

**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:

B22DCAT034 Trương Quốc Bảo

Giảng viên hướng dẫn: TS. Đinh Trường Duy

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 Công cụ bắt dữ liệu mạng tcpdump.....	5
1.2.2 Công cụ bắt dữ liệu mạng Wireshark.....	7
1.2.3 Công cụ bắt dữ liệu mạng Network Miner.....	9
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	12
2.1 Chuẩn bị môi trường	12
2.2 Các bước thực hiện.....	12
2.2.1 Sử dụng tcpdump	12
2.2.2 Sử dụng Wireshark để bắt và phân tích gói tin	19
2.2.3 Sử dụng Network Miner để bắt và phân tích gói tin	24
TÀI LIỆU THAM KHẢO	28

DANH MỤC CÁC HÌNH VẼ

Hình 1 Lệnh tcpdump -D	6
Hình 2 Lệnh tcpdump -r capture.pcap.....	7
Hình 3 Hoạt động của Wireshark.....	8
Hình 4 Thông tin tại tab Host trong giao diện NetworkMiner.....	10
Hình 5 Thông tin tại tab Files trong giao diện NetworkMiner.....	11
Hình 6 Topo mạng cần cấu hình	12
Hình 7 Cấu hình mạng cho máy Linux Sniffer	13
Hình 8 Kiểm tra địa chỉ IP của máy Linux Sniffer	14
Hình 9 Kích hoạt các interfaces hoạt động ở chế độ hỗn hợp.....	15
Hình 10 Bắt gói tin trên dải mạng	15
Hình 11 Đọc các gói tin đã bắt được.....	16
Hình 12 Kiểm tra kết nối.....	16
Hình 13 Bắt các gói tin icmp của eth0	17
Hình 14 File pcap của eth0 ghi lại thông tin	17
Hình 15 Kiểm tra kết nối.....	18
Hình 16 Bắt các gói tin icmp của eth1	18
Hình 17 File pcap của eth1 ghi lại thông tin	19
Hình 18 Tùy chọn giao diện mạng	20
Hình 19 Kết nối ftp tới máy Windows Server Internal	21
Hình 20 Wireshark bắt được gói tin.....	22
Hình 21 Lưu file.....	22
Hình 22 Kết nối ftp tới máy Windows Server External	23
Hình 23 Wireshark bắt được gói tin.....	24
Hình 24 Tải công cụ Network Miner	24
Hình 25 Chạy quyền Administrator	25
Hình 26 Khởi động để bắt các gói tin	26
Hình 27 Kết nối đến trang web của Windows Server	27
Hình 28 Xem thông tin file index.html	27

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
HTTP	HyperText Transfer Protocol	Giao thức truyền tải siêu văn bản
FTP	File Transfer Protocol	Giao thức truyền tập tin
TCP	Transmission Control Protocol	Giao thức điều khiển truyền vận
IP	Internet Protocol	Giao thức mạng
ICMP	Internet Control Message Protocol	Giao thức kiểm soát tin nhắn 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:

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

1.2 Tìm hiểu lý thuyết

1.2.1 Công cụ bắt dữ liệu mạng tcpdump

1.2.1.1 Giới thiệu

Tcpdump là công cụ hỗ trợ phân tích các gói dữ liệu mạng theo dòng lệnh, cho phép khách hàng chặn và lọc các gói tin TCP/IP được truyền đi hoặc được nhận trên một mạng mà máy tính có tham gia. tcpdump sẽ lưu lại những gói tin đã bắt được, sau đó dùng để phân tích. Hiểu đơn giản, Tcpdump là công cụ dò mạng tìm Network, có vai trò trong việc gỡ rối và kiểm tra các vấn đề liên quan đến bảo mật và kết nối mạng.

Để lựa chọn gói tin phù hợp với biểu thức logic mà khách hàng nhập vào, tcpdump 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.

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...

1.2.1.2 Hoạt động với tcpdump

Cài đặt Tcpdump trên Linux

Nếu muốn sử dụng được lệnh tcpdump trên Linux bạn phải cài một gói tên như dưới đây:

Ubuntu, ta dùng lệnh

```
sudo apt-get install tcpdump -y
```

CentOS

```
yum install tcpdump -y
```

Một số lệnh cơ bản sử dụng tcpdump trên Linux

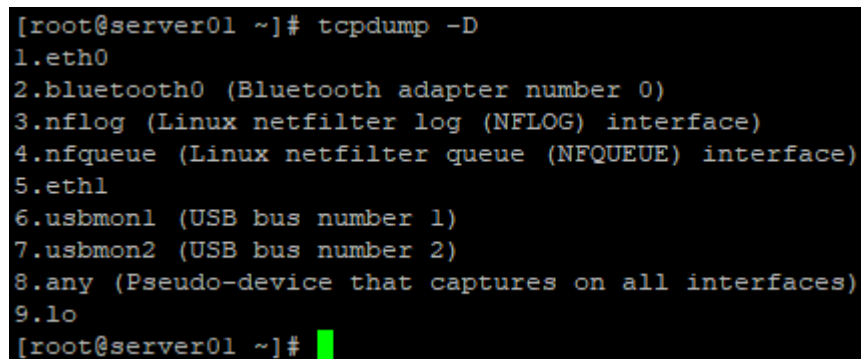
- Bắt gói tin theo địa chỉ nguồn

```
tcpdump -i emp0s3 src 192.168.100.1
```

- Bắt gói tin theo địa chỉ đích

```
tcpdump -i emp0s3 dst 192.168.100.1
```

- Xem các interface đang hoạt động



```
[root@server01 ~]# tcpdump -D
1.eth0
2.bluetooth0 (Bluetooth adapter number 0)
3.nflog (Linux netfilter log (NFLOG) interface)
4.nfqueue (Linux netfilter queue (NFQUEUE) interface)
5.eth1
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
8.any (Pseudo-device that captures on all interfaces)
9.lo
[root@server01 ~]#
```

Hình 1 Lệnh tcpdump -D

- Bắt gói tin trên interface

```
tcpdump -i
```

- Bắt các gói theo port

```
tcpdump -i enp0s3 port 22 -c 5 -n
```

- Bắt theo các gói TCP giữa hai host

```
tcpdump -i enp0s3 tcp -c 5
```

- Bắt gói tin với tùy chọn -c

Mặc định, tcpdump sẽ bắt liên tiếp các gói tin. Thao tác tổ hợp phím Ctrl + C. Nhưng với tùy chọn -c, chúng ta có thể chỉ cho tcpdump biết là "Tôi chỉ muốn bắt n gói."

n - là số gói tin cần bắt

Cú pháp như sau:

tcpdump -c n -i enp0s3

- Lưu file .pcap (Wireshark)

tcpdump -i enp0s3 -w /opt/capture.pcap

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes

4 packets captured

4 packets received by filter

0 packets dropped by kernel

- Đọc file PCAP

```
root@meditech:~# tcpdump -r capture.pcap
reading from file capture.pcap, link-type EN10MB (Ethernet)
16:43:19.889385 IP 192.168.100.192.ssh > 192.168.100.21.56724: Flags [P.], seq 9
05624736:905624800, ack 625881847, win 1497, length 64
16:43:19.889587 IP 192.168.100.192.ssh > 192.168.100.21.56724: Flags [P.], seq 6
4:192, ack 1, win 1497, length 128
16:43:19.889774 IP 192.168.100.21.56724 > 192.168.100.192.ssh: Flags [.], ack 64
, win 61, length 0
16:43:19.890345 IP 192.168.100.192.ssh > 192.168.100.21.56724: Flags [P.], seq 1
92:256, ack 1, win 1497, length 64
16:43:19.890587 IP 192.168.100.21.56724 > 192.168.100.192.ssh: Flags [.], ack 25
6, win 60, length 0
root@meditech:~#
```

Hình 2 Lệnh *tcpdump -r capture.pcap*

1.2.2 Công cụ bắt dữ liệu mạng Wireshark

1.2.2.1 Giới thiệu

Wireshark là một ứng dụng dùng để bắt (capture), phân tích và xác định các vấn đề liên quan đến network như: rớt gói tin, kết nối chậm, hoặc các truy cập bất thường. Phần mềm này cho phép quản trị viên hiểu sâu hơn các Network Packets đang chạy trên hệ thống, qua đó dễ dàng xác định các nguyên nhân chính xác gây ra lỗi.

Sử dụng WireShark có thể capture các packet trong thời gian thực (real time), lưu trữ chúng lại và phân tích chúng offline. Ngoài ra, nó cũng bao gồm các filter, color coding và nhiều tính năng khác, cho phép người dùng tìm hiểu sâu hơn về lưu lượng mạng cũng như inspect (kiểm tra) các packets.

Ứng dụng được viết bằng ngôn ngữ C và hệ điều hành Cross-platform, ngoài ra còn bao gồm có các bản phân phối Linux, Windows, OS X, FreeBSD, NetBSD và OpenBSD. Đây là một phần mềm mã nguồn mở, được cấp phép GPL do đó được miễn phí sử dụng, tự do chia sẻ và sửa đổi.

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.

1.2.2.2 Hoạt động của Wireshark

Wireshark 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.



Hình 3 Hoạt động của Wireshark

Các tính năng nổi bật của phần mềm bắt gói tin Wireshark:

- Hỗ trợ phân tích sâu hàng trăm giao thức và liên tục được cập nhật.
- Live capture và phân tích offline.
- Hoạt động đa nền tảng: Windows, Linux, MacOS, Solaris, FreeBSD, OpenBSD...
- Các gói tin đã capture có thể xem bằng giao diện hoặc sử dụng command line (tshark).
- Display filter mạnh mẽ.
- Hỗ trợ phân tích VoIP chuyên sâu.
- Hỗ trợ read/write nhiều định dạng: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer®

(compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek ...

- File capture được nén bằng gzip có thể được giải nén “on the fly”.
- Capture dữ liệu từ Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI ...
- Hỗ trợ decryption của nhiều giao thức như: IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2.
- Coloring rules cho phép thiết lập màu sắc cho các packet giúp phân tích nhanh và hiệu quả hơn.
- Output có thể export sang XML, PostScript®, CSV, hoặc plain text.

1.2.3 Công cụ bắt dữ liệu mạng Network Miner

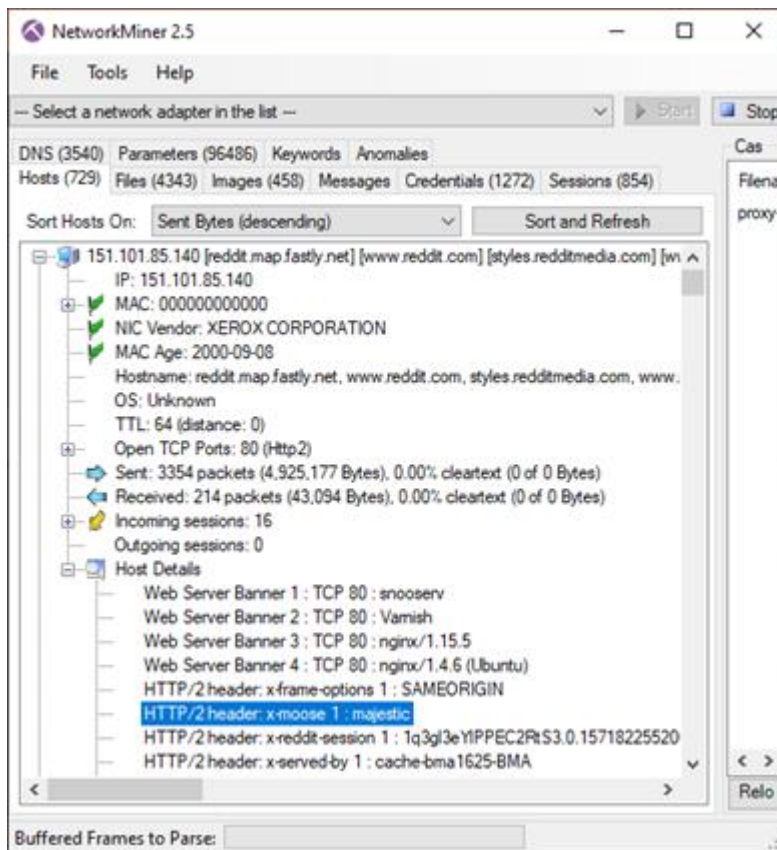
1.2.3.1 Giới thiệu

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. Có hai phiên bản miễn phí và pro (có trả phí) để lựa chọn, trong đó, phiên bản trả phí có tính năng cho phép tìm kiếm trực tuyến thông tin về địa chỉ IP mà máy chủ (cài networkminer) đang có kết nối tới.

1.2.3.2 Hoạt động với Network Miner

Những tính năng chính của NetworkMiner:

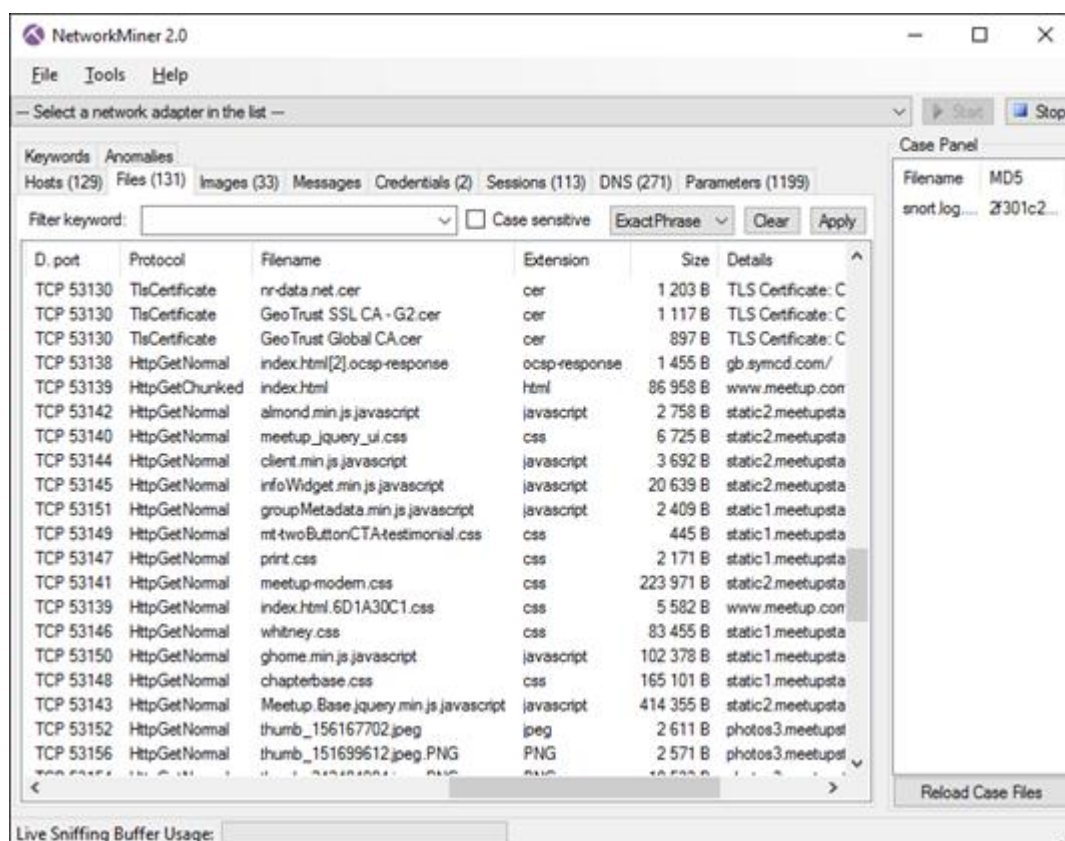
- Giám sát mọi gói tin trao đổi ra/vào máy chủ, trong đó cho phép phát hiện ảnh, các file dữ liệu và tài khoản đăng nhập.
- Dữ liệu hiển thị trực quan
- Dung lượng nhẹ



Hình 4 Thông tin tại tab Host trong giao diện NetworkMiner

Như hình trên, máy chủ cài NetworkMiner đang có kết nối với các địa chỉ IP bên ngoài. Thông tin về từng địa chỉ IP (tên máy chủ, hệ điều hành, cổng, phiên...) sẽ được gộp chi tiết vào một node, chỉ cần click vào là xem được các thông tin chi tiết. Chính vì cách bố trí thông tin này mà NetworkMiner tiện dụng trong việc phân tích máy chủ C&C (Command & Control) hay khi kiểm soát lưu lượng truy cập từ mạng lưới botnet. Tại hình trên ta còn thấy được các thông tin về địa chỉ MAC, các cổng dịch vụ của máy tính ở xa. Toàn bộ các thông tin này có thể được xuất ra file excel để thống kê, phân tích nhằm phát hiện sự bất thường..

Tại tab Files trong NetworkMiner cho phép trích xuất và lưu các tập tin được chuyển giao qua mạng, từ các trang Web chia sẻ trực tuyến, được thực hiện trên các giao thức FTP, TFTP, HTTP và SMB.



Hình 5 Thông tin tại tab Files trong giao diện NetworkMiner

Tại tab Credentials của NetworkMiner có thể thu thập thông tin người dùng gồm tài khoản đăng nhập và mật khẩu, kể cả thông tin người dùng sử dụng cho các dịch vụ trực tuyến phổ biến như Gmail hay Facebook. Tab Keyword cho phép tìm kiếm bằng các từ khóa. Các báo cáo cũng có thể được chuyển sang các tập tin HTML, TXT, Javascript,... Tab Anomalies giúp phát hiện các hiện tượng khả nghi và các sự cố có thể xảy ra đối với hệ thống mạng, giúp admin phòng tránh và xử lý kịp thời.

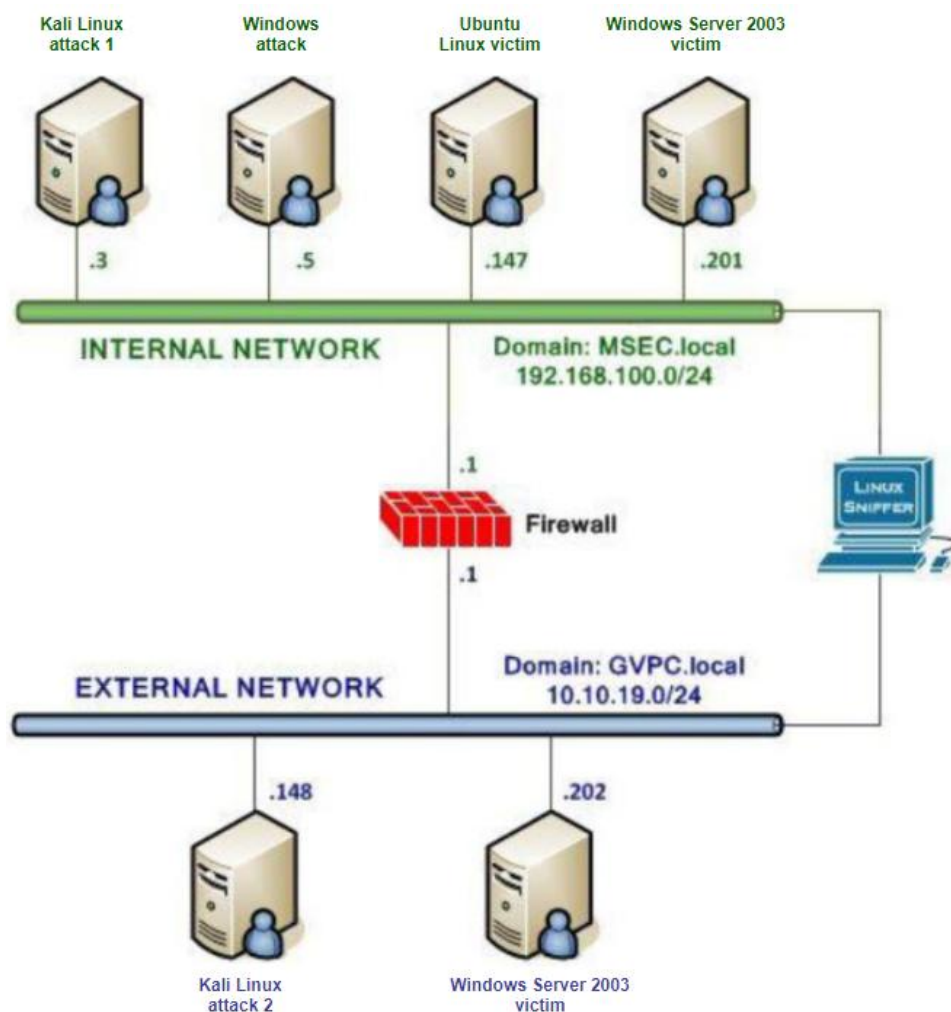
CHƯƠNG 2. NỘI DUNG THỰC HÀNH

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.



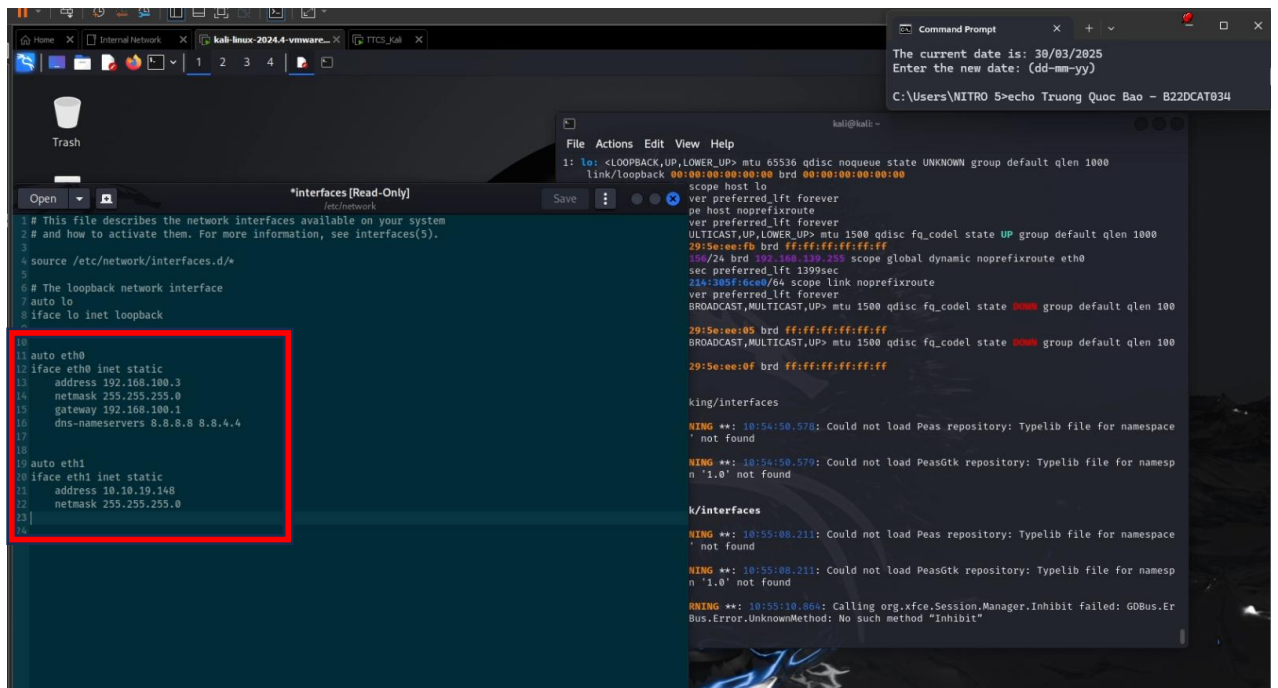
Hình 6 Topo mạng cần cấu hình

2.2 Các bước thực hiện

2.2.1 Sử dụng tcpdump

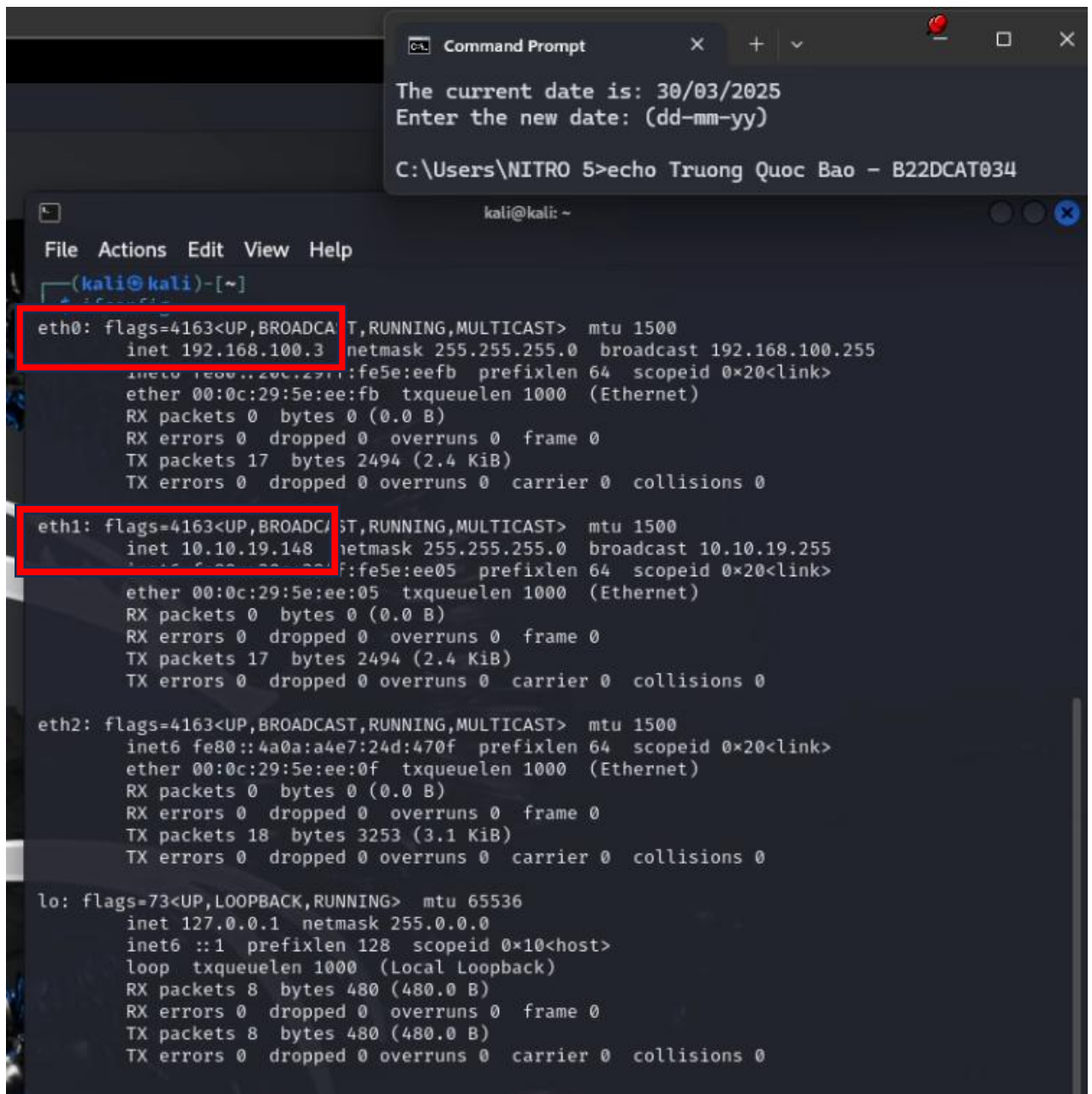
Đăng nhập Linux Sniffer và xem tất cả các interfaces trong hệ thống
(root@bt:~#ifconfig -a)

Cấu hình cho máy Linux Sniffer có 2 card mạng Internal (192.168.100.1) và mạng External (10.10.19.1). Cách làm tương tự các bài thực hành trước đó.



Hình 7 Cấu hình mạng cho máy Linux Sniffer

Kiểm tra cấu hình chính xác chưa bằng lệnh “ifconfig -a”. Nếu thấy các giao diện mạng khớp với địa chỉ ta đã cấu hình trước đó là thành công.



```
Command Prompt
The current date is: 30/03/2025
Enter the new date: (dd-mm-yy)
C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
eth0: flags=4163<UP,BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    ether 00:0c:29:5e:ee:fb txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 2494 (2.4 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
    ether 00:0c:29:5e:ee:05 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17 bytes 2494 (2.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4163<UP,BROADCAST, RUNNING, MULTICAST> mtu 1500
    inet6 fe80::4a0a:a4e7:24d:470f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:5e:ee:0f txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 3253 (3.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

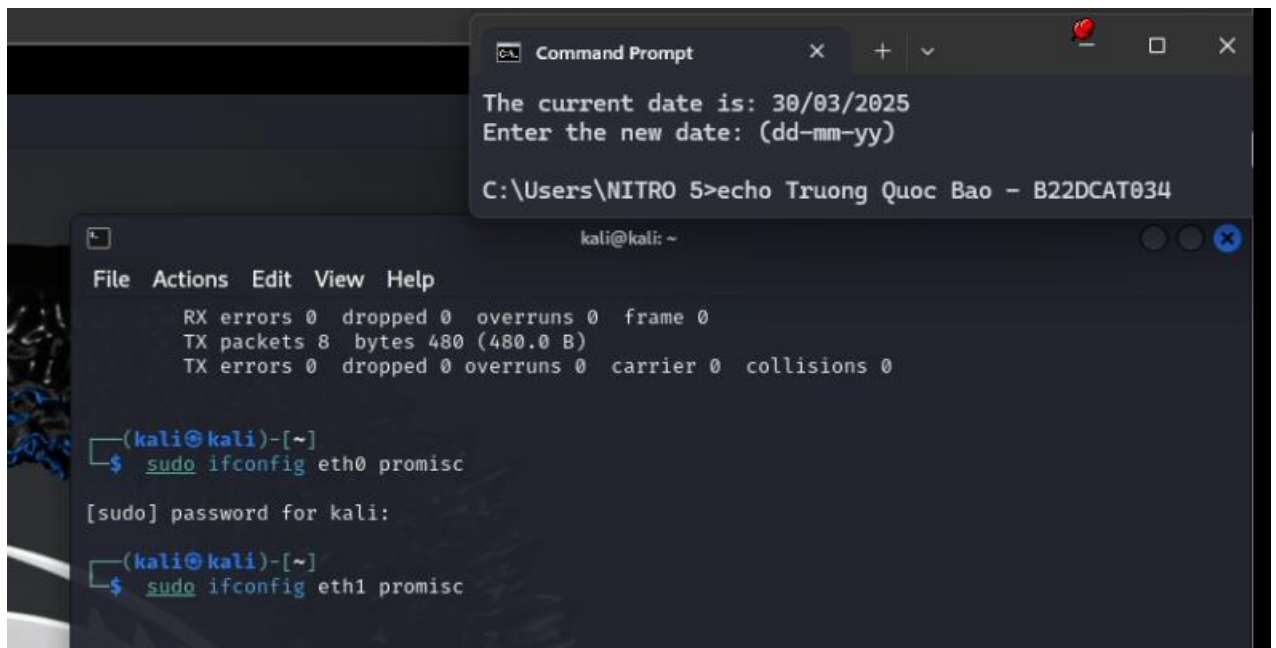
lo: flags=73<UP, LOOPBACK, RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 8 Kiểm tra địa chỉ IP của máy Linux Sniffer

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

sudo ifconfig eth0 promisc

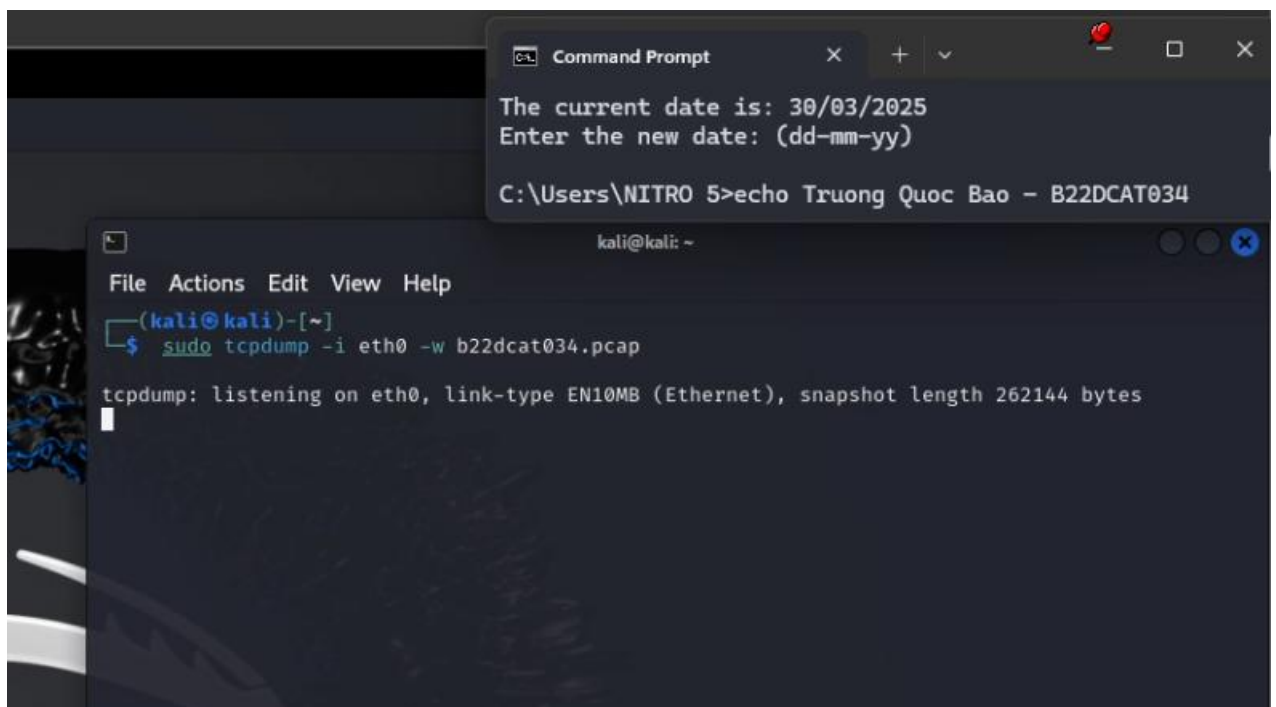
sudo ifconfig eth1 promisc



Hình 9 Kích hoạt các interfaces hoạt động ở chế độ hỗn hợp

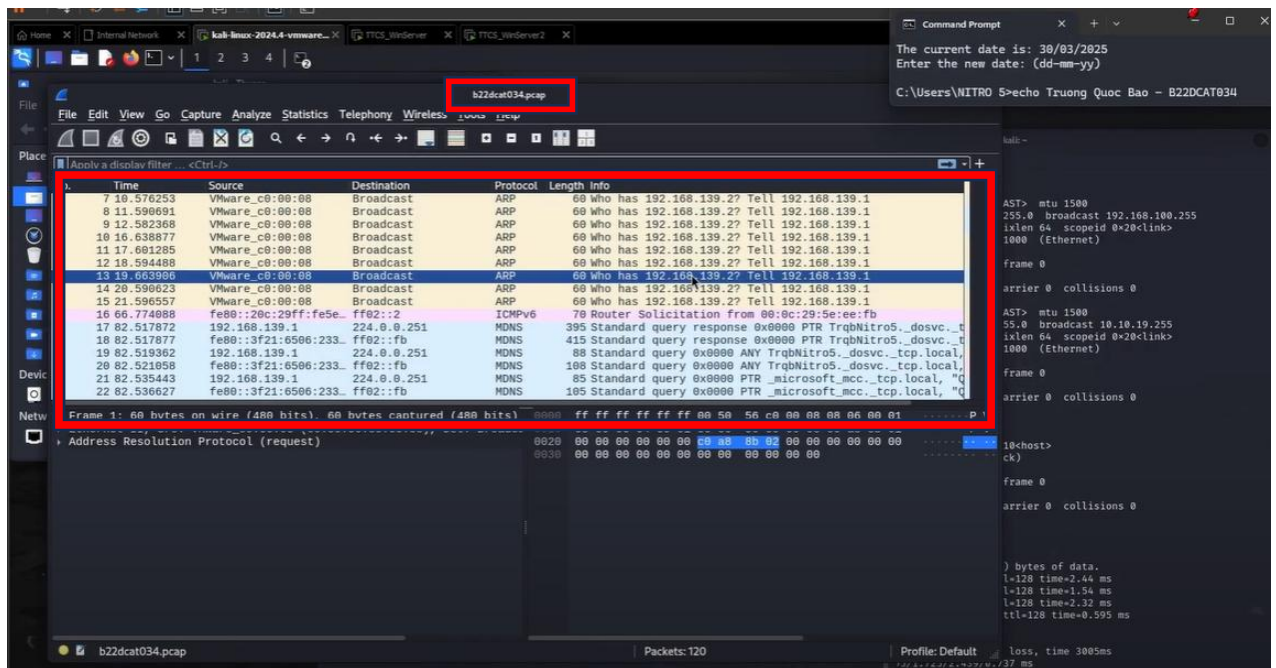
Khởi động tcpdump, bắt gói tin trên dải mạng 192.168.100.0/24 và gửi vào một file (thời gian chờ dữ liệu trong khoảng 5 phút).

Sudo tcpdump -I eth0 -w <tên file>



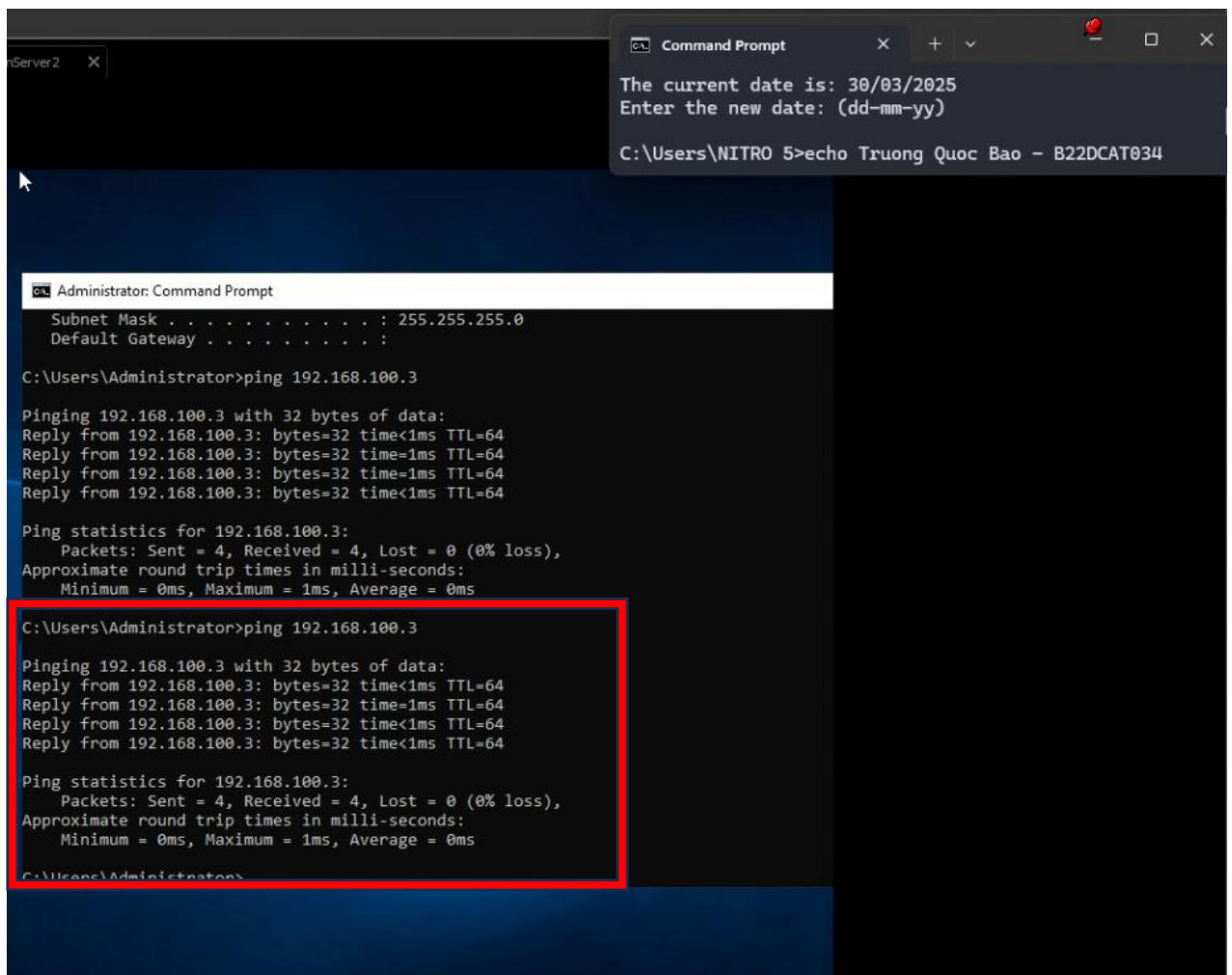
Hình 10 Bắt gói tin trên dải mạng

Sau một thời gian, có thể dùng công cụ Wireshark để đọc các gói tin vừa bắt được.



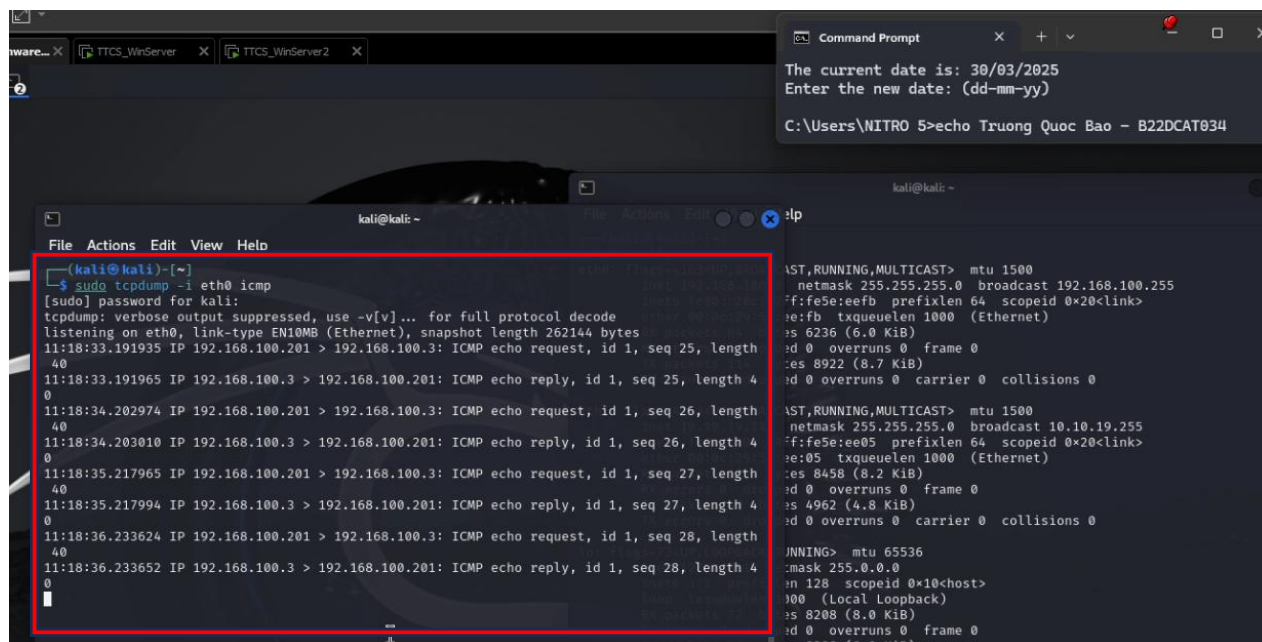
Hình 11 Đọc các gói tin đã bắt được

Đăng nhập Windows Server và ping đến dải mạng Internal



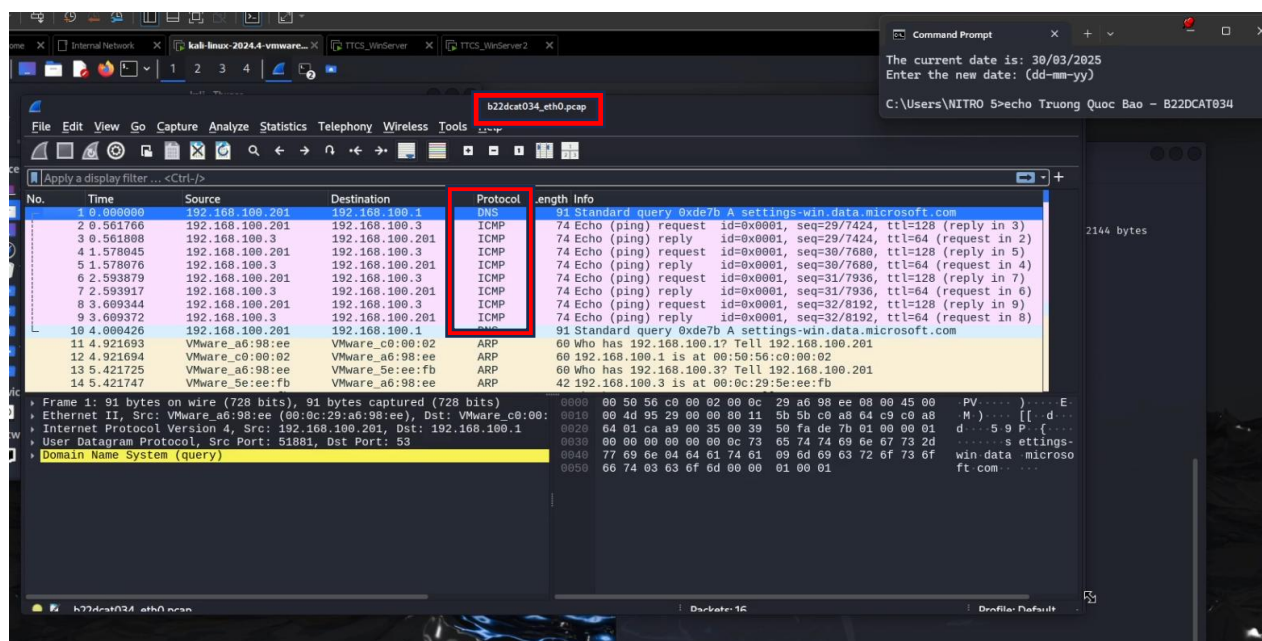
Hình 12 Kiểm tra kết nối

Trên máy Linux Sniffer đã nhận được thông báo về các gói tin icmp



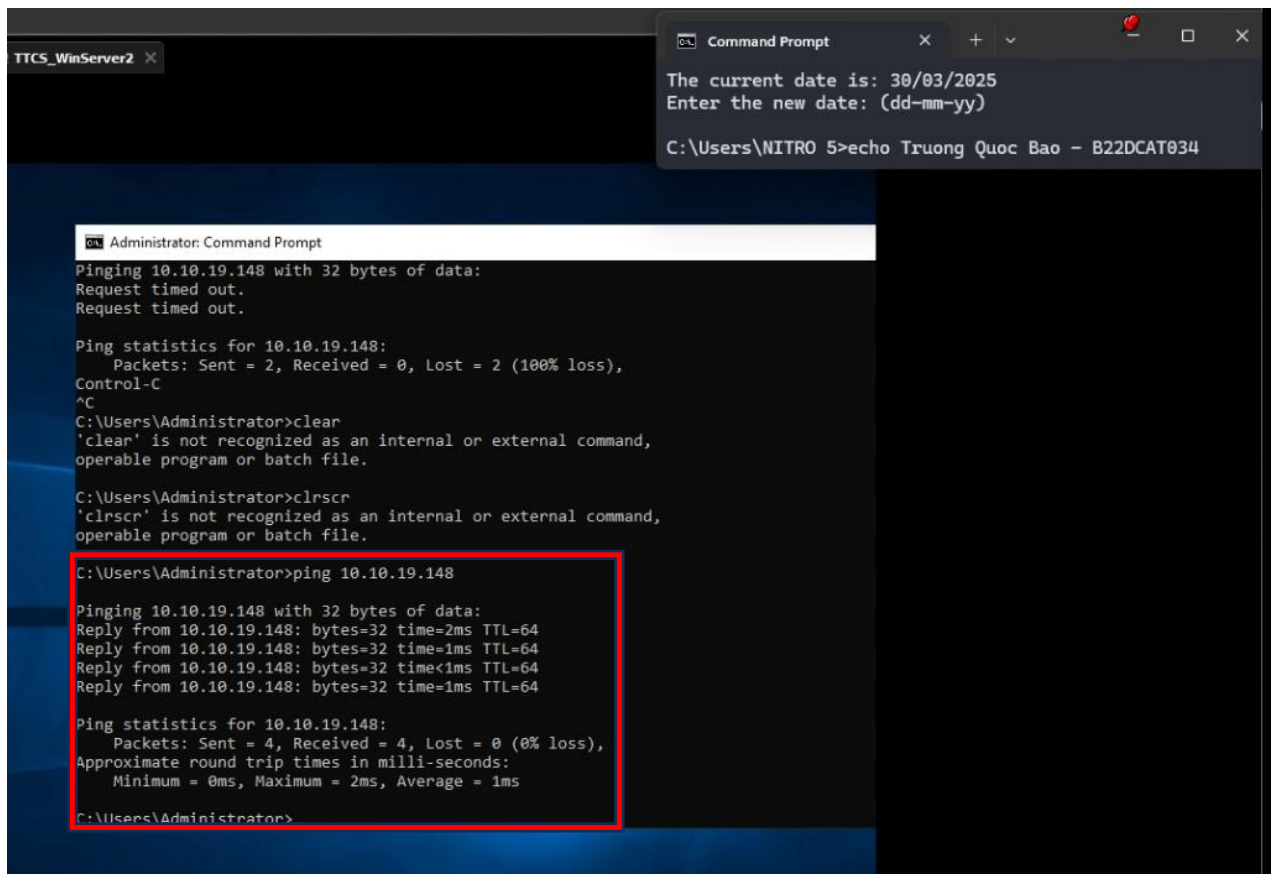
Hình 13 Bắt các gói tin icmp của eth0

Kiểm tra lại bằng Wireshark



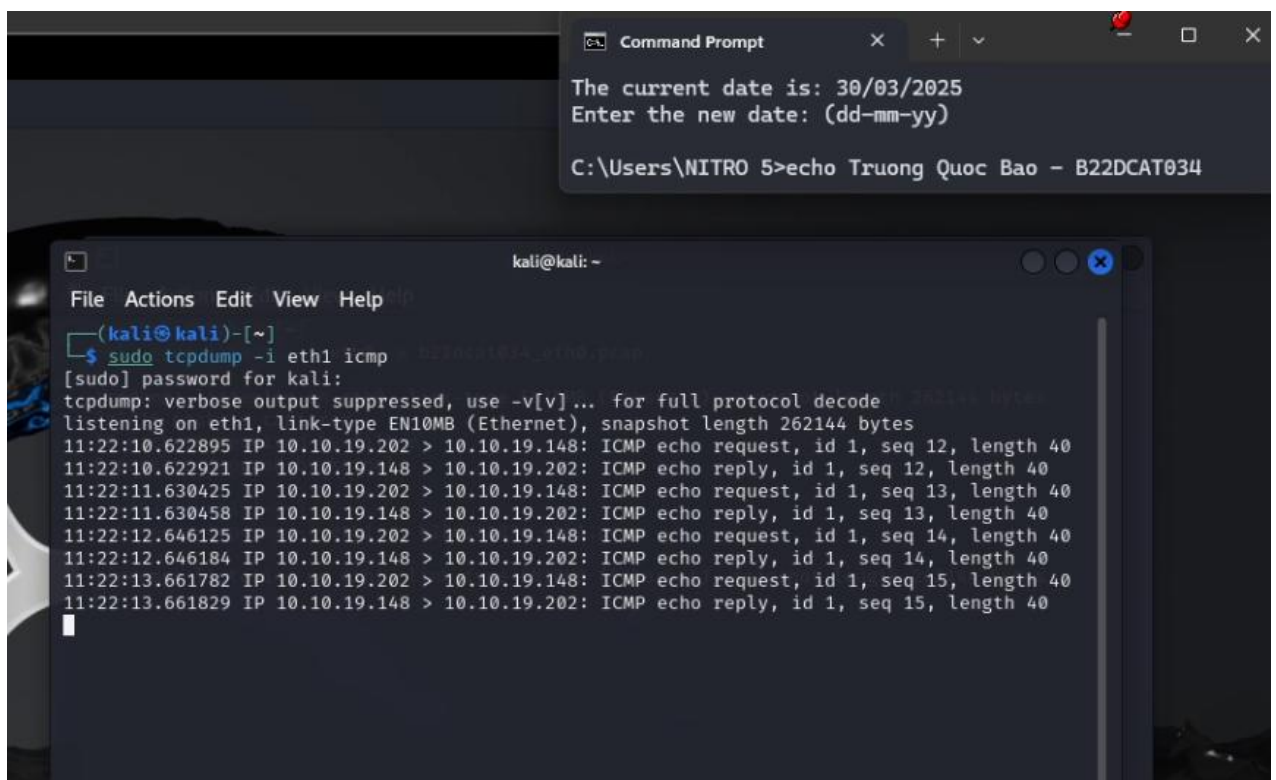
Hình 14 File pcap của eth0 ghi lại thông tin

Làm tương tự với máy Windows Server ở mạng External



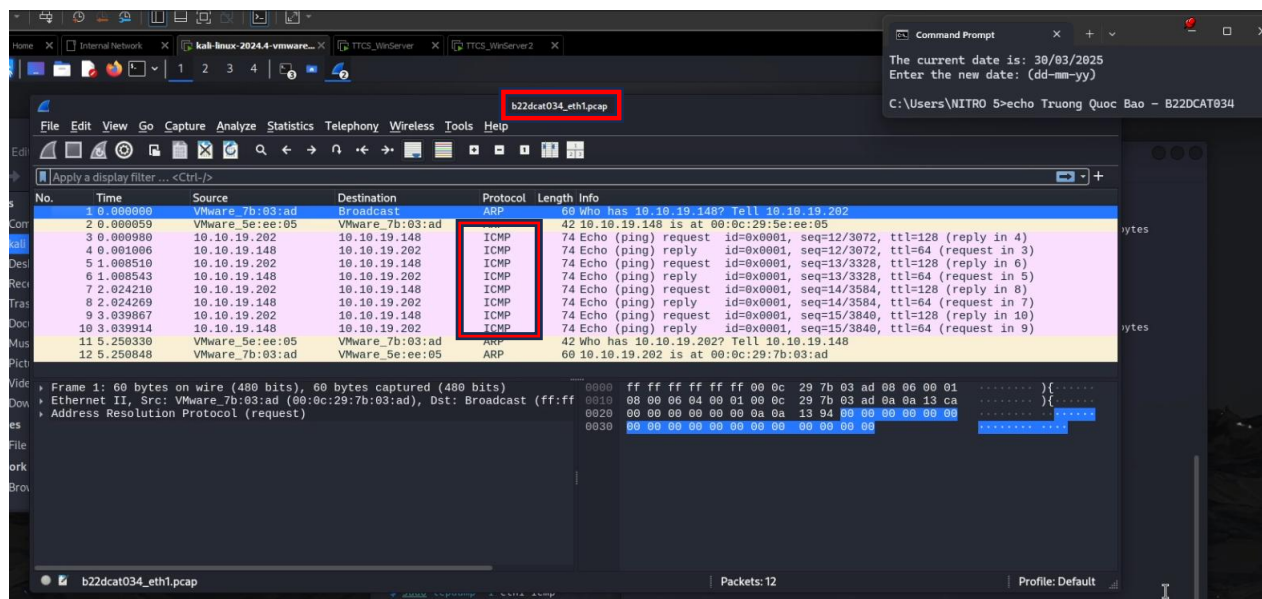
Hình 15 Kiểm tra kết nối

Các gói tin icmp cũng đã được thu thập



Hình 16 Bắt các gói tin icmp của eth1

Kiểm tra lại bằng Wireshark

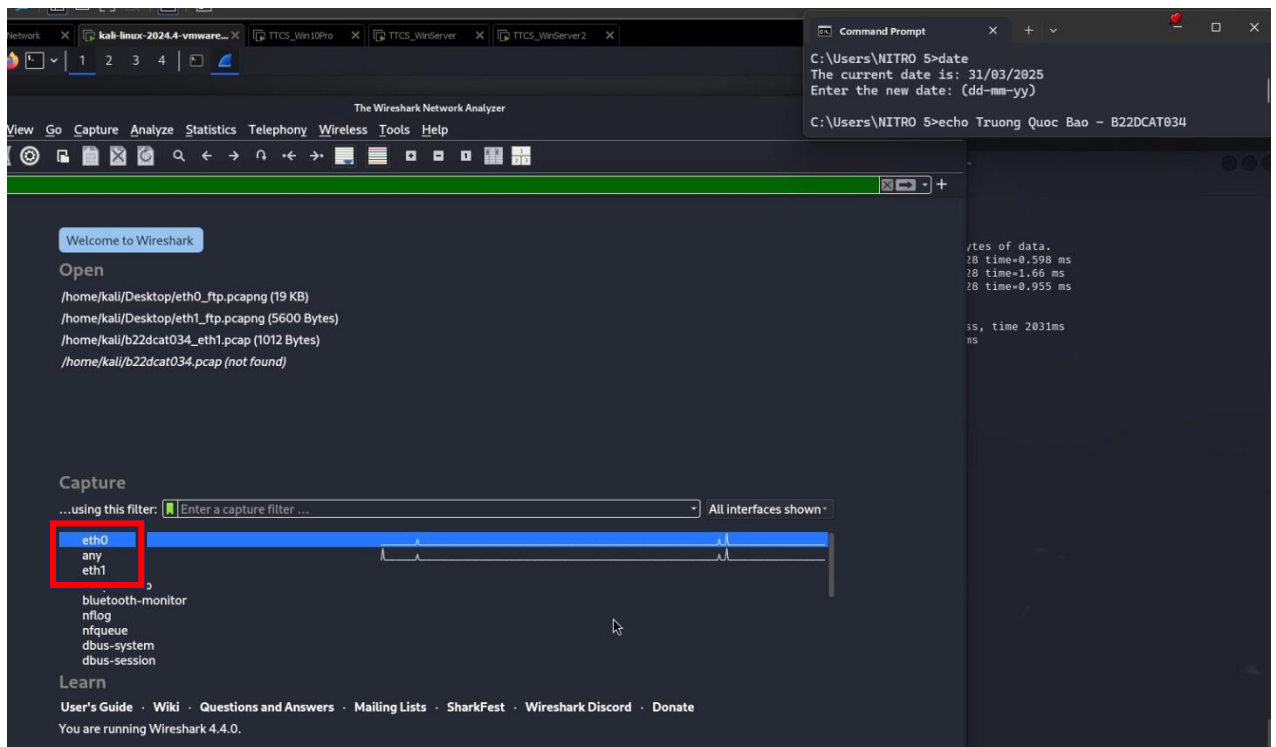


Hình 17 File pcap của eth1 ghi lại thông tin

2.2.2 Sử dụng Wireshark để bắt và phân tích gói tin

Tải Wireshark ở : <http://www.wireshark.org/download.html>

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 192.168.100.0/24, eth1 để bắt các gói tin trên dải mạng 10.10.19.0/24



Hình 18 Tùy chọn giao diện mạng

Trên máy Linux Sniffer kết nối tới ftp server (C:\ftp 192.168.100.201)

Đảm bảo đã chọn giao diện mạng tương ứng (eth0) ở trong Wireshark.

Kiểm tra trước khi kết nối bằng lệnh Ping giữa 2 máy

Máy Windows Server đã cấu hình cho phép kết nối ftp.


```
C:\Users\NITRO 5>date
The current date is: 31/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ftp 192.168.100.201
Connected to 192.168.100.201.
421 Service not available, remote server has closed connection.
ftp>
zsh: suspended ftp 192.168.100.201

(kali@kali)-[~]
$ ftp 192.168.0.1
^Z
zsh: suspended ftp 192.168.0.1

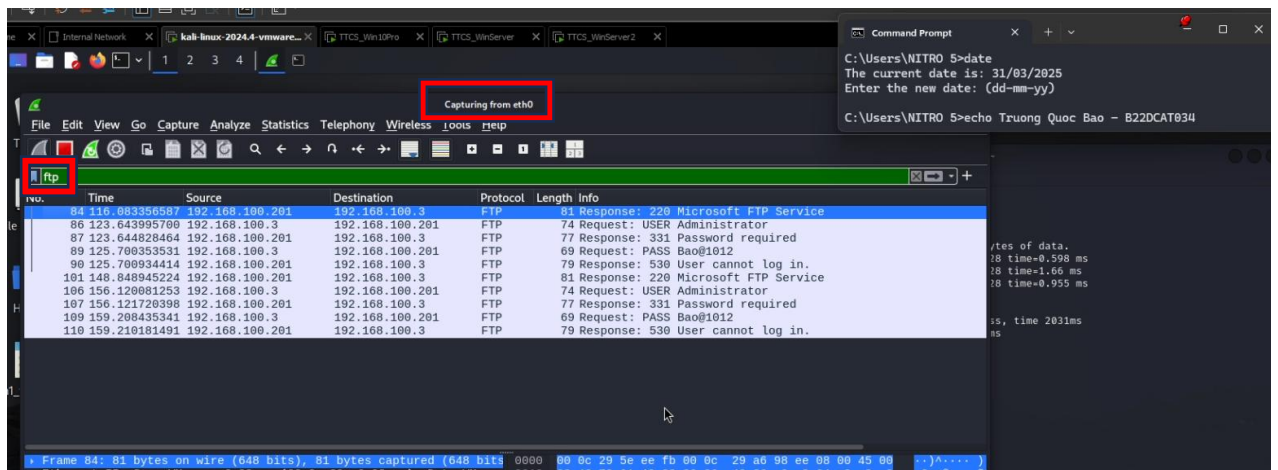
(kali@kali)-[~]
$
(kali@kali)-[~]
$ ping 192.168.100.201
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data:
64 bytes from 192.168.100.201: icmp_seq=1 ttl=128 time=0.598 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=1.66 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=0.955 ms
^C
— 192.168.100.201 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.598/1.071/1.660/0.441 ms

(kali@kali)-[~]
$ ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
Name (192.168.100.201:kali): Administrator
331 Password required
Password:
530 User cannot log in.
ftp: Login failed
ftp>
```

Hình 19 Kết nối ftp tới máy Windows Server Internal

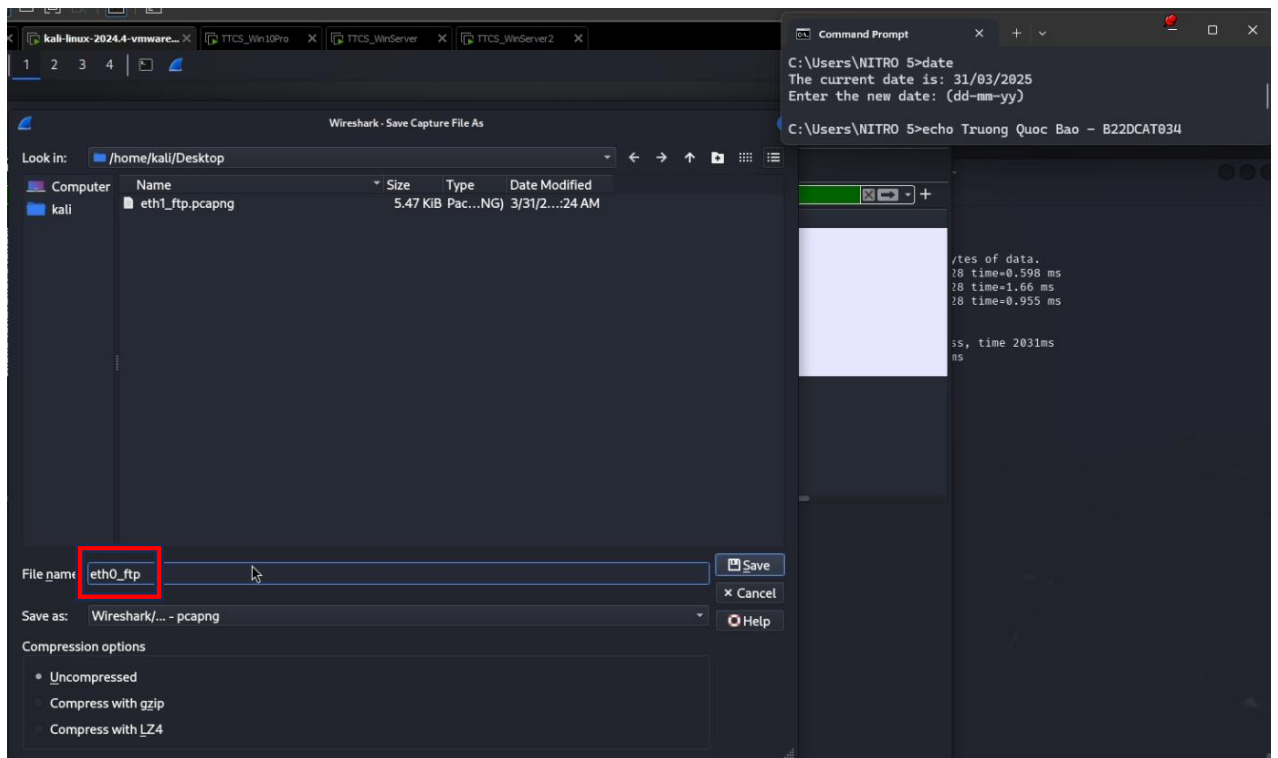
Trên Linux Sniffer dừng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp

Các gói tin thu thập được sẽ chứa thông tin đăng nhập vừa thực hiện và các yêu cầu khác giữa 2 máy.



Hình 20 Wireshark bắt được gói tin

Lưu file pcap sau khi đã hoàn thành.



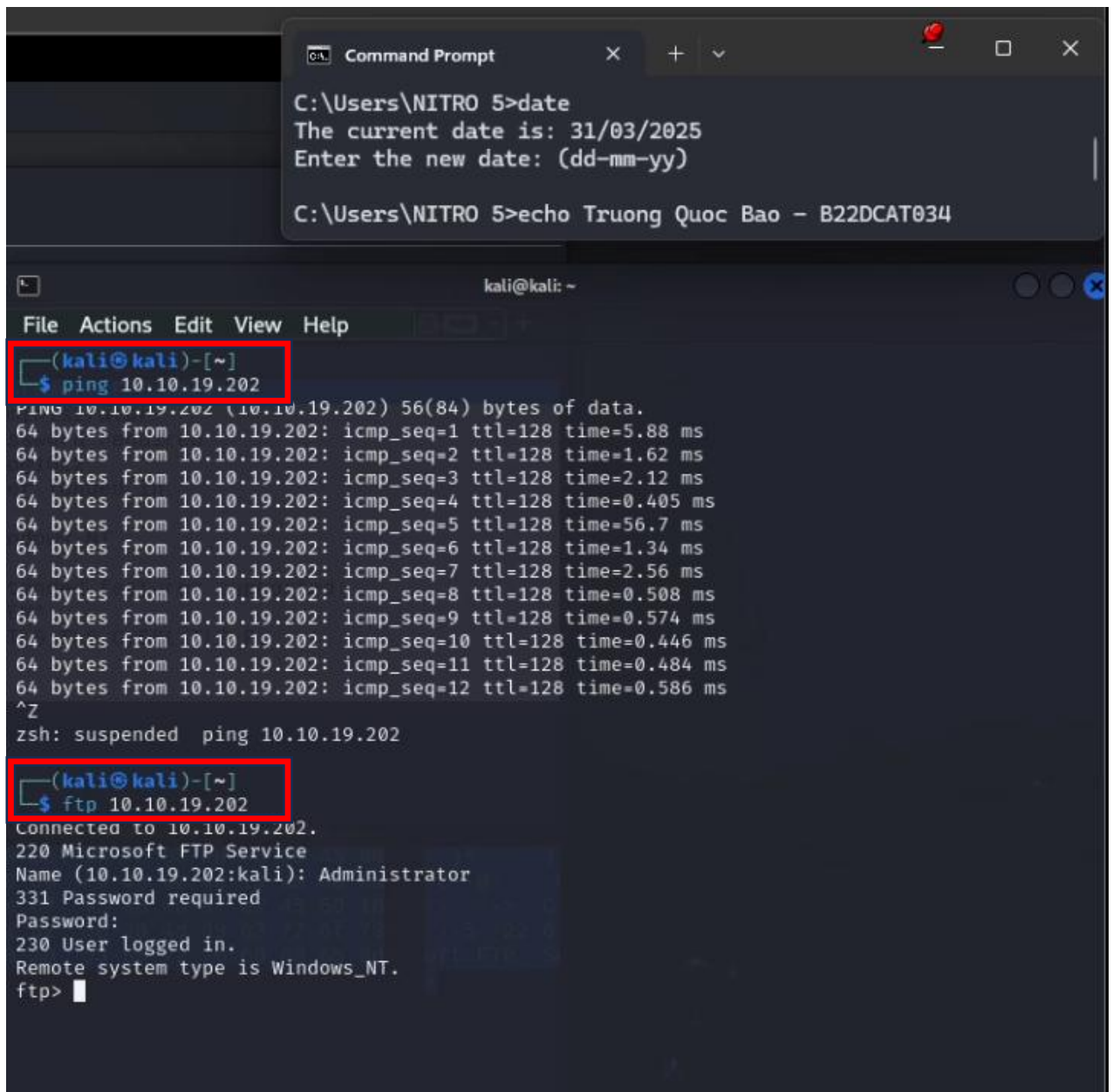
Hình 21 Lưu file

Trên máy Linux Sniffer kết nối tới ftp server (C:\ftp 10.10.19.202)

Đảm bảo đã chọn giao diện mạng tương ứng (eth1) ở trong Wireshark.

Kiểm tra trước khi kết nối bằng lệnh Ping giữa 2 máy

Máy Windows Server đã cấu hình cho phép kết nối ftp.



```
C:\Users\NITRO 5>date
The current date is: 31/03/2025
Enter the new date: (dd-mm-yy)

C:\Users\NITRO 5>echo Truong Quoc Bao - B22DCAT034

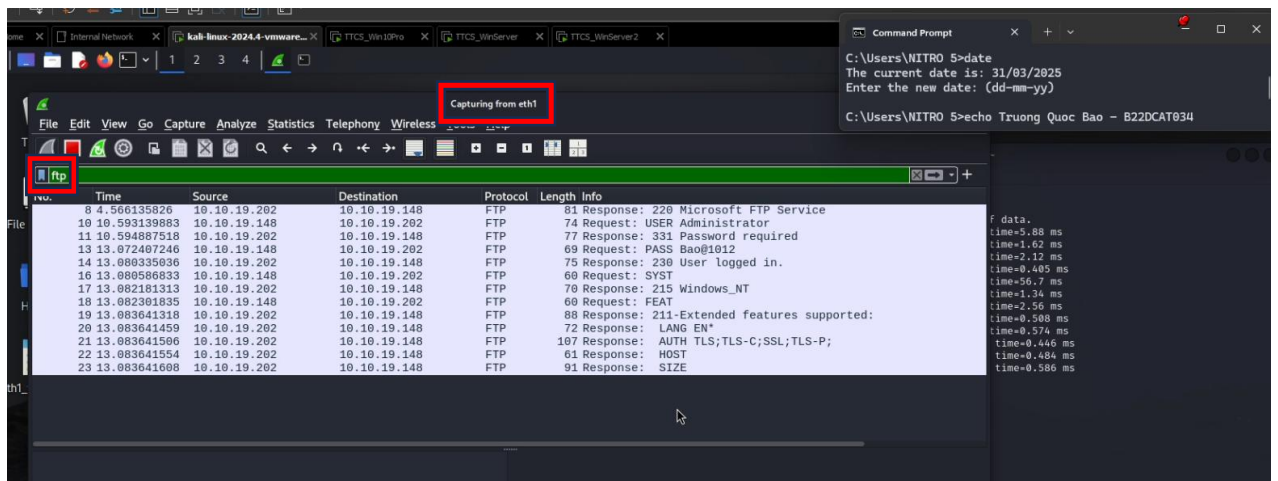
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ping 10.10.19.202
PING 10.10.19.202 (10.10.19.202) 56(84) bytes of data:
64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=5.88 ms
64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=1.62 ms
64 bytes from 10.10.19.202: icmp_seq=3 ttl=128 time=2.12 ms
64 bytes from 10.10.19.202: icmp_seq=4 ttl=128 time=0.405 ms
64 bytes from 10.10.19.202: icmp_seq=5 ttl=128 time=56.7 ms
64 bytes from 10.10.19.202: icmp_seq=6 ttl=128 time=1.34 ms
64 bytes from 10.10.19.202: icmp_seq=7 ttl=128 time=2.56 ms
64 bytes from 10.10.19.202: icmp_seq=8 ttl=128 time=0.508 ms
64 bytes from 10.10.19.202: icmp_seq=9 ttl=128 time=0.574 ms
64 bytes from 10.10.19.202: icmp_seq=10 ttl=128 time=0.446 ms
64 bytes from 10.10.19.202: icmp_seq=11 ttl=128 time=0.484 ms
64 bytes from 10.10.19.202: icmp_seq=12 ttl=128 time=0.586 ms
^Z
zsh: suspended ping 10.10.19.202

(kali@kali)-[~]
$ ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
Name (10.10.19.202:kali): Administrator
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Hình 22 Kết nối ftp tới máy Windows Server External

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

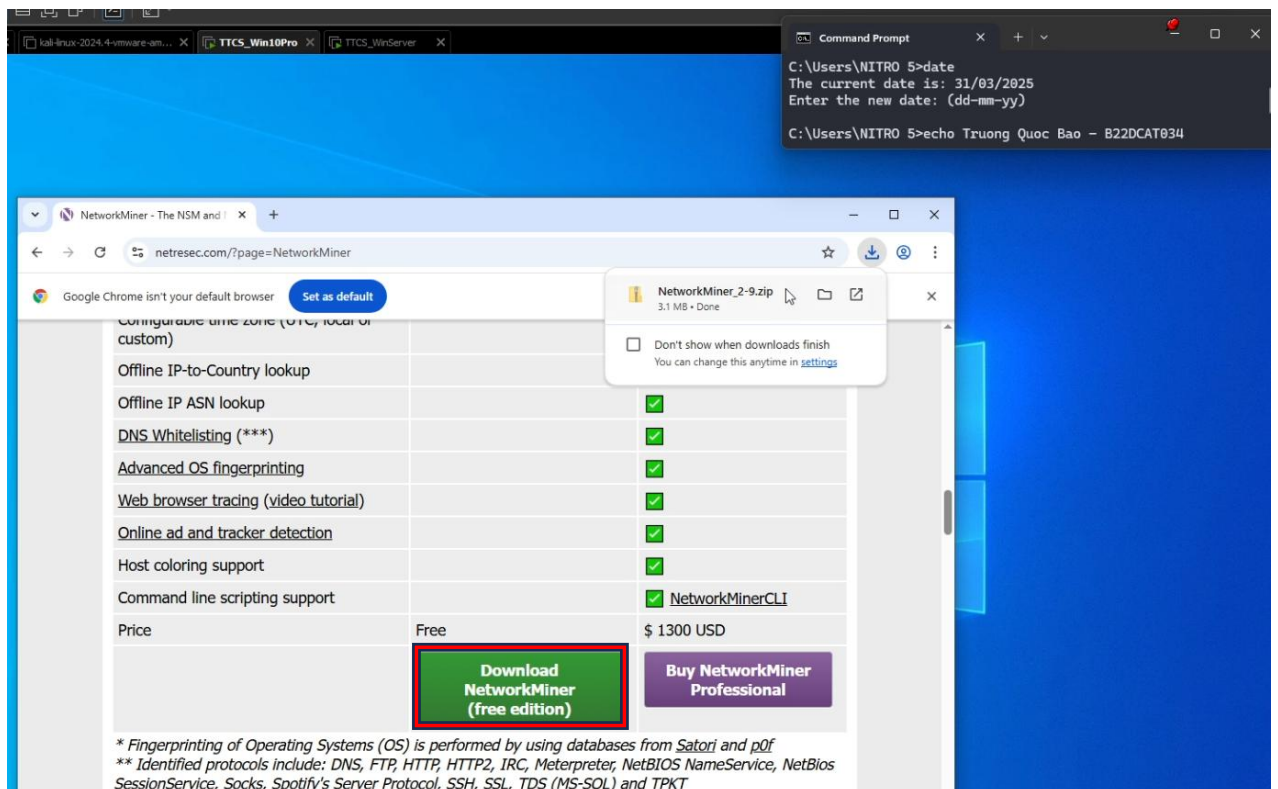
Các gói tin thu thập được sẽ chứa thông tin đăng nhập vừa thực hiện và các yêu cầu khác giữa 2 máy.



Hình 23 Wireshark bắt được gói tin

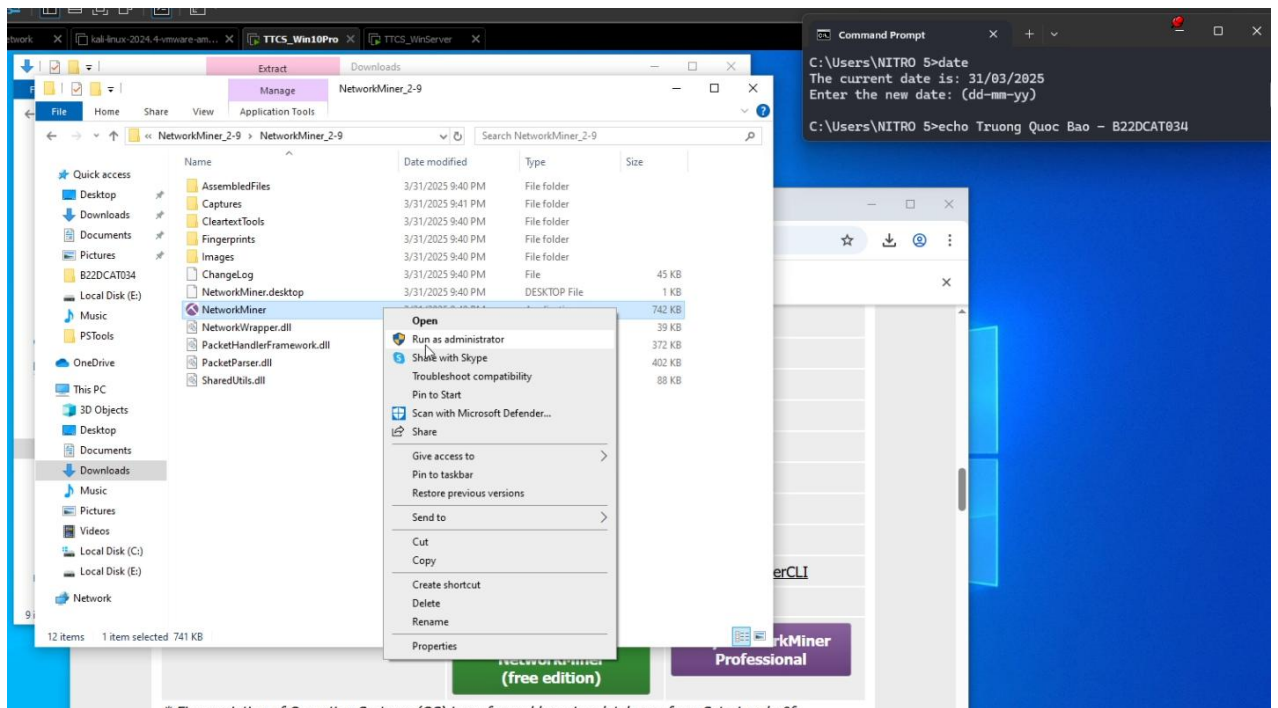
2.2.3 Sử dụng Network Miner để bắt và phân tích gói tin

Tải công cụ Network Miner trên trang chủ.



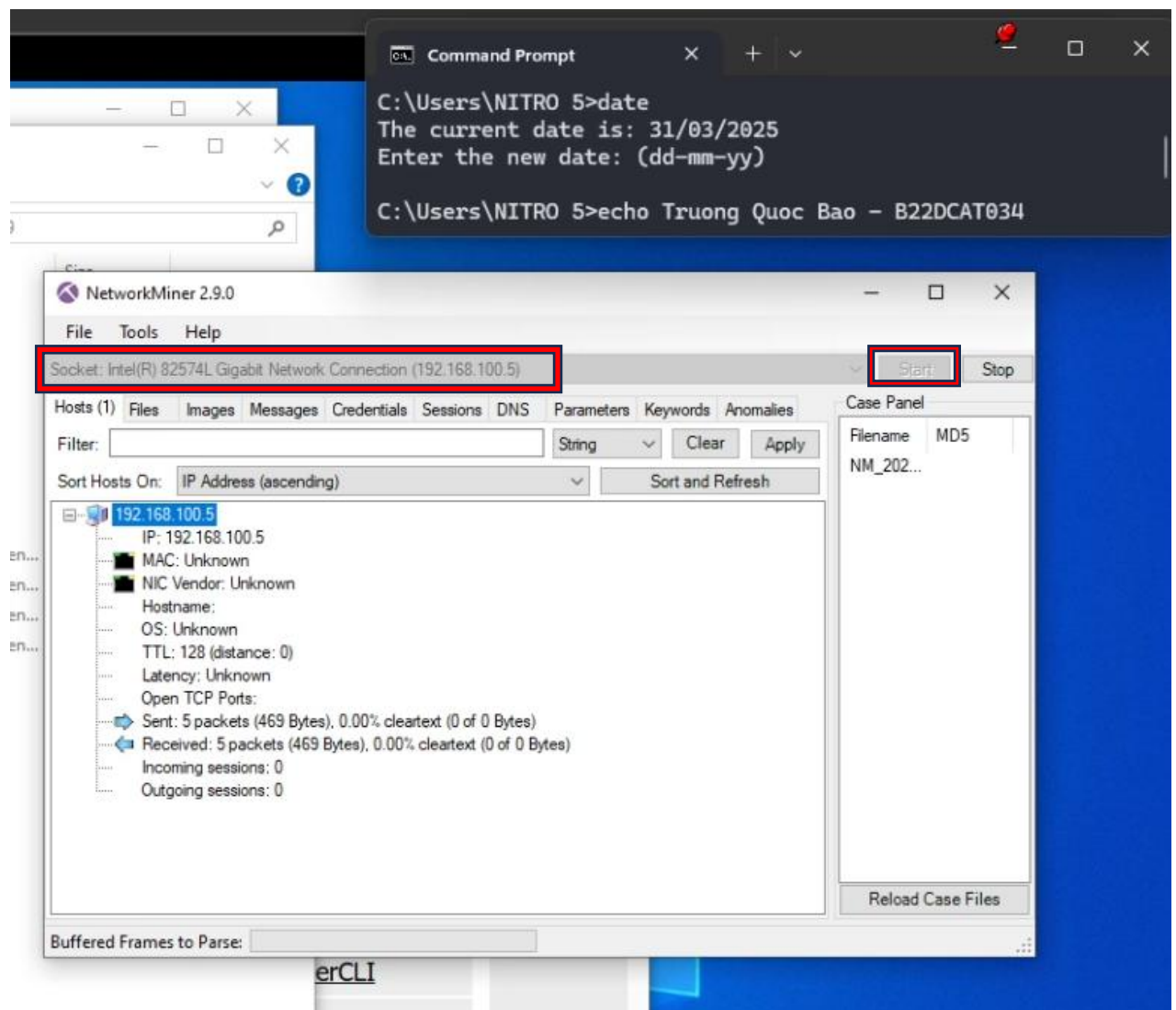
Hình 24 Tải công cụ Network Miner

Tiến hành cài đặt và giải nén. Chọn Run as Administrator.



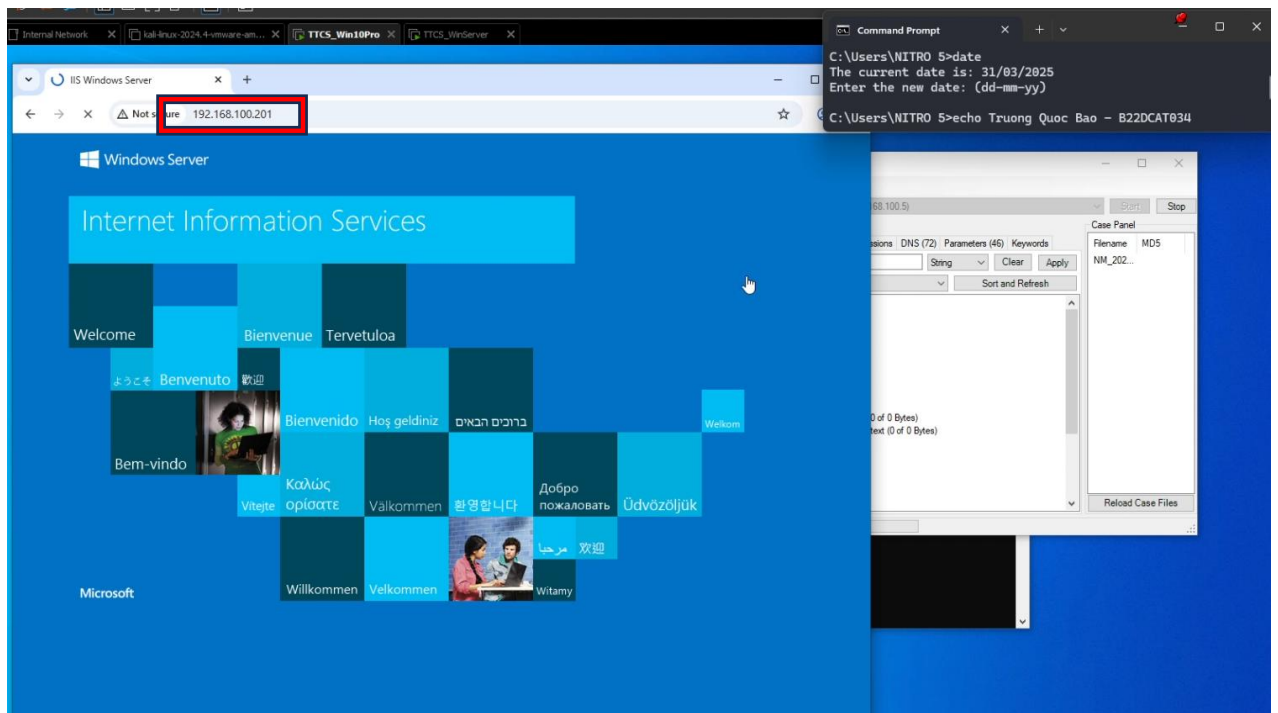
Hình 25 Chạy quyền Administrator

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.



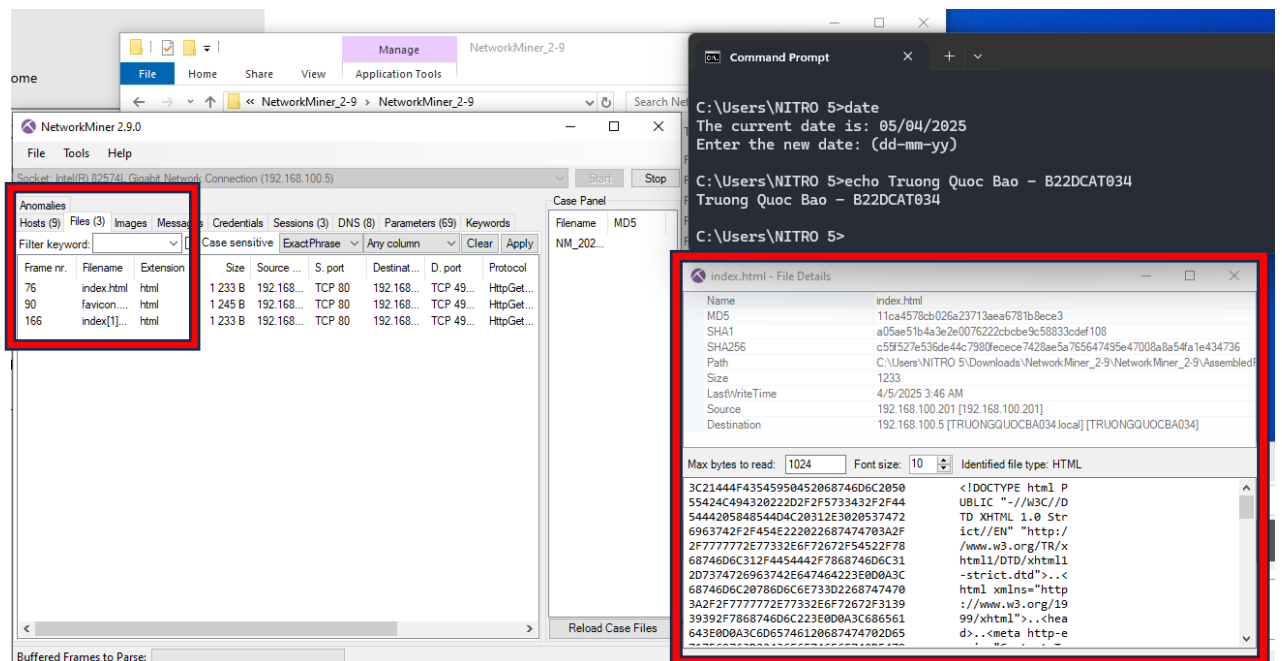
Hình 26 Khởi động để bắt các gói tin

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 27 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 28 Xem thông tin file index.html

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#>