

**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:

B22DCAT063 Lê Tiến Dương

Giảng viên hướng dẫn: PGS. TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

| | |
|--|-----------|
| MỤC LỤC..... | 2 |
| DANH MỤC CÁC HÌNH VẼ..... | 3 |
| DANH MỤC CÁC TỪ VIẾT TẮT..... | 4 |
| CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH | 5 |
| 1.1 Mục đích..... | 5 |
| 1.2 Tìm hiểu lý thuyết | 5 |
| 1.2.1 Sniffer..... | 5 |
| 1.2.2 Tìm hiểu về Tcpdump | 5 |
| 1.2.3 Tìm hiểu về Wireshark..... | 6 |
| 1.2.4 Tìm hiểu về Network Miner..... | 7 |
| 1.2.5 Chế độ hỗn độn trên card mạng | 7 |
| CHƯƠNG 2. NỘI DUNG THỰC HÀNH | 8 |
| 2.1 Chuẩn bị môi trường | 8 |
| 2.2 Các bước thực hiện..... | 9 |
| 2.2.1 Sử dụng tcpdump | 9 |
| 2.2.2 Sử dụng Wireshark để bắt và phân tích các gói tin..... | 13 |
| 2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin..... | 18 |
| TÀI LIỆU THAM KHẢO | 20 |

DANH MỤC CÁC HÌNH VẼ

| | |
|--|----|
| Hình 1 – Cấu hình topo mạng | 8 |
| Hình 2 – Xem các interfaces trong hệ thống | 9 |
| Hình 3 – Kích hoạt các interfaces hoạt động ở chế độ hỗn hợp | 9 |
| Hình 4 – Bắt gói tin trên dải mạng 192.168.100.0/24 | 10 |
| Hình 5 – Dải Internal: Ping từ 192.168.100.201 -> 192.168.100.3 | 10 |
| Hình 6 – Bắt gói tin trên dải 192.168.100.0/24 | 11 |
| Hình 7 – Dải External: Ping từ 10.10.19.202 -> 10.10.19.148 | 11 |
| Hình 8 – Bắt gói tin trên dải 10.10.19.0/24 | 12 |
| Hình 9 – Các dữ liệu đã bắt trên dải Internal | 12 |
| Hình 10 – Các dữ liệu đã bắt trên dải External | 13 |
| Hình 11 – Tải Wireshark trên máy Windows attack | 13 |
| Hình 12 – Cài đặt Wireshark | 14 |
| Hình 13 – Bật các interfaces eth0, eth1 và khởi động Wireshark | 14 |
| Hình 14 – Bắt gói tin trên dải mạng 192.168.100.0/24 | 15 |
| Hình 15 – Windows attack kết nối tới ftp server trên máy Windows Server Internal | 15 |
| Hình 16 – Lọc gói tin theo giao thức ftp | 16 |
| Hình 17 – Ping từ máy 192.168.100.3 đến 192.168.100.201 | 16 |
| Hình 18 – Bắt gói tin bằng Wireshark trên máy Windows attack | 17 |
| Hình 19 – Trên máy Kali Linux External kết nối ftp đến Ftp Server | 17 |
| Hình 20 – Bắt gói tin trên dải 10.10.19.0/24 và lọc theo giao thức ftp | 18 |
| Hình 21 – Chọn Socket và bắt đầu bắt gói tin | 18 |
| Hình 22 – Kết nối đến trang web của Windows 2019 Server Internal | 19 |
| Hình 23 – Xem dữ liệu gói tin index.html vừa bắt được | 19 |

DANH MỤC CÁC TỪ VIẾT TẮT

| Từ viết tắt | Thuật ngữ tiếng Anh/Giải thích | Thuật ngữ tiếng Việt/Giải thích |
|--------------------|---|---|
| FTP | File Transfer Protocol | Giao thức truyền tệp tin |
| TCP/IP | Transmission Control Protocol/Internet Protocol | Giao thức điều khiển truyền nhận/Giao thức Internet |
| DNS | Domain Name System | Hệ thống phân giải tên miền |
| SMTP | Simple Mail Transfer Protocol | Giao thức truyền thư điện tử đơn giản |
| POP3 | Post Office Protocol version 3 | Giao thức bưu điện phiên bản 3 |
| IMAP | Internet Message Access Protocol | Giao thức truy cập thư điện tử qua Internet |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

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

Tìm hiểu về tính năng và hoạt động của một số công cụ bắt dữ liệu mạng như: tcpdump, Wireshark, Network Miner...

1.2.1 Sniffer

Sniffer hay packet sniffer là một chương trình phần mềm nghe trộm gói tin (còn gọi là chương trình phân tích mạng, phân tích giao thức hay nghe trộm Ethernet), có khả năng chặn bắt và ghi lại lưu lượng dữ liệu qua một mạng viễn thông số hoặc một phần của một mạng. Khi các dòng dữ liệu di chuyển qua lại trong một mạng, chương trình sẽ chặn bắt các gói tin rồi giải mã và phân tích nội dung của nó theo đặc tả RFC hoặc các đặc tả thích hợp khác.

Tùy theo cấu trúc mạng (hub hay chuyển mạch) mà có thể nghe trộm tất cả hoặc chỉ một phần lưu lượng dữ liệu qua lại từ một máy trong mạng. Đối với mục đích giám sát mạng (network monitoring), có thể theo dõi tất cả các gói tin trong một mạng LAN bằng cách sử dụng một thiết bị chuyển mạch với một cổng theo dõi (lắp lại tất cả các gói tin đi qua các cổng của thiết bị chuyển mạch).

1.2.2 Tìm hiểu về Tcpdump

Tcpdump là một công cụ dòng lệnh được sử dụng để ghi lại và phân tích gói tin trên mạng. Nó cho phép bạn theo dõi lưu lượng mạng đi qua một giao diện cụ thể trên hệ thống của bạn. Bằng cách sử dụng các cú pháp và tùy chọn khác nhau, bạn có thể lọc và hiển thị các gói tin theo nhiều tiêu chí khác nhau như địa chỉ IP, cổng, giao thức, và nhiều hơn nữa. Tcpdump là một công cụ mạnh mẽ được sử dụng rộng rãi trong quản trị hệ thống và mạng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng.

Tcpdump sẽ giúp bạn 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 tcpdump.
- 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, ftp...

- Ngoài ra tcpdump còn sử dụng nhiều option khác nhau nữa.

Cách hoạt động của Tcpdump:

TCPdump là một công cụ dòng lệnh được sử dụng để theo dõi và phân tích gói tin trên mạng. Nó hoạt động bằng cách lắng nghe và ghi lại các gói tin mạng đang đi qua một giao diện mạng cụ thể trên một máy tính. Khi được chạy, TCPdump sẽ hiển thị thông tin về các gói tin này, bao gồm địa chỉ nguồn và đích, loại giao thức, dữ liệu payload, và nhiều thông tin khác. Người dùng có thể sử dụng các tùy chọn và bộ lọc để tinh chỉnh việc theo dõi và phân tích theo nhu cầu cụ thể của họ.

1.2.3 Tìm hiểu về Wireshark

Wireshark là một công cụ phân tích gói tin mạng mạnh mẽ và đa năng. Nó cho phép bạn chụp, xem xét và phân tích gói tin trên mạng. Wireshark hỗ trợ nhiều loại giao thức mạng và cung cấp các tính năng như lọc gói tin, phân tích luồng dữ liệu, và đồ thị hoạt động mạng. Công cụ này thường được sử dụng để chẩn đoán và gỡ lỗi vấn đề liên quan đến mạng, cũng như để nghiên cứu bảo mật mạng và kiểm tra hiệu suất mạng. Wireshark có giao diện đồ họa dễ sử dụng và được hỗ trợ trên nhiều hệ điều hành khác nhau.

Wireshark là một phần mềm dùng để phân tích và giám sát lưu lượng mạng. Dưới đây là một số chức năng chính của Wireshark:

- *Phân tích gói tin:* Wireshark cho phép bạn theo dõi và phân tích từng gói tin dữ liệu trên mạng. Bạn có thể xem các thông tin chi tiết như nguồn, đích, loại gói tin, dữ liệu payload và nhiều thông tin khác.
- *Đánh giá hiệu suất mạng:* Wireshark cung cấp thông tin về thời gian phản hồi (response time), độ trễ (latency), và các thống kê khác, giúp đánh giá hiệu suất của mạng.
- *Phân tích giao thức:* Wireshark hỗ trợ nhiều giao thức mạng khác nhau. Bạn có thể xem và phân tích giao thức HTTP, TCP, UDP, IP, DNS, và nhiều giao thức khác.
- *Điều tra vấn đề mạng:* Khi xảy ra vấn đề mạng, Wireshark là một công cụ mạnh mẽ để phân tích và xác định nguyên nhân của sự cố.
- *Bảo mật mạng:* Wireshark có thể được sử dụng để phát hiện các hoạt động độc hại trên mạng. Nó cho phép bạn xem gói tin để phát hiện các tấn công mạng, như phishing hoặc kiểm soát truy cập không được ủy quyền.
- *Giáo dục và học tập:* Wireshark là một công cụ hữu ích cho sinh viên, chuyên gia mạng, và người quan tâm đến việc hiểu rõ cách mạng hoạt động. Nó cung cấp một cách thức thực hành để nắm bắt và hiểu các khái niệm mạng.

Cách hoạt động của Wireshark:

Như đã đề cập ở trên, đây là một công cụ dùng để capture và phân tích các packet. Nó capture các lưu lượng mạng trên mạng cục bộ, sau đó sẽ lưu trữ nó để phân tích offline. Có thể capture các lưu lượng mạng từ các kết nối Ethernet, Bluetooth, Wireless (IEEE.802.11),

Token Ring, Frame Relay... Wireshark cho phép thiết lập filter (bộ lọc) trước khi bắt đầu capture hoặc thậm chí là trong quá trình phân tích. Do đó, ta có thể thu hẹp phạm vi tìm kiếm trong quá trình theo dõi mạng.

1.2.4 Tìm hiểu về Network Miner

NetworkMiner là một công cụ phân tích mạng dành cho Windows. Nó cho phép người dùng thu thập dữ liệu từ mạng và phân tích thông tin như các máy chủ, giao thức, trình duyệt web, và nhiều hơn nữa. NetworkMiner tự động phát hiện các hoạt động mạng như kết nối TCP, truy vấn DNS và nó cũng có thể hỗ trợ trong việc phát hiện và phân loại các tập tin được truyền qua mạng. Nó thường được sử dụng để phát hiện các mối đe dọa mạng và phân tích dữ liệu từ gói tin đã chụp.

Những điểm nổi bật của Network Miner:

- Giám sát hầu như mọi gói tin trao đổi ra vào máy chủ, trong đó cho phép phát hiện ảnh, các file dữ liệu và tài khoản đăng nhập.
- Dữ liệu hiển thị ở dạng rất dễ hiểu.
- Dung lượng nhẹ (phiên bản 2.6 sau khi giải nén chỉ chiếm 47,9 MB), không cần cài đặt (chỉ cần tải về, giải nén là sử dụng được ngay) và rất dễ sử dụng.
- Có hai phiên bản miễn phí và pro (trả phí) để lựa chọn. Trong đó, phiên bản trả phí cho phép tìm kiếm trực tuyến thông tin về địa chỉ IP.
- Khả năng phân tích email trao đổi qua các giao thức SMTP, POP3 và IMAP.
- Nâng cấp khả năng phát hiện mật khẩu, phát hiện trao đổi dữ liệu qua giao thức FTP, những dấu hiệu bất thường trong trao đổi dữ liệu qua giao thức HTTP và HTTP/2.
- Nâng cấp khả năng tương thích với hệ điều hành Linux. Hỗ trợ phân tích các gói tin qua giao thức GRE, PPPoE, VXLAN, OpenFlow, MPLS và EoMPLS.

Cách hoạt động của Network Miner:

NetworkMiner là một công cụ phân tích mạng có khả năng thu thập dữ liệu từ gói tin mạng trên một giao diện cụ thể trên máy tính. Sau đó, nó phân tích các gói tin để trích xuất thông tin quan trọng như địa chỉ IP, tên miền, thông tin trình duyệt web và các tập tin được truyền qua mạng. Dữ liệu được hiển thị trên giao diện người dùng và có thể được lưu trữ dưới dạng tập tin PCAP để phân tích và thẩm định sau này.

1.2.5 Chế độ hỗn độn trên card mạng

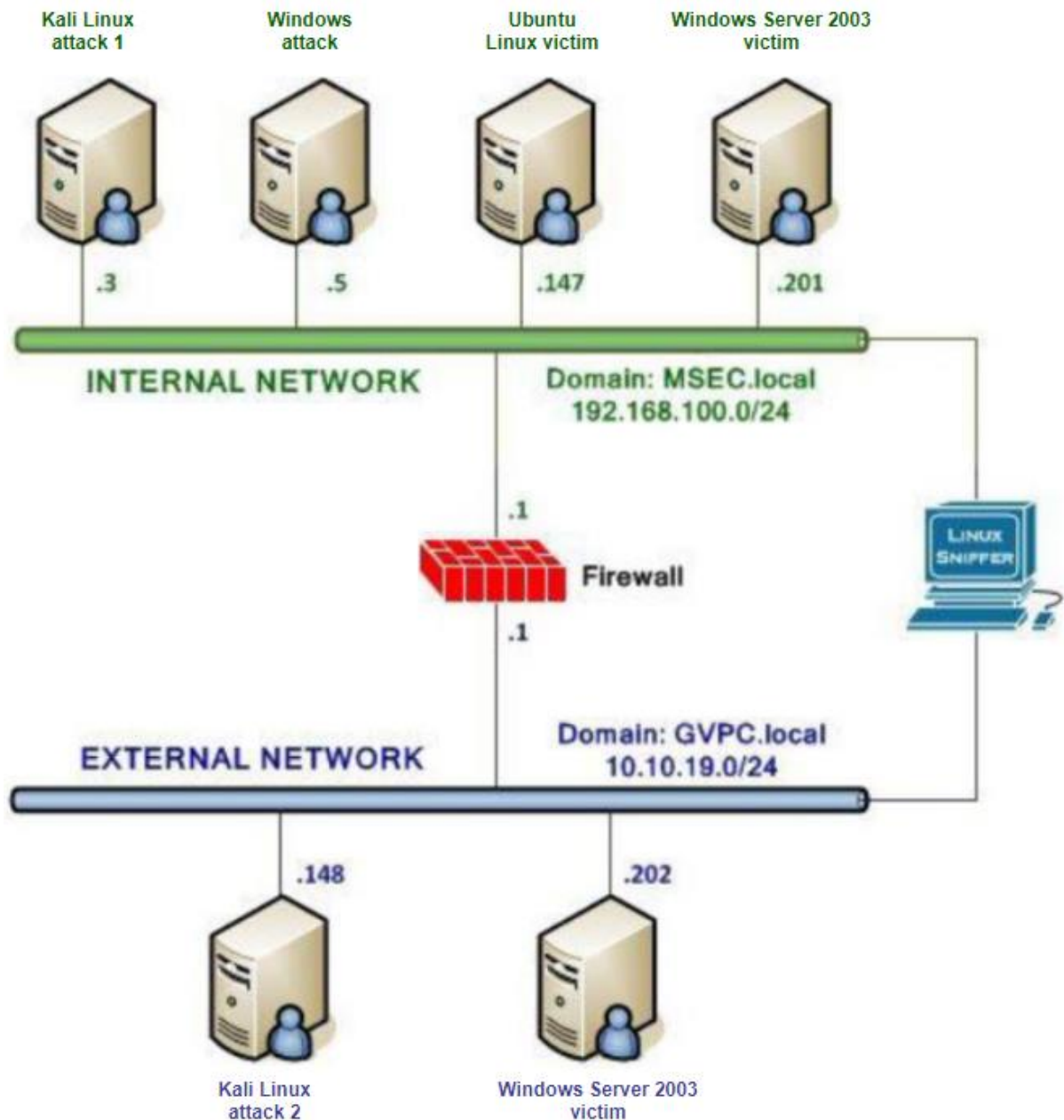
"Chế độ hỗn độn" (hay còn gọi là "promiscuous mode") trên một card mạng là một trạng thái hoạt động đặc biệt của card mạng. Khi một card mạng hoạt động trong chế độ hỗn độn, nó sẽ bắt đầu nhận tất cả các gói tin trên mạng, bao gồm cả những gói tin không địa chỉ cho chính nó. Chế độ hỗn độn thường được sử dụng cho các mục đích giám sát, phân tích mạng, hoặc để phát hiện các vấn đề về bảo mật mạng.

Kích hoạt chế độ hỗn độn trên Linux: `sudo ifconfig <tên card mạng> promisc`

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.

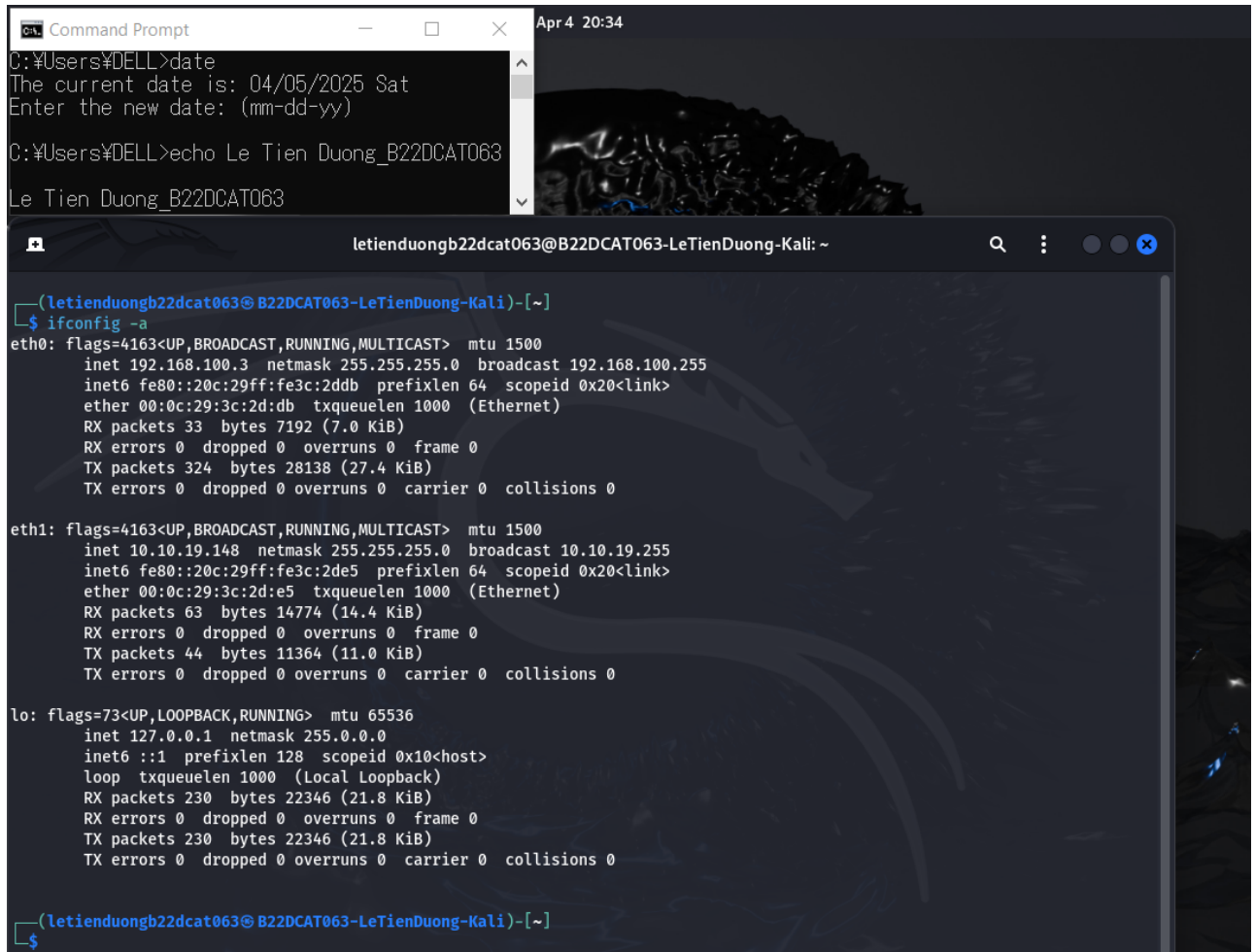


Hình 1 – Cấu hình topo mạng

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 (root@bt:~#ifconfig -a).



```
Command Prompt
C:\Users\DELL>date
The current date is: 04/05/2025 Sat
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

letiendaugb22dcat063@B22DCAT063-LeTienDuong-Kali: ~
[~]
$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fe3c:2ddb prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3c:2d:db txqueuelen 1000 (Ethernet)
    RX packets 33 bytes 7192 (7.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 324 bytes 28138 (27.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

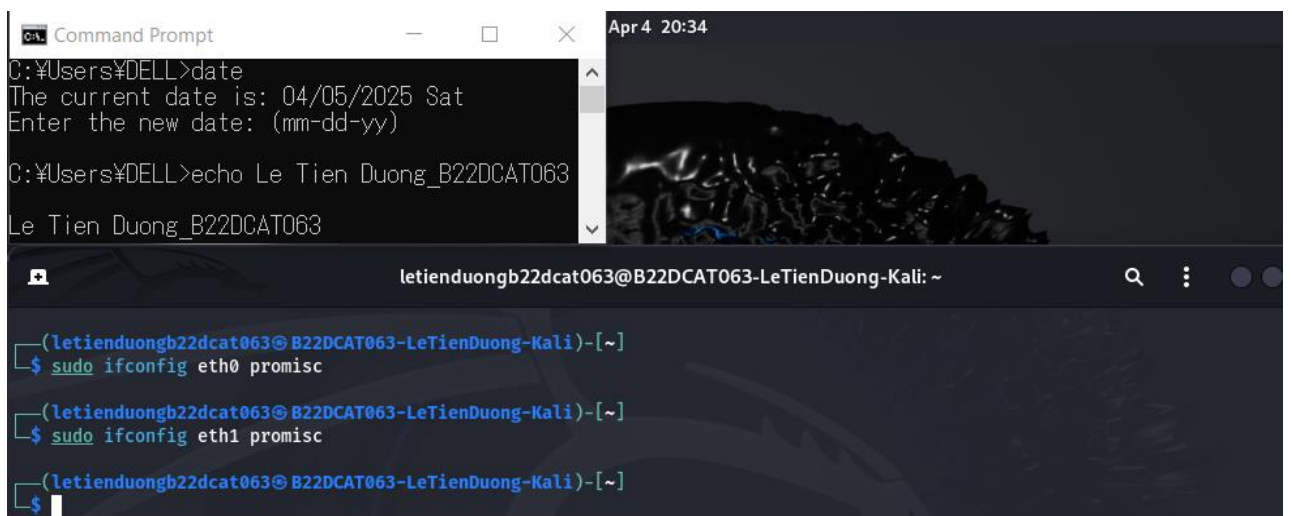
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.148 netmask 255.255.255.0 broadcast 10.10.19.255
    inet6 fe80::20c:29ff:fe3c:2de5 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:3c:2d:e5 txqueuelen 1000 (Ethernet)
    RX packets 63 bytes 14774 (14.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 44 bytes 11364 (11.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 230 bytes 22346 (21.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 230 bytes 22346 (21.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[~]
$
```

Hình 2 – Xem các interfaces trong hệ thống

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



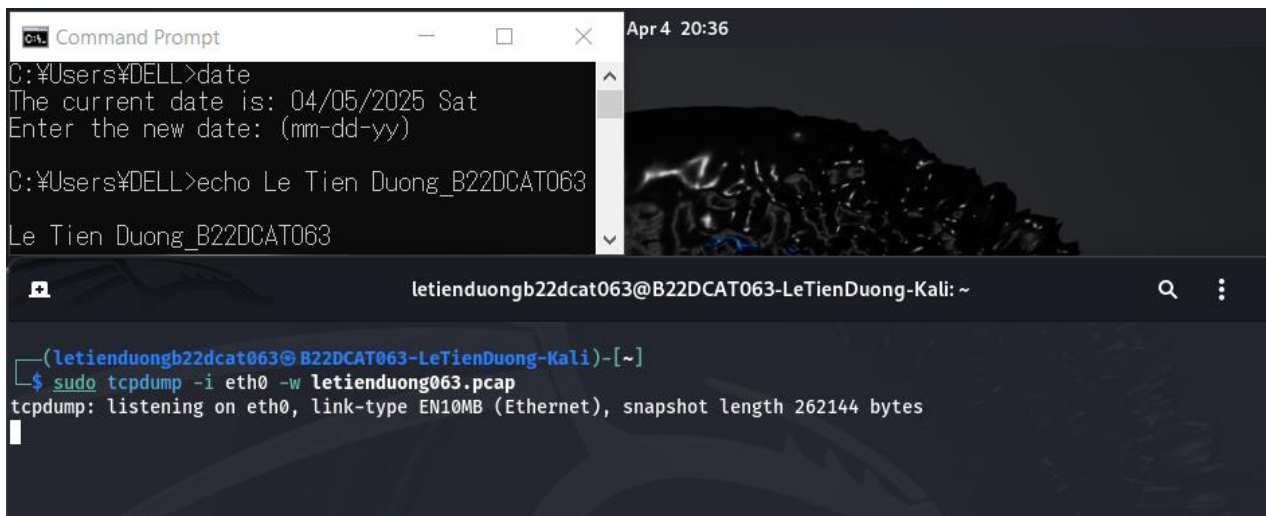
```
Command Prompt
C:\Users\DELL>date
The current date is: 04/05/2025 Sat
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

letiendaugb22dcat063@B22DCAT063-LeTienDuong-Kali: ~
[~]
$ sudo ifconfig eth0 promisc
[~]
$ sudo ifconfig eth1 promisc
[~]
$
```

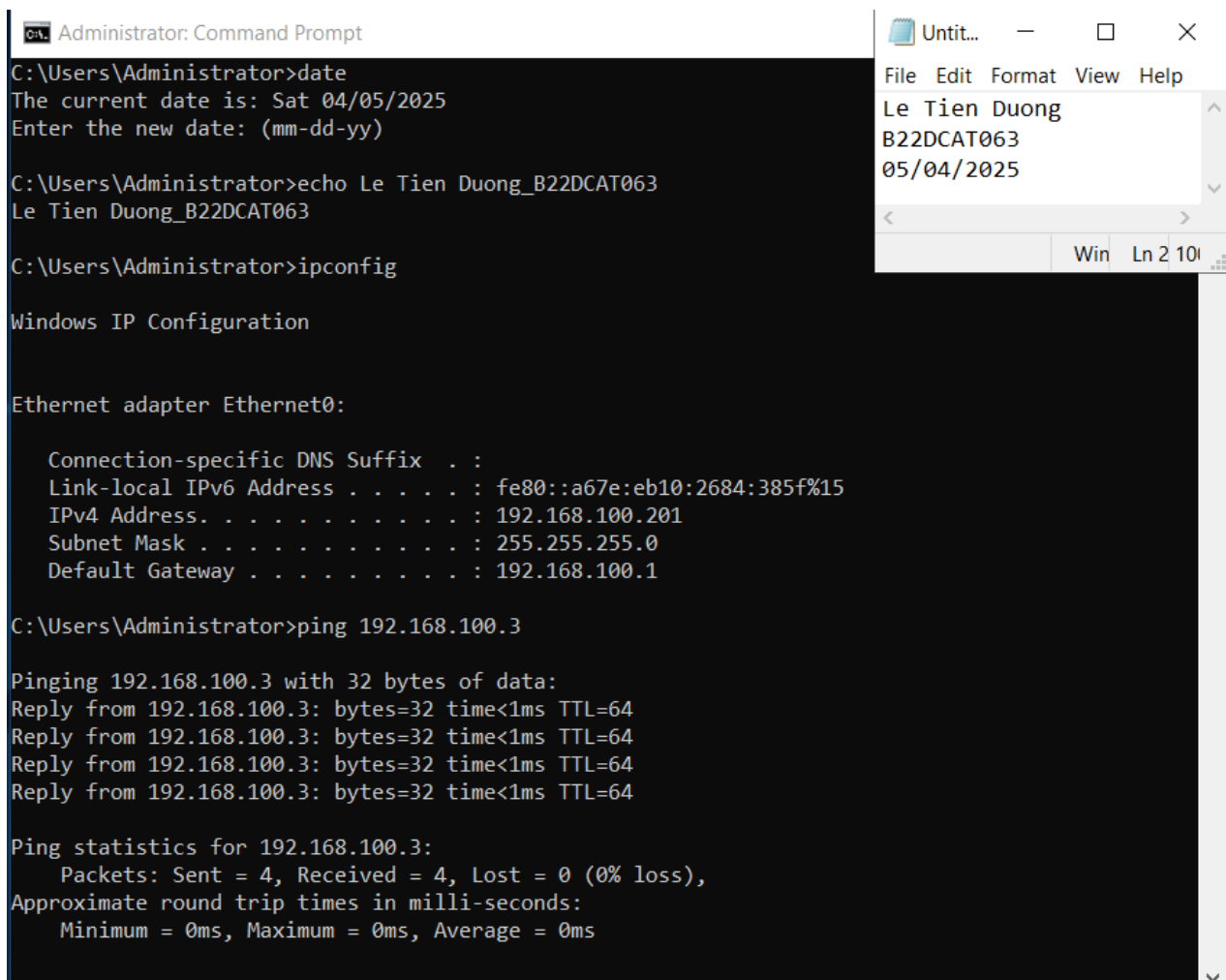
Hình 3 – Kích hoạt các interfaces hoạt động ở chế độ hỗn hợp

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



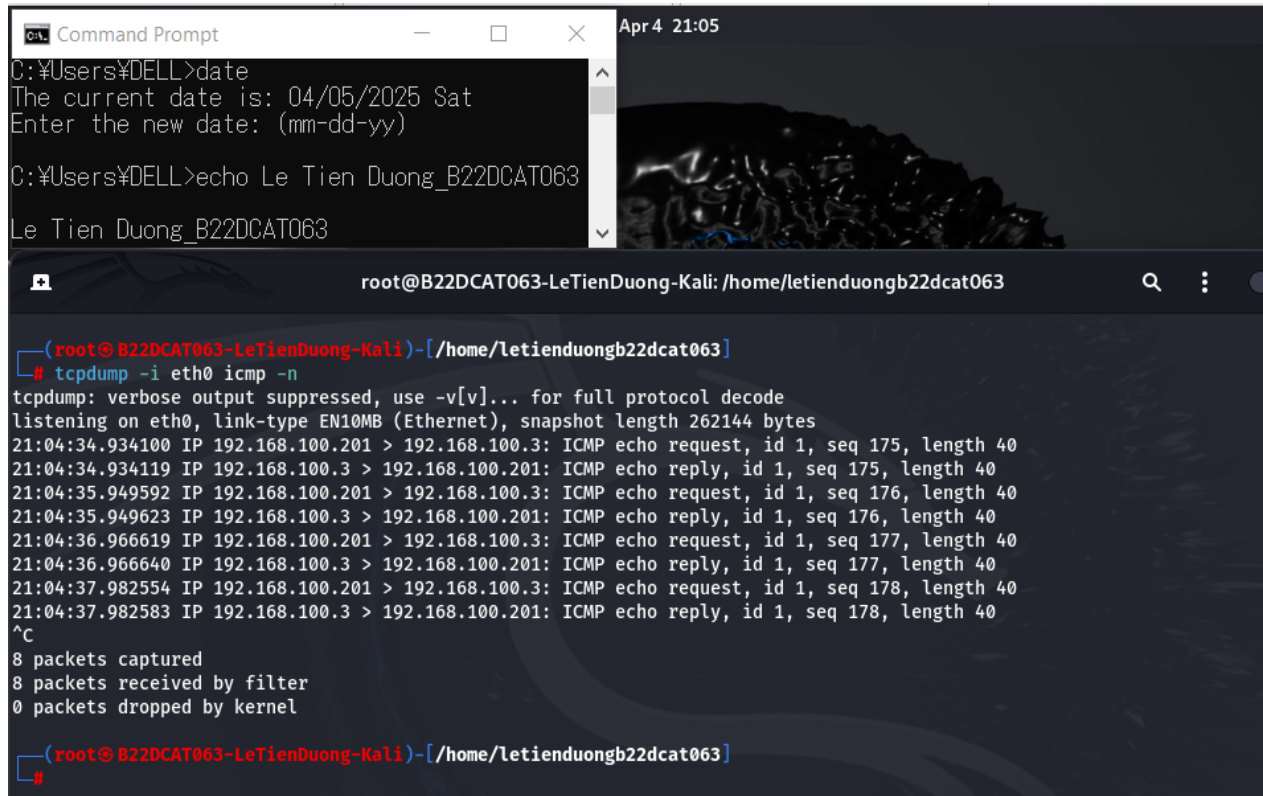
Hình 4 – Bắt gói tin trên dải mạng 192.168.100.0/24

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



Hình 5 – Dải Internal: Ping từ 192.168.100.201 -> 192.168.100.3

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



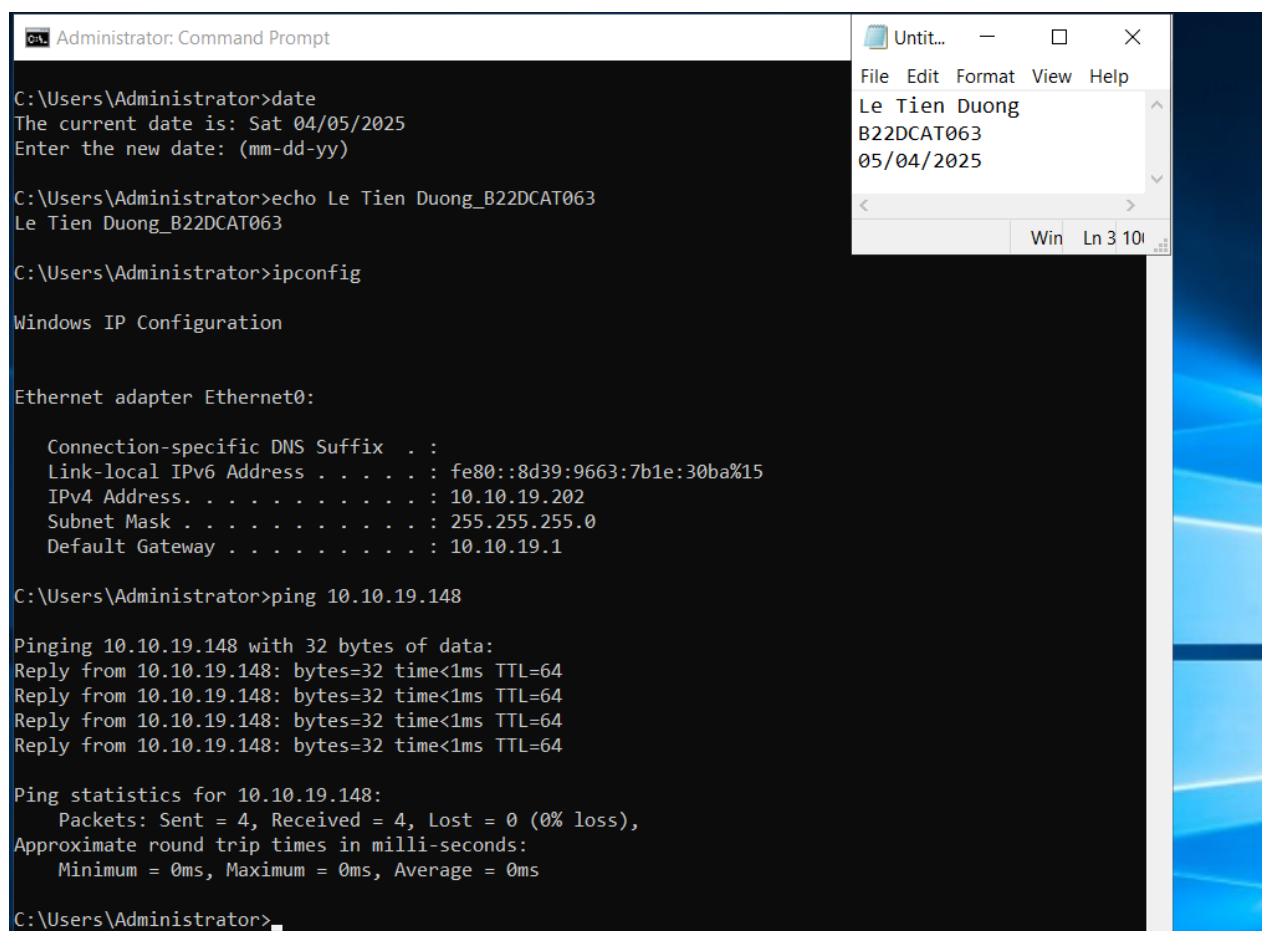
```
Command Prompt
C:\Users\DELL>date
The current date is: 04/05/2025 Sat
Enter the new date: (mm-dd-yy)

C:\Users\DELL>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

root@B22DCAT063-LeTienDuong-Kali: /home/letienduongb22dcat063
(root@B22DCAT063-LeTienDuong-Kali)-[/home/letienduongb22dcat063]
# tcpdump -i eth0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:04:34.934100 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 175, length 40
21:04:34.934119 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 175, length 40
21:04:35.949592 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 176, length 40
21:04:35.949623 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 176, length 40
21:04:36.966619 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 177, length 40
21:04:36.966640 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 177, length 40
21:04:37.982554 IP 192.168.100.201 > 192.168.100.3: ICMP echo request, id 1, seq 178, length 40
21:04:37.982583 IP 192.168.100.3 > 192.168.100.201: ICMP echo reply, id 1, seq 178, length 40
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel

(root@B22DCAT063-LeTienDuong-Kali)-[/home/letienduongb22dcat063]
#
```

Hình 6 – Bắt gói tin trên dải 192.168.100.0/24



```
Administrator: Command Prompt
C:\Users\Administrator>date
The current date is: Sat 04/05/2025
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo Le Tien Duong_B22DCAT063
Le Tien Duong_B22DCAT063

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::8d39:9663:7b1e:30ba%15
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1

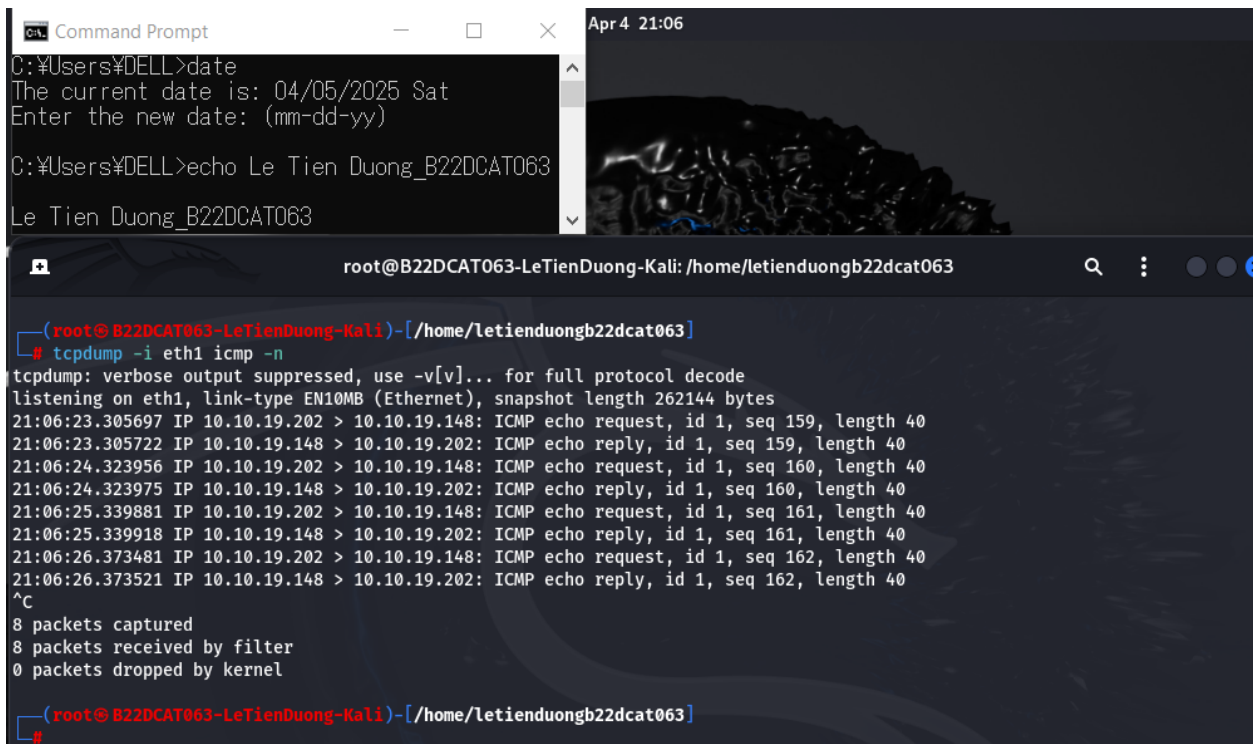
C:\Users\Administrator>ping 10.10.19.148

Pinging 10.10.19.148 with 32 bytes of data:
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64
Reply from 10.10.19.148: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.19.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

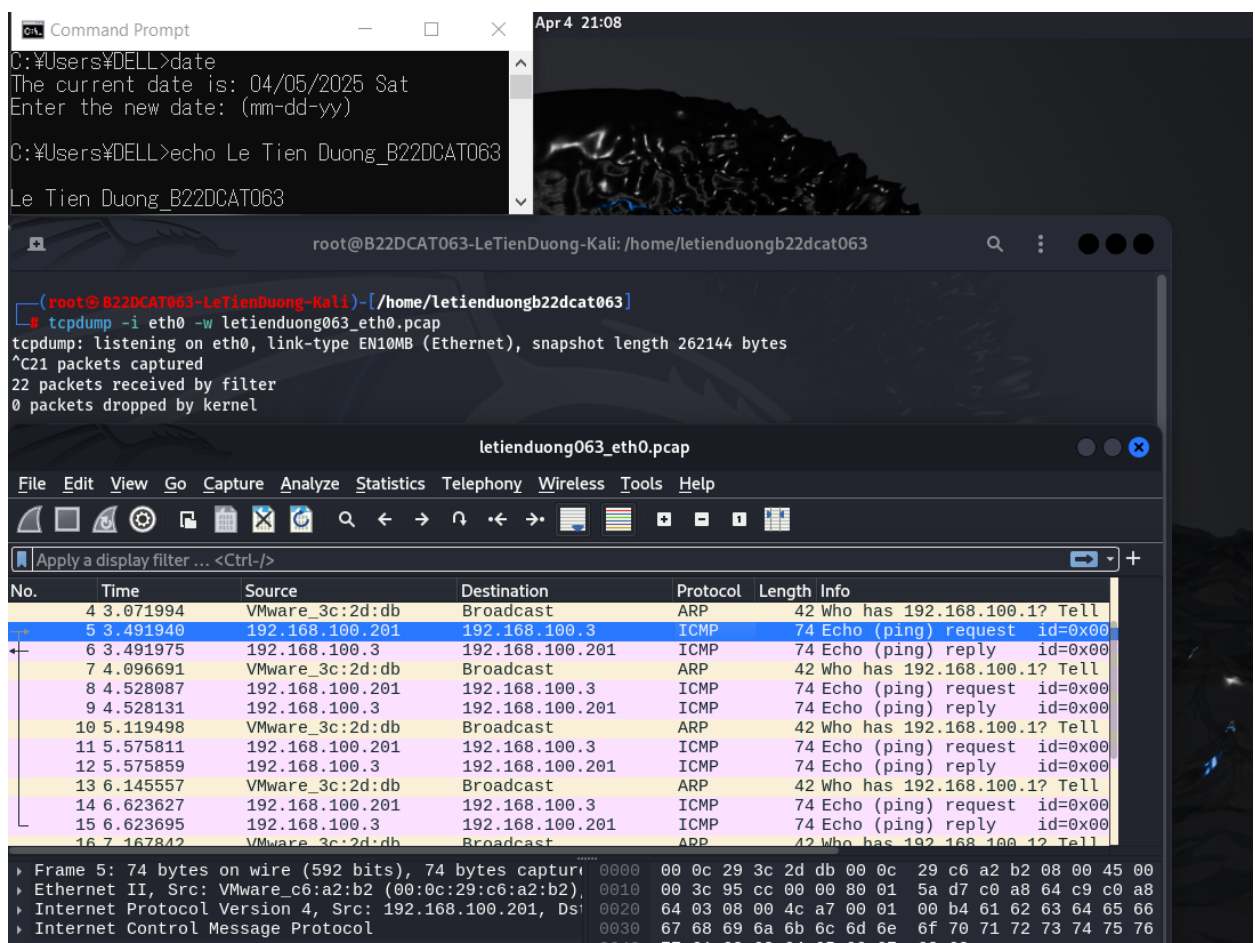
C:\Users\Administrator>
```

Hình 7 – Dải External: Ping từ 10.10.19.202 -> 10.10.19.148

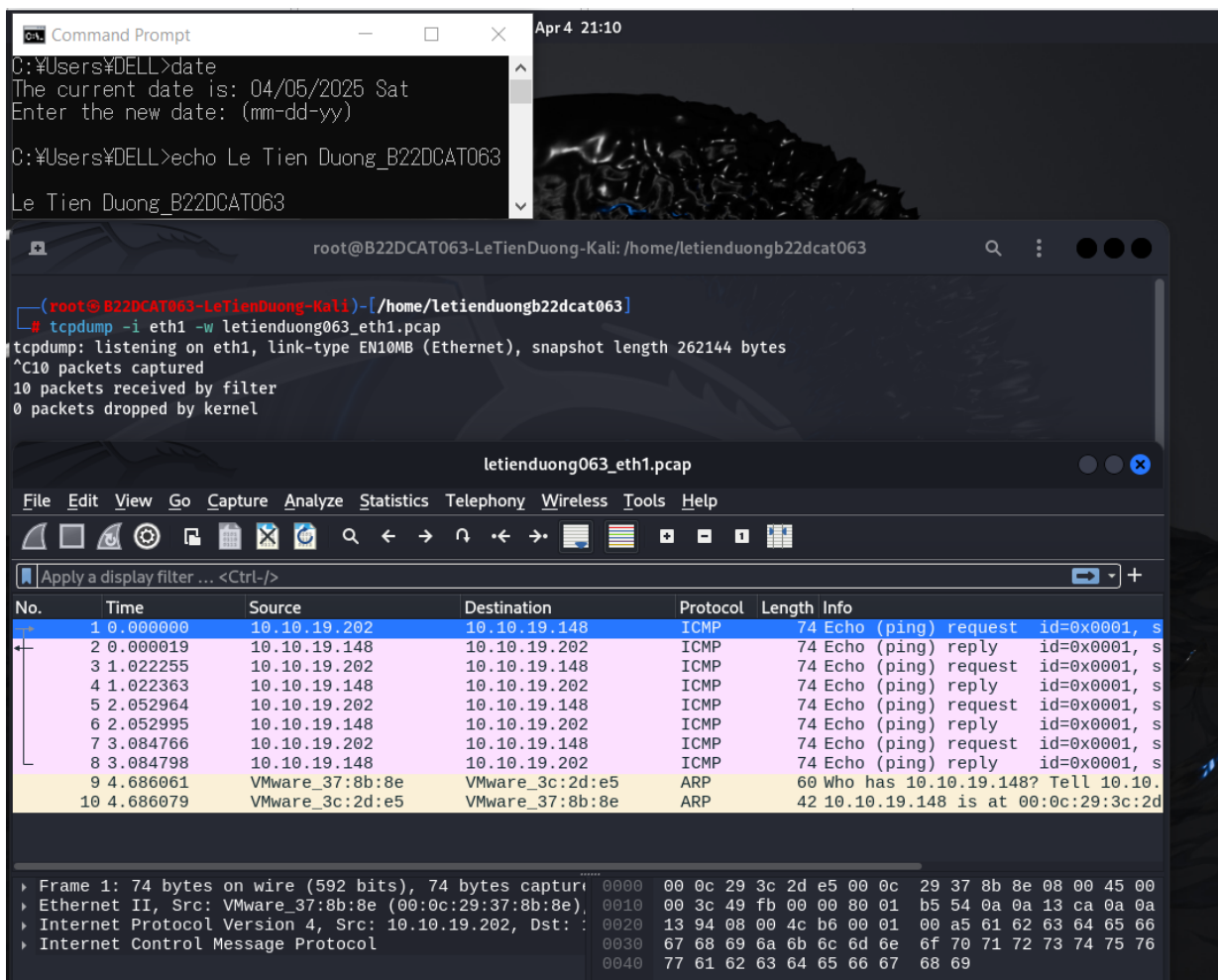


Hình 8 – Bắt gói tin trên dải 10.10.19.0/24

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



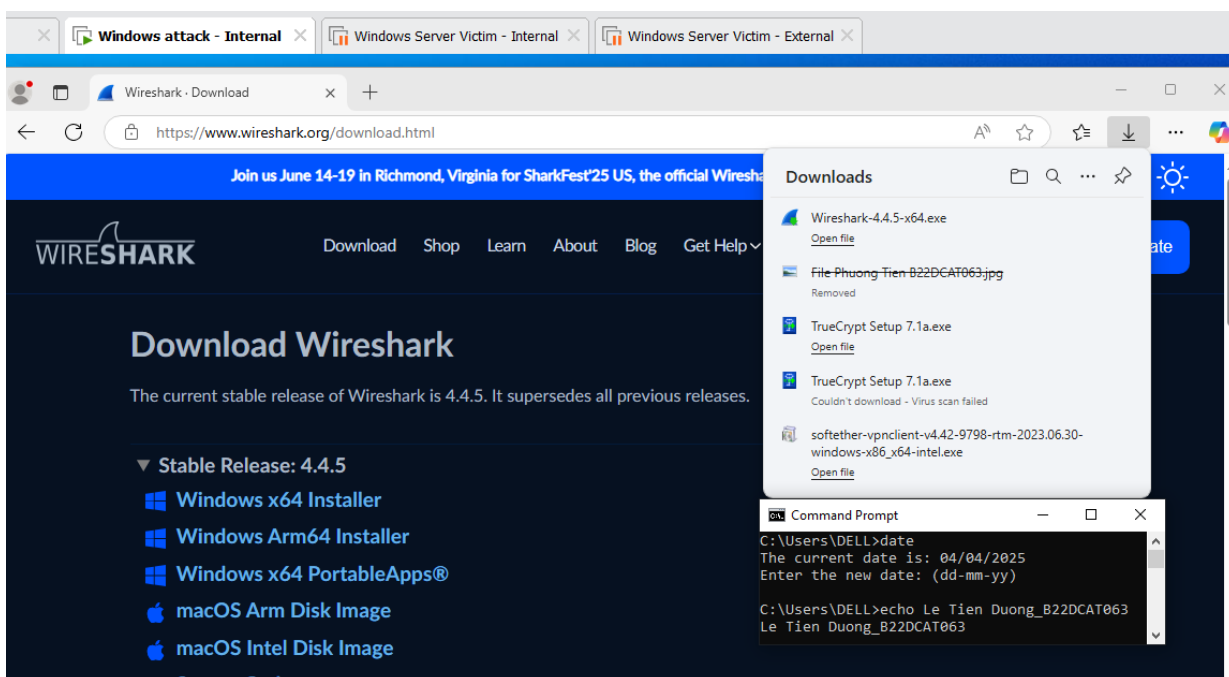
Hình 9 – Các dữ liệu đã bắt trên dải Internal



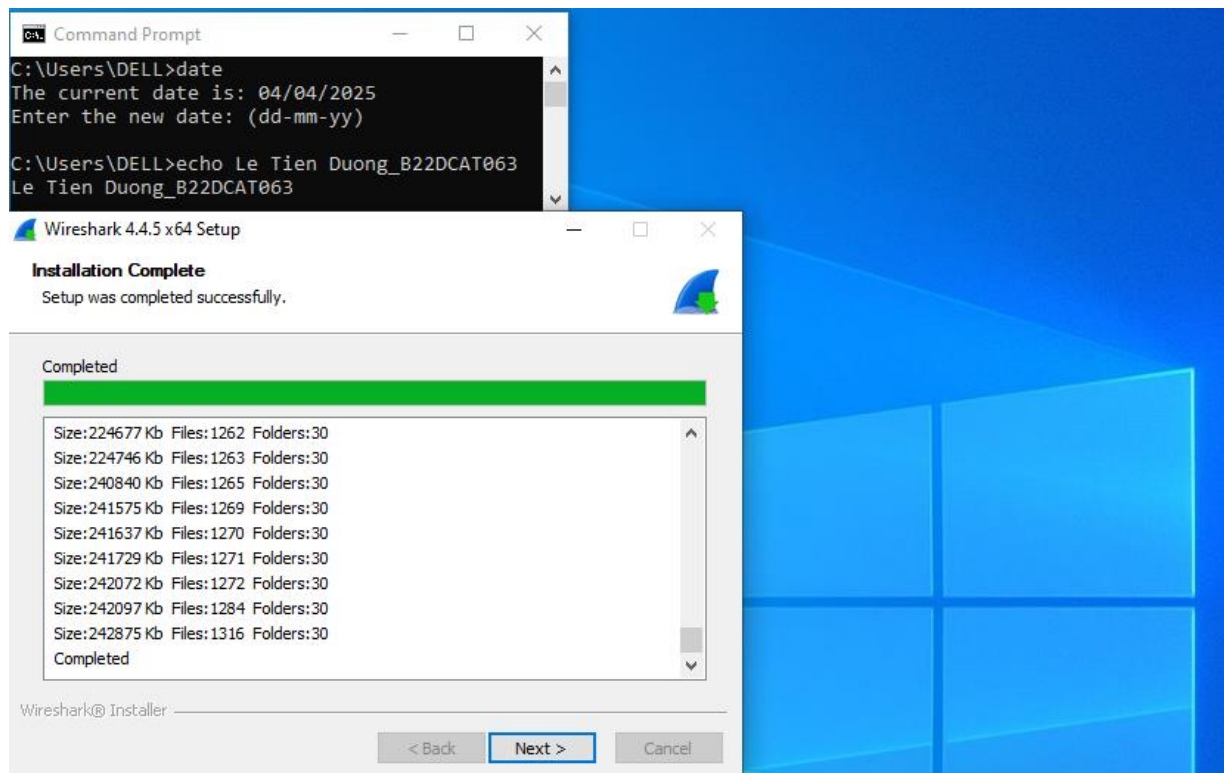
Hình 10 – Các dữ liệu đã bắt trên dải External

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

Có thể tải Wireshark ở đây: <http://www.wireshark.org/download.html>

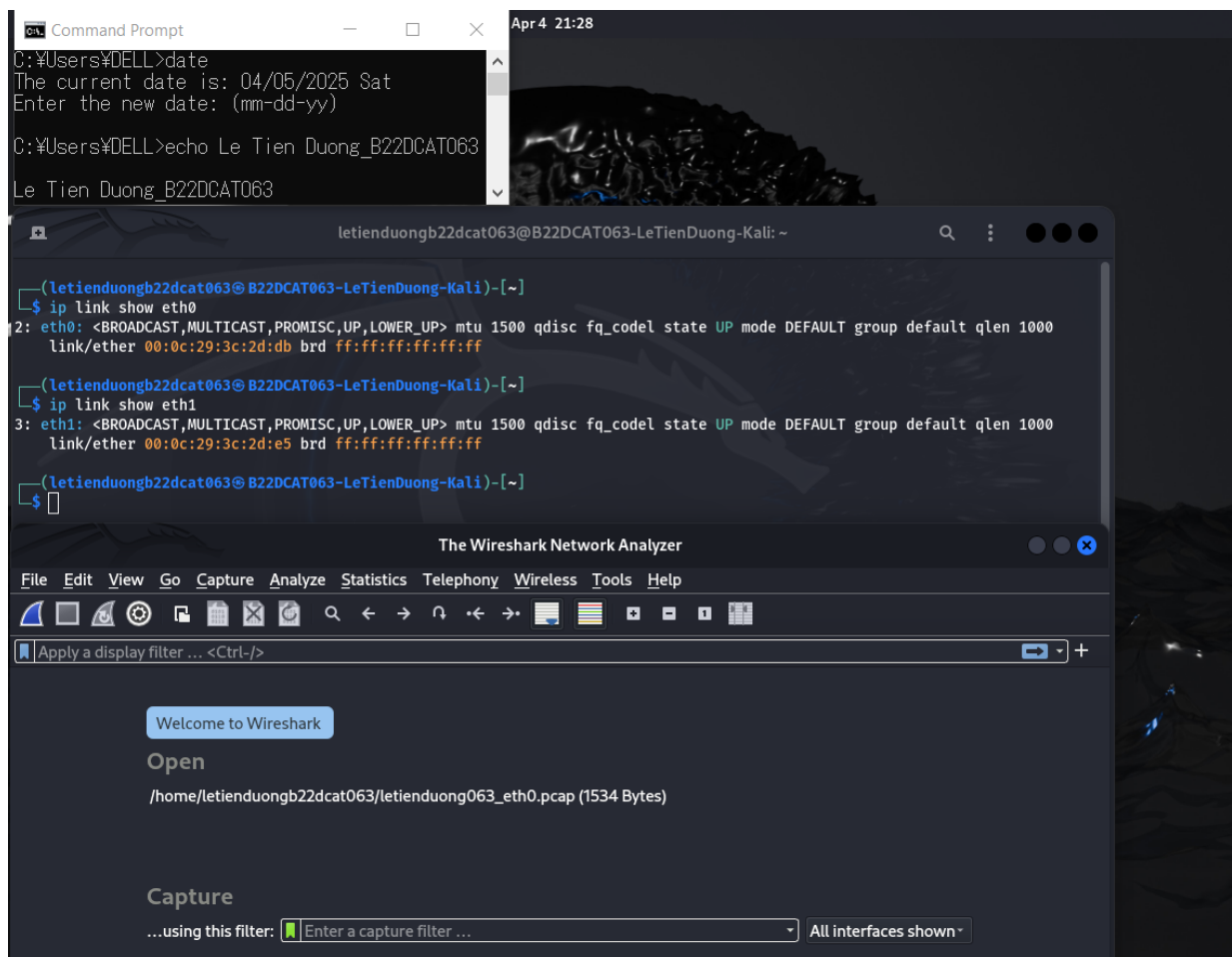


Hình 11 – Tải Wireshark trên máy Windows attack



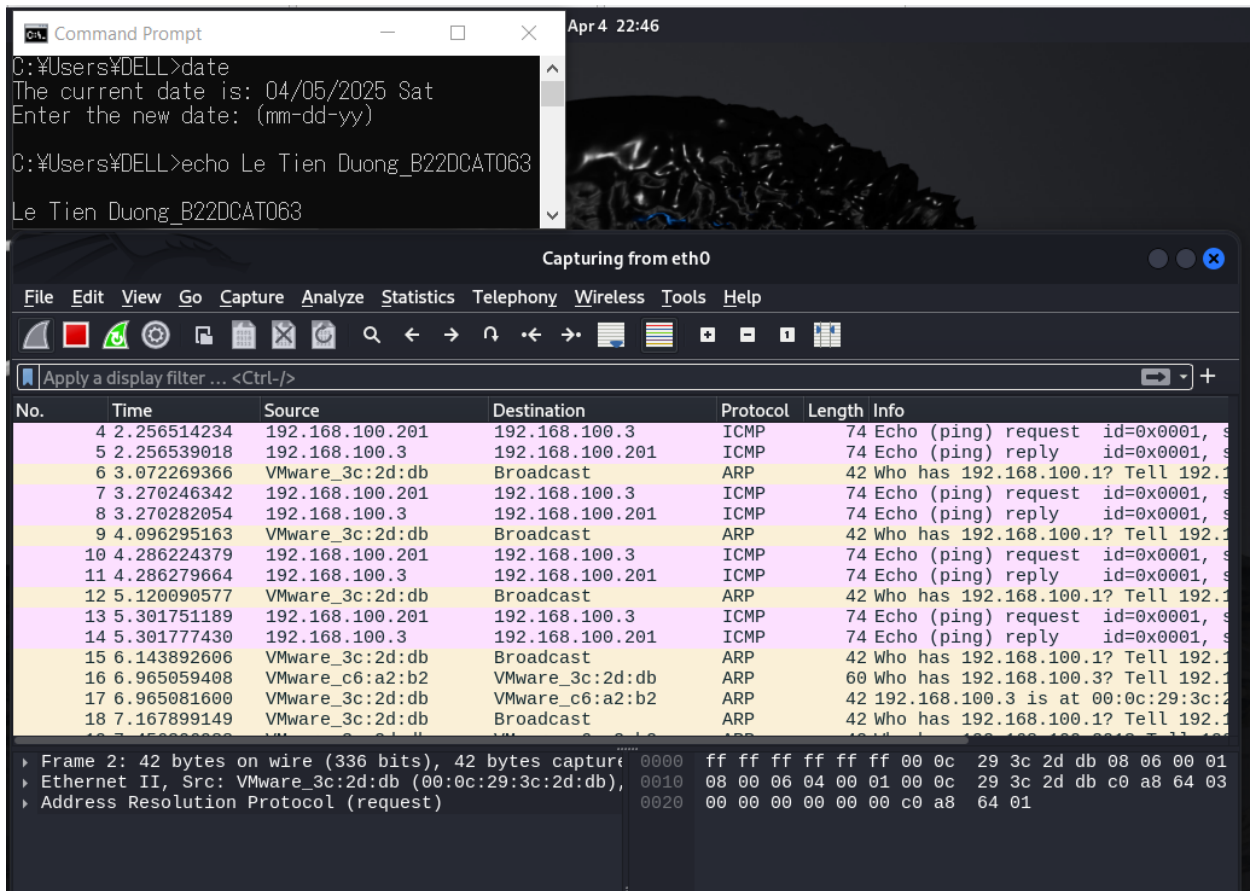
Hình 12 – Cài đặt Wireshark

Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark.



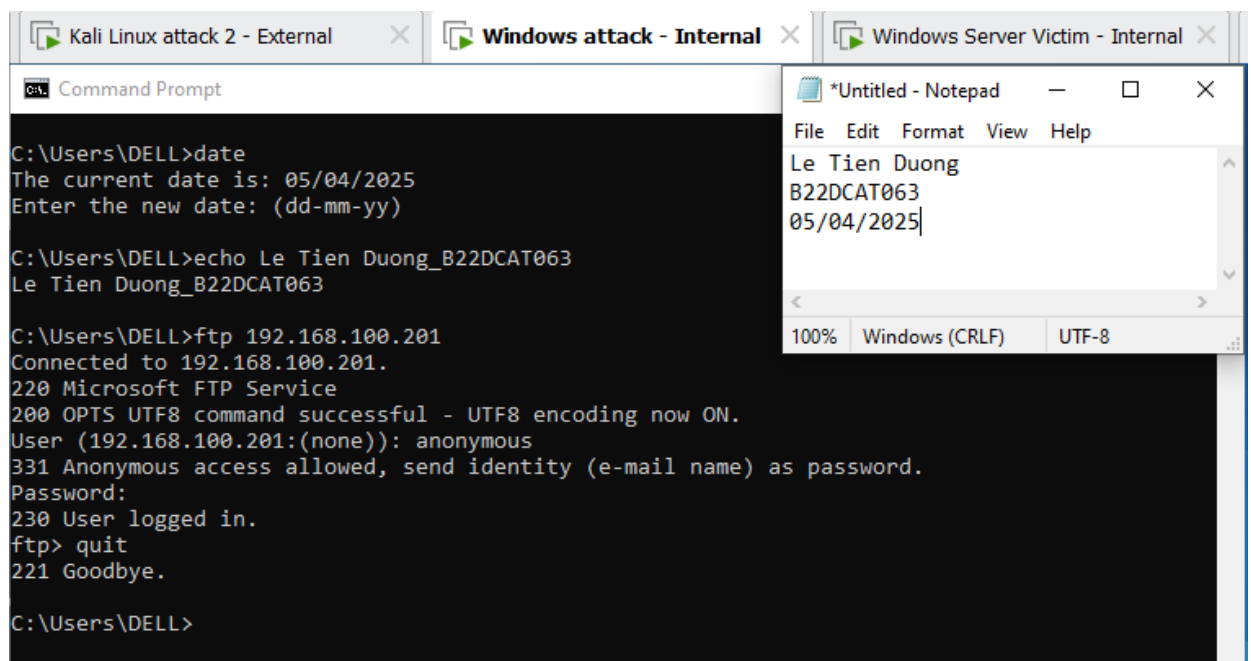
Hình 13 – Bật các interfaces eth0, eth1 và khởi động Wireshark

Trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0 (do máy em cấu hình dải mạng 192.168.100.0 trên interface eth0).



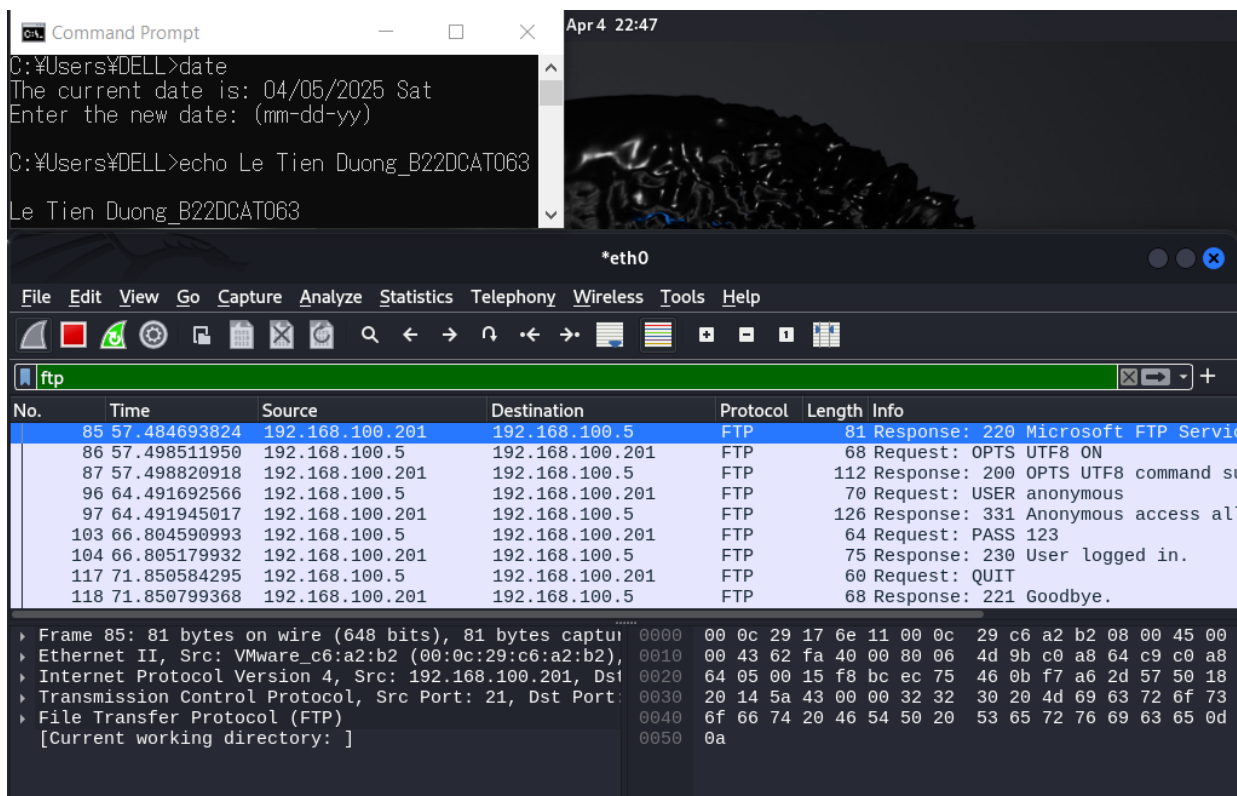
Hình 14 – Bắt gói tin trên dải mạng 192.168.100.0/24

Trên máy Windows 7 Attack kết nối tới ftp server trên máy Window Server Internal Victim.



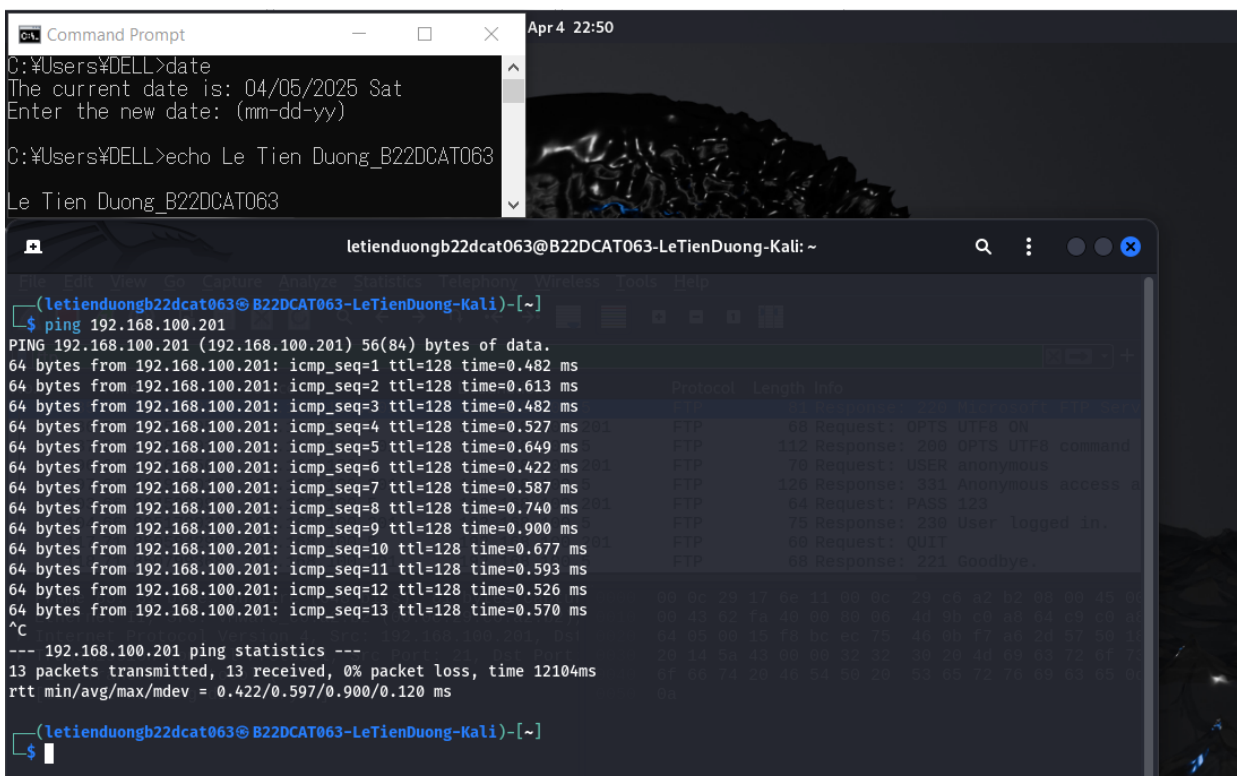
Hình 15 – Windows attack kết nối tới ftp server trên máy Windows Server Internal

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

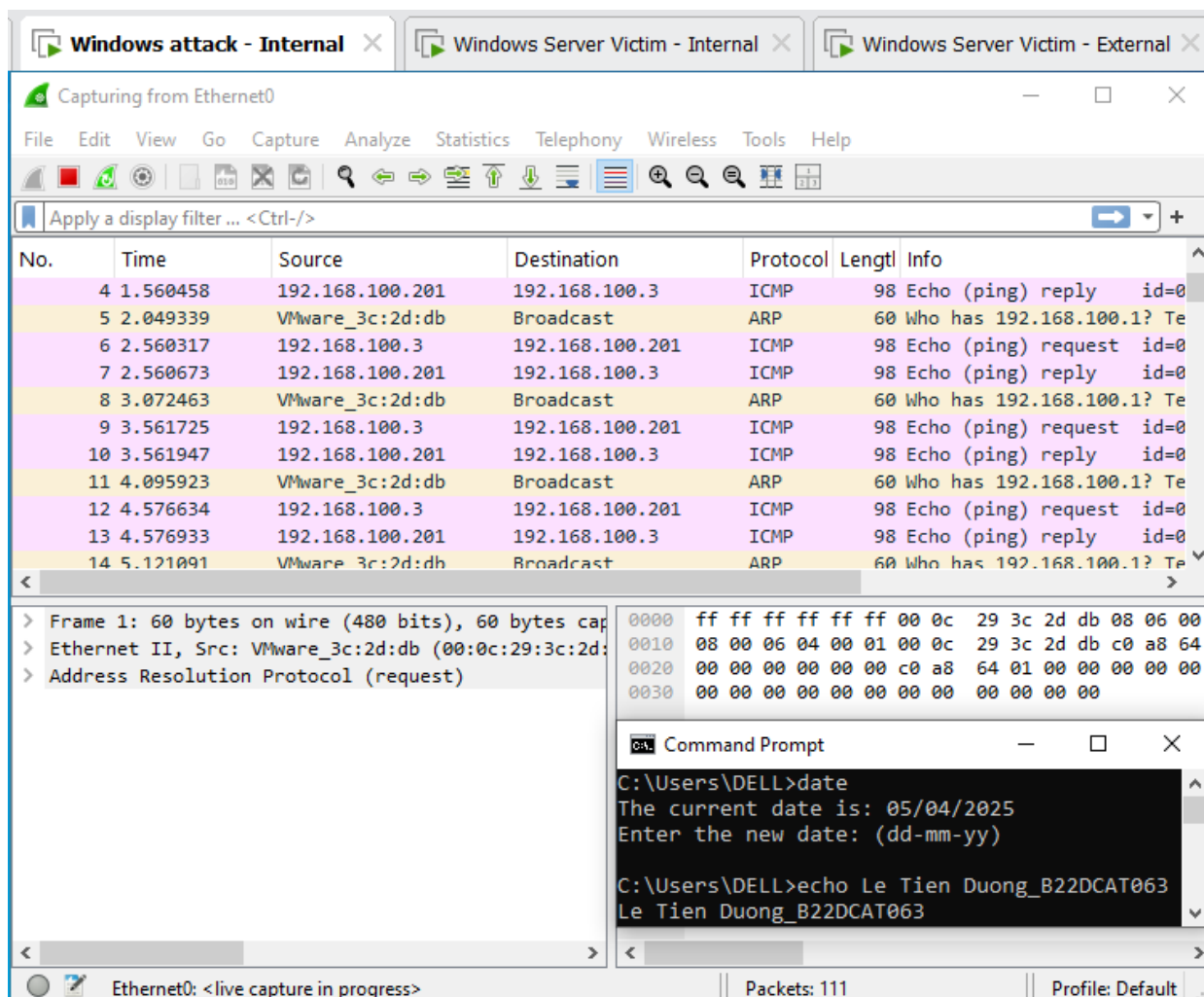


Hình 16 – Lọc gói tin theo giao thức ftp

Trên máy Windows attack (192.168.100.5), trong Capture Interfaces chọn Start ở dòng eth0 để bắt gói tin trên dải mạng 192.168.100.0 (khi ping từ máy 192.168.100.3 đến máy 192.168.100.201)



Hình 17 – Ping từ máy 192.168.100.3 đến 192.168.100.201



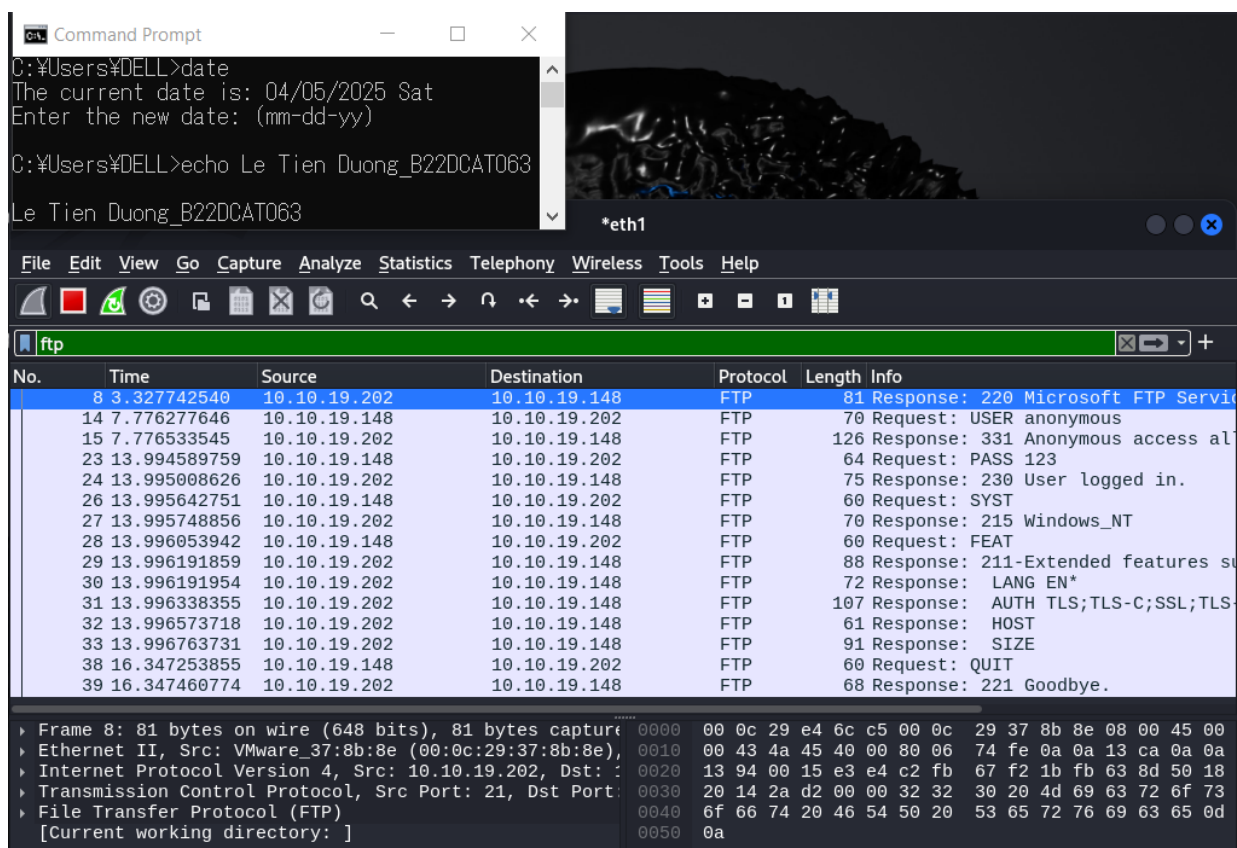
Hình 18 – Bắt gói tin bằng Wireshark trên máy Windows attack

Trên máy Kali Linux Attack External, kết nối với ftp server(root@bt:~#ftp 10.10.19.202).



Hình 19 – Trên máy Kali Linux External kết nối ftp đến Ftp Server

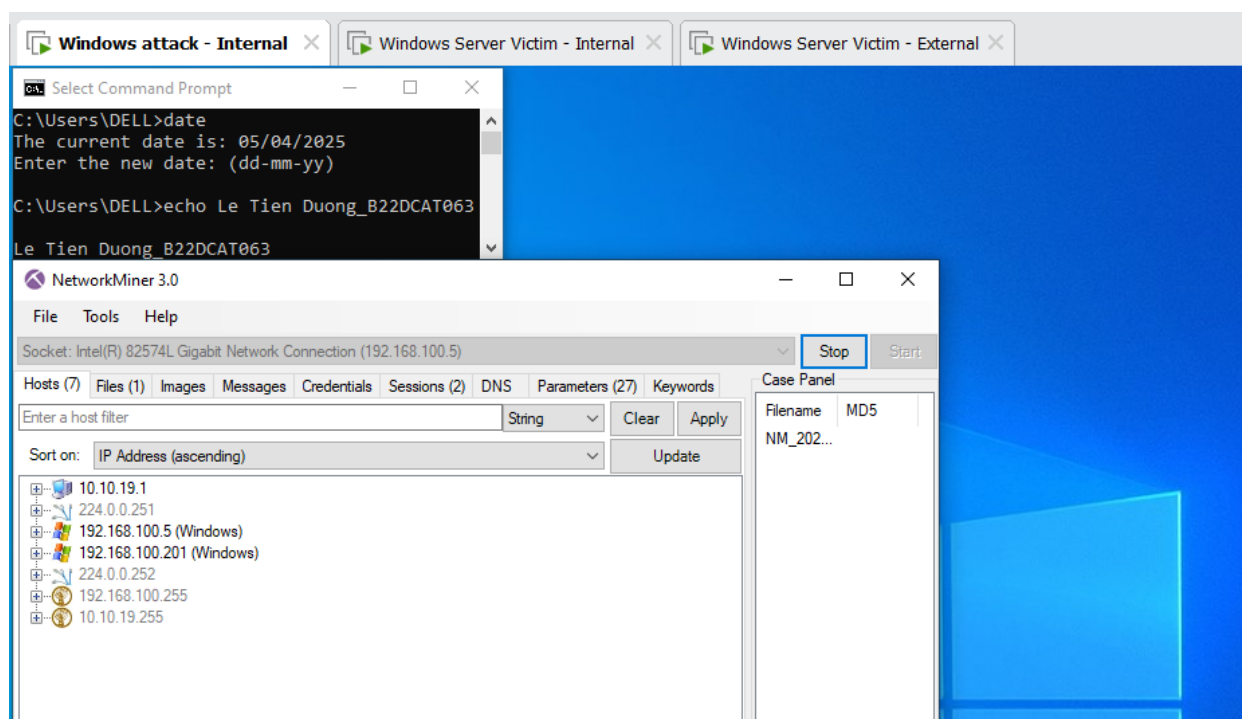
Trên Linux Sniffer dùng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp.



Hình 20 – Bắt gói tin trên dải 10.10.19.0/24 và lọc theo giao thức ftp

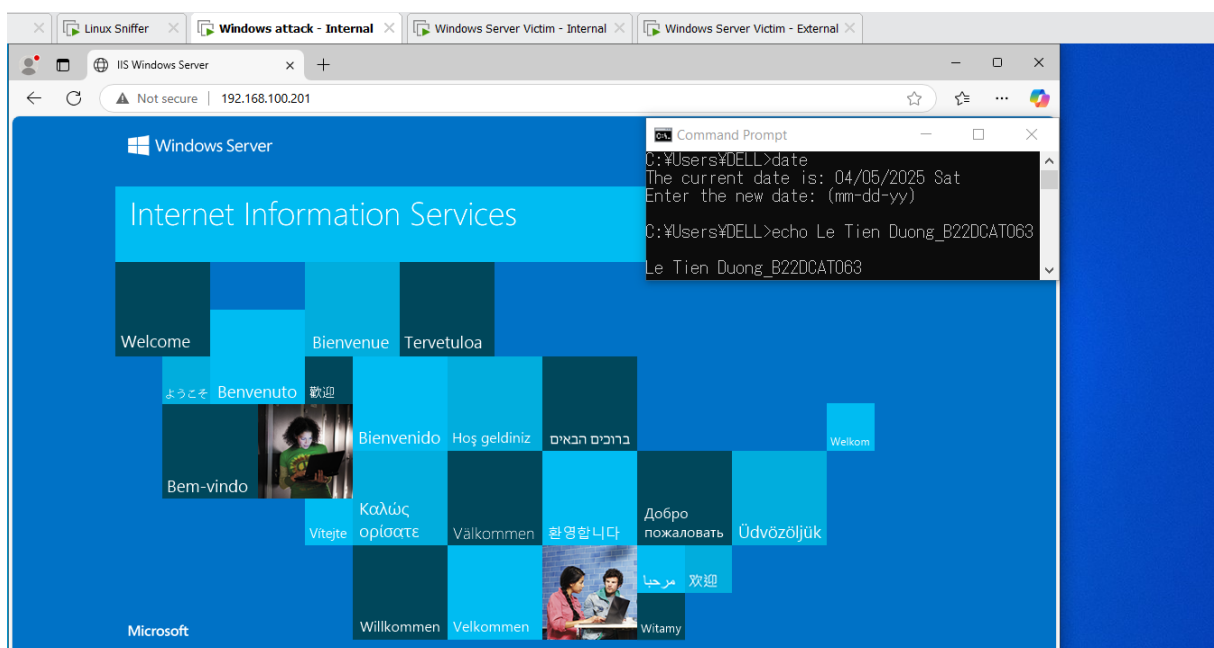
2.2.3 Sử dụng Network Miner để bắt và phân tích các gói tin

Trên máy Windows 10 Internal Attack khởi động Network Miner và chọn Socket: Intel® 82574L Gigabit Network Connection(192.168.100.5) và bắt đầu bắt gói tin.



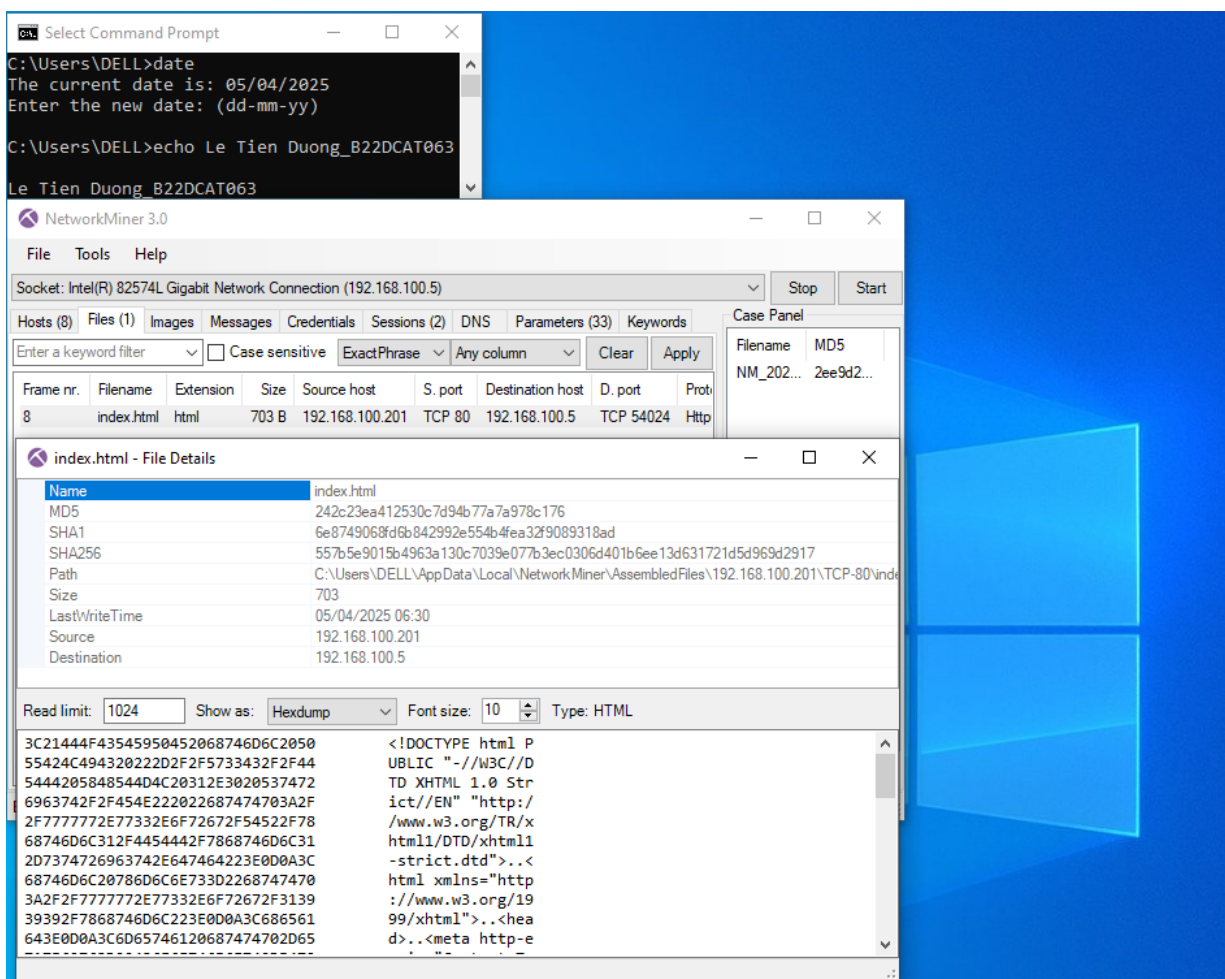
Hình 21 – Chọn Socket và bắt đầu bắt gói tin

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



Hình 22 – Kết nối đến trang web của Windows 2019 Server Internal

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



Hình 23 – Xem dữ liệu gói tin index.html vừa 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#>