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:

B22DCAT199 Đỗ Duy Nam

Giảng viên hướng dẫn: TS.Đinh Trường 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

- 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 Tcpdump

Công cụ tcpdump là một trong những phần mềm phân tích gói tin (packet analyzer) phổ biến nhất trên các hệ điều hành dựa trên Unix/Linux. Nó hoạt động ở giao diện dòng lệnh (command-line interface) và được sử dụng để bắt, phân tích và hiển thị lưu lượng mạng (network traffic) đi qua một giao diện mạng cụ thể.

a) Tính năng chính của tcpdump

- Bắt gói tin (Packet Capture):
  - Tcpdump có thể bắt tất cả các gói tin (packets) được truyền hoặc nhận qua một giao diện mạng cụ thể (ví dụ: eth0, wlan0).
  - Hỗ trợ bắt gói tin từ nhiều giao thức khác nhau như TCP, UDP, ICMP, ARP, v.v., không chỉ giới hạn ở TCP như tên gọi của nó.
- Lọc lưu lượng (Filtering):
  - Sử dụng cú pháp bộ lọc Berkeley Packet Filter (BPF) để chỉ bắt các gói tin đáp ứng tiêu chí cụ thể, ví dụ: theo địa chỉ IP, cổng (port), giao thức, hoặc hướng lưu lượng (source/destination).
  - Ví dụ: tcpdump host 192.168.1.1 chỉ bắt lưu lượng từ hoặc đến IP 192.168.1.1.
- Hiển thị chi tiết gói tin:
  - Cung cấp thông tin chi tiết về tiêu đề (header) của gói tin như địa chỉ IP nguồn/đích, cổng nguồn/đích, giao thức, thời gian, và các cờ (flags) trong TCP.
  - Có thể hiển thị nội dung gói tin ở dạng ASCII hoặc HEX nếu cần (với tùy chọn -A hoặc -x).
- Lưu trữ và đọc lại dữ liệu:
  - Lưu các gói tin đã bắt vào file định dạng .pcap (dùng tùy chọn -w) để phân tích sau này.
  - Đọc lại file .pcap đã lưu bằng tùy chọn -r, hoặc mở bằng các công cụ đồ họa như Wireshark.
- Hoạt động thời gian thực (Real-time Monitoring):
  - Hiển thị lưu lượng mạng ngay khi nó được bắt, giúp theo dõi trực tiếp các sự kiện mạng.
- Tùy chỉnh linh hoạt:

    - Hỗ trợ nhiều tùy chọn dòng lệnh để điều chỉnh mức độ chi tiết (verbose), số lượng gói tin bắt được, kích thước gói tin (snaplen), v.v.
- Nhẹ và đa nền tảng:
    - Tcpdump rất nhẹ, không yêu cầu giao diện đồ họa (GUI), phù hợp cho các hệ thống nhúng hoặc máy chủ từ xa.
    - Có sẵn trên hầu hết các hệ điều hành Unix/Linux và có phiên bản cho Windows (WinDump).

b) Cách hoạt động của tcpdump

Tcpdump hoạt động dựa trên thư viện libpcap (Packet Capture library), một giao diện lập trình độc lập với hệ thống, cho phép nó truy cập vào tầng liên kết dữ liệu (data link layer) của mạng.

- Chọn giao diện mạng:
    - Người dùng chỉ định giao diện mạng để bắt gói tin (dùng tùy chọn -i, ví dụ: -i eth0). Nếu không chỉ định, tcpdump sẽ chọn giao diện mặc định.
    - Có thể dùng -i any để bắt trên tất cả các giao diện.
- Chuyển giao diện sang chế độ Promiscuous (nếu cần):
- Mặc định, tcpdump đặt giao diện mạng vào chế độ "promiscuous", cho phép bắt tất cả lưu lượng đi qua giao diện, kể cả các gói không gửi đến máy chủ đang chạy tcpdump.
- Có thể tắt chế độ này bằng tùy chọn -p nếu chỉ muốn bắt lưu lượng liên quan trực tiếp đến máy.
- Bắt gói tin:
    - Tcpdump sử dụng libpcap để "nghe" (listen) các gói tin từ giao diện mạng.
    - Mỗi gói tin được bắt sẽ bao gồm tiêu đề (header) và dữ liệu (payload), nhưng kích thước mặc định chỉ giới hạn ở 68 hoặc 96 byte (có thể tăng bằng tùy chọn -s).
- Áp dụng bộ lọc (nếu có):
    - Nếu người dùng cung cấp bộ lọc (filter), tcpdump sẽ chỉ xử lý các gói tin phù hợp với điều kiện lọc, bỏ qua các gói khác.
    - Ví dụ: tcpdump port 80 chỉ bắt lưu lượng HTTP.
- Hiển thị hoặc lưu trữ:
    - Gói tin được hiển thị trên màn hình dưới dạng tóm tắt (summary) hoặc chi tiết hơn tùy thuộc vào tùy chọn (như -v, -vv).
    - Nếu dùng -w, dữ liệu được lưu vào file .pcap thay vì hiển thị.
- Kết thúc:
    - Người dùng dừng quá trình bằng cách nhấn Ctrl+C, hoặc tcpdump tự dừng sau khi bắt đủ số gói tin chỉ định (dùng -c).

1.2.2 Wireshark

Wireshark là một công cụ phân tích gói tin (packet analyzer) mã nguồn mở, nổi tiếng với giao diện đồ họa (GUI) thân thiện và khả năng phân tích sâu lưu lượng mạng. Không giống như tcpdump (chủ yếu hoạt động qua dòng lệnh), Wireshark cung cấp trải nghiệm trực quan hơn, phù hợp cho cả người mới bắt đầu và chuyên gia mạng.

a) Tính năng chính của Wireshark

- Bắt gói tin (Packet Capture):
    - Bắt tất cả lưu lượng mạng đi qua giao diện được chọn (ví dụ: Ethernet, Wi-Fi) hoặc đọc từ file .pcap đã lưu trước đó.
    - Hỗ trợ nhiều giao thức từ tầng liên kết dữ liệu (data link layer) đến tầng ứng dụng (application layer).
- Phân tích chi tiết gói tin:
    - Hiển thị cấu trúc từng gói tin theo dạng cây (tree view), phân tích từng trường trong tiêu đề (header) của giao thức (IP, TCP, UDP, HTTP, DNS, v.v.).
    - Hỗ trợ giải mã (decode) nội dung gói tin, ví dụ: xem nội dung HTTP, email, hoặc dữ liệu mã hóa nếu có khóa giải mã.
- Lọc và tìm kiếm mạnh mẽ:
    - Sử dụng bộ lọc hiển thị (display filter) để chỉ xem các gói tin đáp ứng tiêu chí cụ thể (ví dụ: http.request để xem yêu cầu HTTP).
    - Bộ lọc bắt gói (capture filter) tương tự tcpdump, dùng cú pháp BPF (ví dụ: port 80).
- Hỗ trợ giao thức đa dạng:
    - Wireshark nhận diện và phân tích hàng nghìn giao thức, từ TCP/IP cơ bản đến các giao thức ứng dụng như HTTP, FTP, VoIP, DNS, v.v.
    - Có thể phát hiện lỗi giao thức hoặc hành vi bất thường.
- Thống kê và trực quan hóa:
    - Cung cấp các công cụ thống kê như biểu đồ lưu lượng (I/O Graph), bảng phân bố giao thức, hoặc thời gian phản hồi (RTT).
    - Hiển thị luồng hội thoại (conversation) giữa các thiết bị.
- Lưu trữ và xuất dữ liệu:
    - Lưu gói tin vào file .pcap hoặc .pcapng (định dạng nâng cao).
    - Xuất dữ liệu sang định dạng khác (CSV, JSON) để phân tích thêm.
- Hỗ trợ đa nền tảng:

- Chạy trên Windows, macOS, Linux với giao diện đồ họa, hoặc dùng phiên bản dòng lệnh (tshark) nếu cần.

- Tùy chỉnh nâng cao:
  - Người dùng có thể thêm plugin, viết script Lua để mở rộng chức năng, hoặc tùy chỉnh cách hiển thị.

b) Cách hoạt động của Wireshark

Wireshark cũng dựa trên thư viện libpcap (trên Linux/Unix) hoặc WinPcap/Npcap (trên Windows) để bắt gói tin từ giao diện mạng.

- Chọn giao diện mạng:
  - Khi khởi động, Wireshark hiển thị danh sách giao diện mạng (Ethernet, Wi-Fi, v.v.). Người dùng chọn giao diện để bắt gói tin.
- Chuyển sang chế độ Promiscuous:
  - Mặc định, Wireshark bật chế độ "promiscuous" để bắt tất cả lưu lượng đi qua giao diện, không chỉ gói tin gửi đến máy tính.
  - Có thể tắt chế độ này trong cài đặt nếu cần.
- Bắt gói tin:
  - Wireshark sử dụng libpcap/Npcap để thu thập gói tin từ giao diện mạng.
  - Người dùng có thể áp dụng bộ lọc bắt gói (capture filter) để giảm tải dữ liệu (ví dụ: chỉ bắt lưu lượng HTTP).
- Hiển thị thời gian thực:
  - Gói tin được hiển thị ngay lập tức trong giao diện GUI, với ba khung chính:
    - Danh sách gói tin (Packet List): Tóm tắt mỗi gói (thời gian, nguồn, đích, giao thức).
    - Chi tiết gói tin (Packet Details): Cây phân tích từng tầng giao thức.
    - Dữ liệu thô (Packet Bytes): Dạng HEX và ASCII của gói tin.
- Áp dụng bộ lọc hiển thị:
  - Sau khi bắt, người dùng có thể lọc lại dữ liệu đã thu thập bằng bộ lọc hiển thị (display filter) để tập trung vào lưu lượng quan tâm.
- Phân tích và lưu trữ:
  - Dùng các công cụ tích hợp để phân tích (thống kê, theo dõi luồng TCP, v.v.).
  - Lưu dữ liệu vào file .pcap để sử dụng sau.

1.2.3 NetworkMiner

NetworkMiner à một công cụ phân tích mạng mã nguồn mở (open-source) được thiết kế chủ yếu cho mục đích phân tích pháp y mạng (network forensics). Nó khác biệt so với

tcpdump và Wireshark ở cách tiếp cận và mục tiêu sử dụng, tập trung vào việc trích xuất thông tin chi tiết về các thiết bị và dữ liệu từ lưu lượng mạng thay vì chỉ hiển thị gói tin thô.

a) Tính năng chính của NetworkMiner

NetworkMiner được phát triển bởi NETRESEC và có cả phiên bản miễn phí lẫn trả phí (NetworkMiner Professional).

- Bắt gói tin thụ động (Passive Packet Capture):
  - NetworkMiner có thể bắt lưu lượng mạng trực tiếp (live sniffing) hoặc phân tích file .pcap đã được ghi lại trước đó.
  - Không gửi bất kỳ gói tin nào ra mạng, giúp nó hoạt động "thầm lặng" và không ảnh hưởng đến lưu lượng.
- Trích xuất dữ liệu (Artifact Extraction):
  - Tự động trích xuất các tệp (files), hình ảnh, email, chứng chỉ (certificates), và thông tin đăng nhập (credentials) từ lưu lượng mạng.
  - Hỗ trợ các giao thức như HTTP, FTP, TFTP, SMB, SMTP, POP3, IMAP, v.v.
  - Ví dụ: Có thể tái tạo file ảnh hoặc video được truyền qua mạng từ YouTube hoặc các trang web khác.
- Xác định thiết bị (Host Identification):
  - Tạo danh sách thiết bị (host inventory) dựa trên địa chỉ IP, bao gồm thông tin như hệ điều hành (OS), tên máy (hostname), cổng mở (open ports), và địa chỉ MAC.
  - Dùng kỹ thuật nhận diện thụ động (passive fingerprinting) để đoán OS mà không cần quét chủ động.
- Phân tích thông tin đăng nhập (Credentials Analysis):
  - Trích xuất tên người dùng và mật khẩu từ các giao thức như FTP, HTTP, IMAP, POP3, hoặc thậm chí các dịch vụ trực tuyến như Gmail, Facebook (nếu không mã hóa).
  - Hiển thị thông tin này trong tab "Credentials".
- Tìm kiếm từ khóa (Keyword Search):
  - Cho phép tìm kiếm chuỗi hoặc mẫu byte cụ thể trong dữ liệu đã bắt hoặc lưu trữ.
- Giao diện thân thiện:
  - Tập trung vào thông tin theo từng host (host-centric) thay vì danh sách gói tin (packet-centric) như Wireshark, giúp dễ dàng phân tích hơn.
  - Hiển thị hình ảnh thu nhỏ (thumbnails) của các file ảnh trích xuất.

- Hỗ trợ đa nền tảng:
    - Chủ yếu thiết kế cho Windows, nhưng có thể chạy trên Linux, macOS, FreeBSD qua Mono (một framework .NET mã nguồn mở).
- Phiên bản di động (Portable):
    - Không cần cài đặt, có thể chạy trực tiếp từ USB hoặc thư mục giải nén.

b) Cách hoạt động của NetworkMiner

NetworkMiner cũng dựa trên thư viện libpcap (hoặc WinPcap/Npcap trên Windows) để bắt gói tin, nhưng cách xử lý và trình bày dữ liệu của nó khác biệt:

- Chọn nguồn dữ liệu:
    - Người dùng có thể chọn giao diện mạng để bắt trực tiếp (live capture) hoặc mở file .pcap đã ghi trước (offline analysis).
    - Trên Windows, cần chạy với quyền admin và cấu hình firewall để bắt gói tin thô (raw sockets).
- Bắt và phân tích gói tin:
    - NetworkMiner thu thập gói tin từ giao diện mạng hoặc file .pcap.
    - Phân tích thụ động, không tương tác trực tiếp với mạng.
- Tái tạo và trích xuất:
    - Tái tạo các luồng dữ liệu (streams) từ giao thức như HTTP, FTP, SMB để trích xuất tệp hoặc thông tin.
    - Ví dụ: Nếu một file PDF được tải qua HTTP, NetworkMiner sẽ lưu file đó vào thư mục cục bộ.
- Tổ chức dữ liệu theo host:
    - Dữ liệu được nhóm theo địa chỉ IP trong tab "Hosts", hiển thị thông tin như OS, hostname, số byte gửi/nhận, DNS queries, v.v.
    - Các tab khác như "Files", "Credentials", "Sessions" cung cấp chi tiết cụ thể.
- Hiển thị và lưu trữ:
    - Kết quả được hiển thị trong GUI, với các tab chuyên biệt cho từng loại dữ liệu (Hosts, Files, Messages, Credentials, v.v.).
    - Có thể lưu file trích xuất hoặc xuất báo cáo để phân tích thêm.

1.3 Kết chương

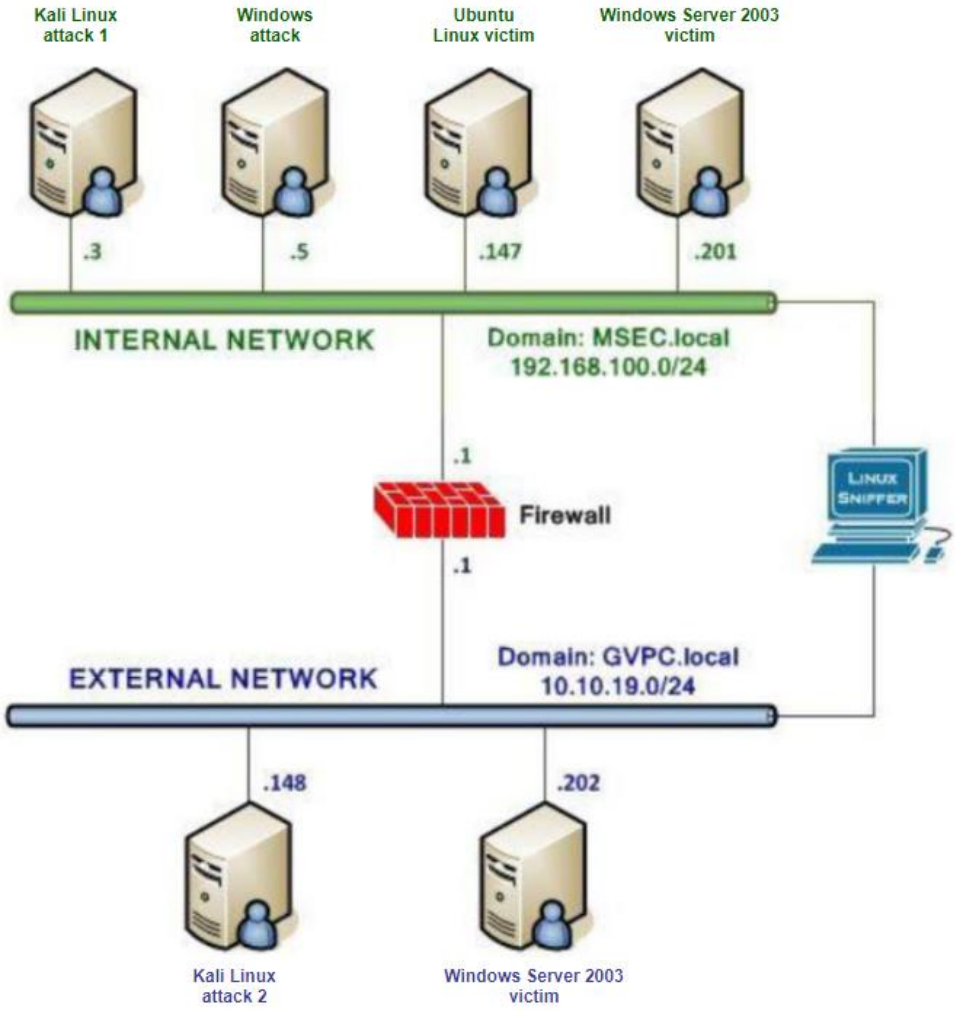
Ở chương này đã trình bày về các tính năng và cách hoạt động của một số công cụ bắt dữ liệu mạng như tcpdump, Wireshark và NetworkMiner.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Máy Windows attack
- Máy Windows Server Victim
- Máy Kali Linux attack
- Máy Linux Sniffer

Các máy cần được cấu hình địa chỉ IP như topo dưới đây:

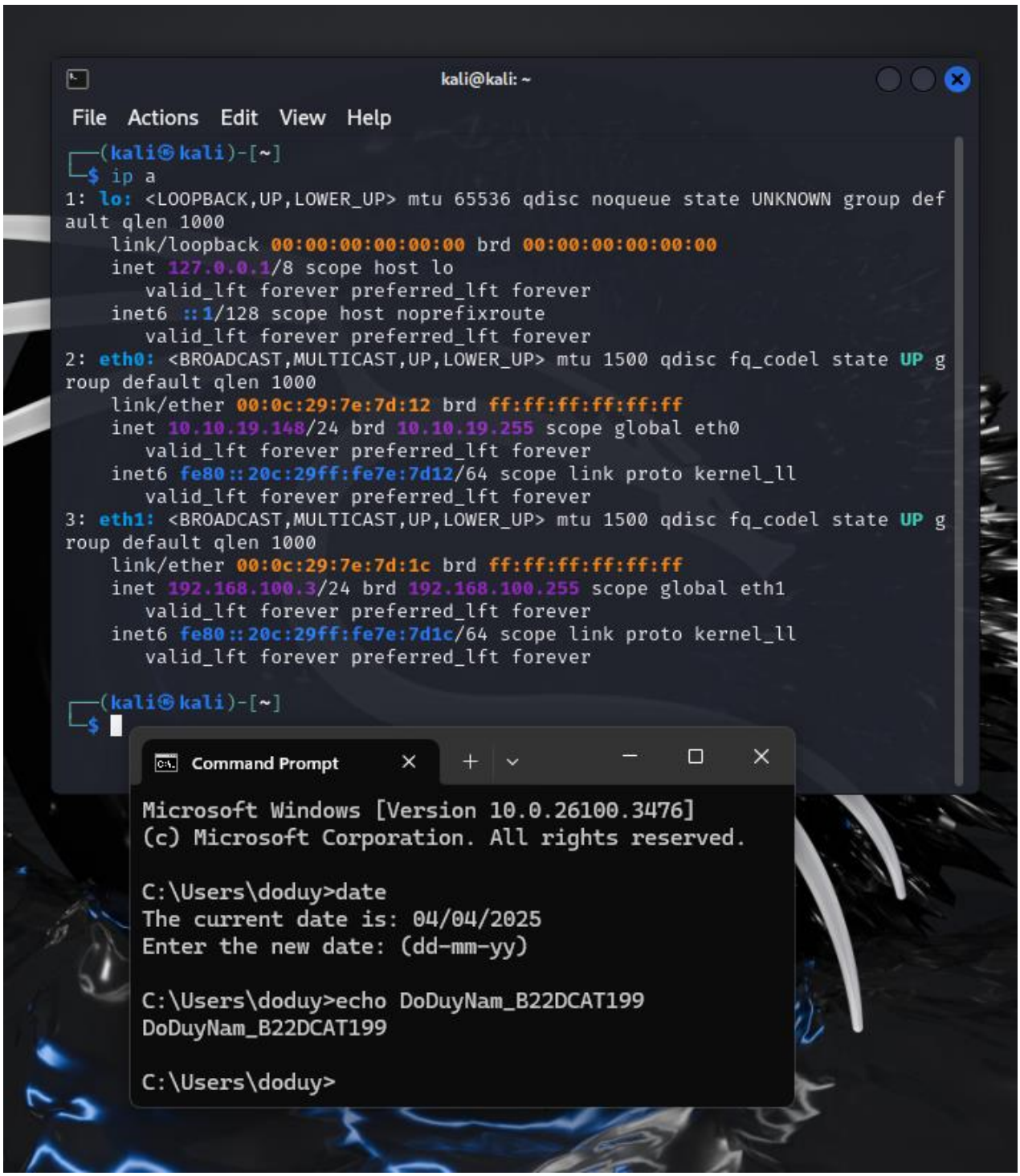


Hình 1 Cấu hình topo mạng

2.2 Các bước thực hiện

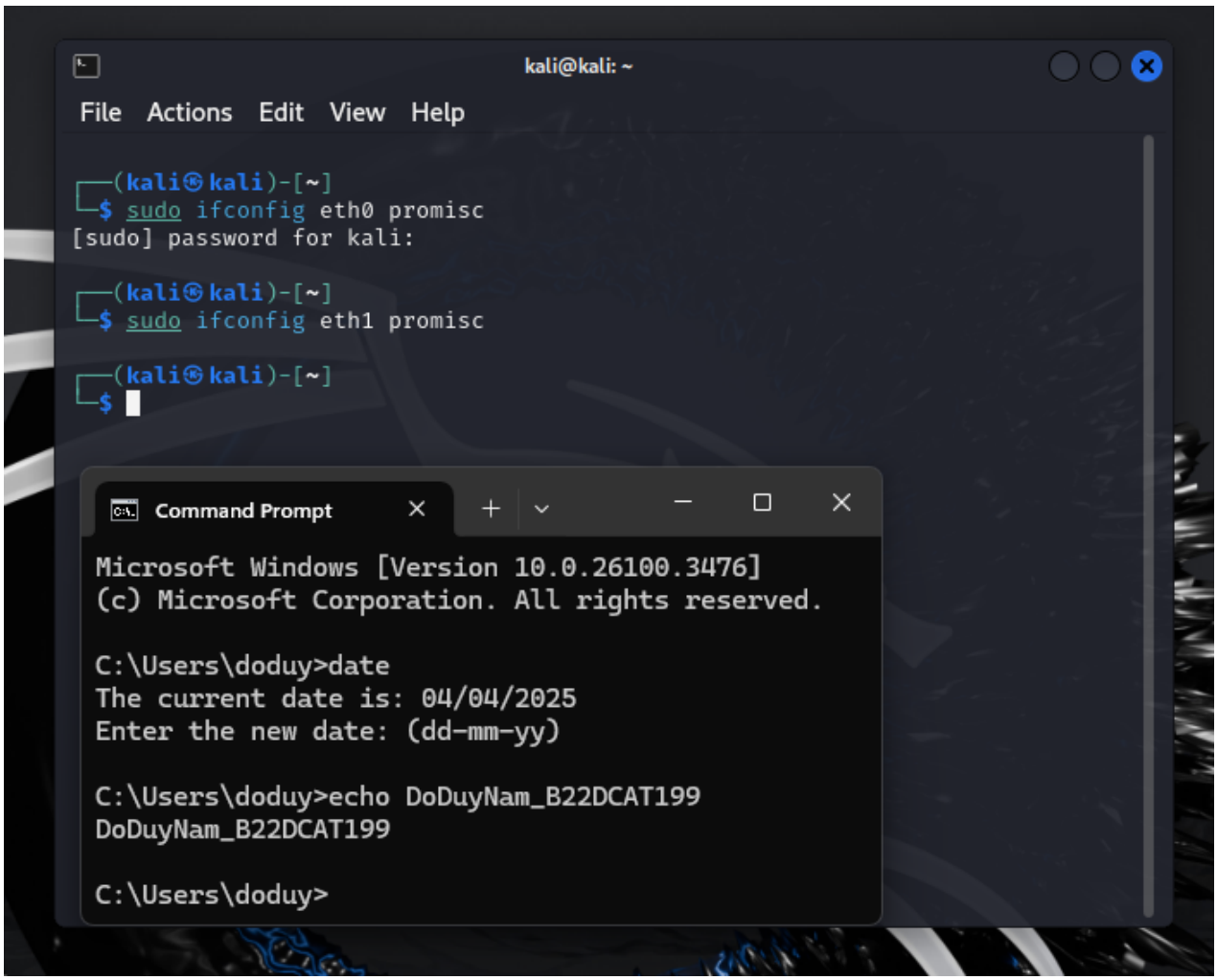
2.2.1 Sử dụng tcpdump

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



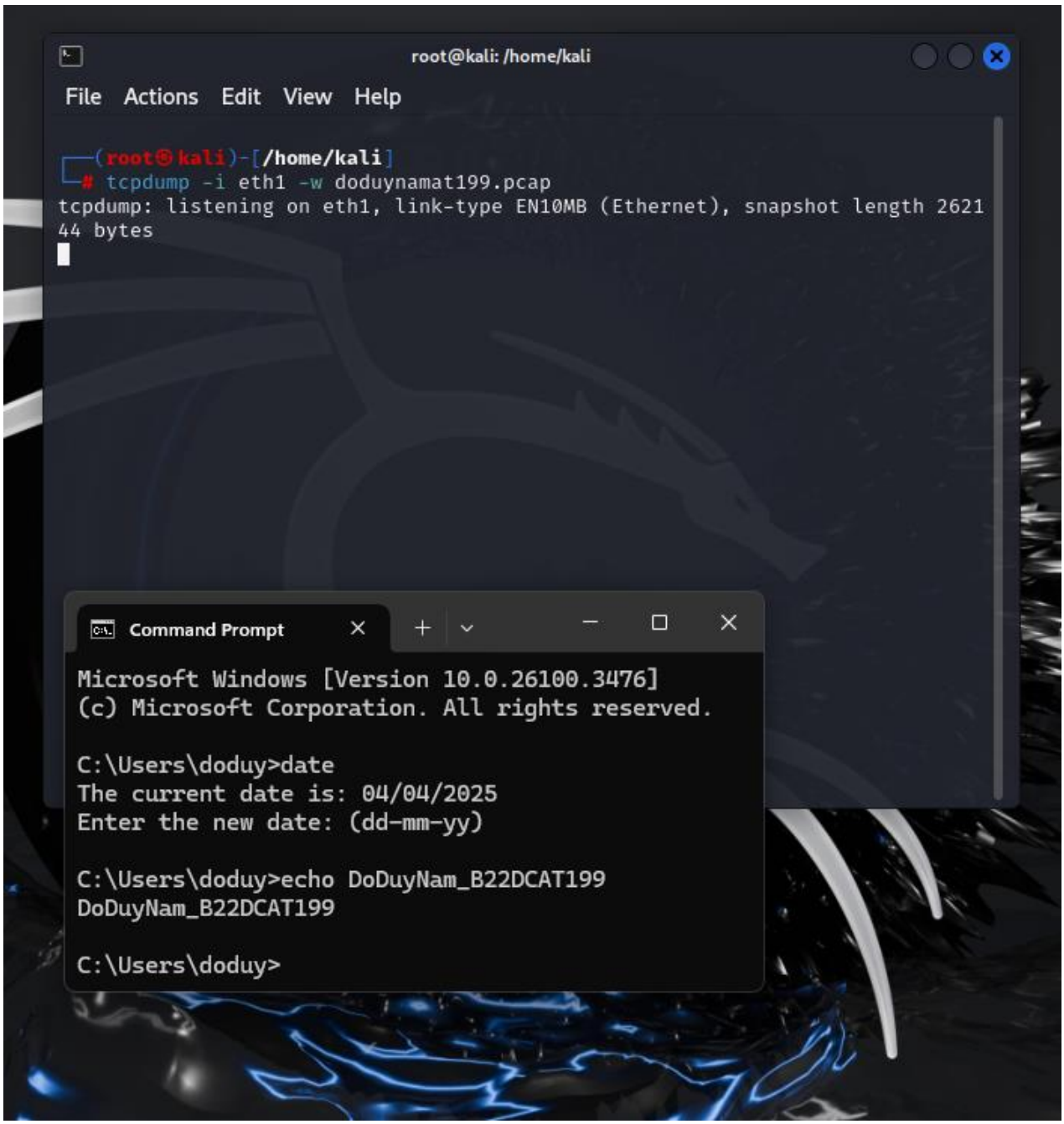
Hình 2 Các interfaces có trong hệ thống Linux Sniffer

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



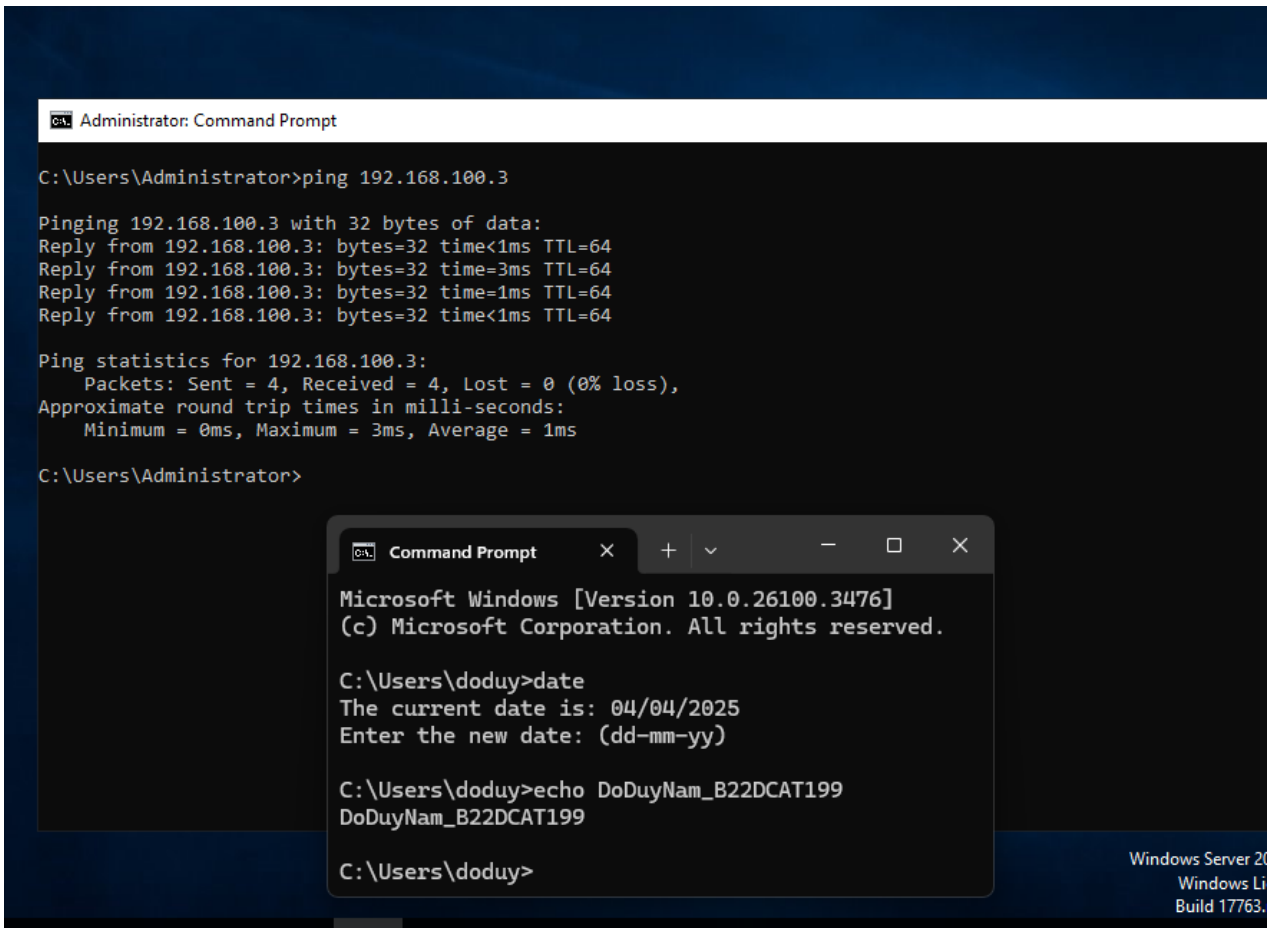
Hình 3 Kích hoạt các interfaces ở chế độ hỗn hợp

- Sau đó khởi động tcpdump. Bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file(thời gian chờ dữ liệu trong khoảng 5 phút).

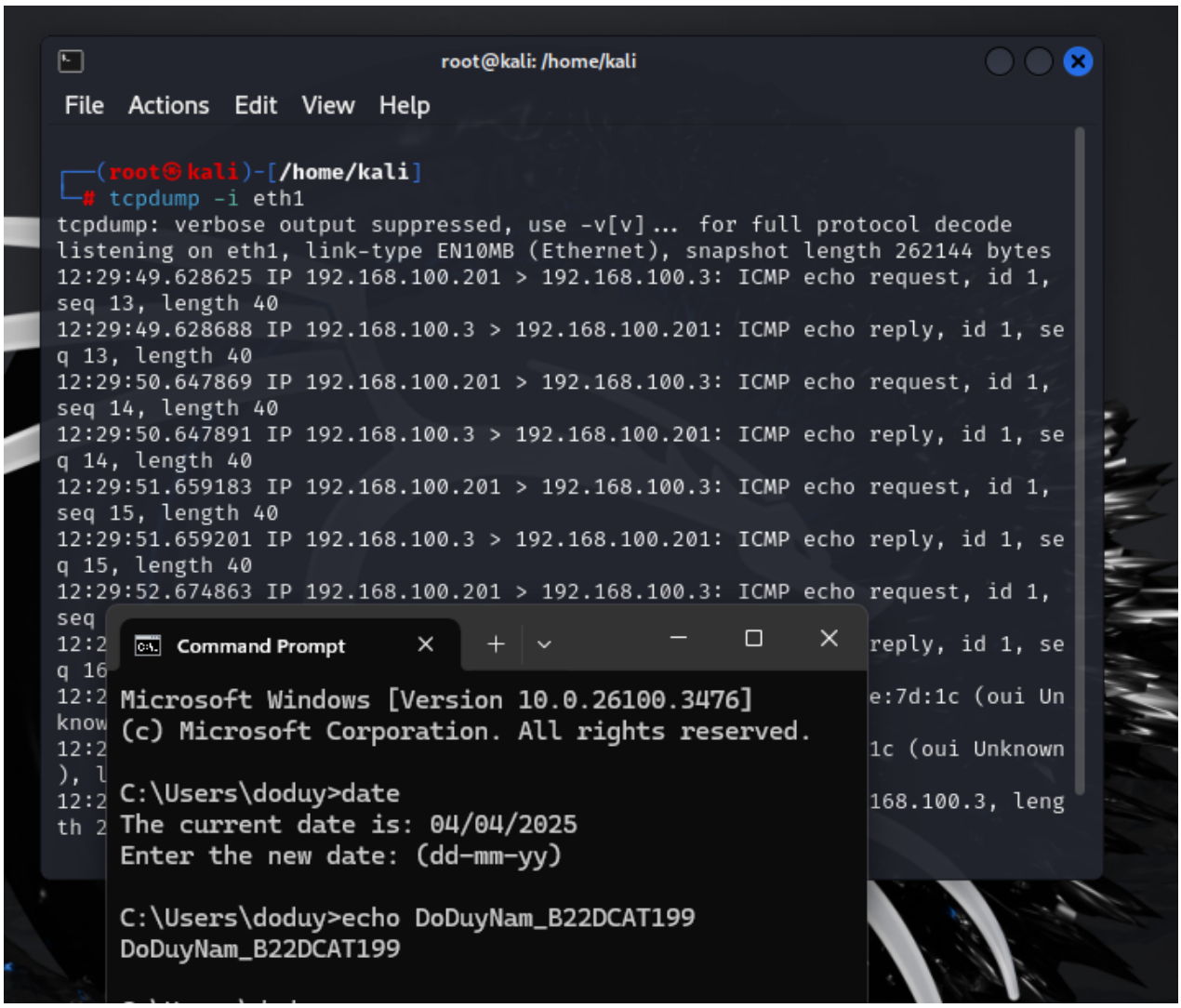


Hình 4 Bắt gói tin trên dải mạng 192.168.100.0/24

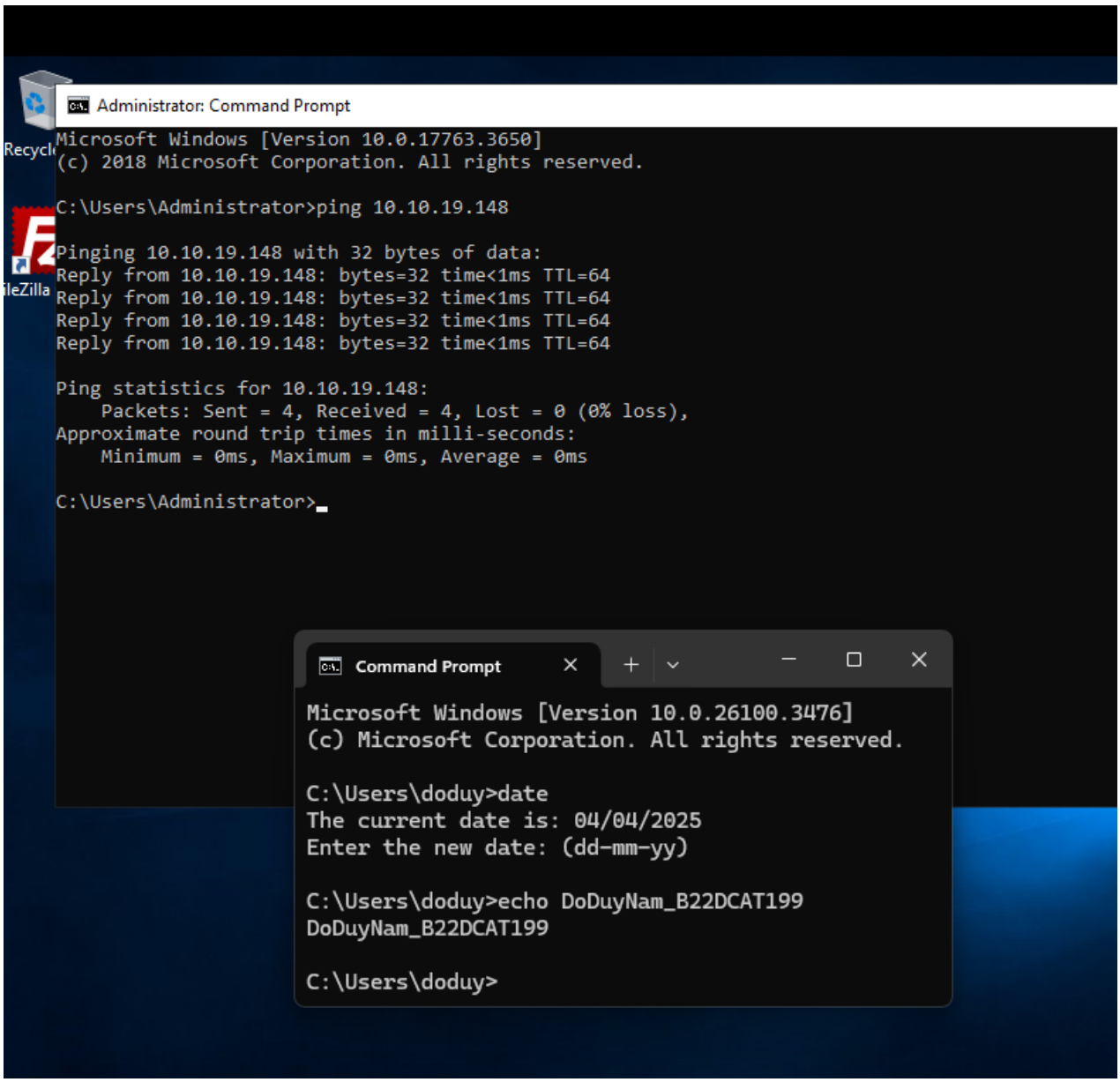
- Đăng nhập Window Server 2003 và tiến hành ping đến dải mạng internal và dải mạng external



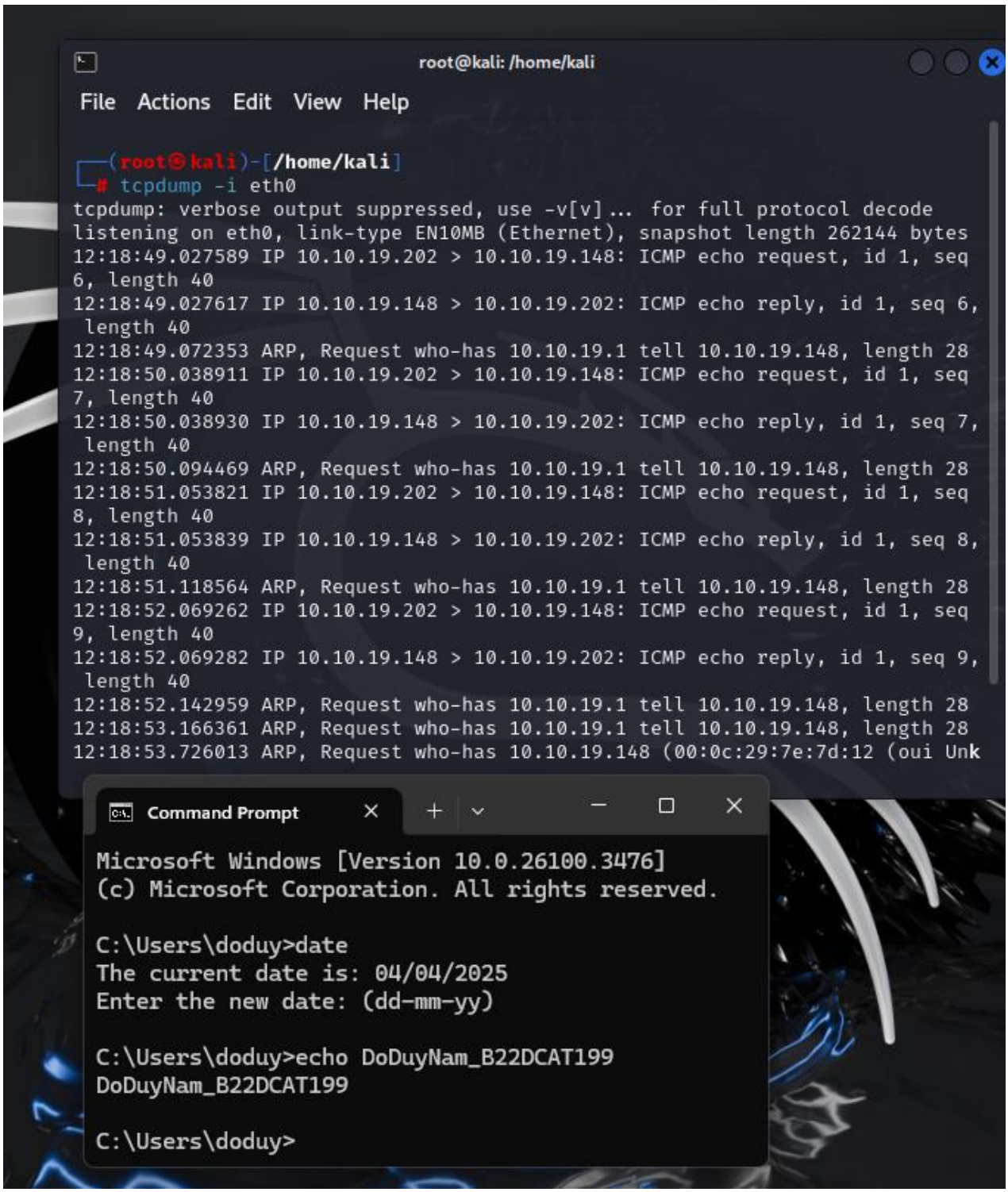
Hình 5 Máy Windows Server trên dải Internal ping đến máy Linux Sniffer



Hình 6 Trên máy Linux Sniffer, bắt gói tin trên dải 192.168.100.0/24

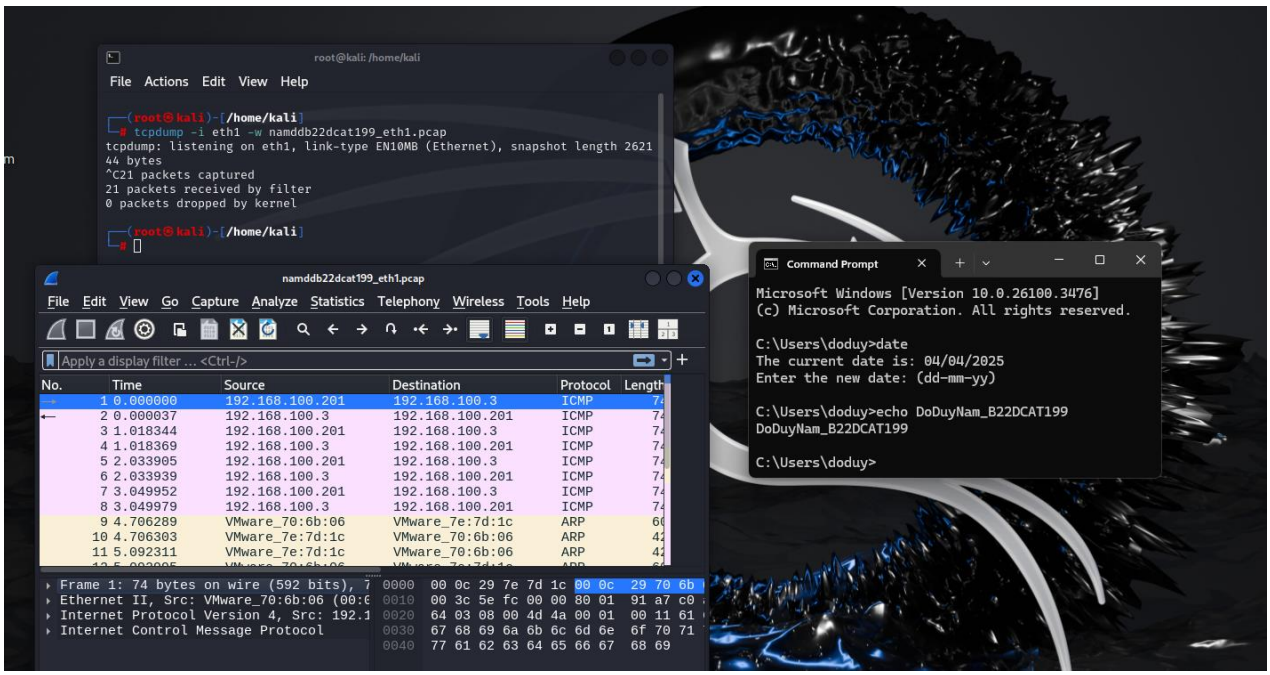


Hình 7 Trên máy Windows Server trên dải External ping đến máy Linux Sniffer

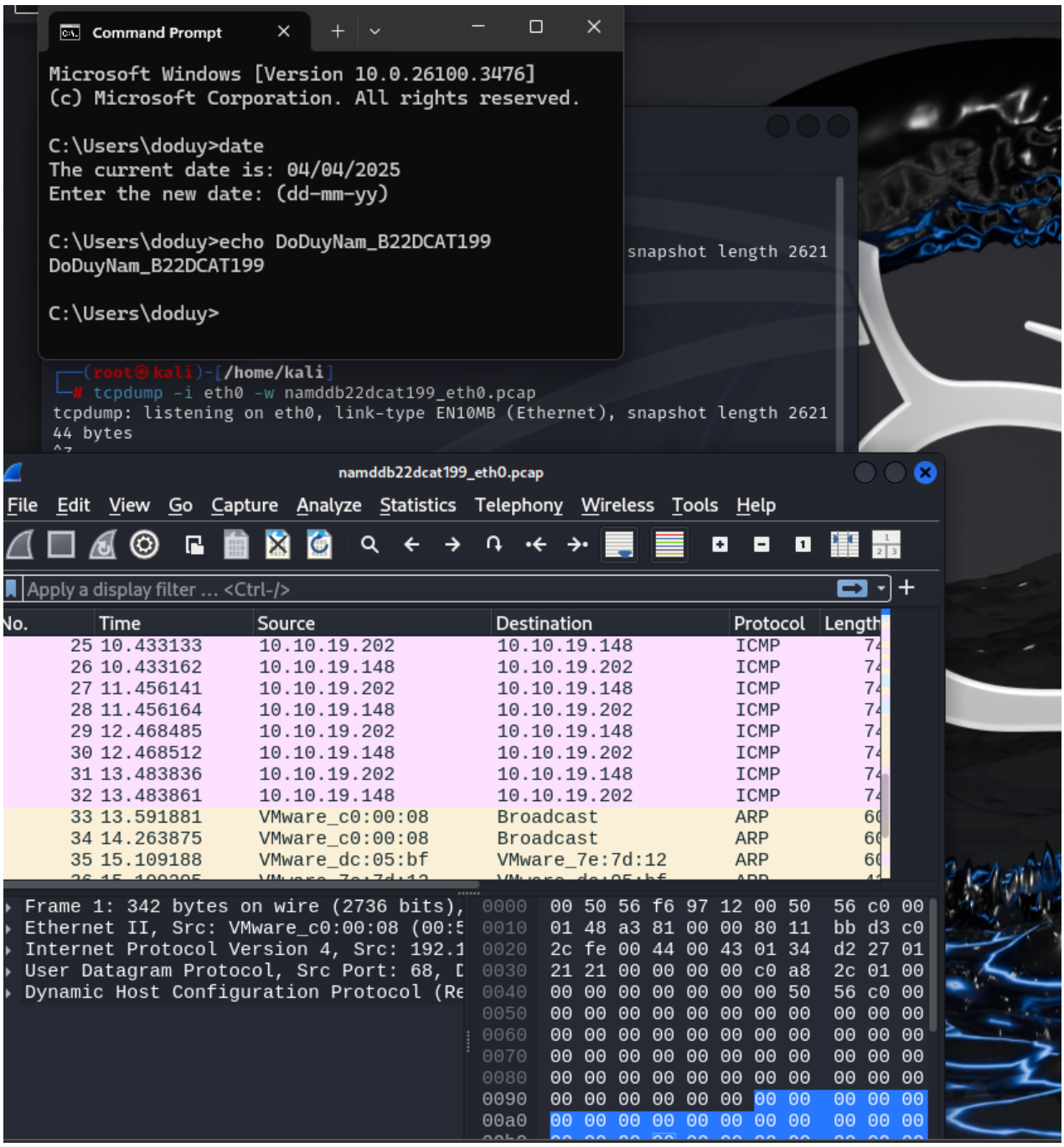


Hình 8 Trên máy Linux Sniffer, bắt gói tin trên dải 10.10.19.0/24

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



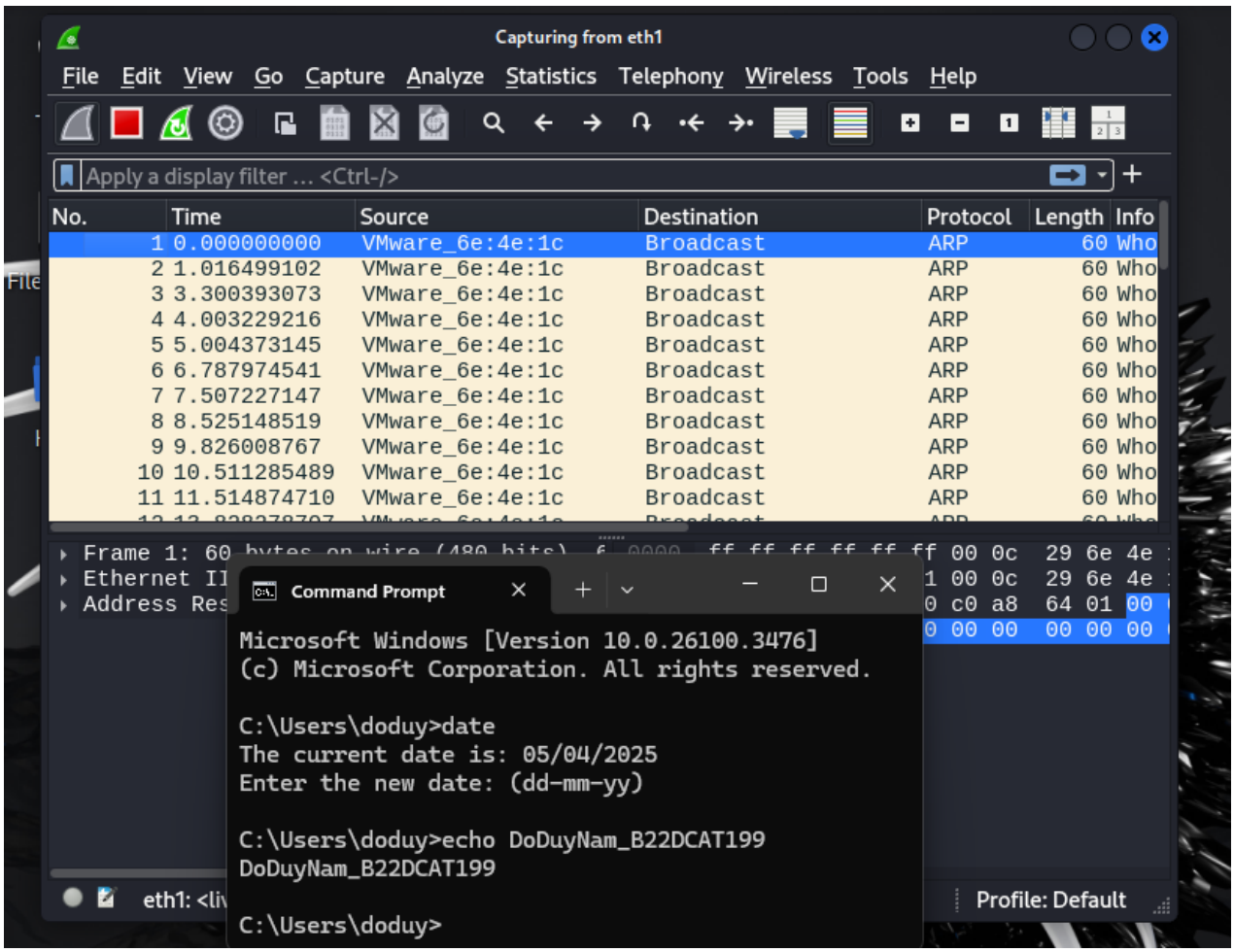
Hình 9 Các dữ liệu đã bắt trên dải Internal



Hình 10 Các dữ liệu đã bắt trên dải External

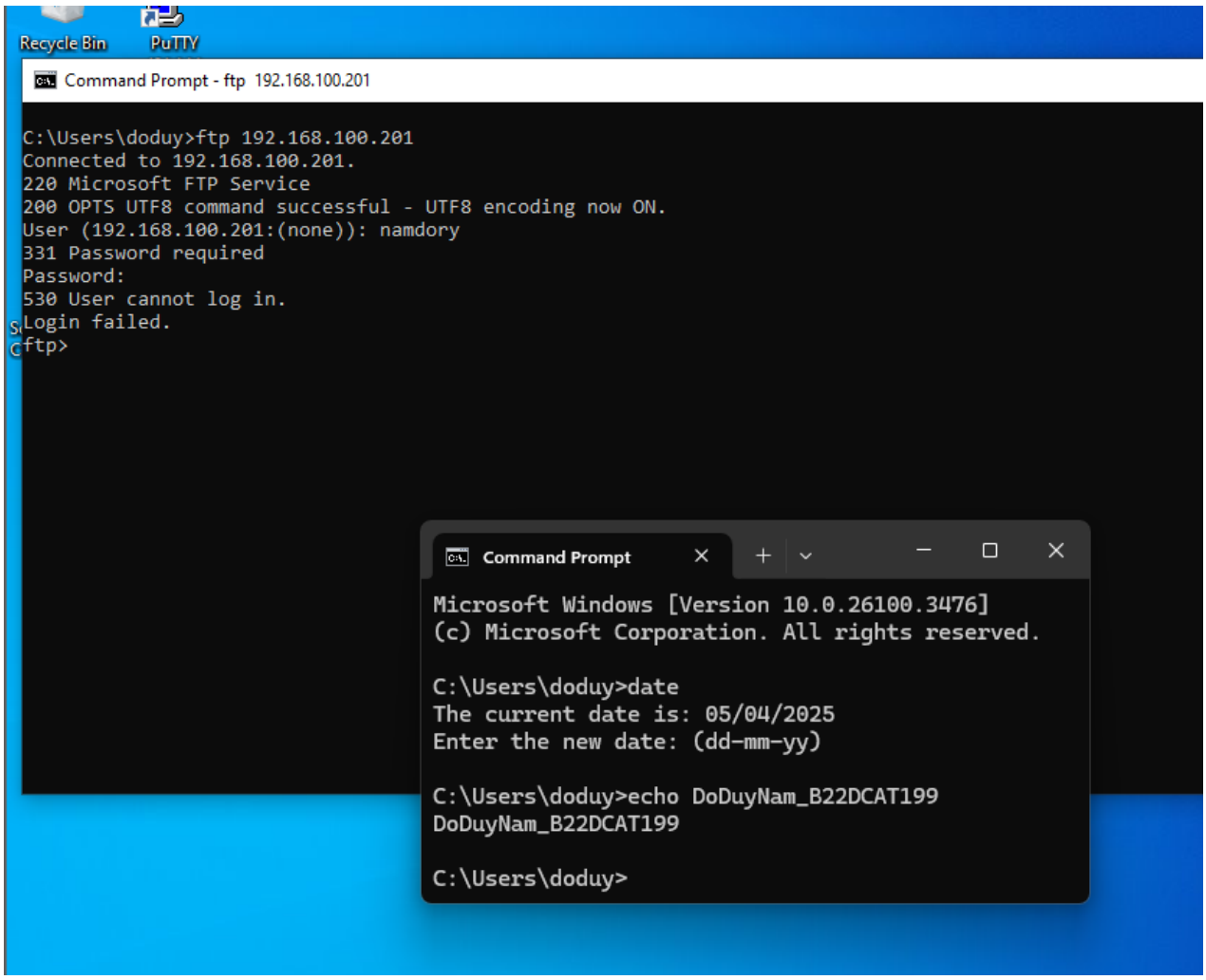
2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin

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



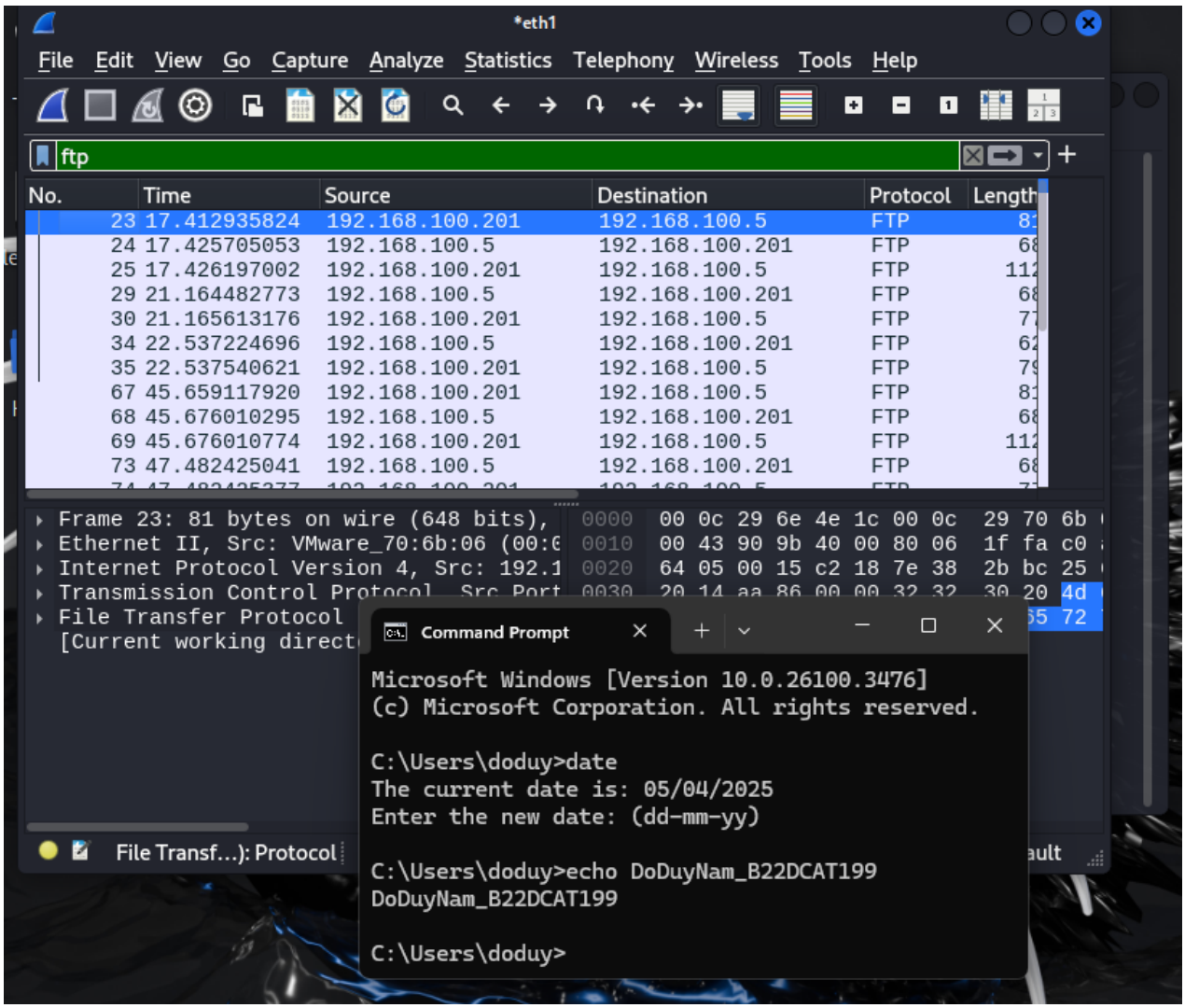
Hình 11 Khởi động WireShark trên máy Linux Sniffer chọn eth1 để bắt gói tin trên dải mạng 192.168.100.0

- Trên máy Windows attack kết nối tới ftp server trên máy Windows Server Internal Victim



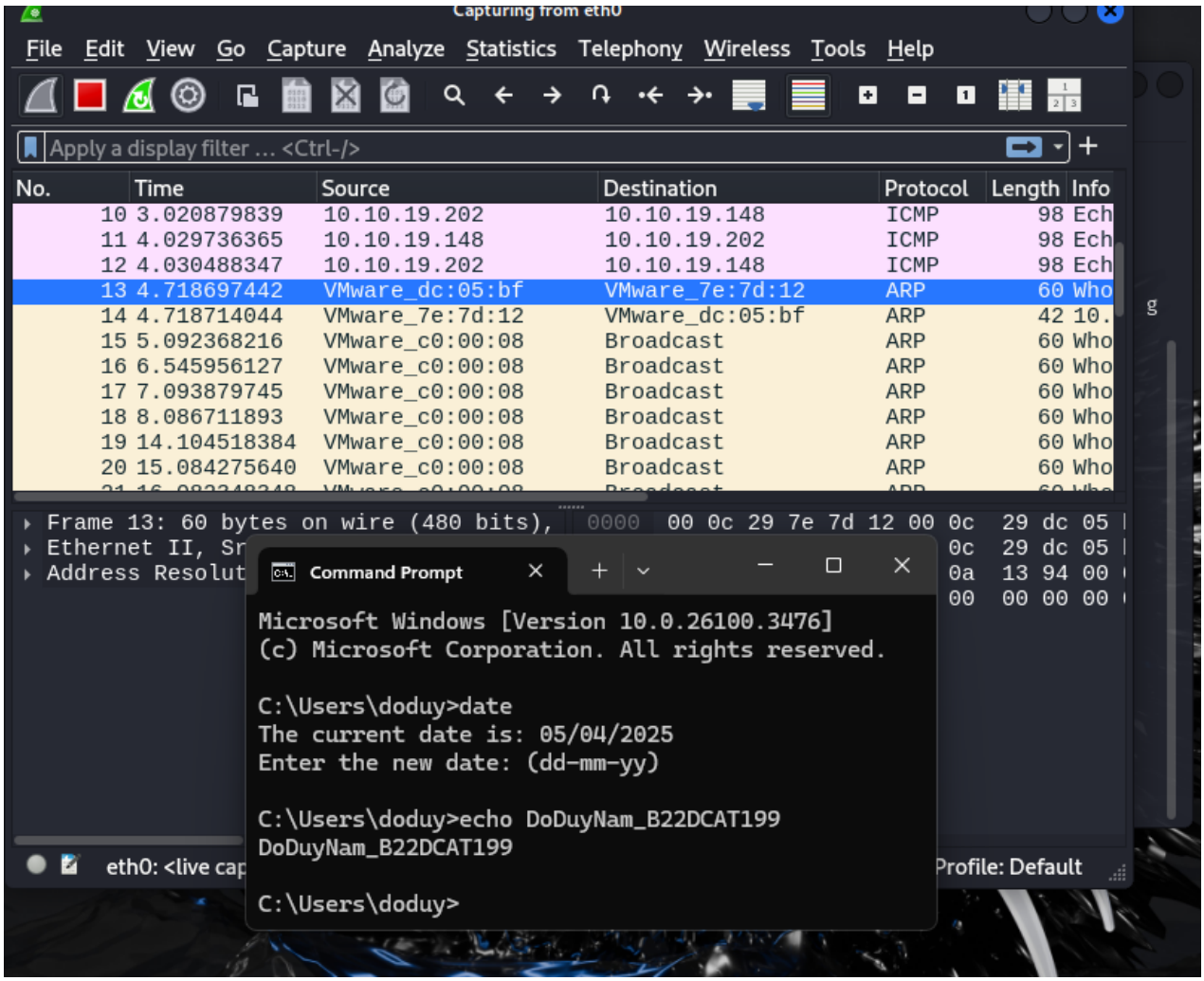
Hình 12 Máy Windows attack kết nối tới ftp Server trên máy Windows Server Internal

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



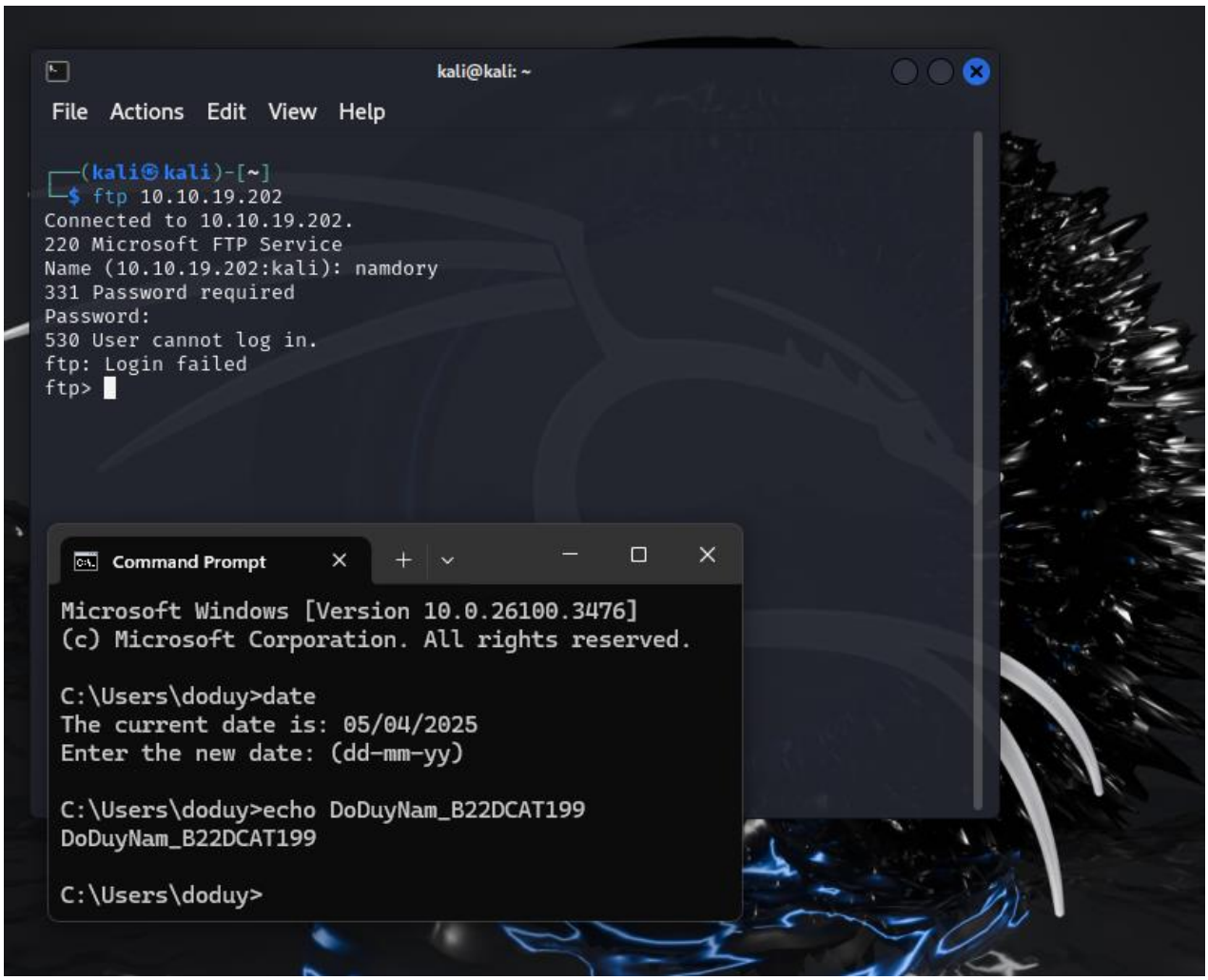
Hình 13 Lọc gói tin theo giao thức ftp

- Trên máy Linux Sniffer, trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 10.10.19.0



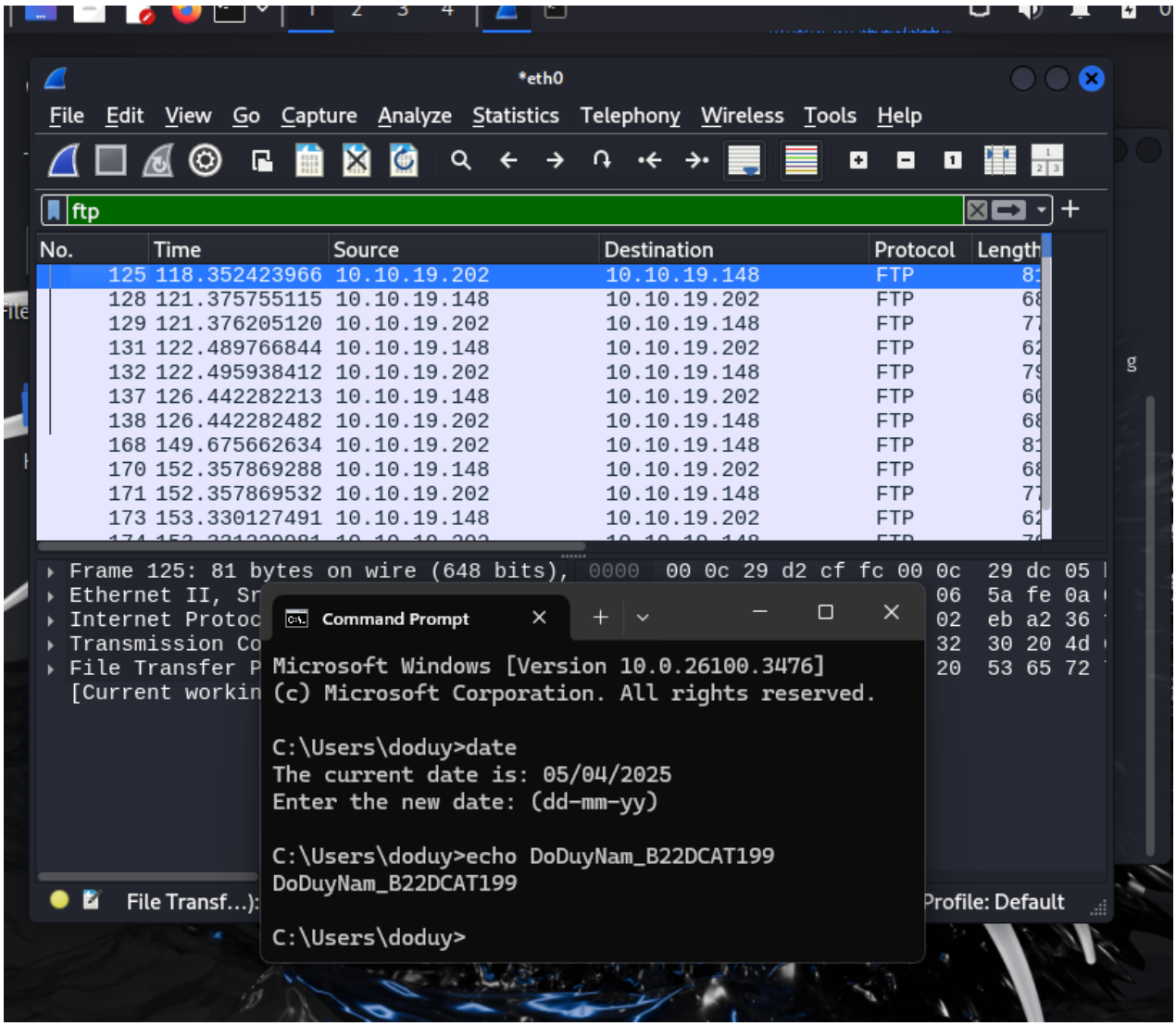
Hình 14 Khởi động WireShark trên máy Linux Sniffer chọn eth0 để bắt gói tin trên dải mạng 10.10.19.0

- Trên máy Kali Linux attack kết nối với ftp Server trên máy Windows Server Victim trong mạng External



Hình 15 Máy Kali Linux attack kết nối tới ftp Server trên máy Windows Server Internal

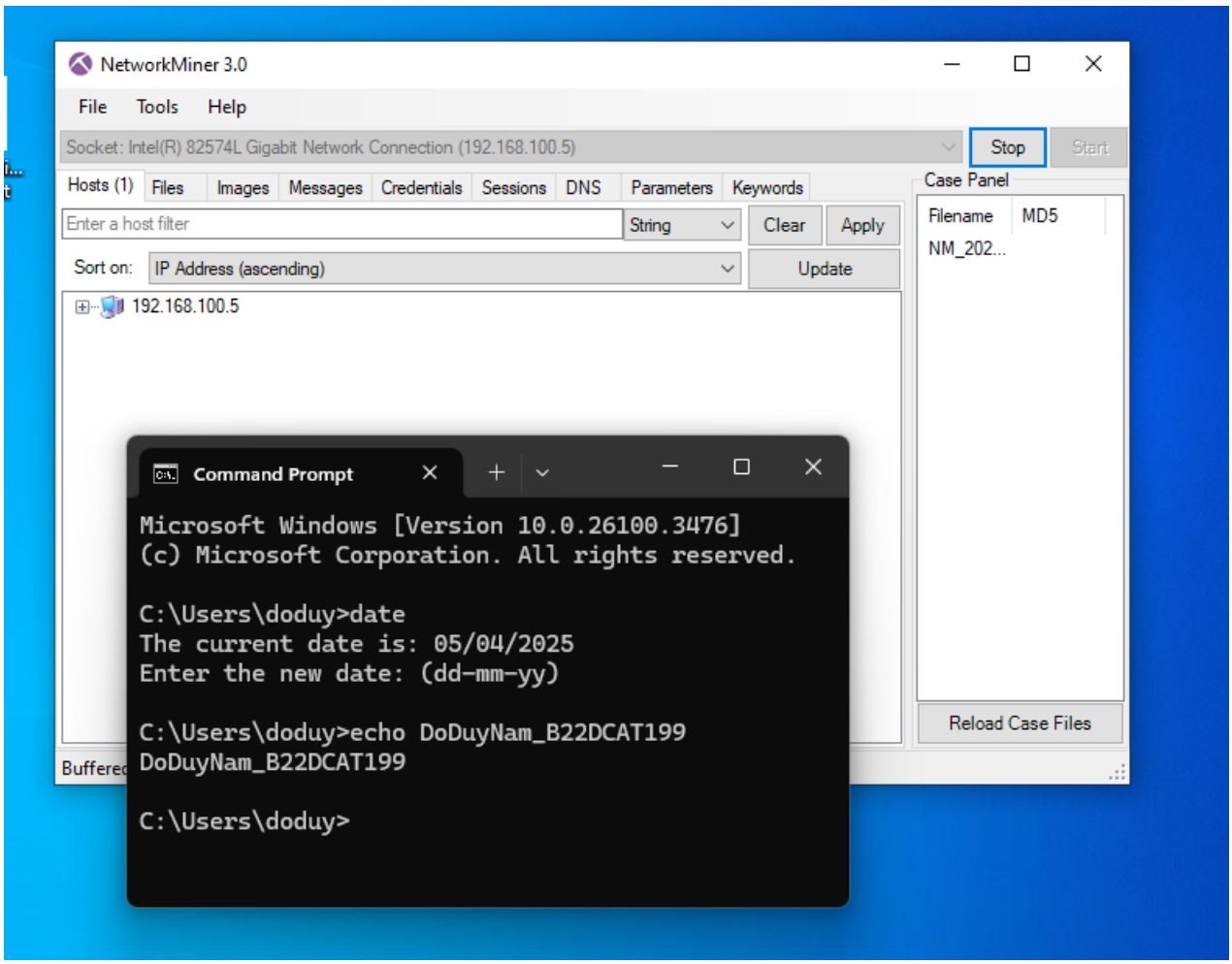
- Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



Hình 16 Lọc gói tin theo giao thức ftp

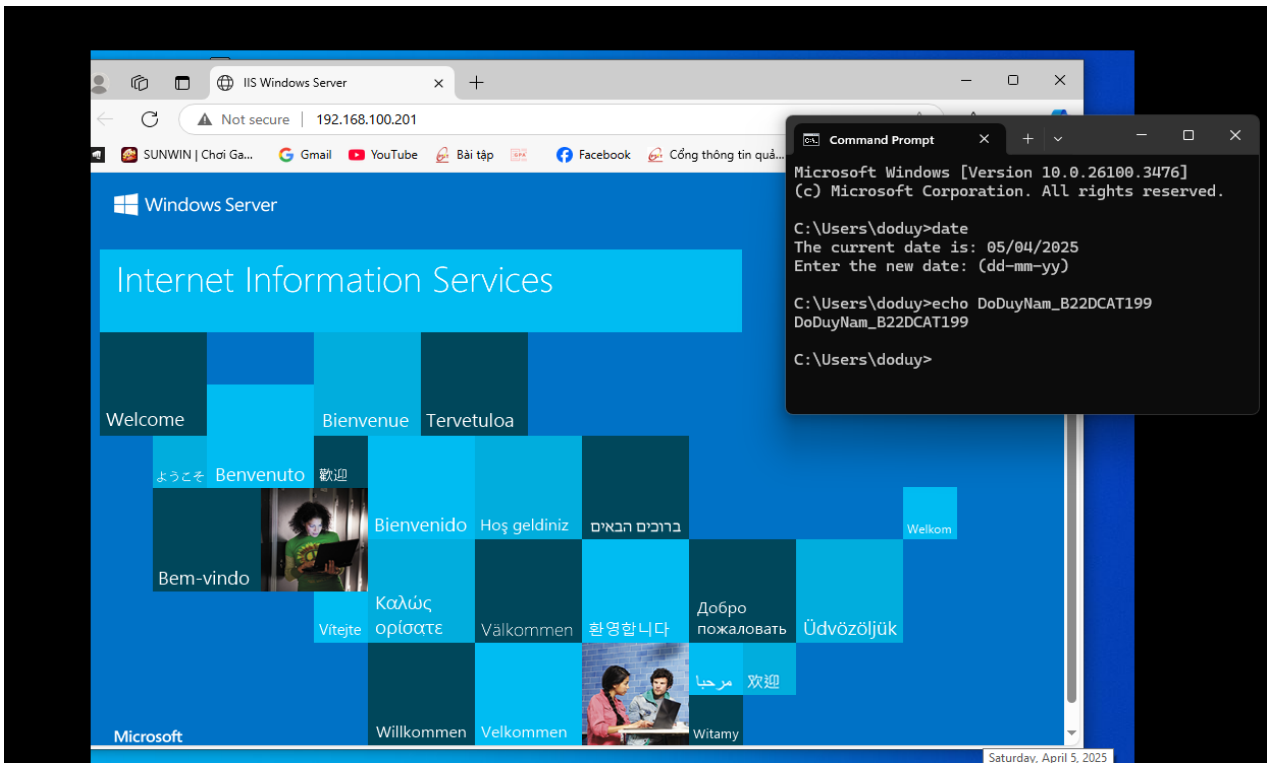
2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin

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



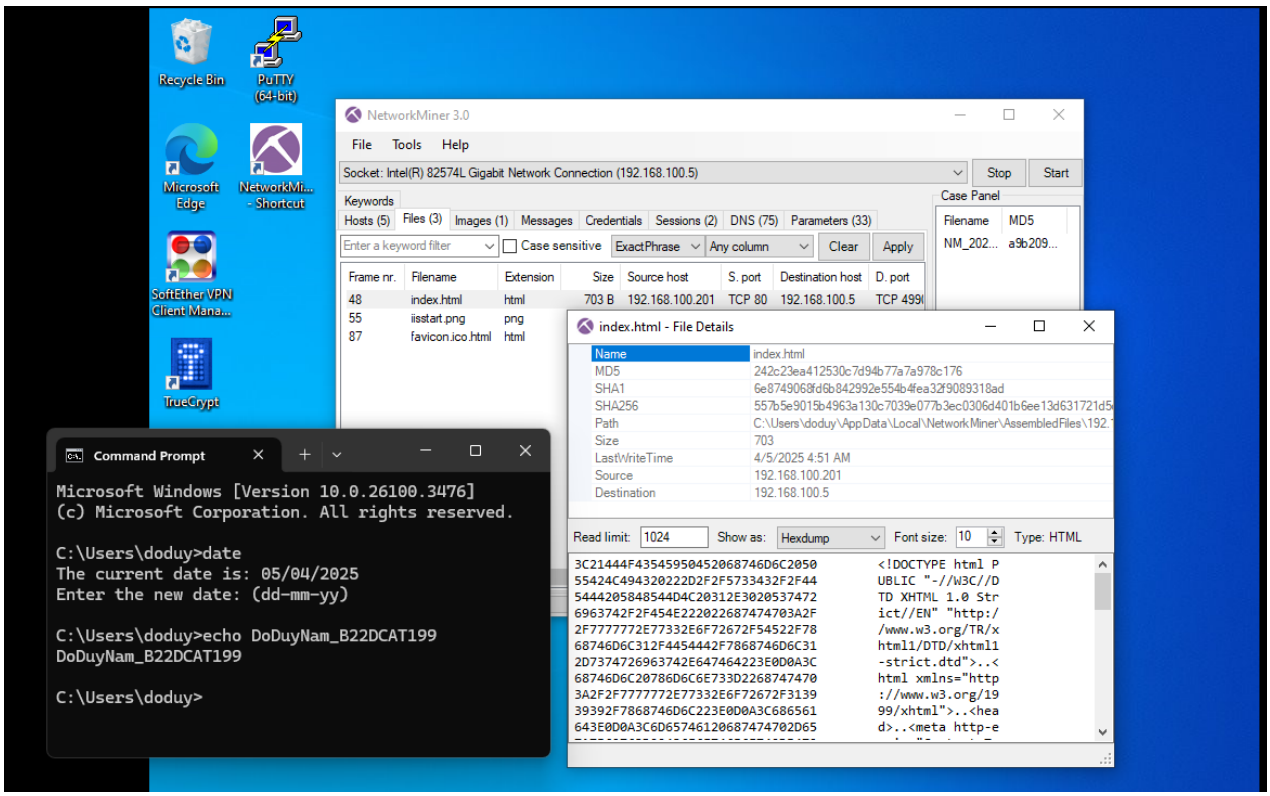
Hình 17 Chuẩn bị để bắt các gói tin

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



Hình 18 Kết nối đến trang web của Windows Server

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



Hình 19 Dữ liệu gói tin vừa bắt được

2.3 Kết chương

Ở chương này đã thực hiện thành công việc sử dụng tcpdump, Wireshark, Network Miner để bắt và phân tích các gói tin.

KẾT LUẬN

- Tìm hiểu về tính năng và hoạt động của một số công cụ bắt dữ liệu mạng như: tcpdump, Wireshark, Network Miner…
- Sử dụng thành công các công cụ tcmdump, Wireshark và Network Miner để bắt và phân tích các gói tin

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#