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

Sinh viên thực hiện:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

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 Bắt và Phân tích Dữ liệu Mạng

- Bắt dữ liệu mạng (network packet capturing) là một kỹ thuật quan trọng trong quản trị mạng, bảo mật, và nghiên cứu giao thức. Quá trình này liên quan đến việc ghi lại các gói tin (packets) truyền qua mạng, từ đó phân tích để phát hiện sự cố, tối ưu hiệu suất, hoặc điều tra các vấn đề bảo mật. Các công cụ như tcpdump, Wireshark, và NetworkMiner đã trở thành những giải pháp tiêu biểu nhờ khả năng thu thập, xử lý, và trình bày dữ liệu mạng một cách hiệu quả.
- Mục tiêu của báo cáo này là trình bày chi tiết về tính năng, cơ chế hoạt động, và ứng dụng thực tế của ba công cụ trên. Mỗi công cụ có đặc điểm riêng, phục vụ các nhu cầu khác nhau từ giám sát nhanh, phân tích sâu, đến điều tra pháp y mạng. Nội dung sẽ được tổ chức để làm rõ vai trò của chúng trong lĩnh vực kỹ thuật theo dõi và giám sát an toàn mạng, đồng thời cung cấp cái nhìn so sánh để hỗ trợ người dùng lựa chọn công cụ phù hợp.

1.2.2 Công cụ tcpdump

1.2.2.1 Giới thiệu

- Tcpdump là một công cụ dòng lệnh mã nguồn mở, được phát triển từ những năm 1980, dành cho việc bắt và phân tích gói tin mạng. Với tính đơn giản và hiệu suất cao, tcpdump được sử dụng rộng rãi trên các hệ điều hành Unix/Linux, đặc biệt trong môi trường máy chủ hoặc thiết bị nhúng. Công cụ này cho phép người dùng ghi lại lưu lượng mạng với độ chính xác cao và tiêu tốn tài nguyên tối thiểu.

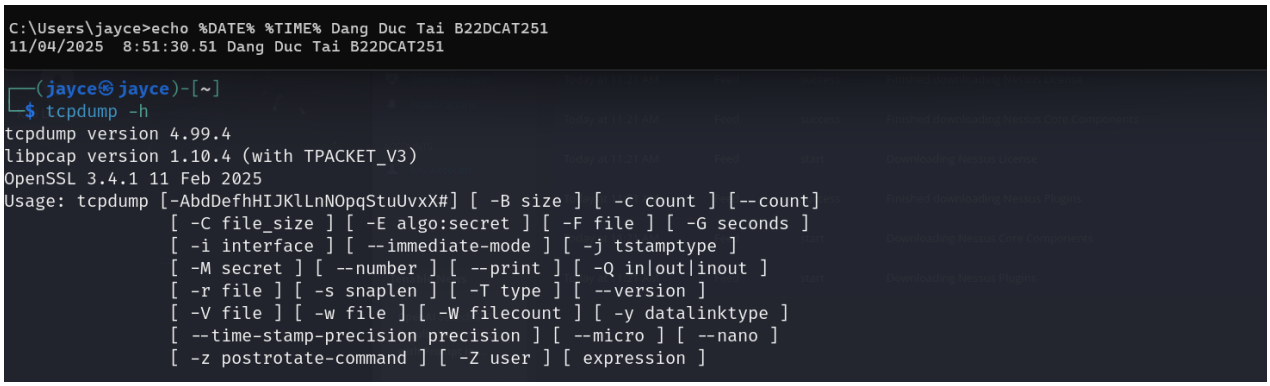
1.2.2.2 Các tính năng chính

- Bắt gói tin theo thời gian thực: tcpdump ghi lại các gói tin đi qua một giao diện mạng, cung cấp thông tin chi tiết như địa chỉ IP nguồn/đích, cổng, giao thức, và thời gian.
- Lọc gói tin linh hoạt: Sử dụng biểu thức lọc dựa trên giao thức (TCP, UDP, ICMP, HTTP…), địa chỉ IP, cổng, hoặc các điều kiện logic phức tạp. Ví dụ: lọc lưu lượng từ một IP cụ thể hoặc chỉ ghi lại các gói tin HTTPS.
- Lưu trữ dữ liệu: Hỗ trợ xuất gói tin ra file định dạng PCAP, tương thích với các công cụ phân tích khác như Wireshark.
- Hỗ trợ đa giao thức: Ghi nhận lưu lượng từ nhiều giao thức mạng, bao gồm cả các giao thức ít phổ biến như ARP, SNMP.

- Hiệu suất tối ưu: Thiết kế nhẹ, phù hợp cho các hệ thống có cấu hình thấp hoặc môi trường không có giao diện đồ họa.
- Giám sát từ xa: Có thể kết hợp với các công cụ như SSH để bắt gói tin từ các thiết bị từ xa.
- Tùy chỉnh đầu ra: Cho phép định dạng đầu ra (text, hex, hoặc tóm tắt) để phù hợp với nhu cầu phân tích.

1.2.2.3 Cơ chế hoạt động

- Tcpdump hoạt động bằng cách đặt giao diện mạng vào chế độ promiscuous mode (lắng nghe tất cả lưu lượng đi qua) hoặc chế độ chọn lọc (chỉ ghi lưu lượng liên quan đến thiết bị). Người dùng chỉ định giao diện mạng (eth0, eth1, wlan0, …) và áp dụng bộ lọc nếu cần. Các bước cơ bản bao gồm:
    - Khởi động: Chạy lệnh với các tham số, *tcpdump -i eth0* để ghi lại tất cả lưu lượng trên giao diện eth0.
    - Lọc dữ liệu: Sử dụng biểu thức lọc, như *tcpdump -i eth0 port 80* để chỉ ghi lưu lượng HTTP hoặc *tcpdump -i eth0 host 192.168.1.1* để tập trung vào một địa chỉ IP.
    - Hiển thị hoặc lưu trữ: Kết quả có thể hiển thị trực tiếp trên terminal (dạng văn bản) hoặc lưu vào file PCAP, ví dụ: *tcpdump -i eth0 -w capture.pcap*
- Hướng dẫn sử dụng tcpdump

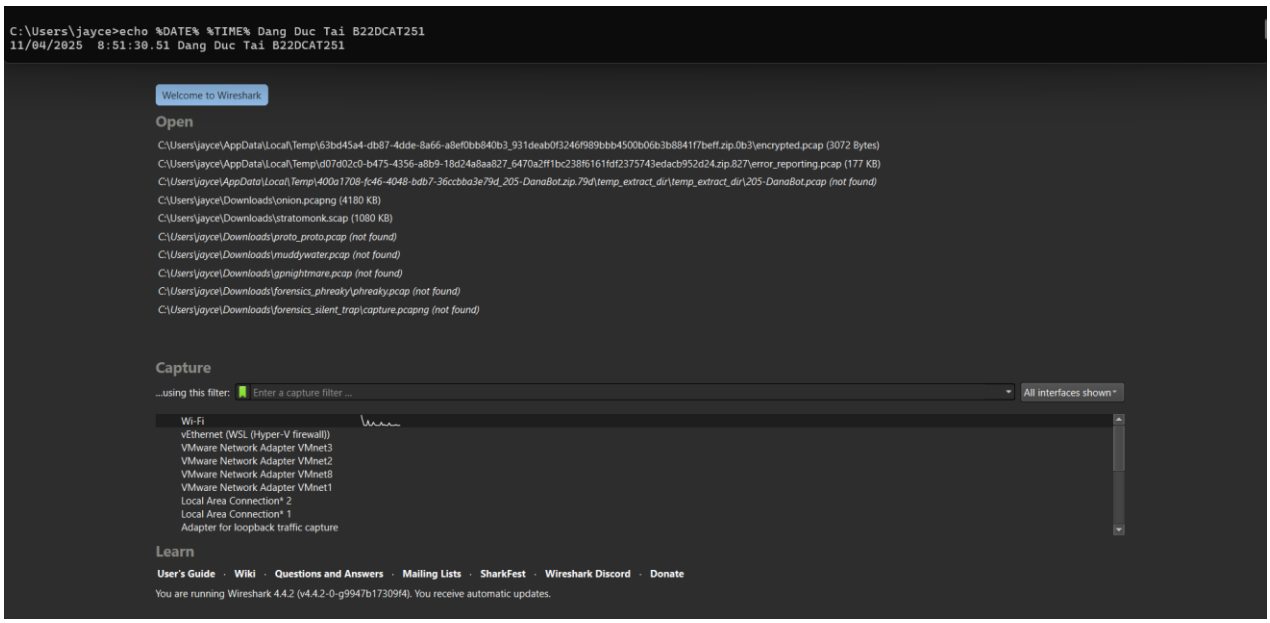


Hình 1 Tùy chọn -h hiển thị hướng dẫn sử dụng công cụ tcpdump

1.2.3 Công cụ wireshark

1.2.3.1 Giới thiệu

- Wireshark là công cụ phân tích giao thức mạng mã nguồn mở, được sử dụng rộng rãi nhất trên thế giới. Nó cung cấp giao diện đồ họa thân thiện và khả năng phân tích sâu các gói tin mạng.



Hình 2 Giao diện đồ họa của công cụ wireshark

1.2.3.2 Các tính năng chính

Một số tính năng chính có thể kể đến của wireshark:

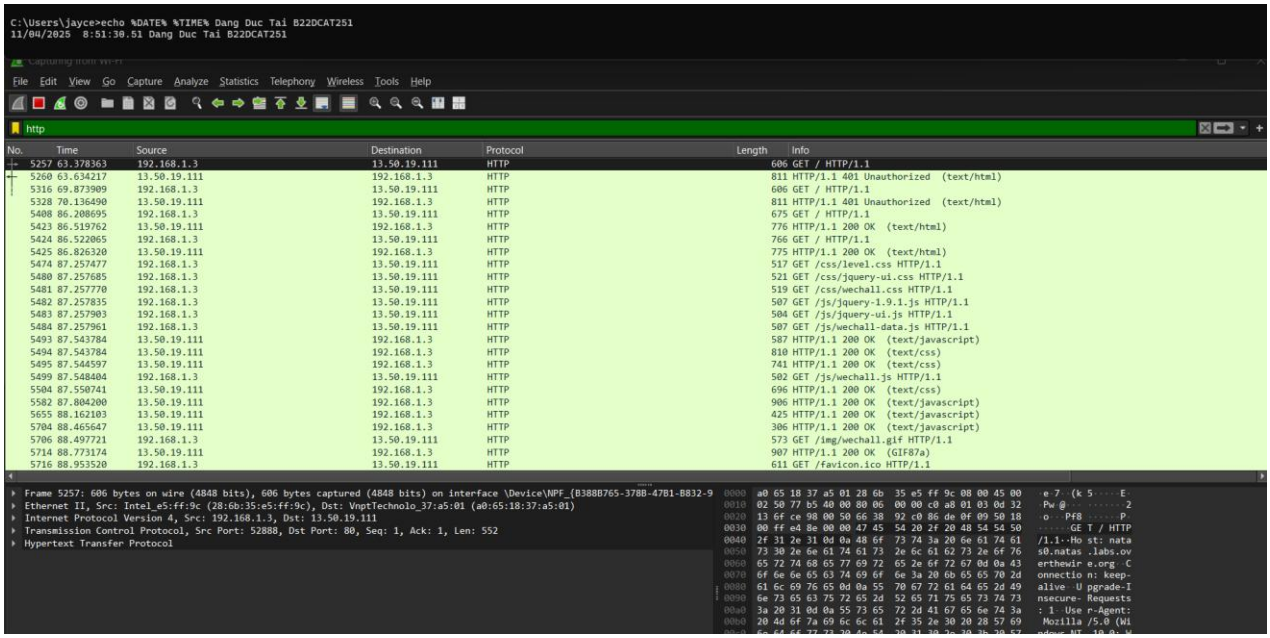
- Bắt và phân tích gói tin: Hỗ trợ ghi lại lưu lượng mạng theo thời gian thực hoặc phân tích các file PCAP đã ghi trước đó.
- Hỗ trợ đa giao thức: Phân tích sâu các giao thức từ tầng liên kết dữ liệu (Ethernet) đến tầng ứng dụng (HTTP, DNS, VoIP…).
- Bộ lọc mạnh mẽ:

- Capture Filter: Lọc gói tin trong quá trình ghi để giảm tải hệ thống, ví dụ: port 80 để chỉ ghi lưu lượng HTTP.
- Display Filter: Lọc dữ liệu hiển thị sau khi ghi, ví dụ: ip.src == 192.168.1.1 để chỉ xem lưu lượng từ một IP nguồn.

- Giao diện đồ họa trực quan: Hiển thị gói tin qua ba phần:

- Packet List: Danh sách gói tin với thông tin tóm tắt (thời gian, nguồn, đích, giao thức).
- Packet Details: Chi tiết từng gói tin, phân tích theo lớp giao thức (Ethernet, IP, TCP…).
- Packet Bytes: Dữ liệu thô dạng hex và ASCII.

- Phân tích thống kê: Cung cấp biểu đồ luồng (TCP stream), thống kê giao thức, độ trễ, và hiệu suất mạng.
- Phân tích VoIP: Cho phép kiểm tra chất lượng cuộc gọi qua mạng, phát hiện jitter hoặc mất gói tin.
- Tùy chỉnh giao diện: Hỗ trợ tô màu gói tin theo trạng thái (ví dụ: xanh cho TCP, đỏ cho lỗi) để dễ phân biệt.
- Giải mã giao thức: Có thể giải mã một số giao thức mã hóa (như SSL/TLS) nếu cung cấp khóa giải mã.



Hình 3 Ví dụ về lọc gói tin http trên wireshark

1.2.3.3 Cơ chế hoạt động

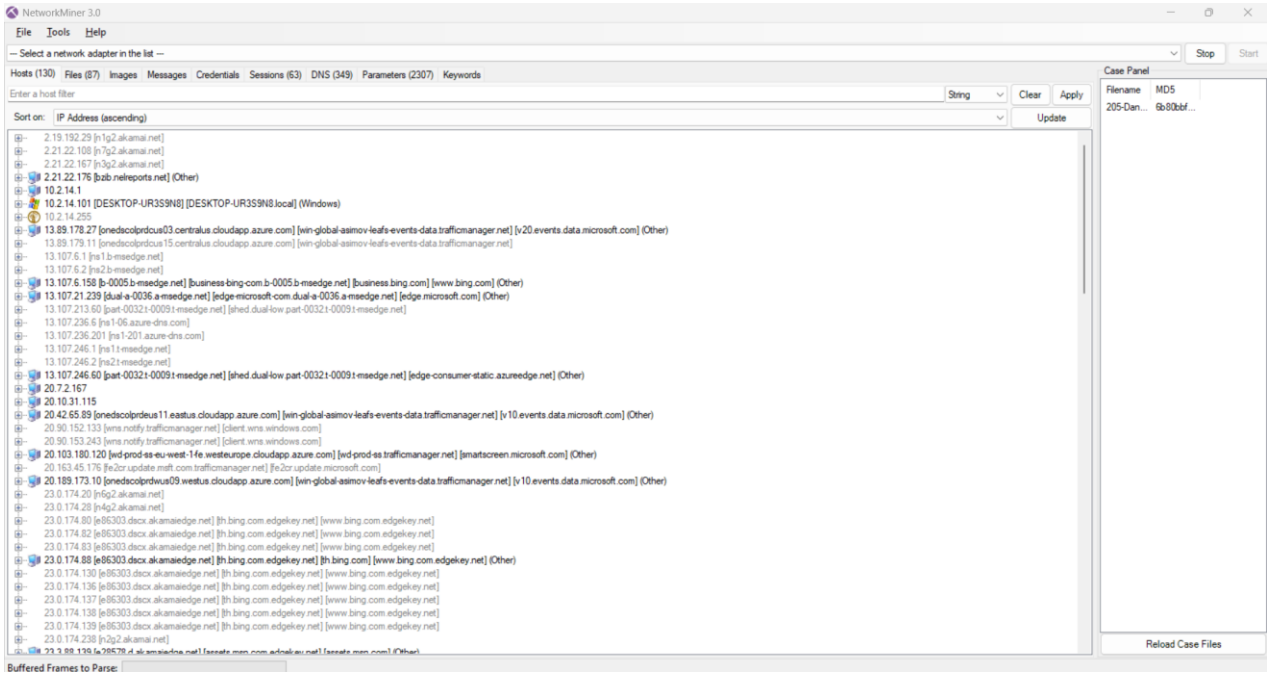
- Wireshark hoạt động dựa trên thư viện libpcap (trên Linux) hoặc WinPcap/Npcap (trên Windows) để ghi lại gói tin. Quy trình hoạt động bao gồm:

- Chọn giao diện: Người dùng chọn giao diện mạng (Ethernet, Wi-Fi…) để bắt đầu ghi.
- Ghi dữ liệu: Wireshark ghi lại tất cả lưu lượng hoặc chỉ lưu lượng được lọc (ví dụ: port 443 để ghi HTTPS).
- Phân tích: Dữ liệu được hiển thị trong giao diện đồ họa, cho phép người dùng xem chi tiết từng gói tin, tái tạo luồng giao tiếp, hoặc tìm kiếm gói tin cụ thể.
- Lưu trữ và xuất: Dữ liệu có thể lưu dưới dạng PCAP hoặc xuất sang các định dạng như CSV, JSON để báo cáo.

1.2.4 Công cụ Network Miner

1.2.4.1 Giới thiệu

- NetworkMiner là một công cụ phân tích pháp y mạng (Network Forensic Analysis Tool - NFAT), được thiết kế để trích xuất thông tin từ lưu lượng mạng mà không tạo ra lưu lượng chủ động. Ra mắt vào năm 2007, công cụ này tập trung vào việc thu thập dữ liệu meta (metadata) và tái tạo nội dung, đặc biệt hữu ích trong điều tra bảo mật và pháp y mạng.



Hình 4 Phân tích gói tin .pcap trên Network Miner

1.2.4.2 Các tính năng chính

- Phân tích thụ động: Lắng nghe lưu lượng mạng mà không gửi gói tin, đảm bảo không làm gián đoạn hoạt động mạng.
- Trích xuất thông tin: Tự động phát hiện thông tin như địa chỉ IP, tên máy chủ, hệ điều hành, cổng mở, và các phiên kết nối.
- Tái tạo nội dung: Khôi phục các tệp được truyền qua mạng (hình ảnh, tài liệu, video…) từ lưu lượng HTTP, FTP, SMB.
- Phân tích file PCAP: Hỗ trợ phân tích offline từ các file PCAP, tái tạo chứng chỉ SSL hoặc thông tin đăng nhập.
- Phát hiện tài khoản: Trích xuất thông tin đăng nhập (username/password) từ các giao thức không mã hóa như HTTP, FTP.

1.2.4.3 Cơ chế hoạt động

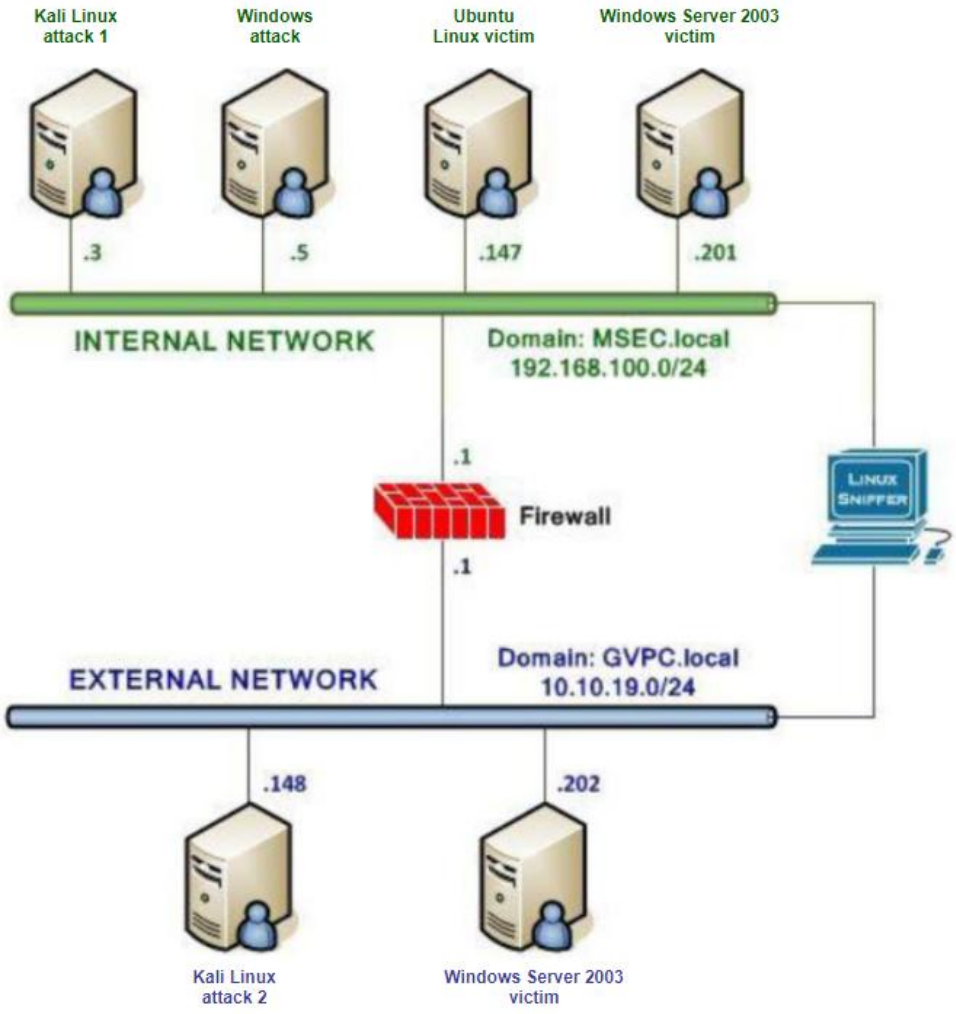
- NetworkMiner hoạt động ở chế độ thụ động, sử dụng giao diện mạng hoặc file PCAP làm nguồn dữ liệu. Quy trình hoạt động bao gồm:

- Thu thập dữ liệu: Lắng nghe lưu lượng từ giao diện mạng hoặc đọc file PCAP.
- Phân loại thông tin: Tự động phân loại dữ liệu thành các danh mục:
    - Hosts: Thông tin thiết bị (IP, hostname, hệ điều hành…).
    - Sessions: Các phiên kết nối (TCP, UDP…).
    - Files: Tệp được truyền qua mạng (hình ảnh, tài liệu…).
    - Credentials: Thông tin đăng nhập từ các giao thức không mã hóa.
- Tái tạo nội dung: Khôi phục các tệp hoặc nội dung, ví dụ: tái tạo hình ảnh từ lưu lượng HTTP.
- Hiển thị và xuất: Kết quả được trình bày trong giao diện đồ họa hoặc xuất ra dạng CSV, XML để báo cáo.

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 trong bài 5.



Hình 5 Topo mạng

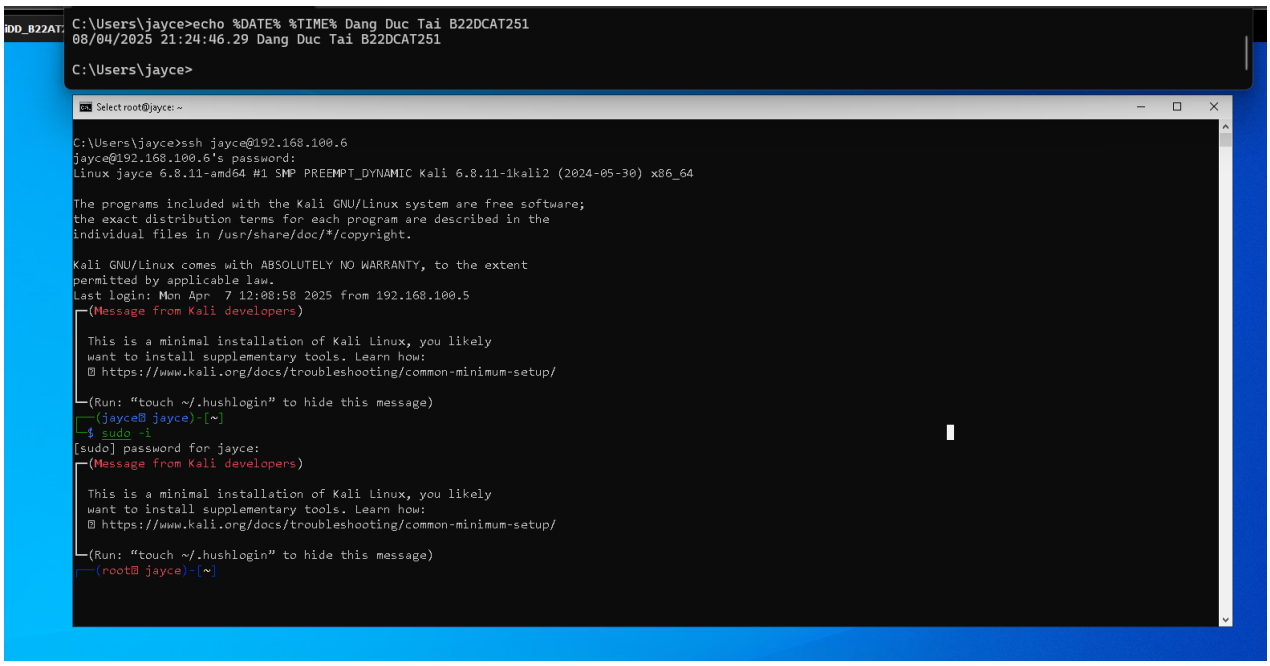
2.2 Các bước thực hiện

2.2.1 Sử dụng tcpdump

- Trên máy Windows attack trong mạng Internal, đăng nhập Linux Sniffer.

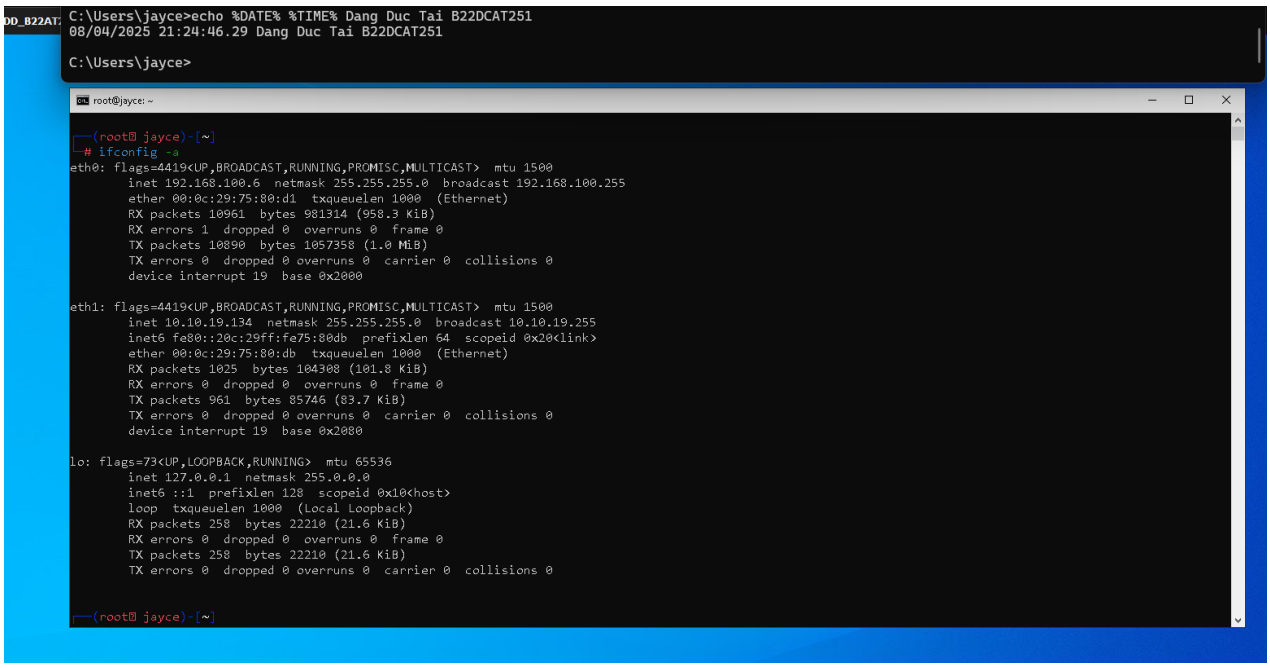
  ssh USER@192.168.100.6

  sudo -i



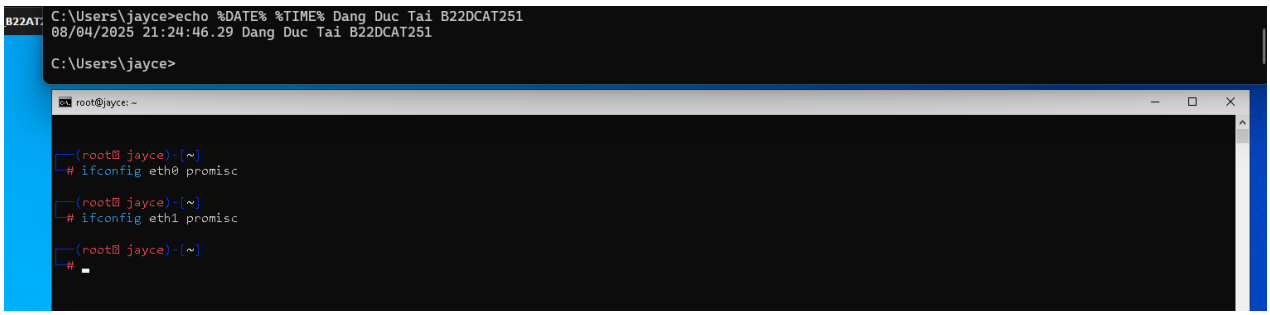
Hình 6 Đăng nhập vào Linux Sniffer

- Xem tất cả các interfaces trong hệ thống
  ifconfig -a



Hình 7 Xem các interfaces trong hệ thống

- Trên máy Windows attack trong mạng Internal, kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp, sau đó khởi động tcpdump.
  ifconfig eth0 promisc
  ifconfig eth1 promisc

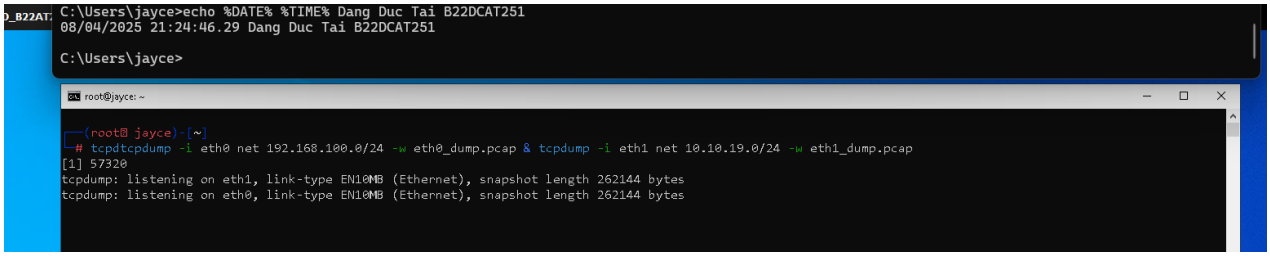


Hình 8 Kích hoạt chế độ hỗn hợp

- Bắt gói tin trên dải mạng 192.168.100.0/24, 10.10.19.0/24 (eth0, eth1) và gửi vào một file(thời gian chờ dữ liệu trong khoảng 5 phút).

  tcpdump -I eth0 net 192.168.100.0/24 -w eth0_dump.pcap

  tcpdump -I eth1 net 10.10.19.0/24 -w eth1_dump.pcap

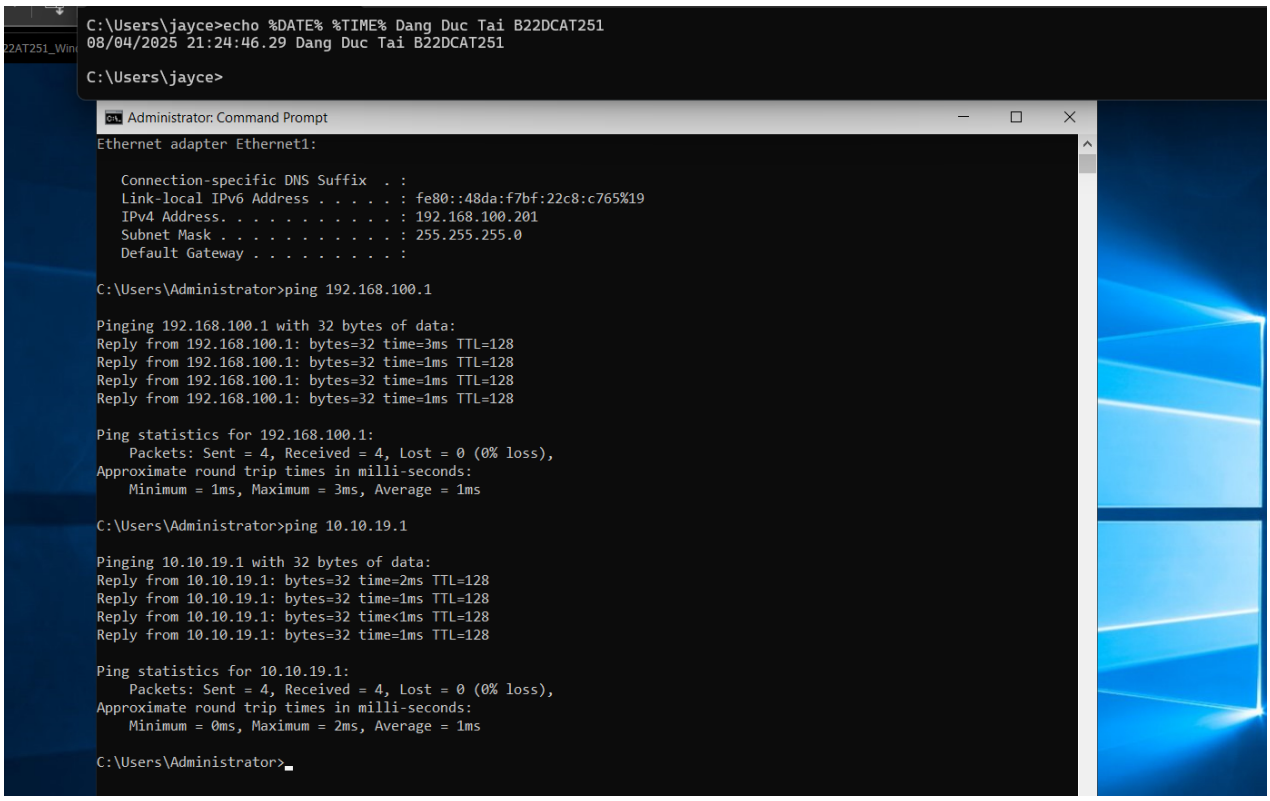


Hình 9 Bắt gói tin trên dải mạng eth0, eth1

- Cùng lúc trên máy Window Server, tiến hành ping đến dải mạng internal và dải mạng external

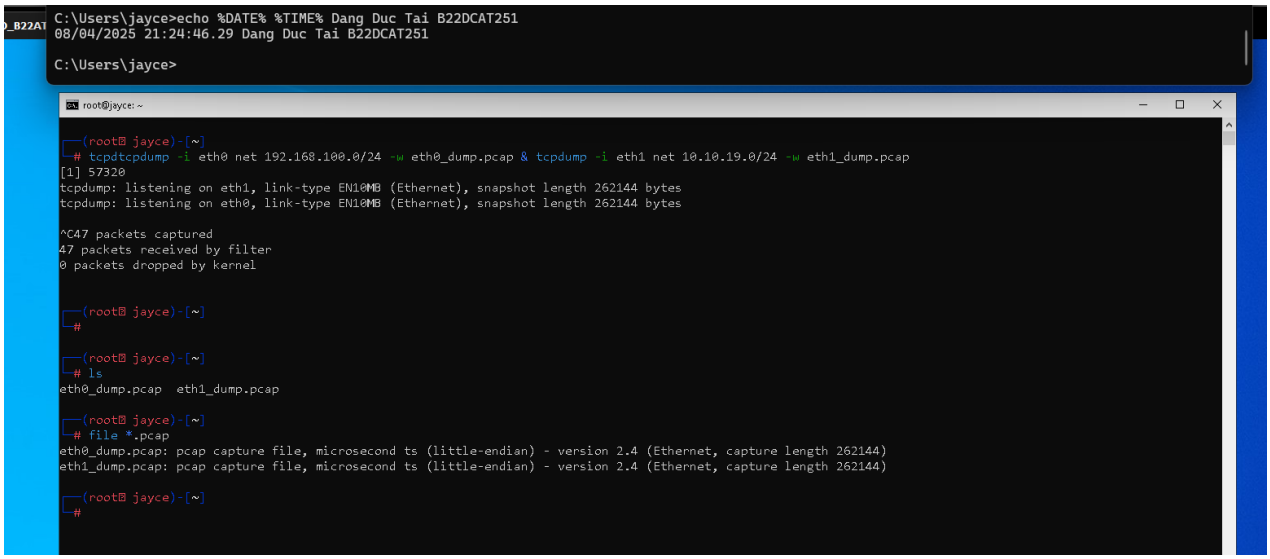
  ping 192.168.100.1

  ping 10.10.19.1



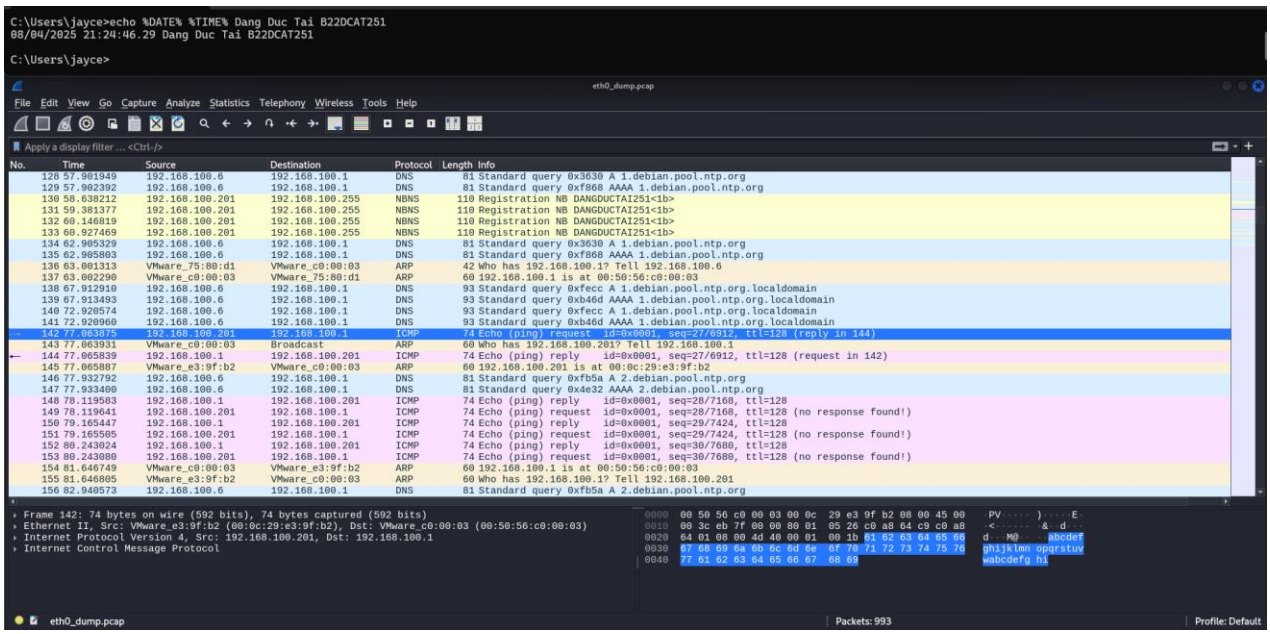
Hình 10 Ping từ Windows Server tới dải eth0, eth1

- Trên máy Window attack, tiến hành bắt gói tin bằng tcpdump, và lưu dữ liệu vào file pcap.



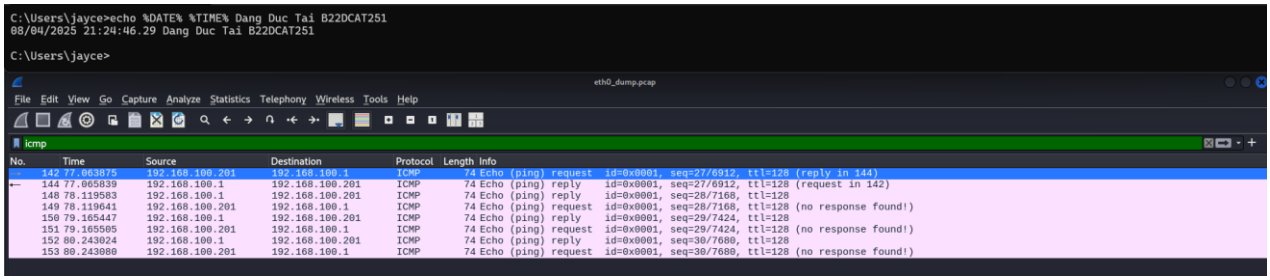
Hình 11 Lưu gói tin bắt được bằng tcpdump

- Các gói .pcap đã bắt được và lưu vào trong file
- File eth0.pcap



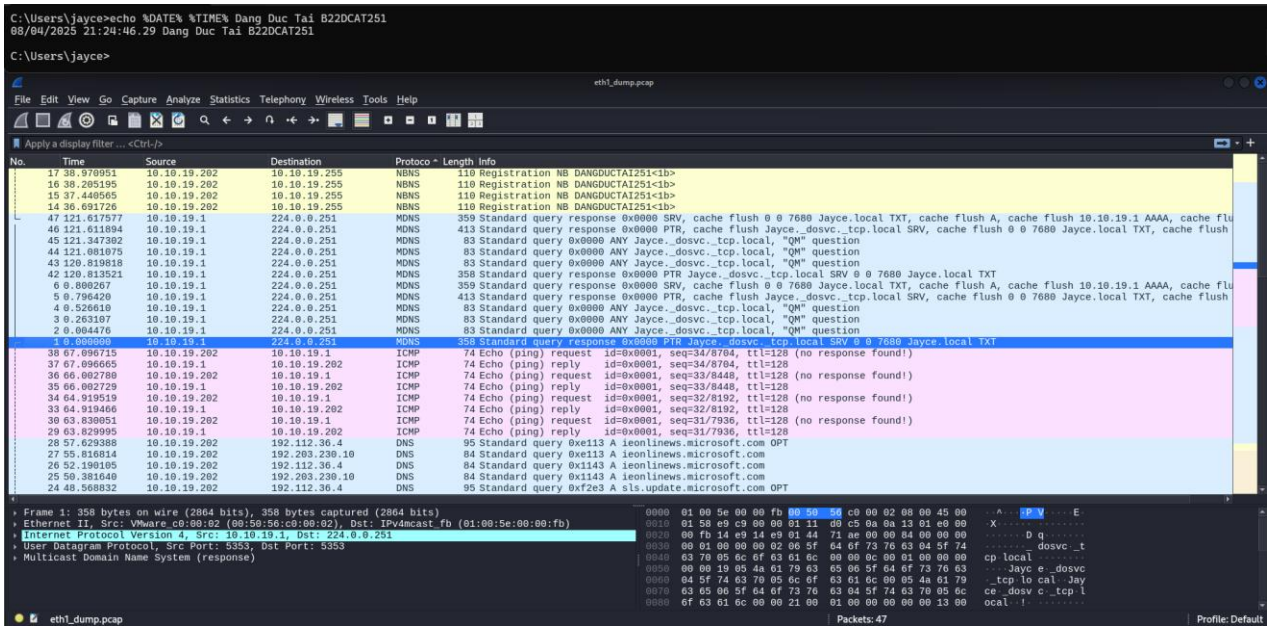
Hình 12 Xem file eth0.pcap

- Lọc các gói tin ICMP trên file eth0.pcap (Tương tự lệnh tcpdump –i eth0 icmp)



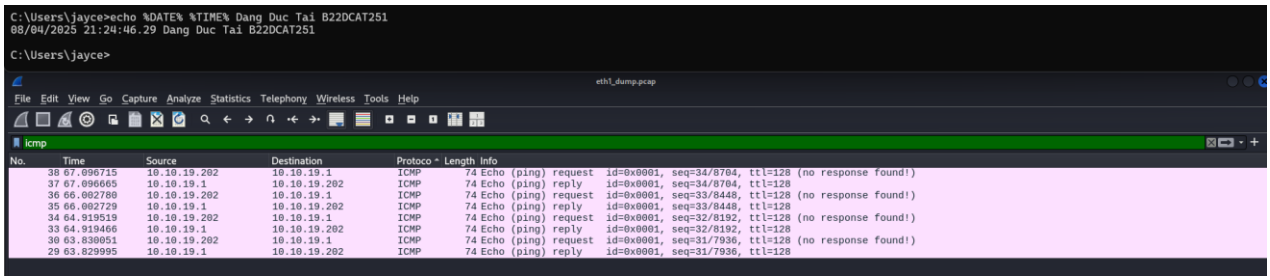
Hình 13 Lọc các gói tin ICMP trên file eth0.pcap

- File eth1.pcap



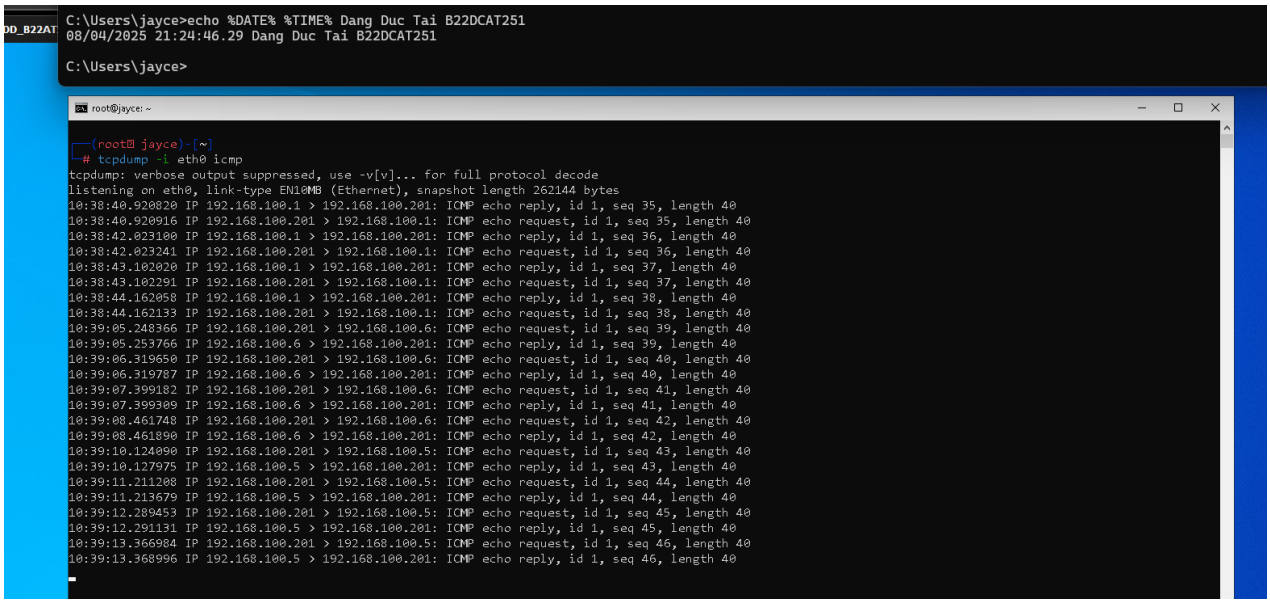
Hình 14 Xem file eth1.pcap

- Lọc các gói tin ICMP trên file eth1.pcap (Tương tự với lệnh tcpdump –i eth1 icmp)



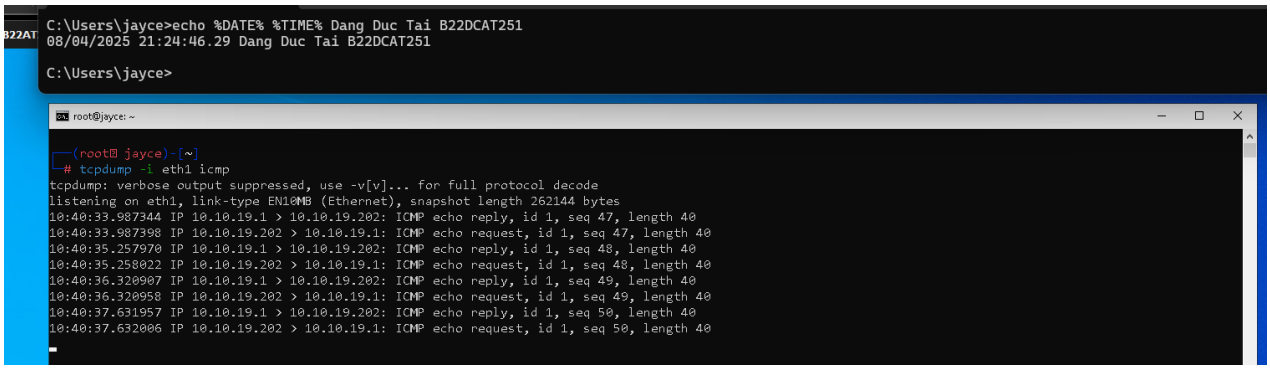
Hình 15 Lọc các gói tin ICMP trên file eth1.pcap

- Chỉ bắt lại các gói ICMP bằng tcpdump
  tcpdump –i eth0 icmp



Hình 16 Bắt gói ICMP bằng tcpdump trên eth0

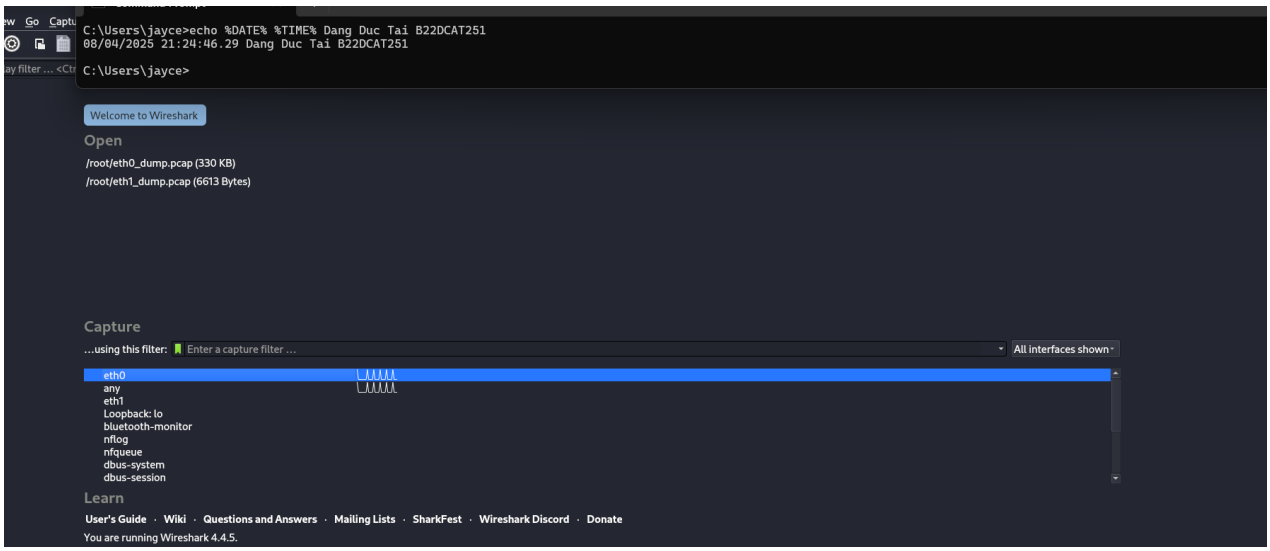
- Tương tự với eth1
  tcpdump –i eth1 icmp



Hình 17 Bắt gói ICMP bằng tcpdump trên eth1

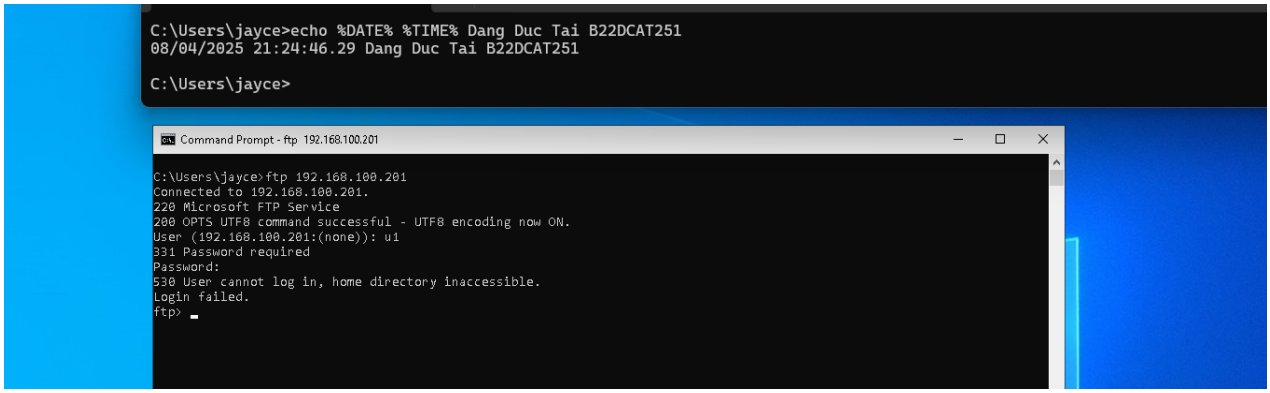
2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin

- Sử dụng wireshark để bắt gói tin trên card mạng eth0 (192.168.100.0/24)



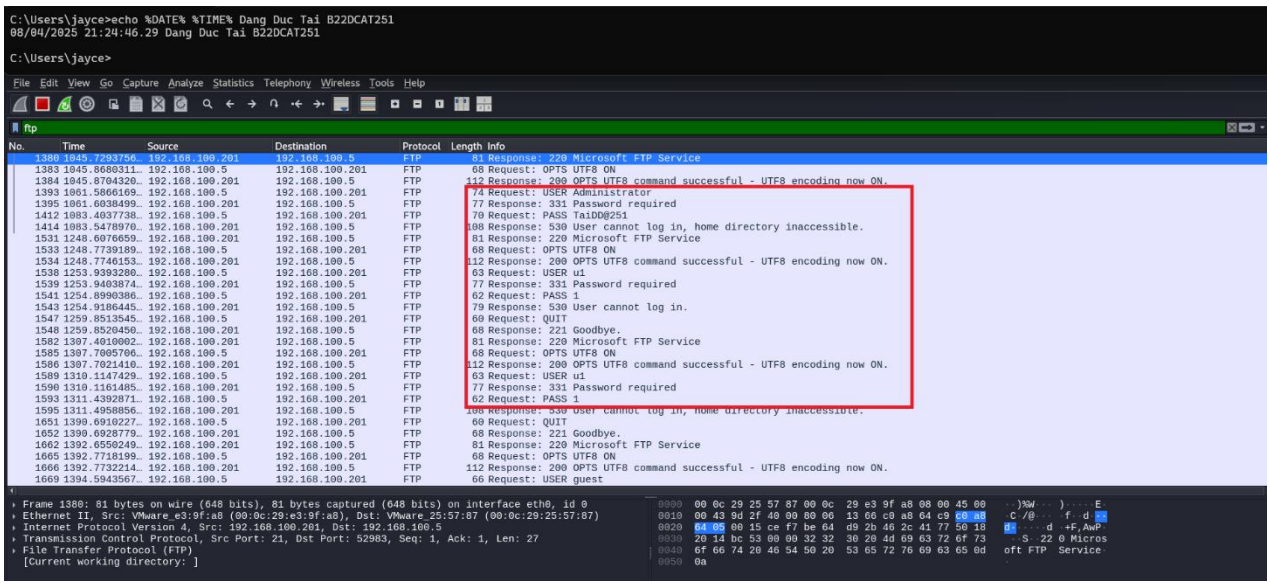
Hình 18 Khởi động wireshark trên eth0

- Cùng lúc đó ở máy windows 10, tiến hành phiên ftp vào windows server (Thử đăng nhập thất bại)
  ftp 192.168.100.201



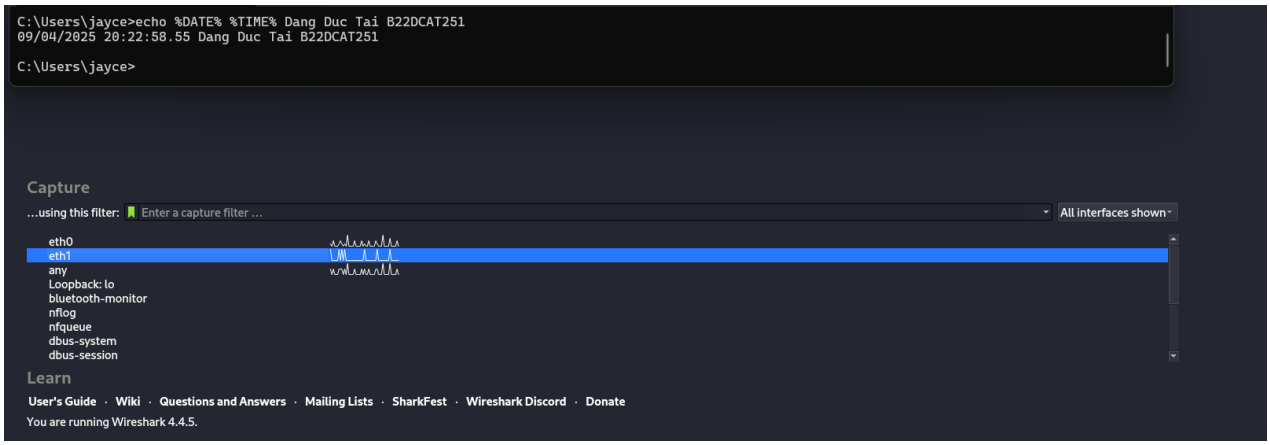
Hình 19 Thực hiện phiên ftp tới máy windows server

- Lọc các gói tin ftp trên wireshark và quan sát thấy phiên các thông báo (USER, PASS, 530 User cannot log in …) được hiển thị



Hình 20 Lọc các gói tin ftp trên wireshark với mạng eth0

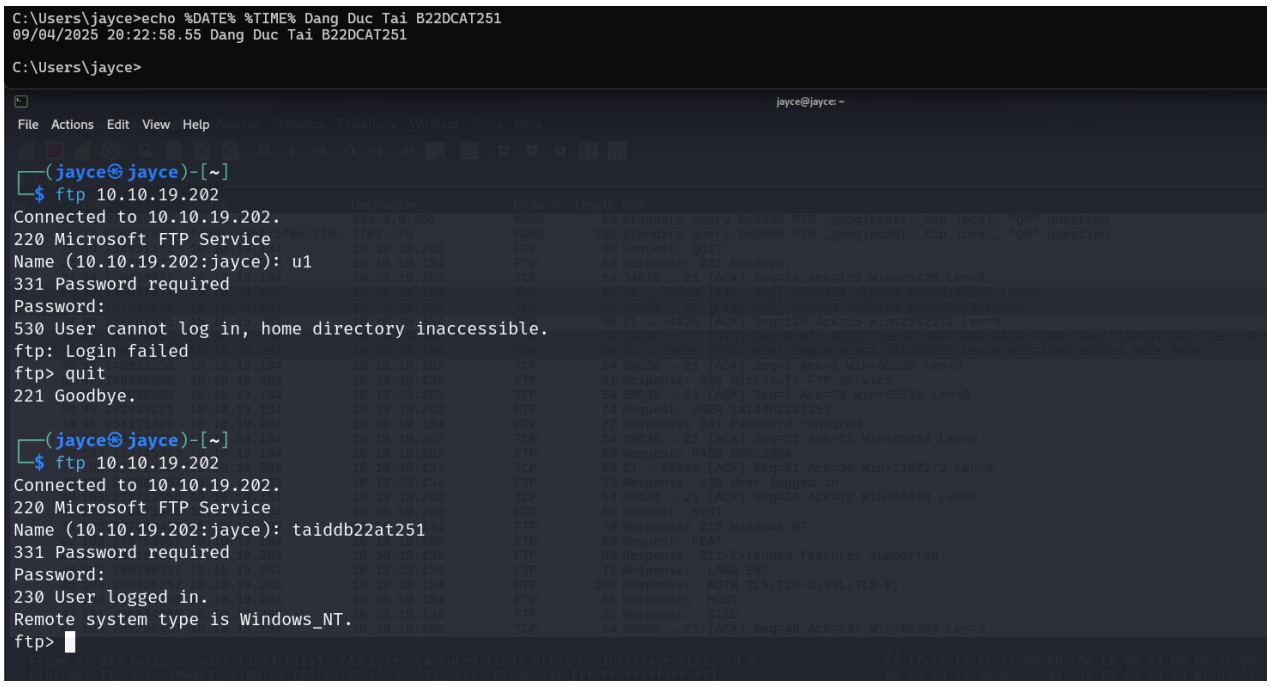
- Tương tự với eth1



Hình 21 Khởi động wireshark trên eth1

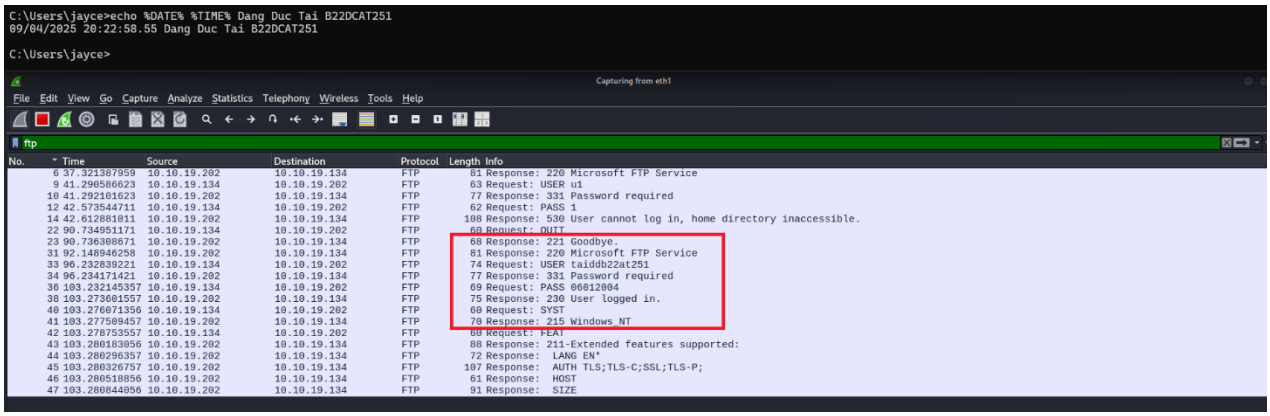
- Đăng nhập lại vào ftp trên máy Kali Linux attack, nhưng lần này đăng nhập thành công

  ftp 10.10.19.202



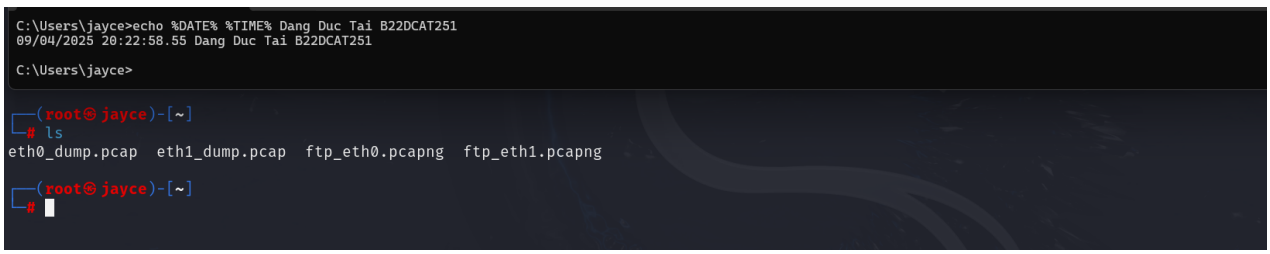
Hình 22 Thực hiện phiên ftp tới máy windows server

- Lọc các gói tin ftp trên wireshark và quan sát thấy phiên các thông báo đăng nhập thành công (230 User logged in) được hiển thị



Hình 23 Lọc các gói tin ftp trên wireshark với mạng eth1

- Các file bắt được trong bài này

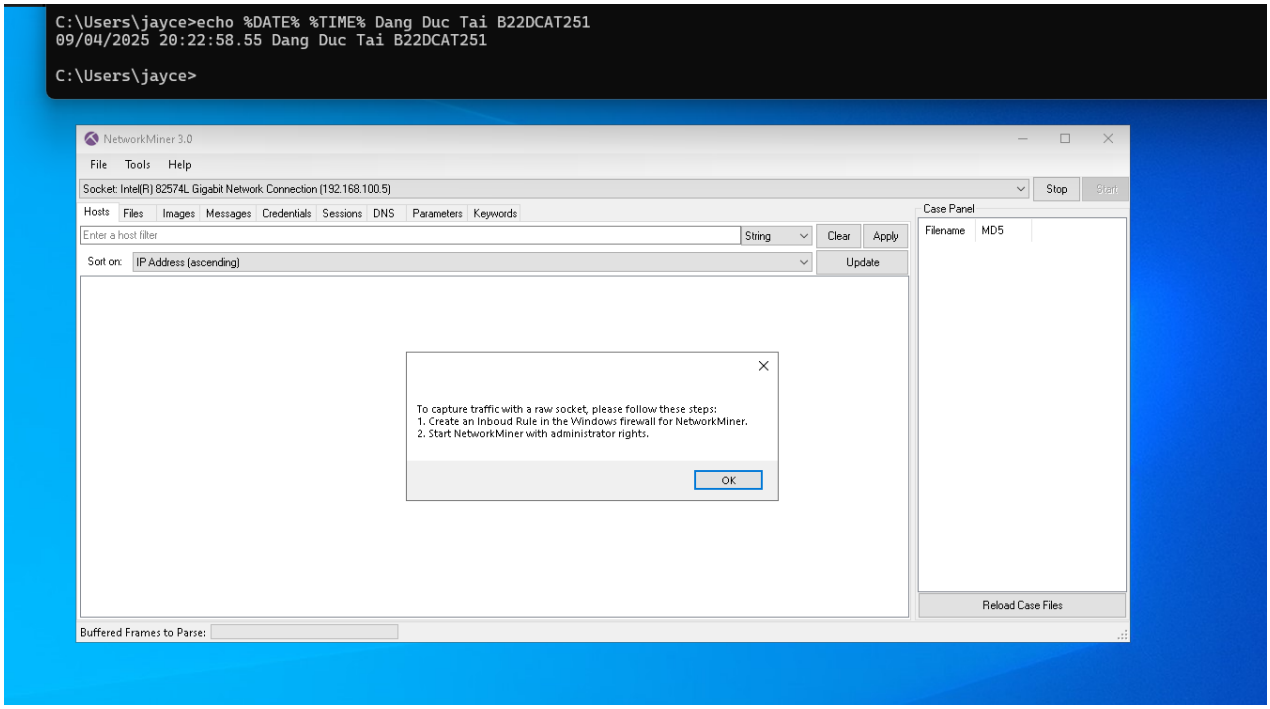


Hình 24 Các file pcap bắt được

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

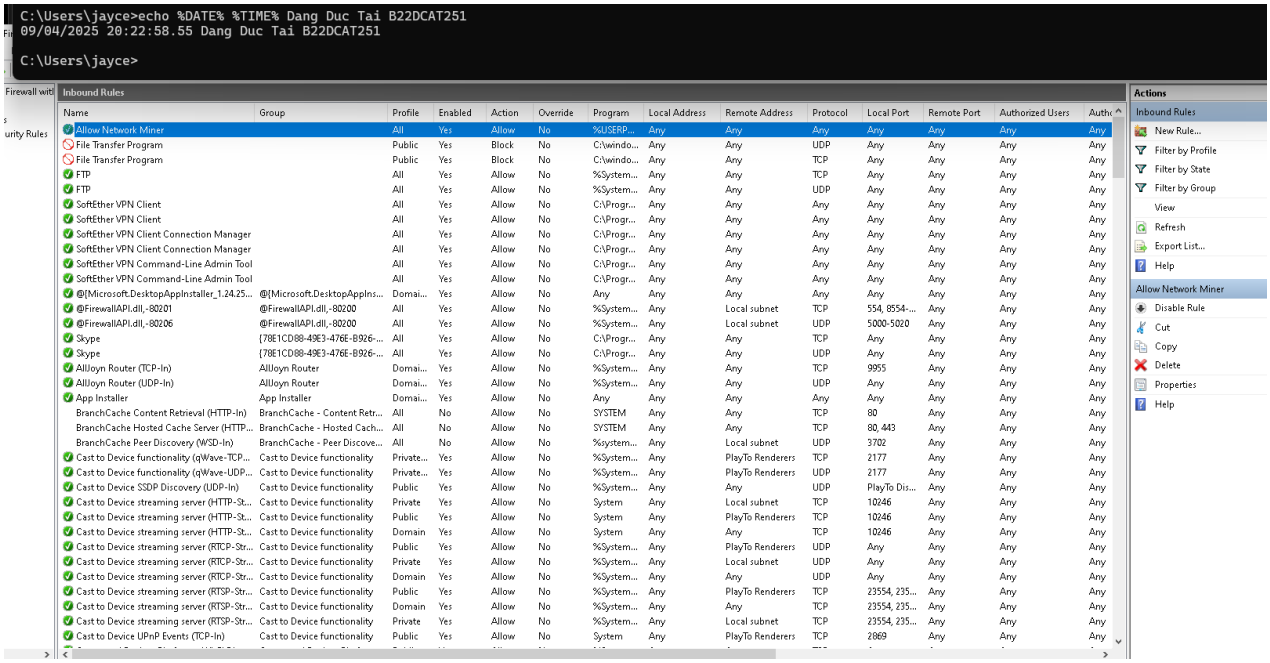
- Cài đặt network miner tại

- Giao diện của network miner, trong bài này sử dụng Socket: Intel® 82574L Gigabit Network Connection(192.168.100.5), tuy nhiên phải thực hiện các việc sau để có thể bắt gói tin bằng network miner
- Tạo Inboud Rule trên windows firewall cho network miner
- Chạy network miner với quyền admin



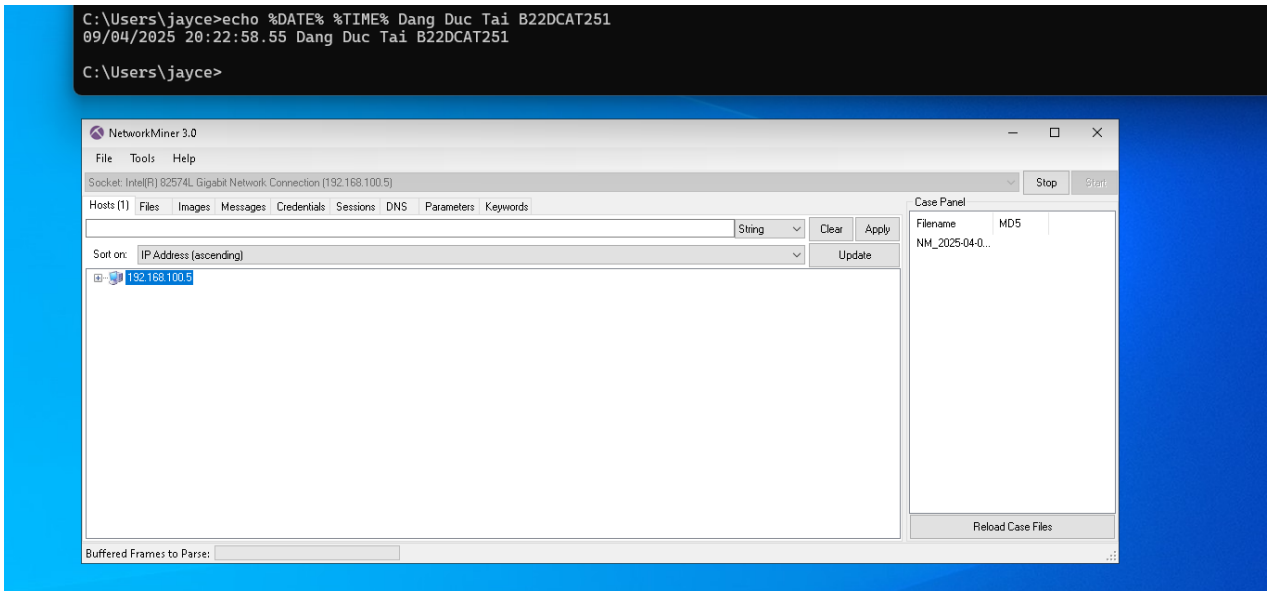
Hình 25 Giao diện network miner

- Tiến hành tạo Rule Inboud trên windows firewall cho network miner



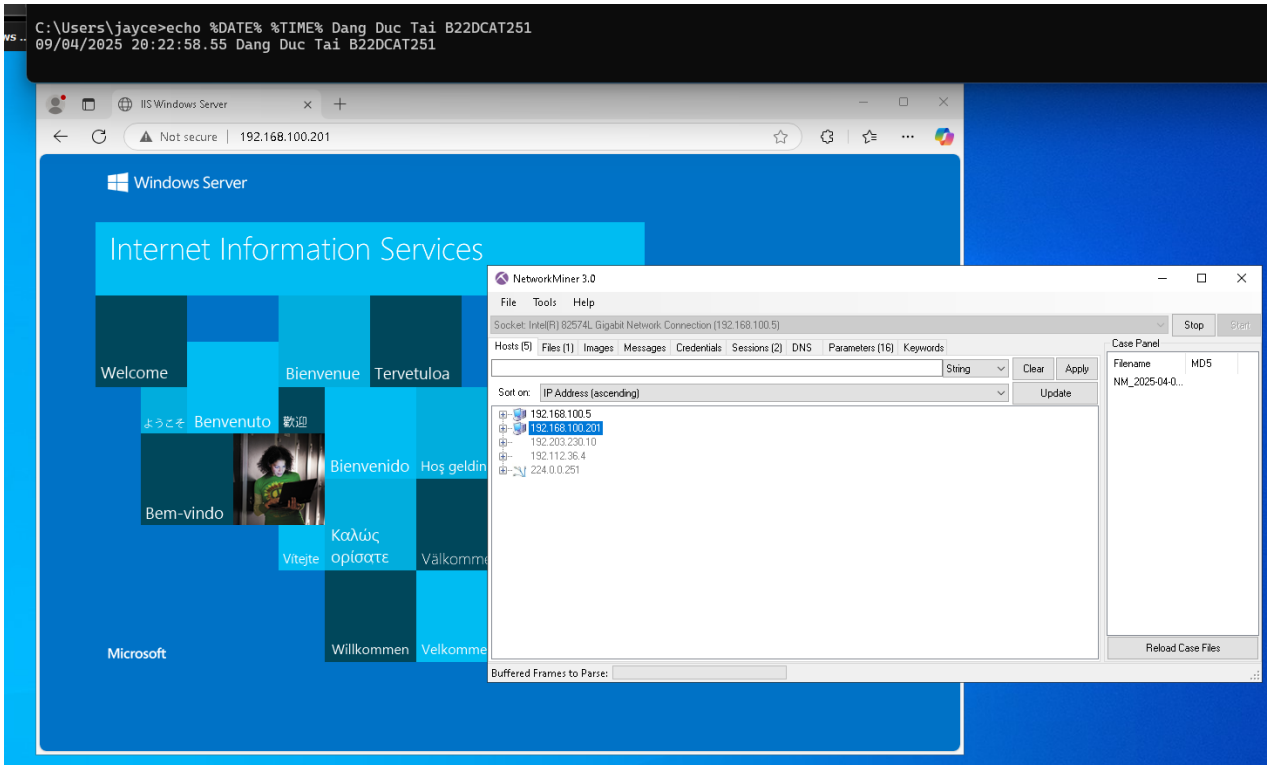
Hình 26 Tạo rule inboud cho network miner

- Chạy lại network miner với quyền admin, bắt gói tin trên Socket (192.168.100.5) đã chọn



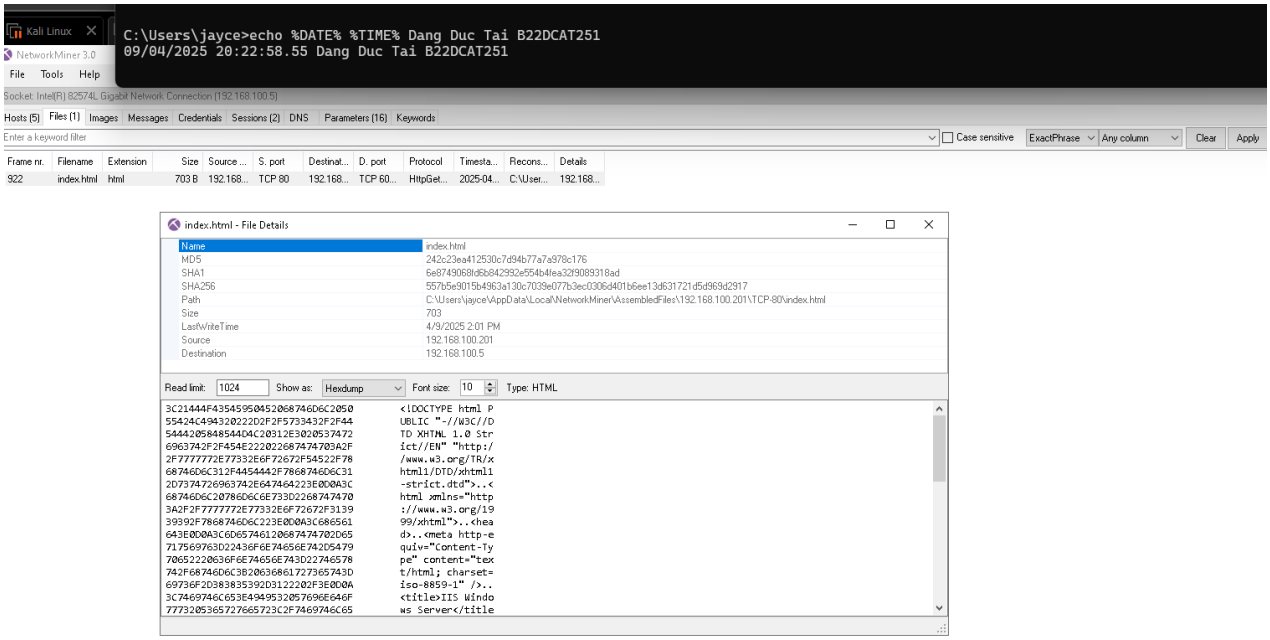
Hình 27 Bắt gói tin trên Socket

- Cùng lúc đó, truy cập vào Windows Server tại địa chỉ [http://192.168.100.201/.](http://192.168.100.201/)



Hình 28 Truy cập địa chỉ của Windows Server

- Dừng bắt gói tin, chọn File/ index.html để xem dữ liệu gói tin vừa bắt được.



Hình 29 Xem gói html bắt được

TÀI LIỆU THAM KHẢO

[1] Chương 4, Bài giảng Kỹ thuật theo dõi giám sát an toàn mạng, HVCN BCVT 2021

[2] https://www.tcpdump.org/index.html#documentation

[3] https://www.wireshark.org/docs/wsug_html/

[4] https://docs.securityonion.net/en/2.3/networkminer.html#