

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

BỘ MÔN THỰC TẬP CƠ SỞ



BÀI 8: BẮT DỮ LIỆU MẠNG

Giảng viên : Nguyễn Ngọc Diệp

Sinh viên : Nguyễn Đức Anh

Mã sinh viên : B21DCAT031

Hệ : Đại học chính quy

Hà Nội, 3/2024

Table of Contents

1. Mục đích	3
2. Nội dung thực hành	3
2.1 Tìm hiểu lý thuyết.....	3
2.2 Tài liệu tham khảo.....	4
2.3 Chuẩn bị môi trường	4
2.4 Các bước thực hiện	4
a. Sử dụng tcpdump	4
b. Sử dụng Wireshark để bắt và phân tích các gói tin	10
c. Sử dụng Network Miner để bắt và phân tích các gói tin	14
3. Kết quả đạt được.....	16

1. Mục đích

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)

2. Nội dung thực hành

2.1 Tìm hiểu lý thuyết

- TCPDUMP thực chất là công cụ được phát triển nhằm mục đích nhận diện và phân tích các gói dữ liệu mạng theo dòng lệnh.
- TCPDUMP cho phép khách hàng chặn và hiển thị các gói tin được truyền đi hoặc được nhận trên một mạng có sự tham gia của máy tính.
- TCPDUMP xuất ra màn hình nội dung các gói tin (chạy trên card mạng mà máy chủ đang lắng nghe) phù hợp với biểu thức logic chọn lọc mà khách hàng nhập vào. Với từng loại tùy chọn khác nhau khách hàng có thể xuất những mô tả về gói tin này ra một file “pcap” để phân tích sau, và có thể đọc nội dung của file “pcap” đó với option -r của lệnh TCPDUMP, hoặc sử dụng các phần mềm khác như là : Wireshark.
- Trong trường hợp không có tùy chọn, lệnh TCPDUMP sẽ tiếp tục chạy cho đến khi nào nó nhận được một tín hiệu ngắt từ phía 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.

- Wireshark là một bộ phân tích gói mạng (network packet analyzer). Một network packet analyzer sẽ cố gắng nắm bắt các network packets và cố gắng hiển thị dữ liệu gói đó càng chi tiết càng tốt.

Sử dụng Wireshark nhằm các mục đích sau:

- Network administrators sử dụng Wireshark để khắc phục sự cố mạng.
- Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.
- Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.
- Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.
- Mọi người sử dụng Wireshark để học internals giao thức mạng.

- Cách hoạt động của Wireshark:

1. Bắt gói – Packet Capture
2. Lọc – Filtering

3. Hiện thị trực quan – Visualization

- Network Miner là một công cụ phân tích bảo mật mạng Nguồn Mở di động có thể giám sát lưu lượng của bộ điều hợp mạng được kết nối trong hệ điều hành Windows. Nó sử dụng một công cụ thu thập gói / dò tìm mạng thụ động có thể phát hiện IP, tên máy chủ, hệ điều hành, cổng và nhiều thông tin khác của bất kỳ kết nối nào. Công cụ bảo mật mạng yêu cầu cài đặt - riêng biệt - của WinPcap để hoạt động đúng và đáng tin cậy.

- Mục đích chính của Network Miner là thu thập dữ liệu để phân tích trong tương lai (chẳng hạn như phân tích bằng chứng pháp y) hơn là thu thập dữ liệu liên quan đến lưu lượng trên mạng. Thông tin được nhóm theo máy chủ chứ không phải theo gói hoặc khung mặc dù có thể chuyển đổi chế độ xem dễ dàng trong giao diện phần mềm.

2.2 Tài liệu tham khảo

- Đỗ Xuân Chợt, Bài giảng Mật mã học cơ sở, Học viện Công Nghệ Bưu Chính Viễn Thông, 2021.

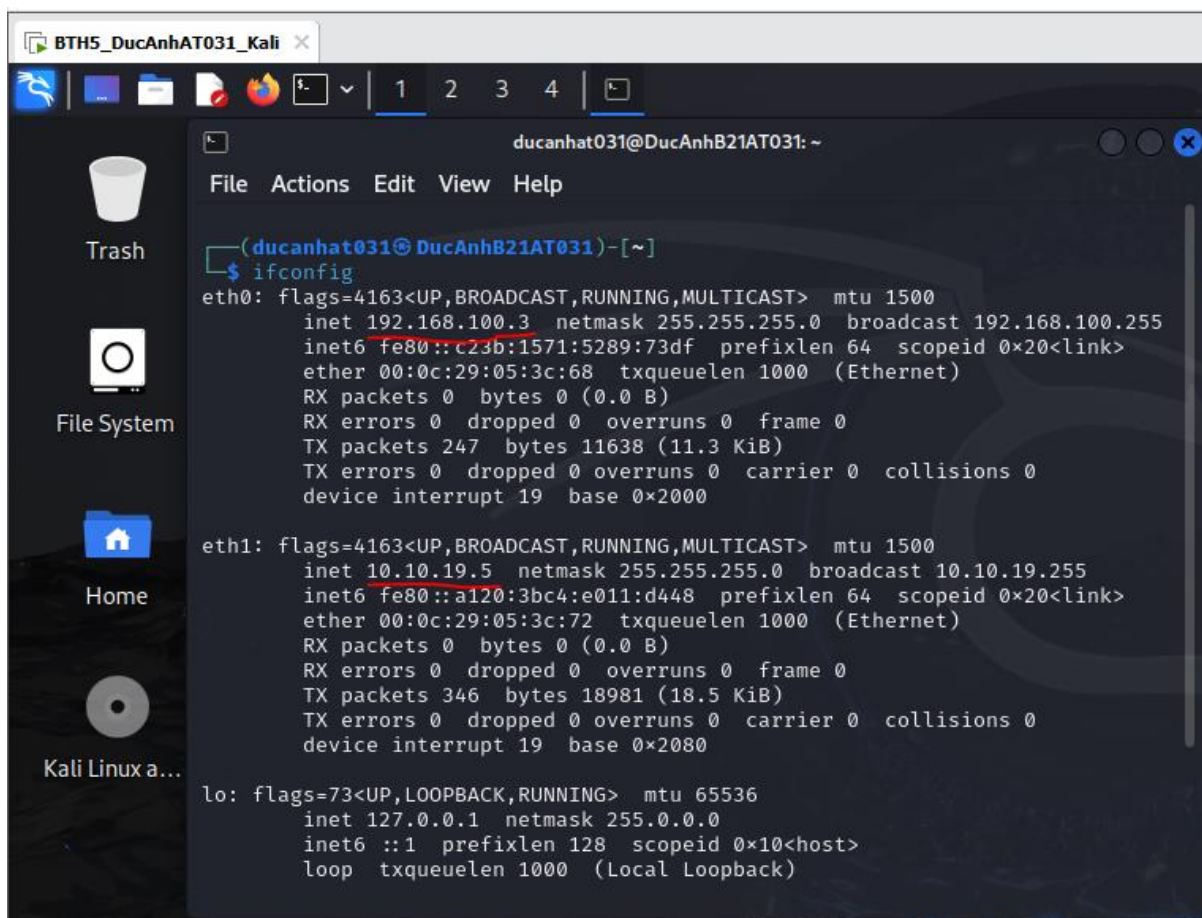
2.3 Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm 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.
- Topo mạng như đã cấu hình trong bài 5.

2.4 Các bước thực hiện

a. Sử dụng tcpdump

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



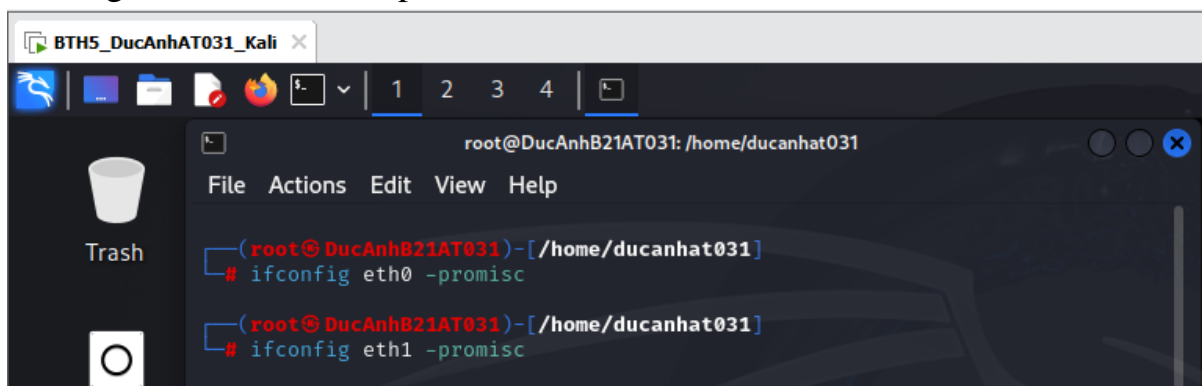
```
BTH5_DucAnhAT031_Kali x
ducanhat031@DucAnhB21AT031: ~
File Actions Edit View Help
(ducanhat031@DucAnhB21AT031)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::c23b:1571:5289:73df prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:3c:68 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 247 bytes 11638 (11.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.5 netmask 255.255.255.0 broadcast 10.10.19.255
    inet6 fe80::a120:3bc4:e011:d448 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:3c:72 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 346 bytes 18981 (18.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2080

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)
```

ip của 2 interfaces trên máy Kali

Kích hoạt các interfaces(eth0, eth1) hoạt động ở chế độ hỗn hợp bằng lệnh:
ifconfig <tên interfaces> -promisc



```
BTH5_DucAnhAT031_Kali x
root@DucAnhB21AT031: /home/ducanhat031
File Actions Edit View Help
(root@DucAnhB21AT031)-[/home/ducanhat031]
# ifconfig eth0 -promisc

(root@DucAnhB21AT031)-[/home/ducanhat031]
# ifconfig eth1 -promisc
```

IP các máy thuộc giải mạng Internal

```
BTH5_DucAnhAT031_Linux x Winserver Internal x
Terminal
ducanhat031@ducanhat031: ~
ducanhat031@ducanhat031:~$ ifconfig
ens33      Link encap:Ethernet  HWaddr 00:0c:29:b3:2f:c9
            inet addr:192.168.100.147  Bcast:192.168.100.255  Mask:255.255.255.0
            inet6 addr: fe80::7486:19aa:e725:1f30/64  Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:852 errors:0 dropped:0 overruns:0 frame:0
            TX packets:760 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:965492 (965.4 KB)  TX bytes:81456 (81.4 KB)
            Interrupt:19 Base address:0x2000

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128  Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:15636 errors:0 dropped:0 overruns:0 frame:0
            TX packets:15636 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1256872 (1.2 MB)  TX bytes:1256872 (1.2 MB)

ducanhat031@ducanhat031:~$ echo NguyenDucAnh_AT031
NguyenDucAnh_AT031
ducanhat031@ducanhat031:~$
```

```
BTH5_DucAnhAT031_Linux x Winserver Internal x
AnhAT031_Kali rator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e319:acb3:51b0:cde7%3
    IPv4 Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>
```

Tiến hành ping giữa hai máy:

```
BTH5_DucAnhAT031_Linux x Winserver Internal x
Terminal
ducanhat031@ducanhat031: ~
ducanhat031@ducanhat031:~$ 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=103 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=0.508 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=0.461 ms
64 bytes from 192.168.100.201: icmp_seq=4 ttl=128 time=0.392 ms
64 bytes from 192.168.100.201: icmp_seq=5 ttl=128 time=0.464 ms
64 bytes from 192.168.100.201: icmp_seq=6 ttl=128 time=0.435 ms
64 bytes from 192.168.100.201: icmp_seq=7 ttl=128 time=0.554 ms
64 bytes from 192.168.100.201: icmp_seq=8 ttl=128 time=0.459 ms
64 bytes from 192.168.100.201: icmp_seq=9 ttl=128 time=27.8 ms
64 bytes from 192.168.100.201: icmp_seq=10 ttl=128 time=0.463 ms
64 bytes from 192.168.100.201: icmp_seq=11 ttl=128 time=0.447 ms
64 bytes from 192.168.100.201: icmp_seq=12 ttl=128 time=0.439 ms
64 bytes from 192.168.100.201: icmp_seq=13 ttl=128 time=0.425 ms
64 bytes from 192.168.100.201: icmp_seq=14 ttl=128 time=0.389 ms
64 bytes from 192.168.100.201: icmp_seq=15 ttl=128 time=0.341 ms
64 bytes from 192.168.100.201: icmp_seq=16 ttl=128 time=0.488 ms
^C
--- 192.168.100.201 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 1529ms
rtt min/avg/max/ndev = 0.341/12.343/163.423/39.564 ms
ducanhat031@ducanhat031:~$

Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

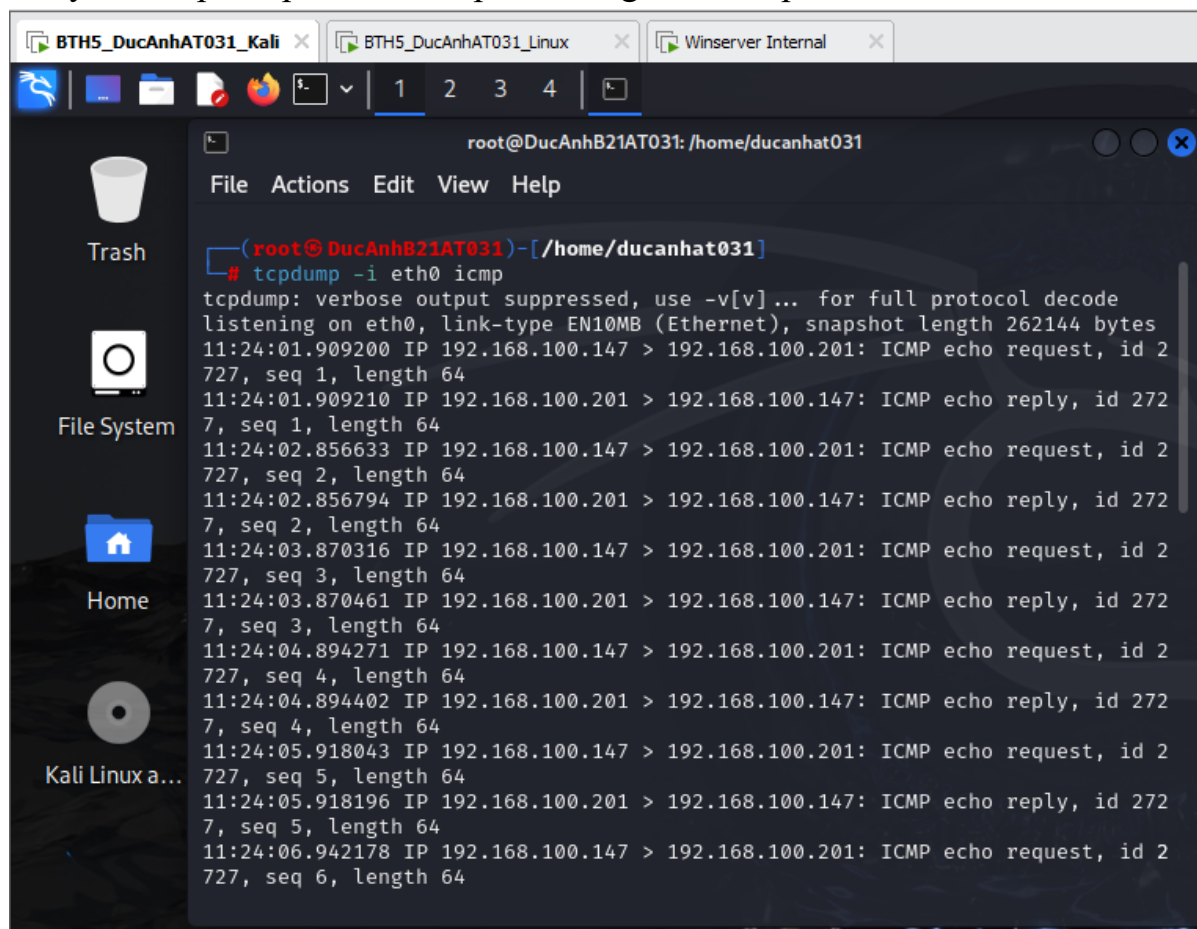
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e319:acb3:51b0:cde7%3
    IPv4 Address. . . . . : 192.168.100.201
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>ping 192.168.100.147

Pinging 192.168.100.147 with 32 bytes of data:
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64
Reply from 192.168.100.147: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.100.147:
    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>
```

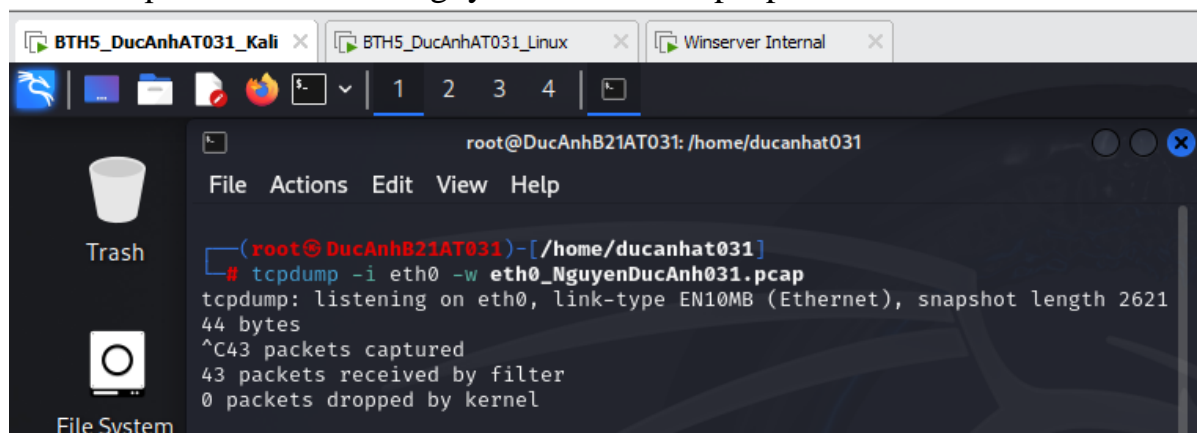
Chạy lệnh tcpdump -i eth0 icmp để hiện gói tin icmp



```
root@DucAnhB21AT031: /home/ducanhat031
File Actions Edit View Help

(root@DucAnhB21AT031)-[/home/ducanhat031]
# tcpdump -i eth0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:24:01.909200 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 1, length 64
11:24:01.909210 IP 192.168.100.201 > 192.168.100.147: ICMP echo reply, id 2727, seq 1, length 64
11:24:02.856633 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 2, length 64
11:24:02.856794 IP 192.168.100.201 > 192.168.100.147: ICMP echo reply, id 2727, seq 2, length 64
11:24:03.870316 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 3, length 64
11:24:03.870461 IP 192.168.100.201 > 192.168.100.147: ICMP echo reply, id 2727, seq 3, length 64
11:24:04.894271 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 4, length 64
11:24:04.894402 IP 192.168.100.201 > 192.168.100.147: ICMP echo reply, id 2727, seq 4, length 64
11:24:05.918043 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 5, length 64
11:24:05.918196 IP 192.168.100.201 > 192.168.100.147: ICMP echo reply, id 2727, seq 5, length 64
11:24:06.942178 IP 192.168.100.147 > 192.168.100.201: ICMP echo request, id 2727, seq 6, length 64
```

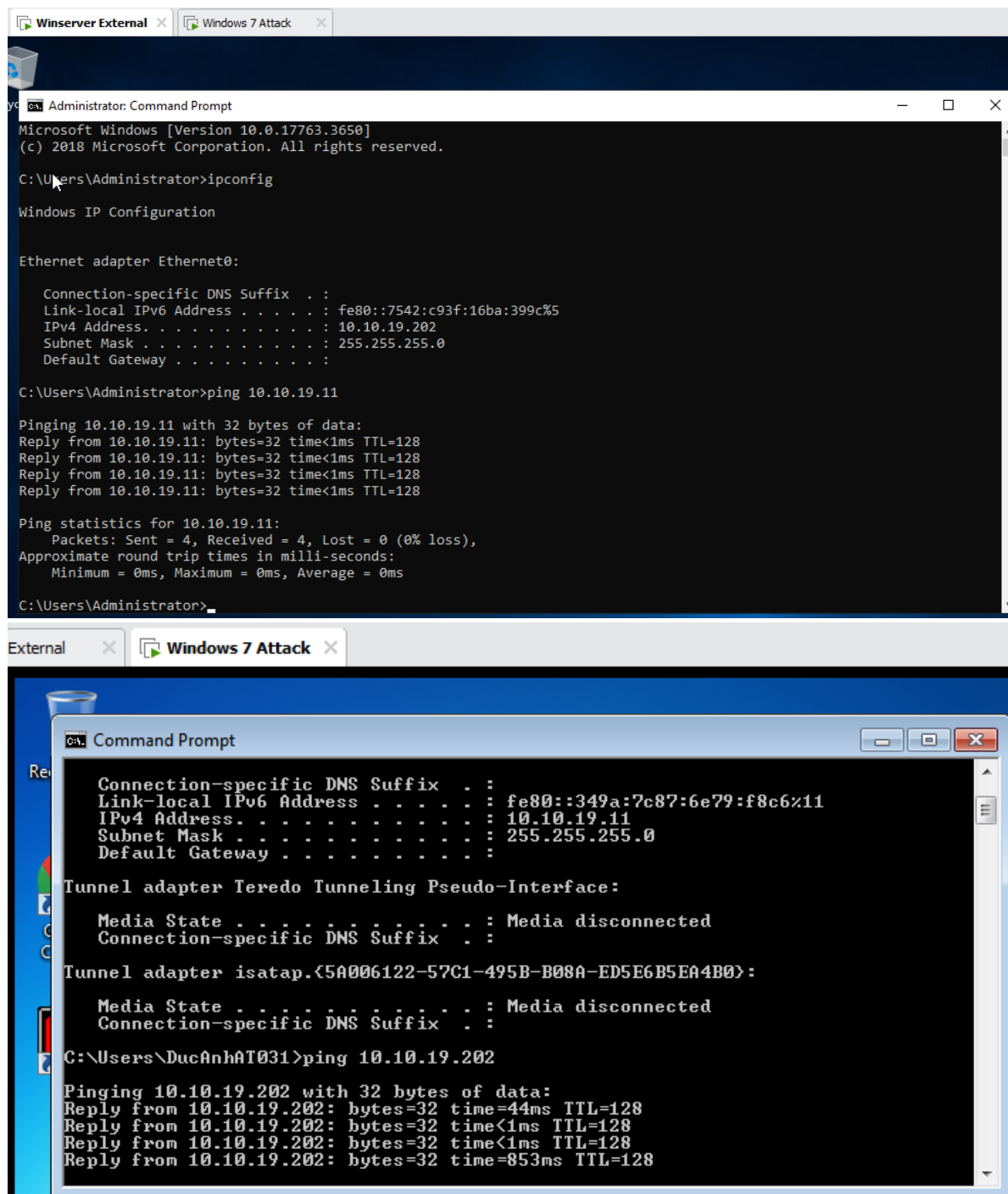
Lưu kết quả vào file eth0_NguyenDucAnh031.pcap



```
root@DucAnhB21AT031: /home/ducanhat031
File Actions Edit View Help

(root@DucAnhB21AT031)-[/home/ducanhat031]
# tcpdump -i eth0 -w eth0_NguyenDucAnh031.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C43 packets captured
43 packets received by filter
0 packets dropped by kernel
```

Tiến hành tương tự với interfaces eth1:



Hai máy mạng External có thể ping cho nhau

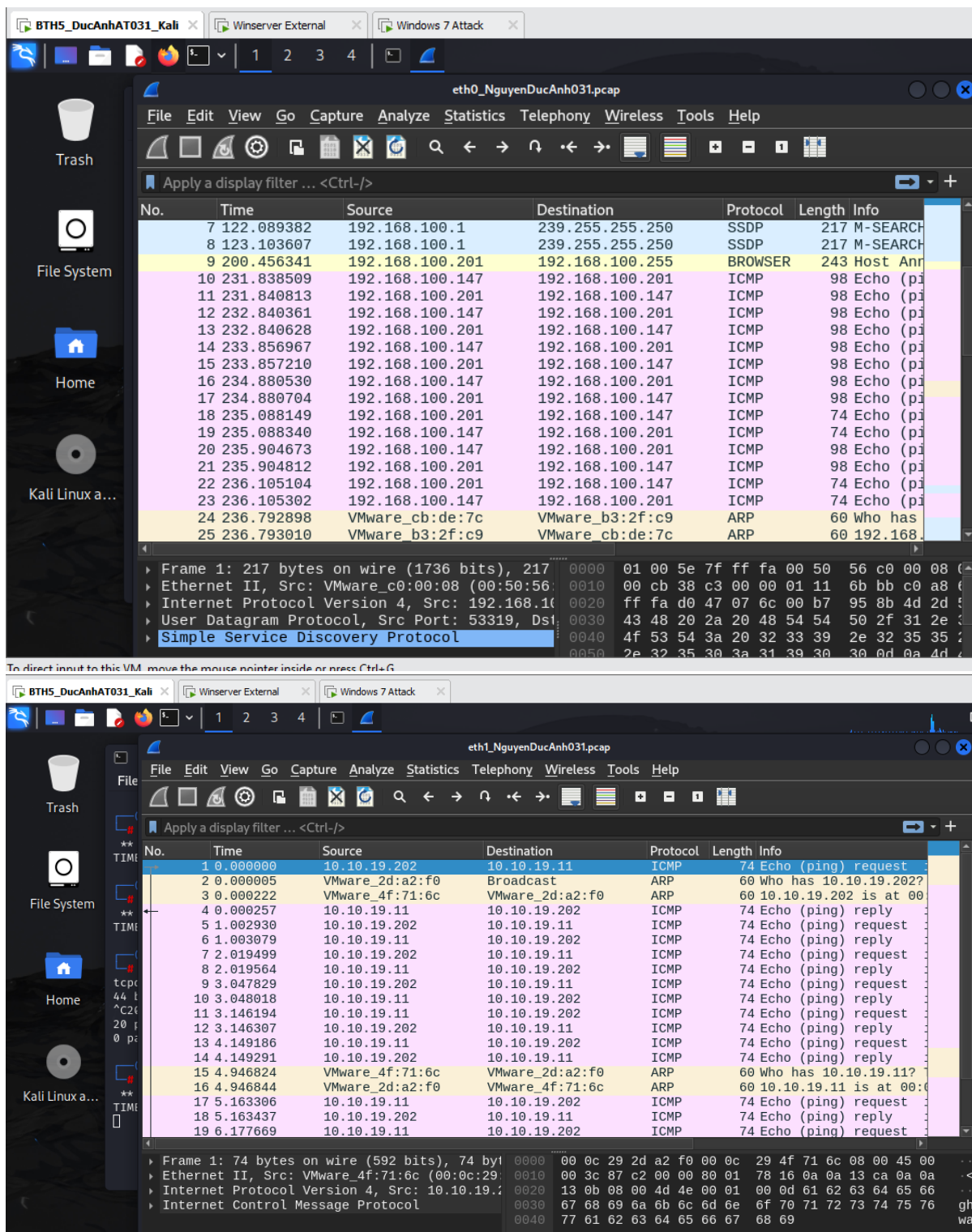
Các gói tin mà máy Linux Sniffer bắt được

Lưu các gói tin đã bắt vào file pcap

Dùng wireshark để xem file vừa lưu bằng cách chạy lệnh :

wireshark -r eth0_NguyenDucAnh031.pcap

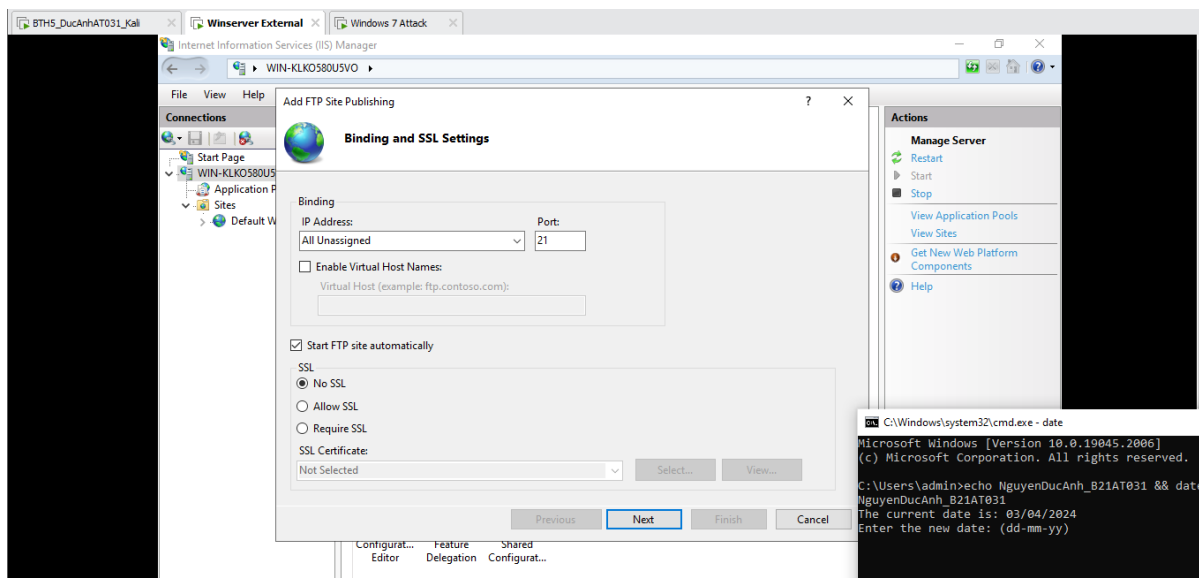
wireshark -r eth1_NguyenDucAnh031.pcap



b. Sử dụng Wireshark để bắt và phân tích các gói tin

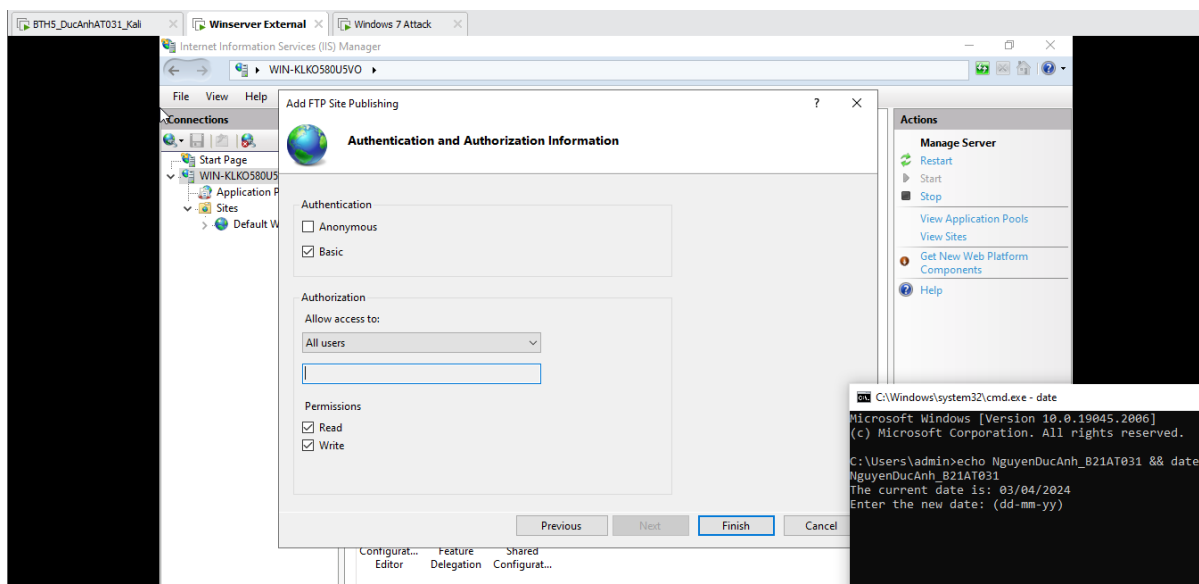
Trên máy Linux Sniffer, bật các interfaces eth0, eth1 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 10.10.19.0

Trước hết ta cài đặt IIS và FTP server cho các máy windows server ở cả mạng Internal và External.



```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

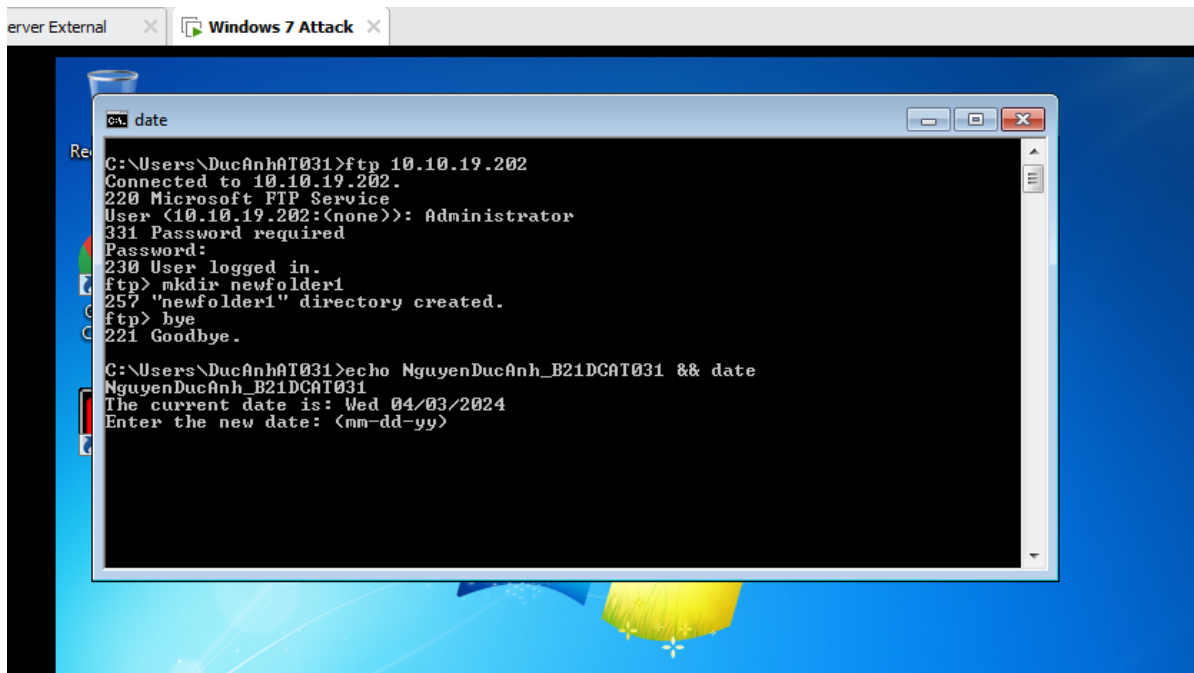
C:\Users\admin>echo NguyenDucAnh_B21AT031 && date
NguyenDucAnh_B21AT031
The current date is: 03/04/2024
Enter the new date: (dd-mm-yy)
```



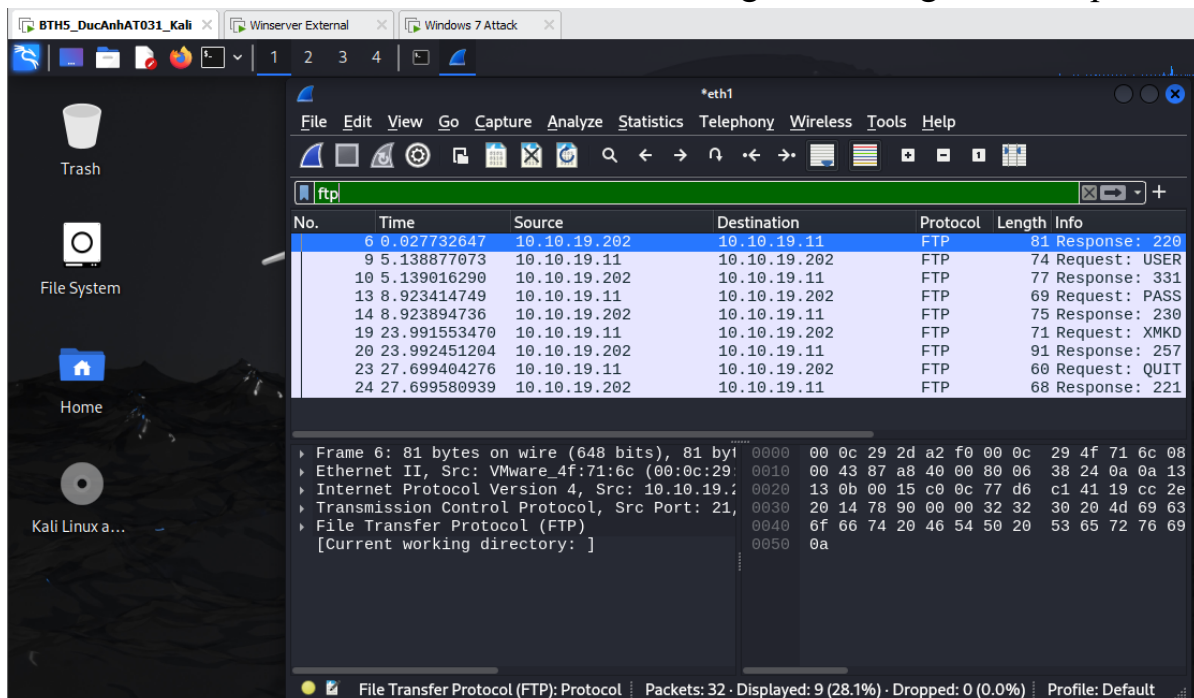
```
C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>echo NguyenDucAnh_B21AT031 && date
NguyenDucAnh_B21AT031
The current date is: 03/04/2024
Enter the new date: (dd-mm-yy)
```

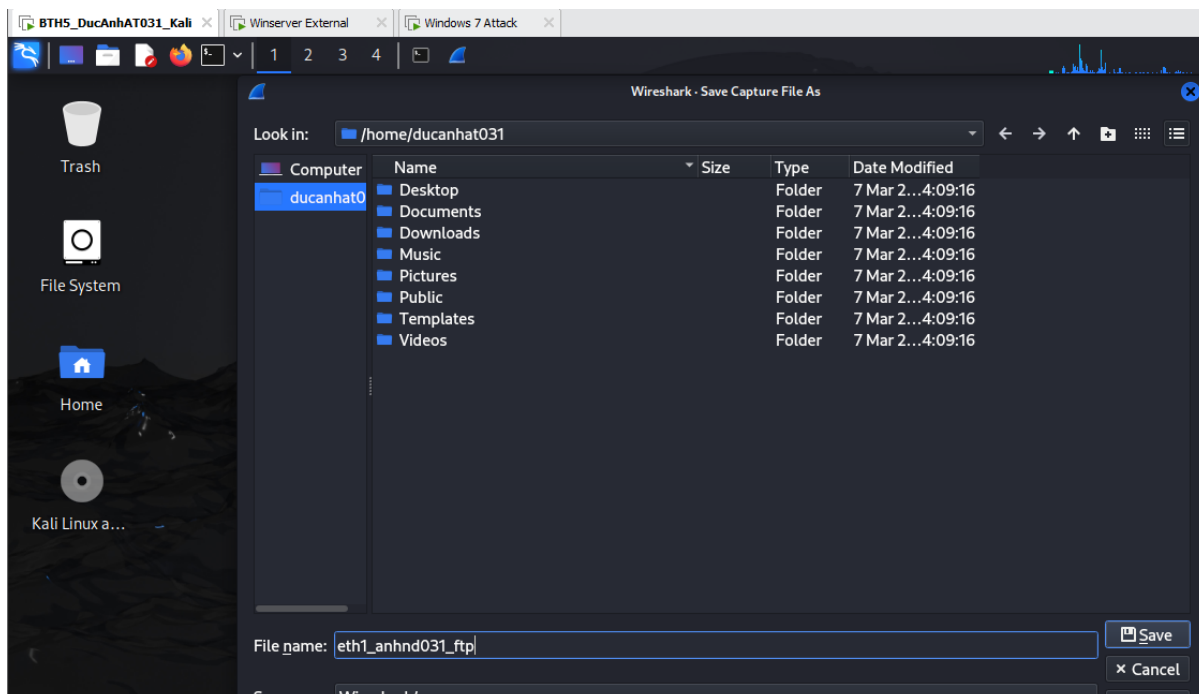
Thực hiện giao thức ftp ở dải mạng External



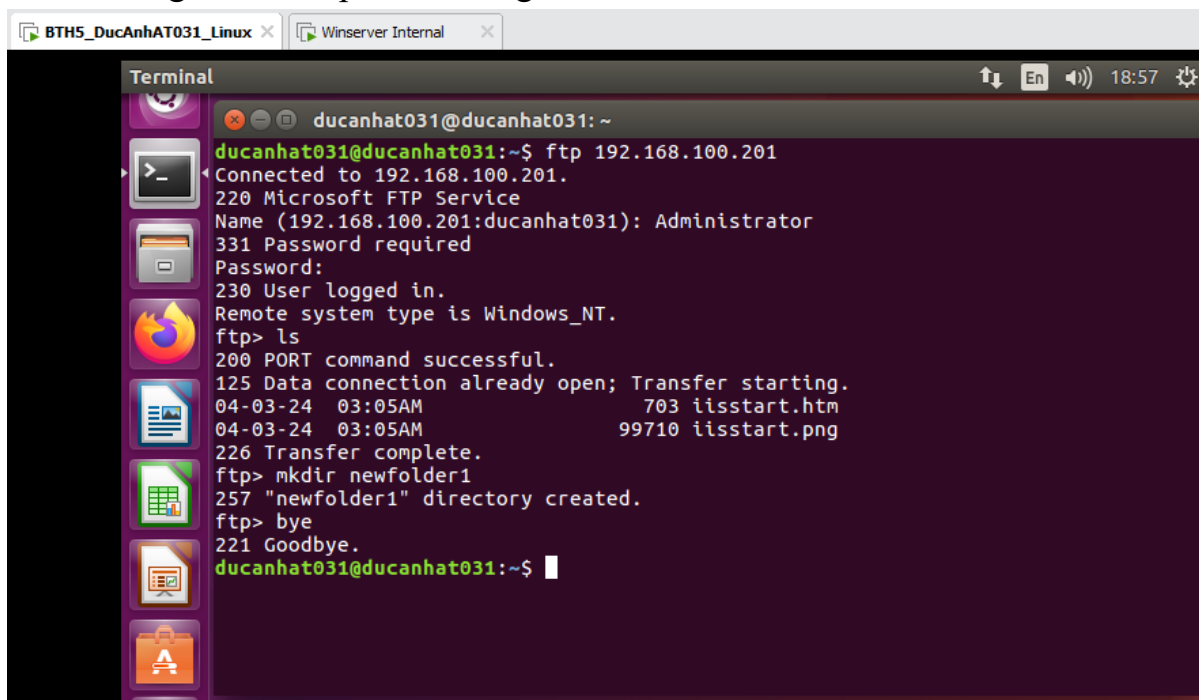
Trên linux sniffer mở wireshark và tiến hành lọc gói tin theo giao thức ftp



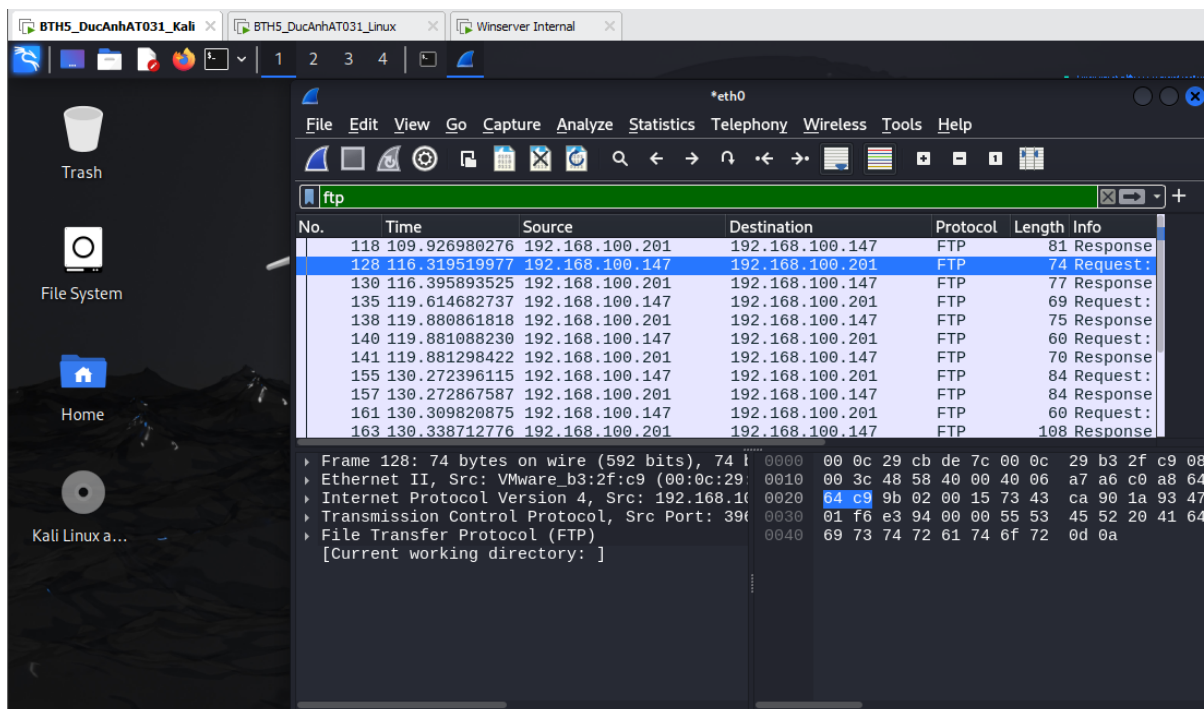
Lưu dữ liệu và file eth1_anhnd031_ftp.pcap



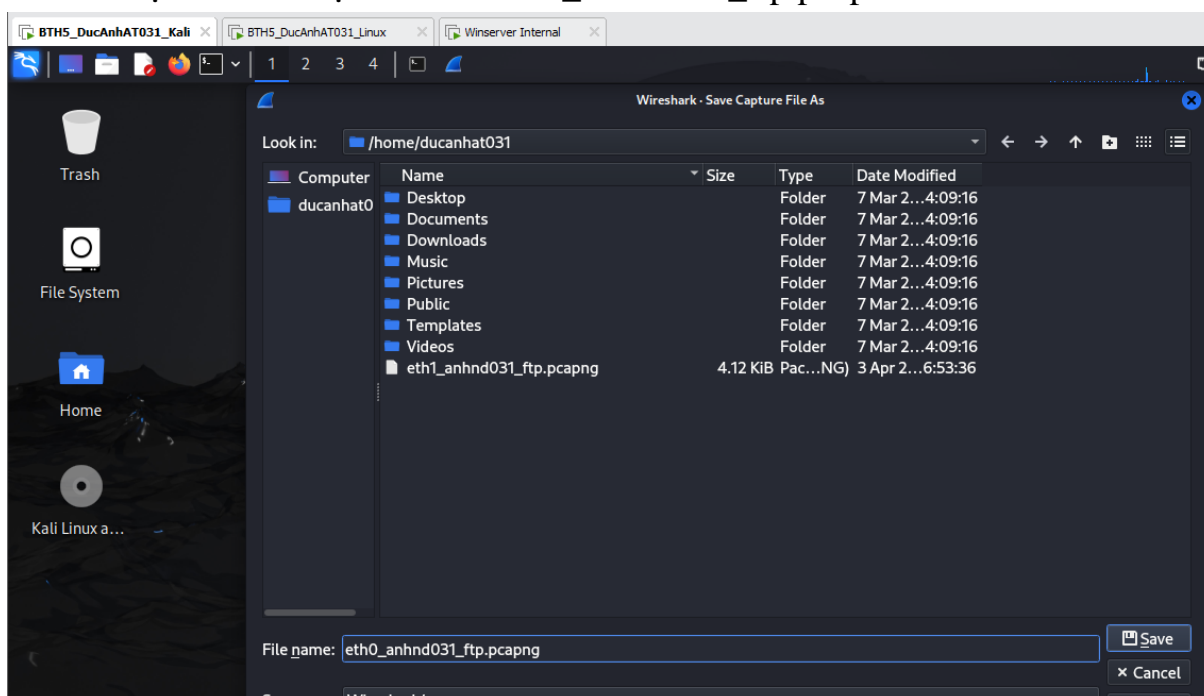
Thực hiện giao thức ftp ở dải mạng internal



Trên linux sniffer mở wireshark và bắt gói tin theo giao thức ftp

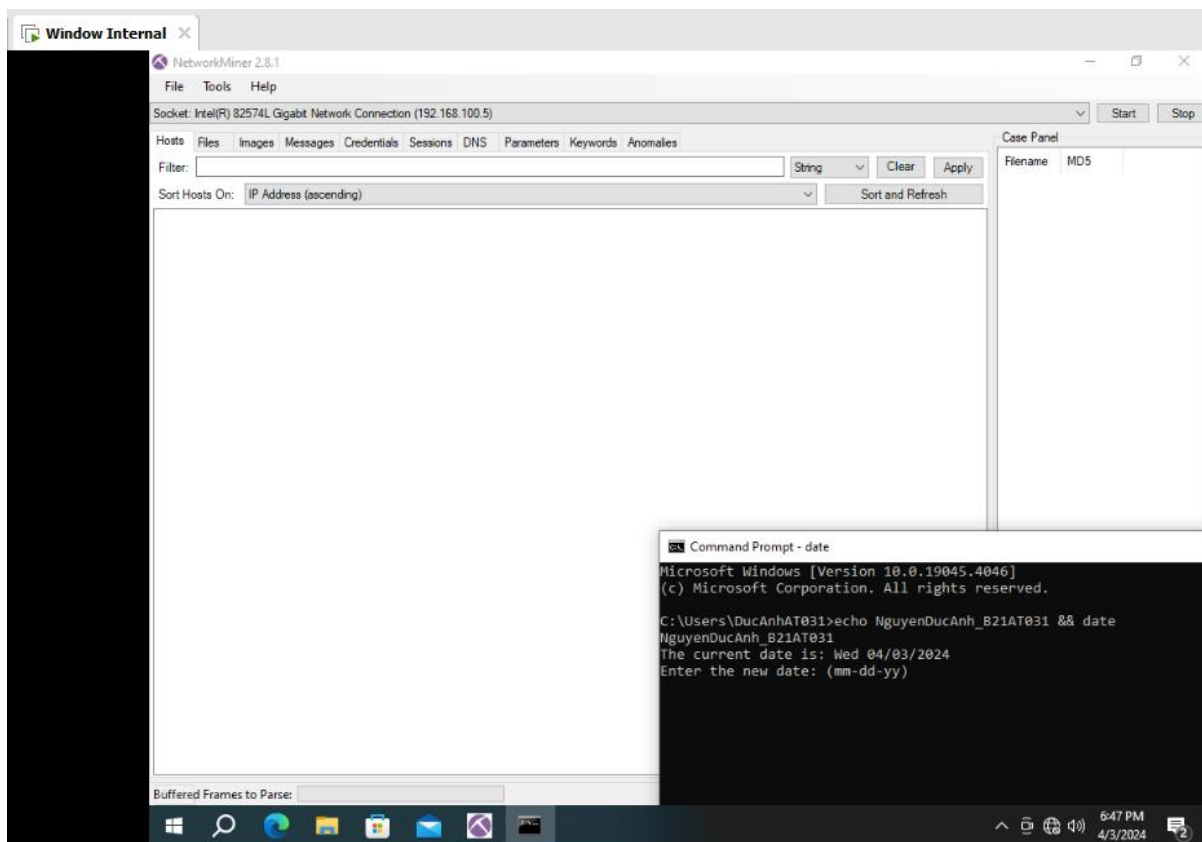


Lưu dữ liệu đã bắt được vào file eth0_anhnd031_ftp.pcap

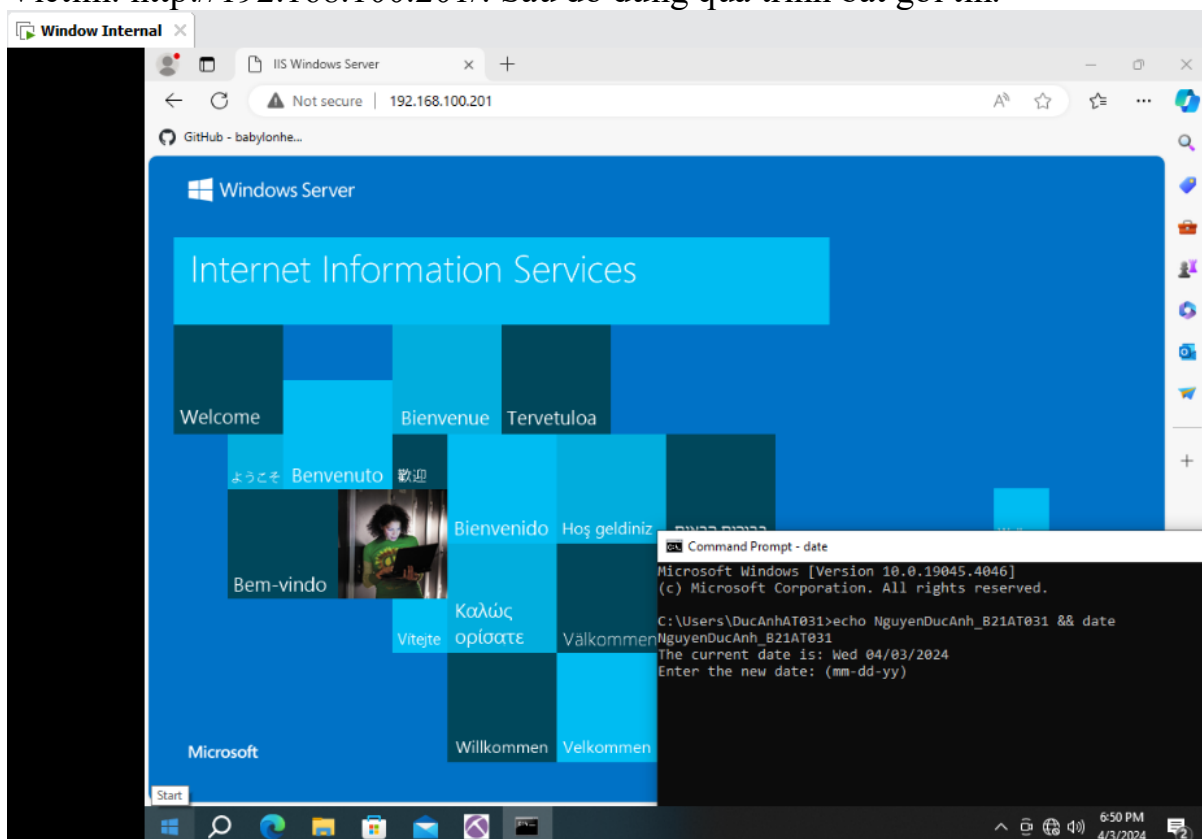


c. Sử dụng Network Miner để bắt và phân tích các gói tin

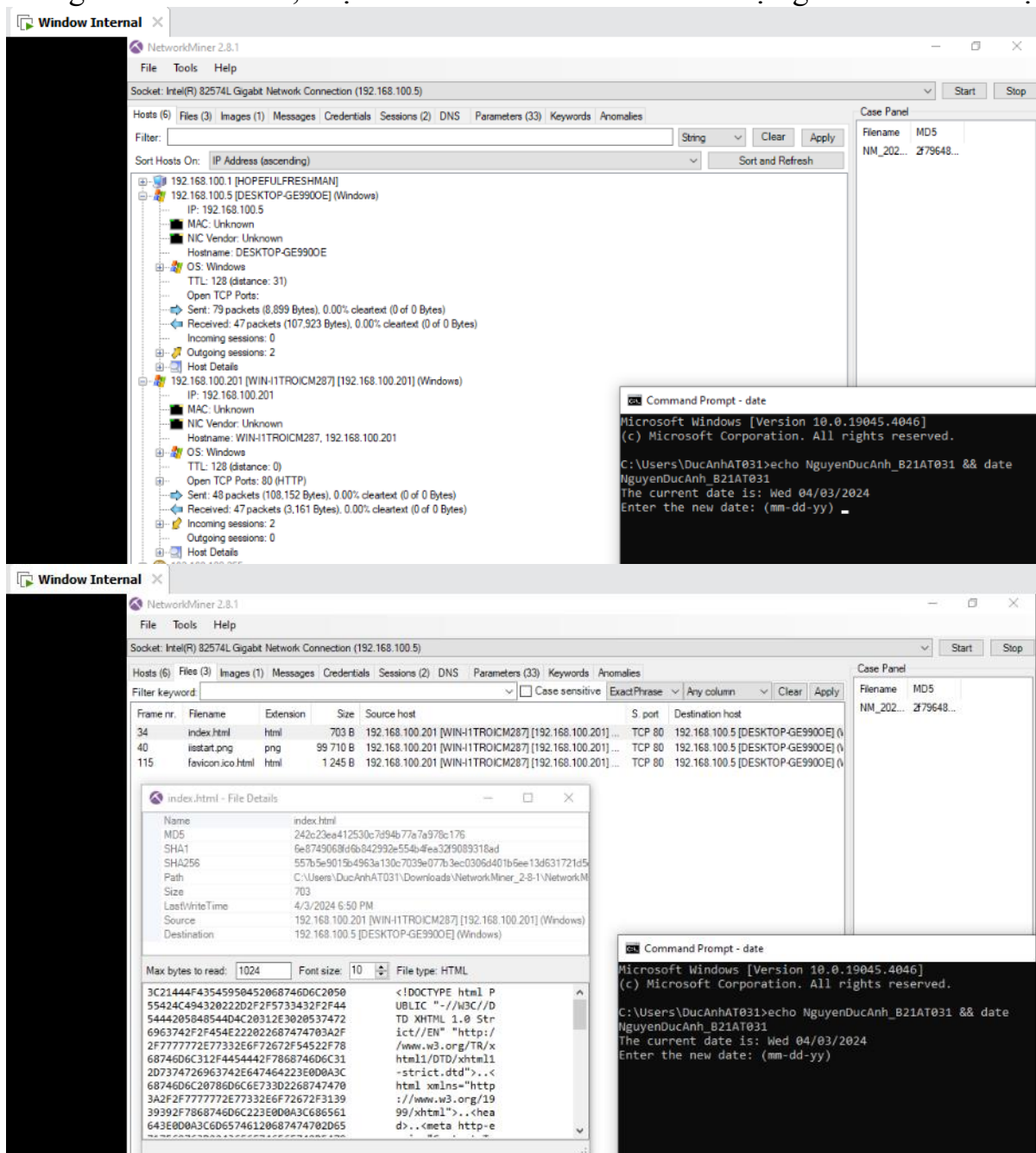
Trên máy windows 10 internal attack khởi động network miner và chọn Socket: Intel® 82574L Gigabit Network Connection(192.168.100.5) và bắt đầu bắt gói tin



Sử dụng Internet Explorer để kết nối đến trang web của Windows 2003 Server Internal Victim: <http://192.168.100.201/>. Sau đó dùng quá trình bắt gói tin.



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



3. Kết quả đạt được

- Sử dụng tcpdump để bắt các gói tin mạng
- Sử dụng Wireshark để bắt các gói tin từ phiên FTP
- Sử dụng Network Miner bắt thành công các gói tin từ quá trình truy cập Website