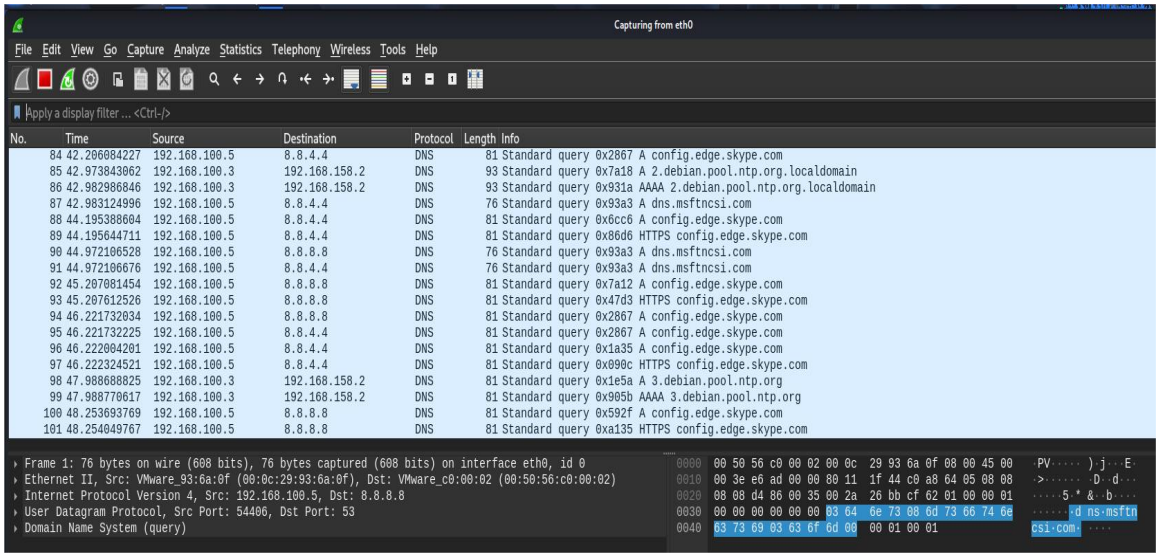


Hình 10. Giao diện Wireshark

Trong giao diện Wireshark:

- interfaces eth0: dải mạng 192.168.100.0
- interfaces eth1: dải mạng 10.10.19.0

Chọn eth0 để bắt đầu bắt gói tin:

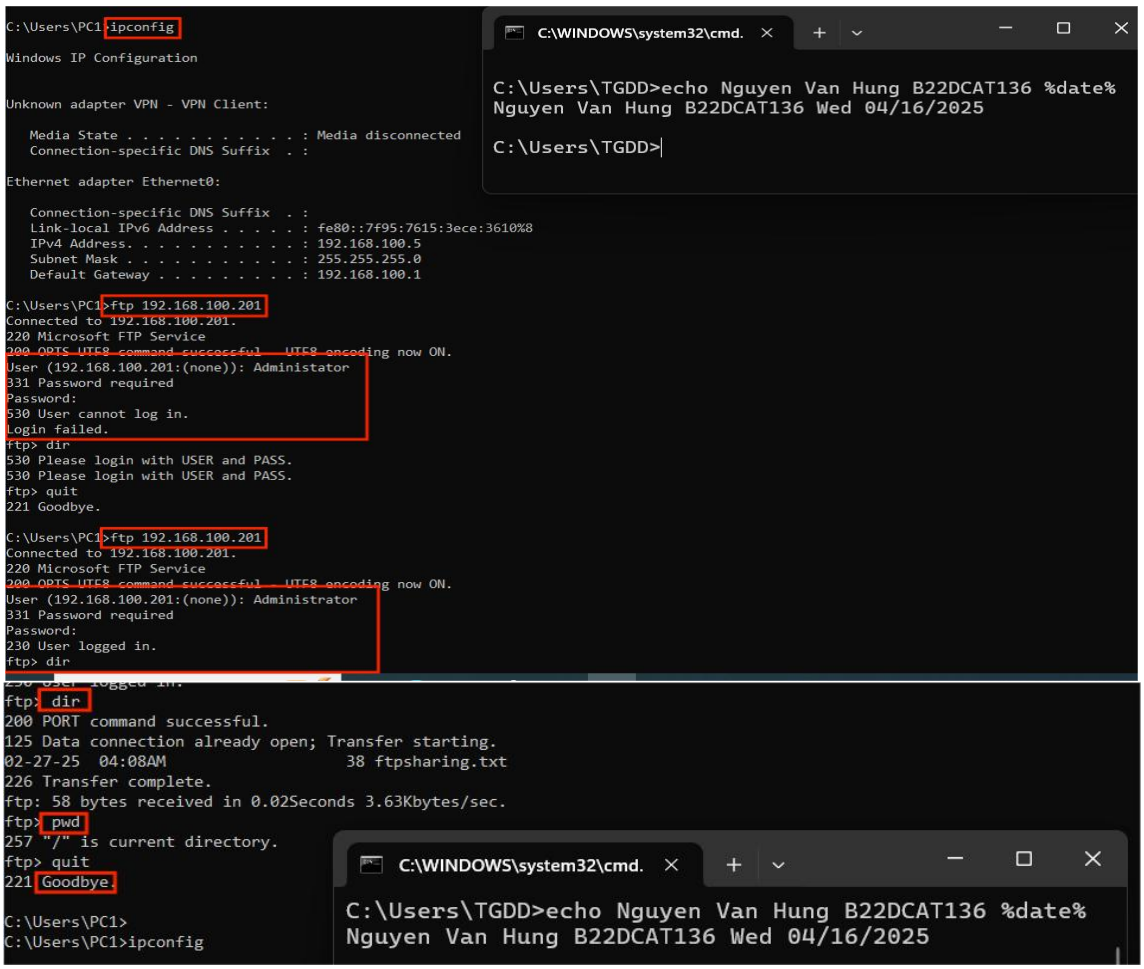


Hình 11. Bắt gói tin eth0

Mở máy Windows 10 Internal thực hiện lệnh ftp tới máy Windows Server 2019 Internal: *ftp 192.168.100.201*

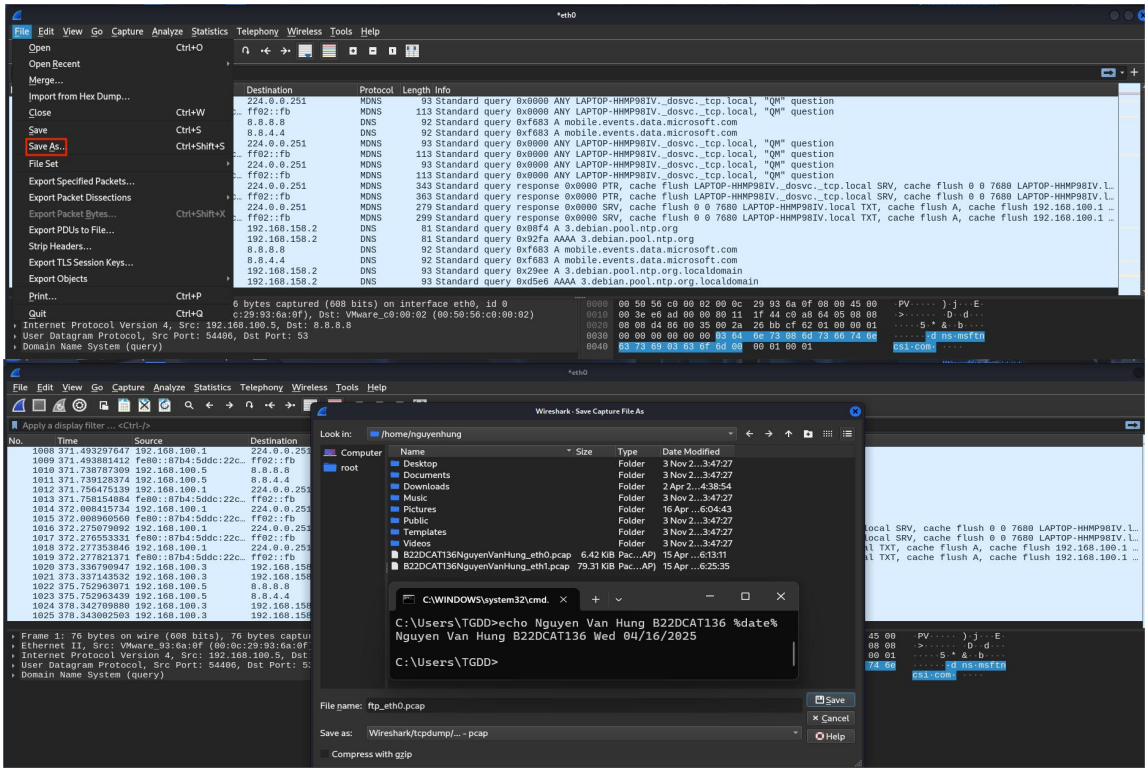
Đăng nhập và thực hiện một số lệnh FTP: *dir, pwd*

Thoát kết nối: *quit*



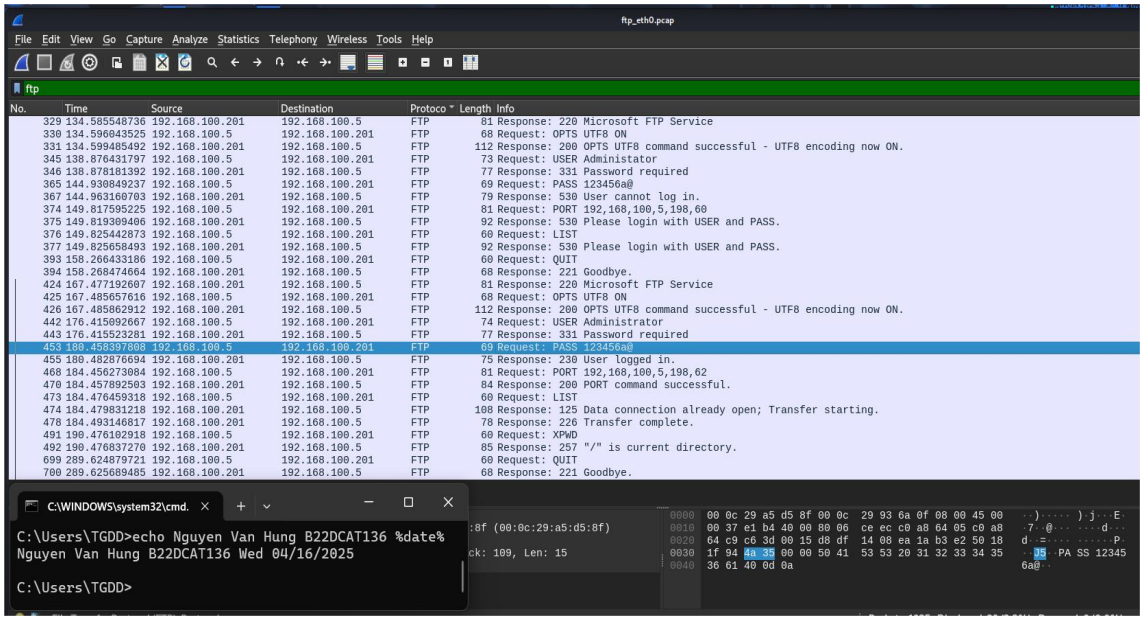
Hình 12. Thực hiện kết nối ftp đến Windows Server Internal

Trở lại Linux Sniffer, dừng bắt gói tin, lưu file dưới dạng pcap: **File → Save As... → Đặt tên file: ftp_eth0.pcap → Save**



Hình 13. Lưu file bắt gói tin eth0

Thực hiên lọc danh sách các gói tin FTP:



Hình 14. Danh sách các gói tin FTP trên interface eth0

Ta có thể thấy các gói tin bị bắt:

USER Administrator → Tên đăng nhập

Request: PASS 123456a@ → Mật khẩu truyền dạng plain text bị lộ

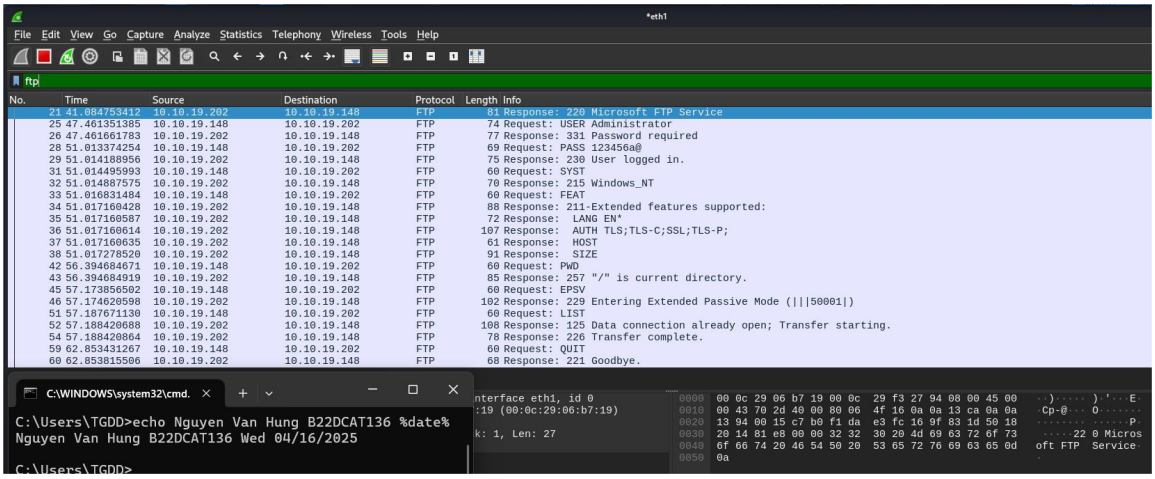
Response: 530 User cannot log in. → Lỗi đăng nhập

Response: 230 User logged in. → Đăng nhập thành công

QUIT → Lệnh thoát kết nối

Ta có thể thấy vì FTP là giao thức không mã hóa nên rất dễ lộ thông tin quan trọng, một số giao thức cũ không mã hóa khác cũng có nguy cơ tương tự: HTTP, SMTP/POP3, ...

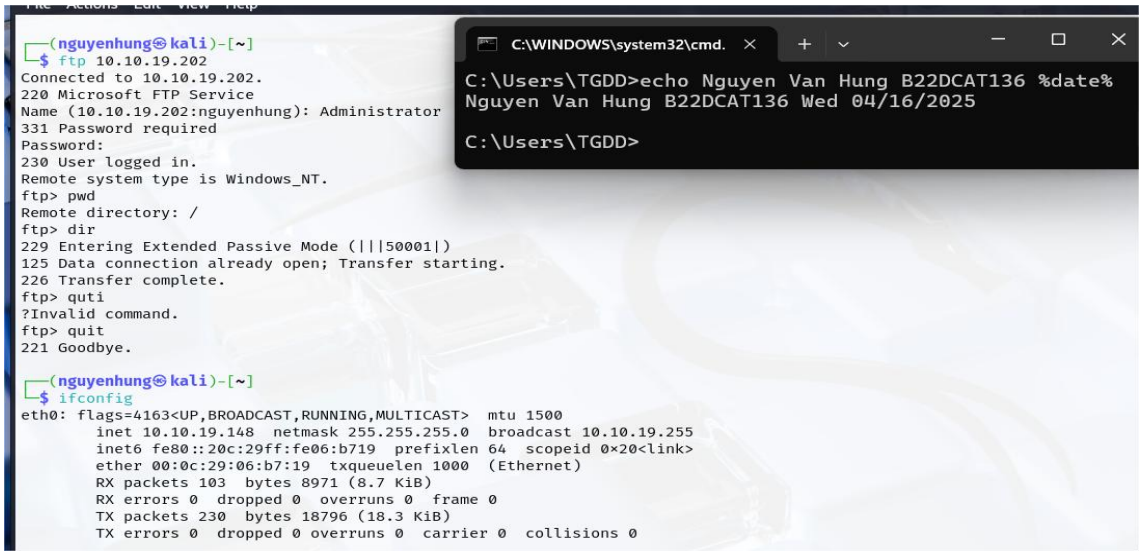
Trở lại bài thực hành, với eth1, ta thực hiện bắt gói tin tương tự các bước trên:



Hình 15. Bắt gói tin eth1

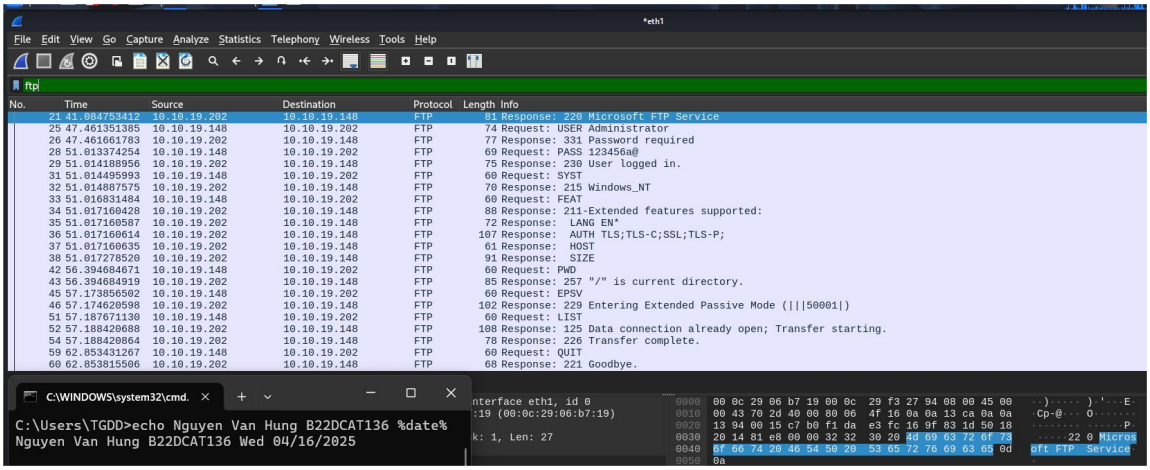
Từ máy Kali Linux External thực hiện kết nối ftp đến Windows Server 2019 External:

ftp 10.10.19.202

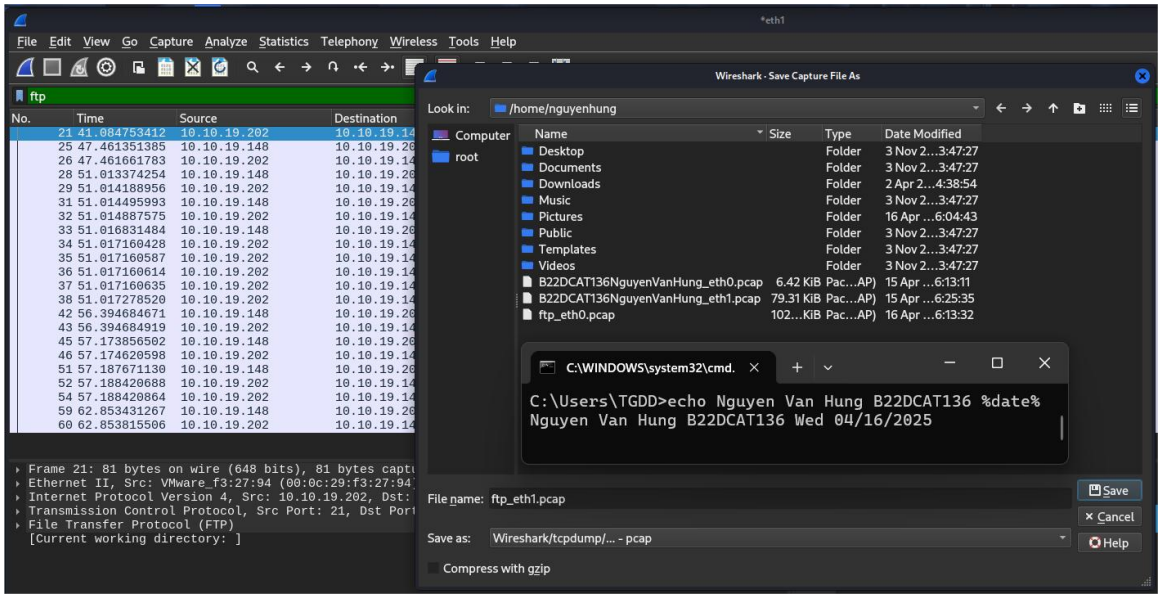


Hình 16. Thực hiện ftp tới máy Windows Server External

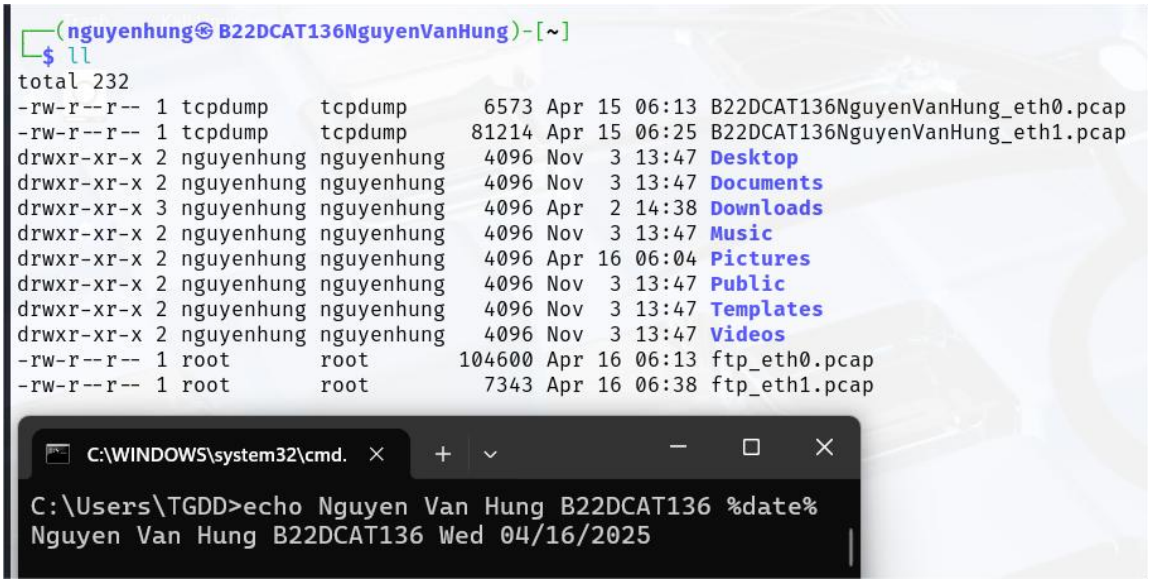
Lọc danh sách gói tin FTP:



Hình 17. Danh sách các gói tin FTP trên interface eth0



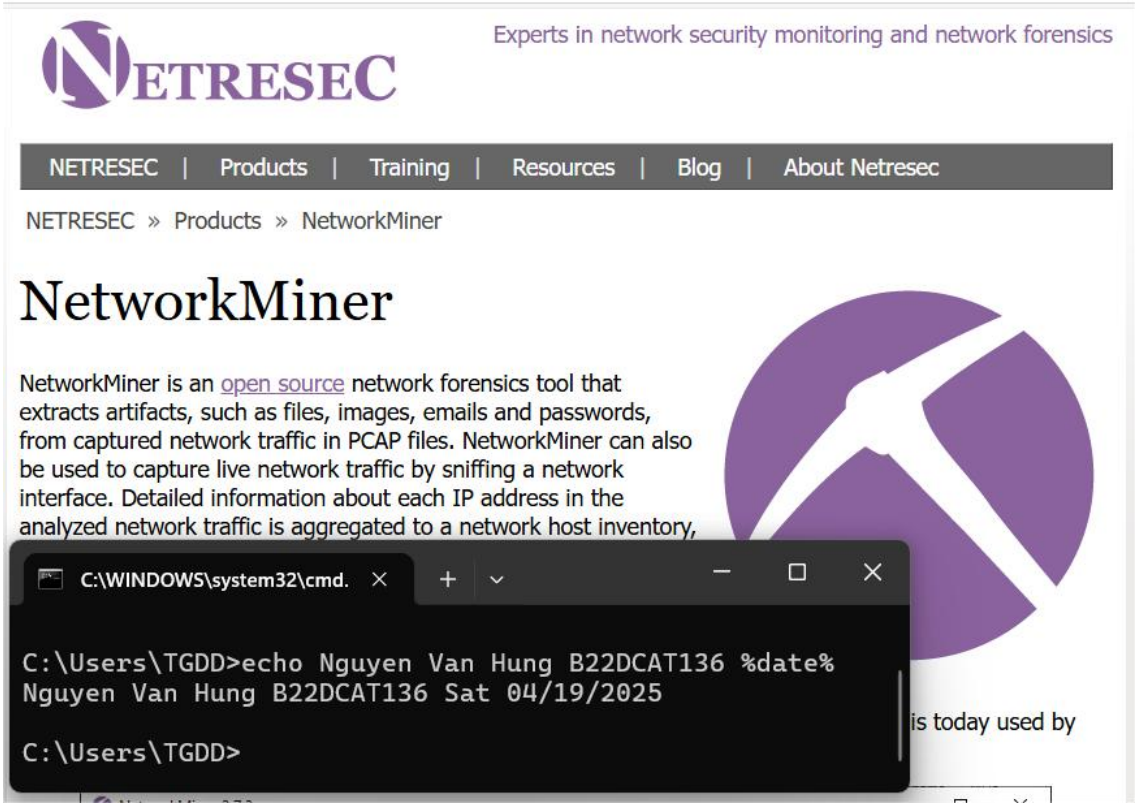
Hình 18. Lưu file bắt gói tin eth1



Hình 19. Các file bắt gói tin

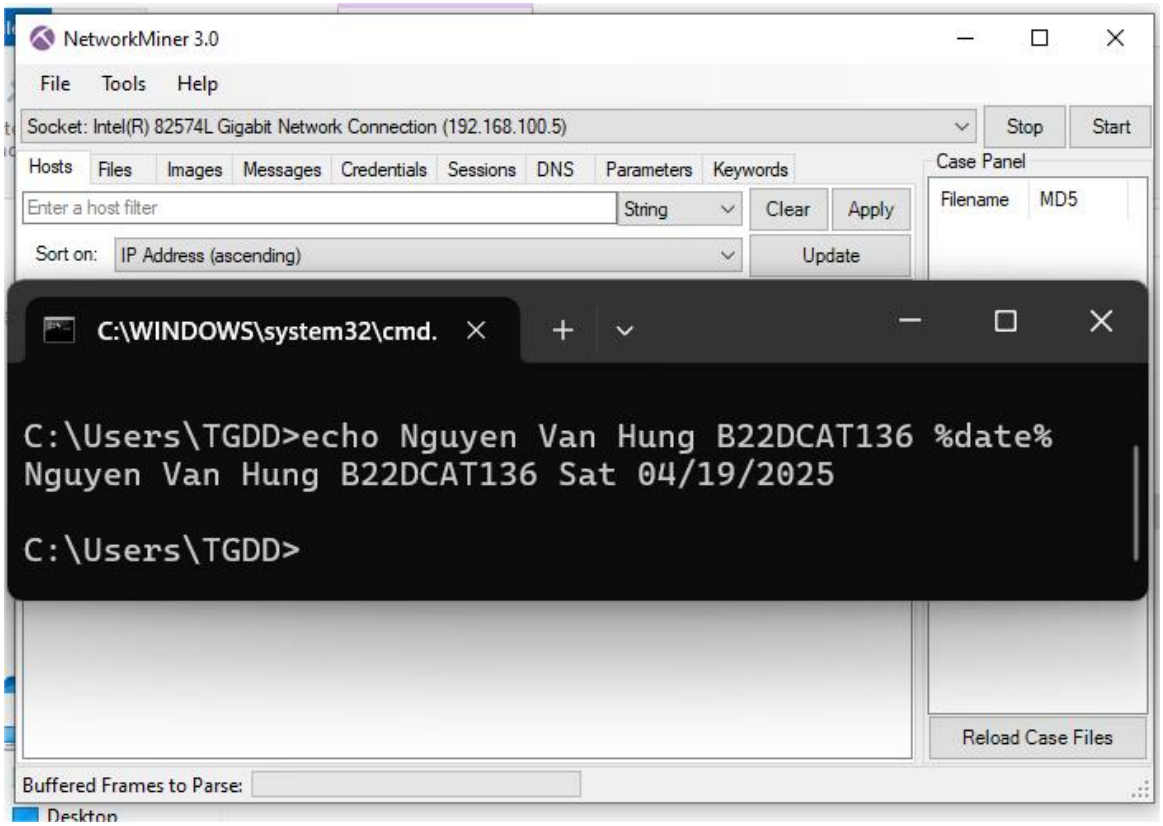
2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin

Tải Network Miner bản mới nhất trên trang https://www.netresec.com/ và cài đặt:



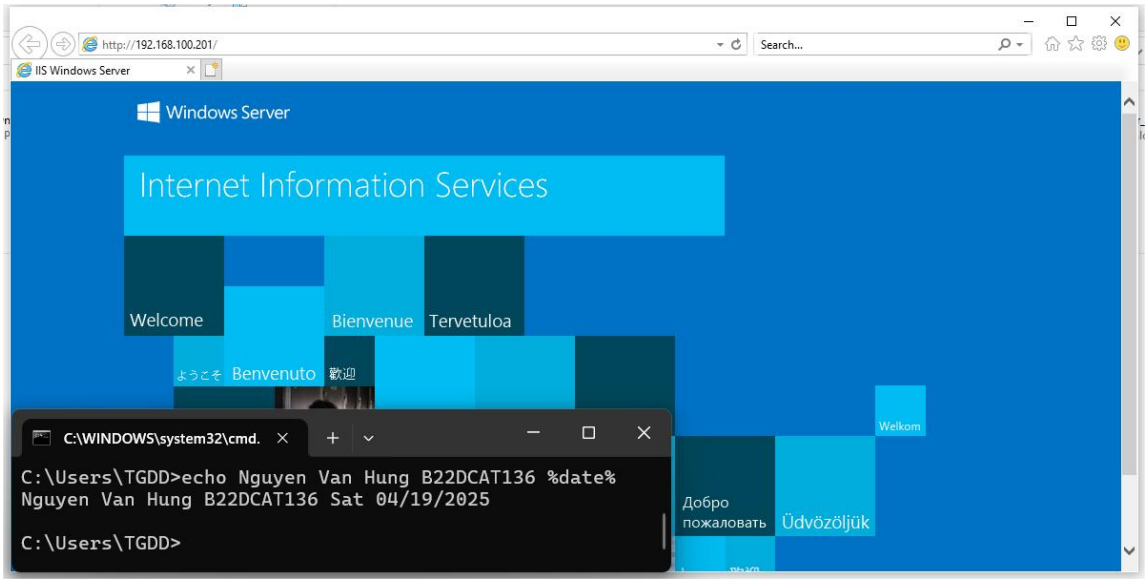
Hình 20. Tải Network Miner

Mở NetWork Miner dưới quyền Adsministrator, chọn **Socket: Intel(R) 82574L Gigabit Network Connection (192.168.100.5)** sau đó nhấn Start để bắt đầu bắt gói tin:

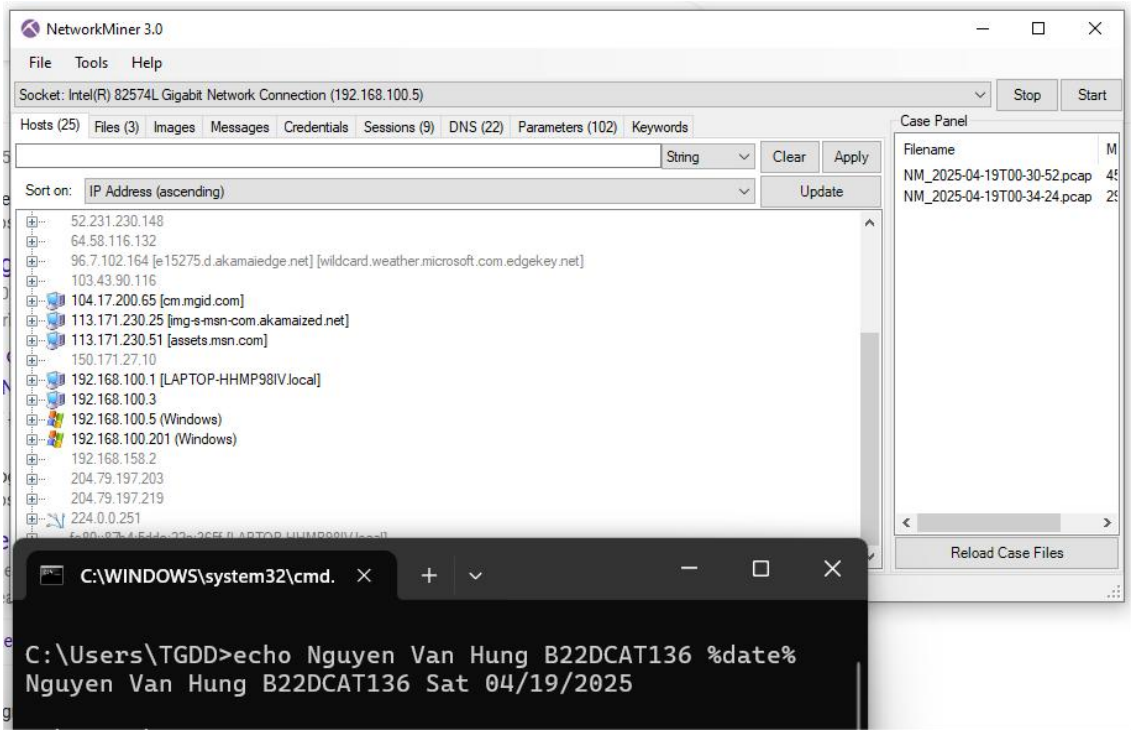


Hình 21. Mở Network Miner và chọn Socket

Sử dụng Internet Explorer để kết nối đến trang web của Windows Server 2019 Internal: http://192.168.100.201/. Sau đó dừng quá trình bắt tin:

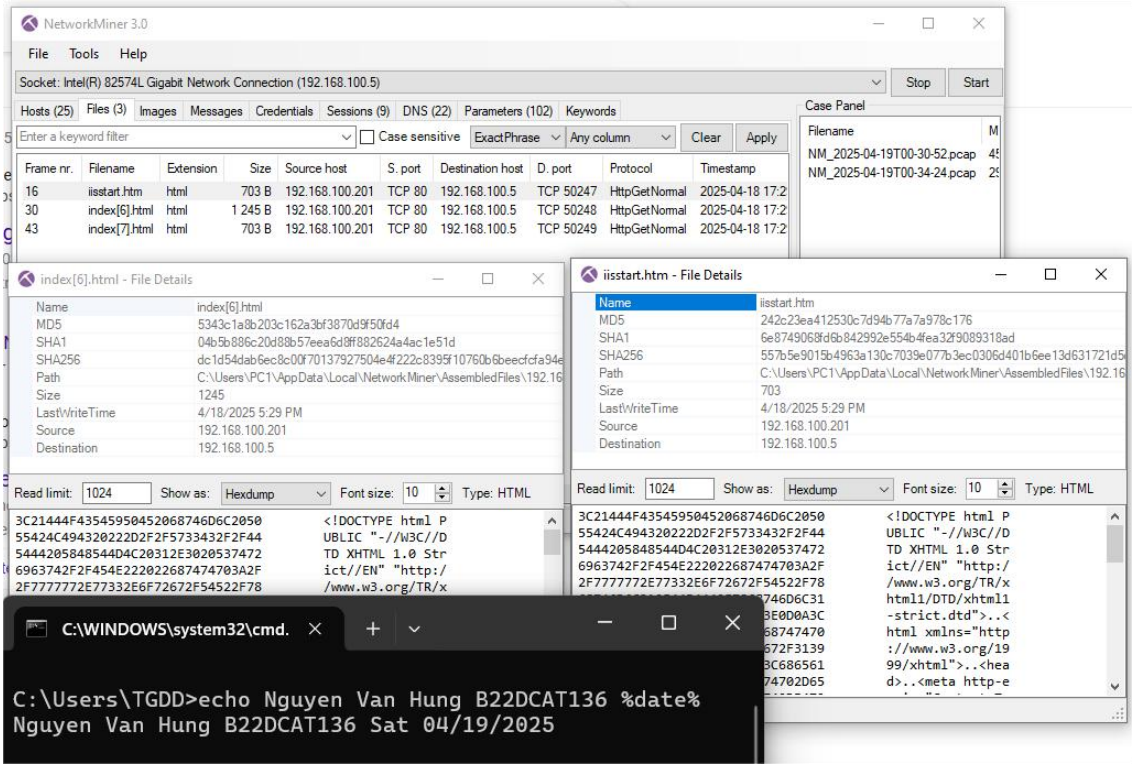


Hình 22. Kết nối trang web của Windows Server Internal



Hình 23. Dừng bắt gói tin

Chọn File và xem dữ liệu gói tin vừa bắt được:



Hình 24. Xem gói dữ liệu bắt được

TÀI LIỆU THAM KHẢO

[1] https://whitehat.vn/threads/thu-thap-thong-tin-ve-he-thong-ics-scada-bang-networkminer.15217/

[2] https://fptshop.com.vn/tin-tuc/danh-gia/sniffer-la-gi-166978

[3] https://viblo.asia/p/huong-dan-su-dung-wireshark-zOQJwQdxVMP

[4] https://www.techtarget.com/searchnetworking/tutorial/How-to-capture-and-analyze-traffic-with-tcpdump