

**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 MẠNG**

Sinh viên thực hiện:
B22DCAT206 PHẠM ĐỨC NAM

Giảng viên hướng dẫn: Đỗ Xuân Chợt

HỌC KỲ 2 NĂM HỌC 2024-2025

Mục lục

1.	Mục đích.....	3
2.	Nội dung thực hành	3
2.1.	Cơ sở lý thuyết	3
2.1.1.	Sniffer là gì?	3
2.1.2.	Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Tcpdump	3
2.1.3.	Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Wireshark	4
2.1.4.	Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng Network Miner..	5
2.2.	Nội dung thực hành	6
2.2.1.	Chuẩn bị môi trường	6
2.2.2.	Sử dụng Tcpdump	7
2.2.3.	Sử dụng Wireshark để bắt và phân tích các gói tin.....	11
2.2.4.	Sử dụng Network Miner để bắt và phân tích các gói tin	14
3.	Kết luận	16
4.	Tài liệu tham khảo	16

Danh mục hình ảnh

Cấu hình topo mạng	7
xem tất cả các interfaces trong hệ thống	8
Kích hoạt các interfaces (eth0, eth1) hoạt động ở chế độ hỗn hợp	8
Bắt gói tin trên dải mạng 192.168.100.0/24	9
Dải Internal: 192.168.100.201 → 192.168.100.3	9
Trên máy Linux Sniffer, bắt gói tin trên dải 192.168.100.0/24	9
Dải External: 10.10.19.202 → 10.10.19.148	10
Trên máy Linux Sniffer, bắt gói tin trên dải 10.10.19.0/24	10
Các dữ liệu đã bắt trên dải Internal	11
Các dữ liệu đã bắt trên dải External	11
Windows 7 Attack kết nối tới ftp server trên máy Window Server Internal	12
Lọc gói tin theo giao thức ftp	13
Trên máy Kali Linux External kết nối ftp đến máy Ftp Server	14
Bắt gói tin trên dải 10.10.19.0/24 và lọc theo giao thức ftp	14
Kết nối đến trang web của Windows 2003 Server Internal	15
Chọn File/ index.html để xem dữ liệu gói tin vừa bắt được	16

1. Mục đích

Bài thực hành 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 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

2. Nội dung thực hành

2.1. Cơ sở lý thuyết

2.1.1. Sniffer là gì?

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).

2.1.2. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng 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 mạng 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

Định dạng chung của một dòng giao thức tcpdump:

time-stamp src > dst: flags data-seqno ack window urgent options

Trong đó:

- Time-stamp: hiển thị thời gian gói tin được capture.
- Src và dst: hiển thị địa IP của người gửi và người nhận.
- Cờ Flag thì bao gồm các giá trị sau:
 - + S(SYN): Được sử dụng trong quá trình bắt tay của giao thức TCP.
 - + .(ACK): Được sử dụng để thông báo cho bên gửi biết là gói tin đã nhận được dữ liệu thành công.
 - + F(FIN): Được sử dụng để đóng kết nối TCP.
 - + P(PUSH): Thường được đặt ở cuối để đánh dấu việc truyền dữ liệu.
 - + R(RST): Được sử dụng khi muốn thiết lập lại đường truyền.
- Data-seqno: Số sequence number của gói dữ liệu hiện tại.
- ACK: Mô tả số sequence number tiếp theo của gói tin do bên gửi truyền (số sequence number mong muốn nhận được).
- Window: Vùng nhớ đệm có sẵn theo hướng khác trên kết nối này.
- Urgent: Cho biết có dữ liệu khẩn cấp trong gói tin.

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.

2.1.3. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng 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.

2.1.4. Tìm hiểu tính năng và hoạt động của công cụ bắt dữ liệu mạng 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 NetworkMiner phải kể đến:

- 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 NetworkMiner

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.

2.1.5. Một số điều cần biết

thêm 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.

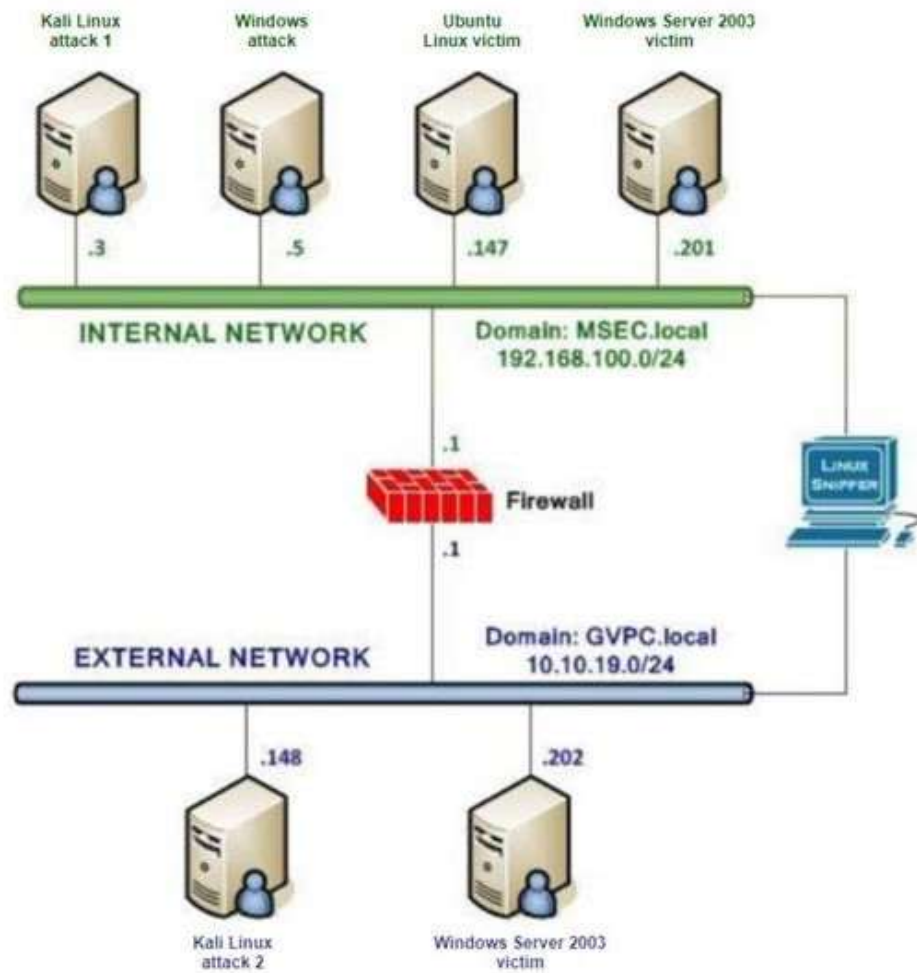
Kích hoạt chế độ hỗn độn trên Linux:

```
sudo ifconfig <tên card mạng> promisc
```

2.2. Nội dung thực hành

2.2.1. 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.



Cấu hình topo mạng

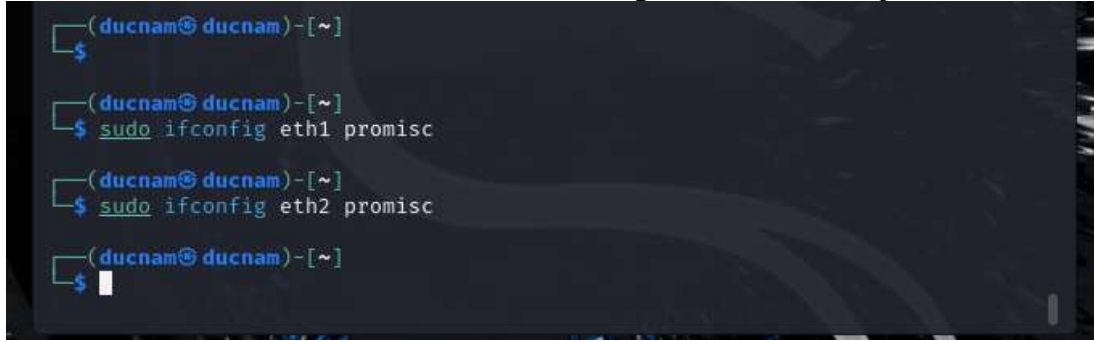
2.2.2. Sử dụng Tcpdump

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

```
ducnam@ducnam: ~  
File Actions Edit View Help  
    valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
    valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKN  
OWN group default qlen 1000  
    link/ether 00:0c:29:62:b0:8b brd ff:ff:ff:ff:ff:ff  
    inet 192.168.19.143/24 brd 192.168.19.255 scope global dynamic noprefixro  
ute eth0  
    valid_lft 1143sec preferred_lft 1143sec  
    inet6 fe80::20c:29ff:fe62:b08b/64 scope link noprefixroute  
    valid_lft forever preferred_lft forever  
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKN  
OWN group default qlen 1000  
    link/ether 00:0c:29:62:b0:95 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.10/24 brd 192.168.100.255 scope global eth1  
    valid_lft forever preferred_lft forever  
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKN  
OWN group default qlen 1000  
    link/ether 00:0c:29:62:b0:9f brd ff:ff:ff:ff:ff:ff  
    inet 10.100.19.10/24 brd 10.100.19.255 scope global eth2  
    valid_lft forever preferred_lft forever  
  
(ducnam@ ducnam)~  
$ ping 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
From 192.168.100.10 icmp_seq=1 Destination Host Unreachable
```

xem tất cả các interfaces trong hệ thống

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



```
(ducnam@ducnam)~$  
(ducnam@ducnam)~$ sudo ifconfig eth1 promisc  
(ducnam@ducnam)~$ sudo ifconfig eth2 promisc  
(ducnam@ducnam)~$
```

Kích hoạt các interfaces (eth0, eth1) 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).

```
3 packets transmitted, 3 received, 0% packet loss, time 2016ms
rtt min/avg/max/mdev = 0.804/1.182/1.414/0.269 ms

(ducnam@ducnam)-[~]
$ sudo tcpdump -i eth1 icmp
[sudo] password for ducnam:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Bắt gói tin trên dải mạng 192.168.100.0/24

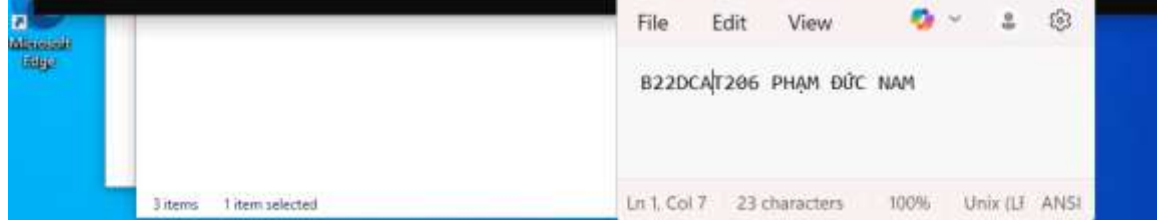
- Đăng nhập Window Server 2019 và tiến hành ping đến dải mạng internal và dải mạng external.

```
C:\Users\nam8d>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

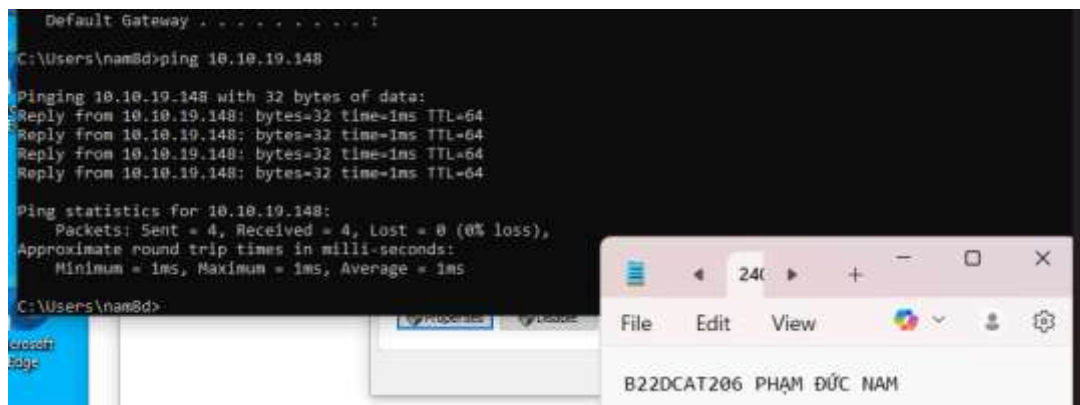
C:\Users\nam8d>
```



Dải Internal: 192.168.100.201 → 192.168.100.3

```
(ducnam@ducnam)-[~]
$ sudo tcpdump -i eth1 icmp
[sudo] password for ducnam:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:23:51.289313 IP 192.168.100.5 > 192.168.100.147: ICMP echo request, id 1,
seq 5, length 40
05:23:51.289315 IP 192.168.100.147 > 192.168.100.5: ICMP echo reply, id 1, se
q 5, length 40
```

Trên máy Linux Sniffer, bắt gói tin trên dải 192.168.100.0/24(tcpdump -i eth0)

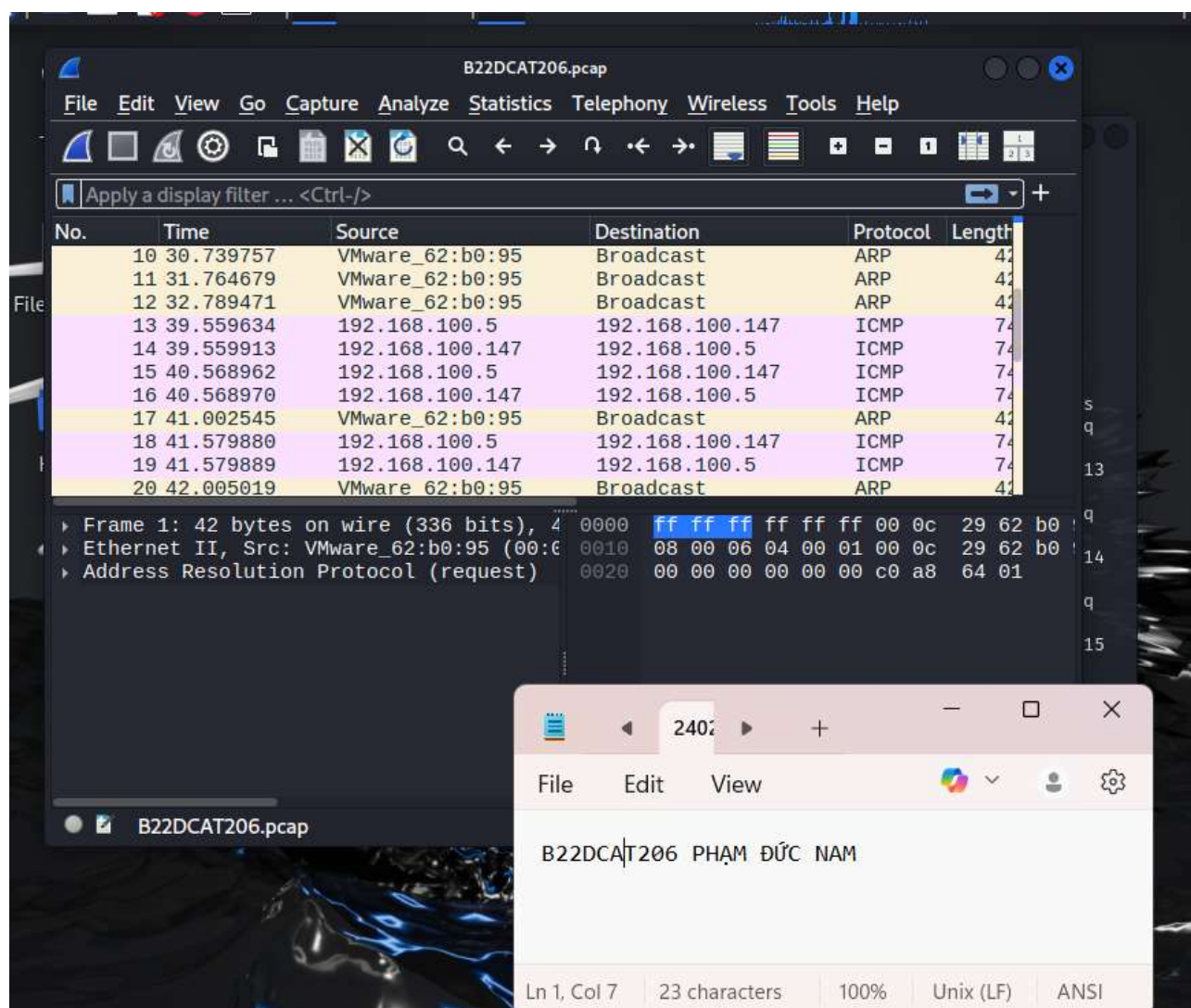


Dải External: 10.10.19.202→ 10.10.19.148

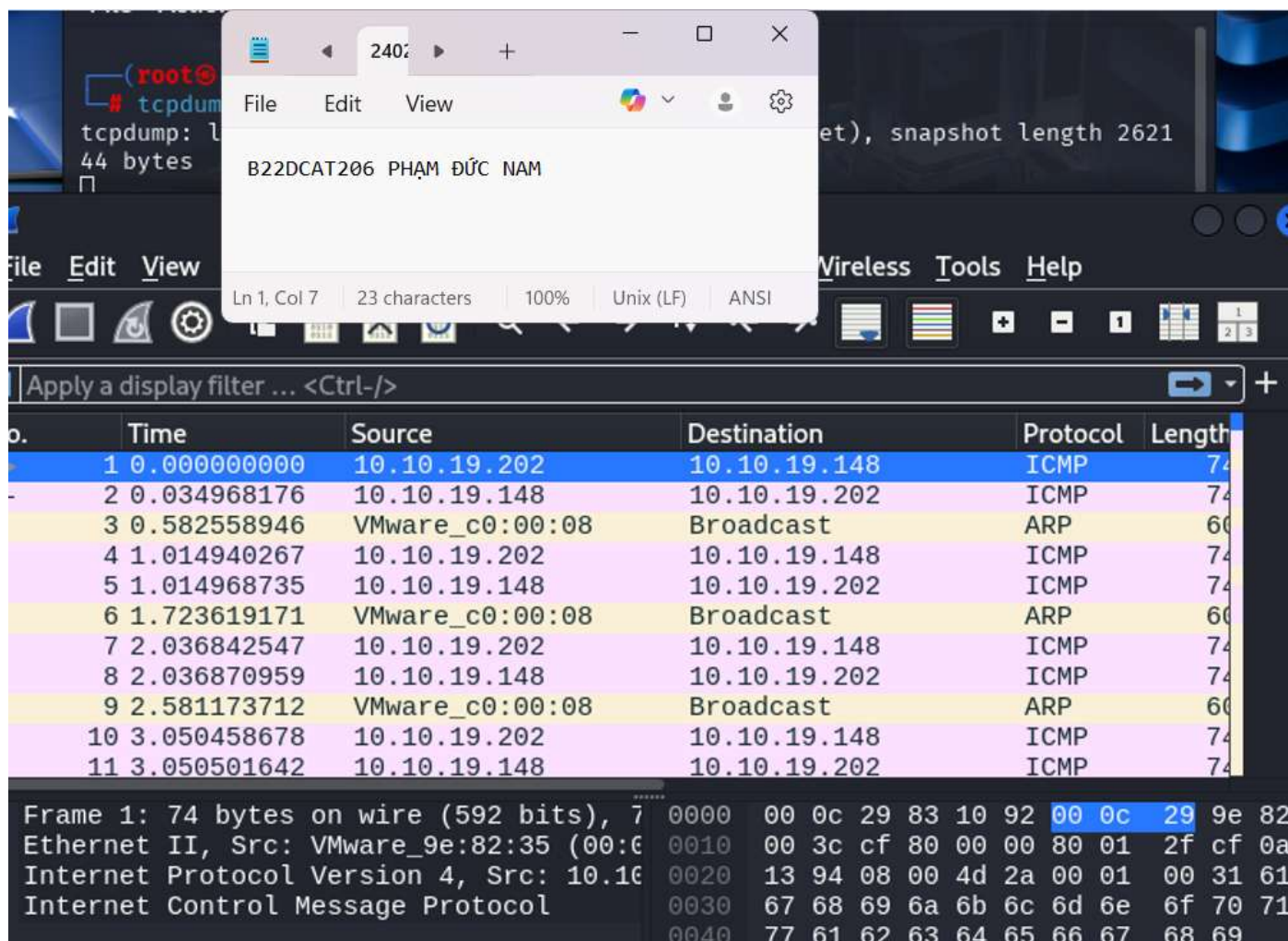
```
—(ducnam@ducnam)-[~]
—$ sudo tcpdump -i eth2 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), snapshot length 262144 bytes
05:44:48.499289 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 13, length 40
05:44:48.499797 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 13, length 40
05:44:49.526277 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 14, length 40
05:44:49.526284 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 14, length 40
05:44:50.542372 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 15, length 40
05:44:50.542733 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 15, length 40
05:44:51.559011 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 16, length 40
05:44:51.559507 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 16, length 40
```

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.



Các dữ liệu đã bắt trên dải Internal

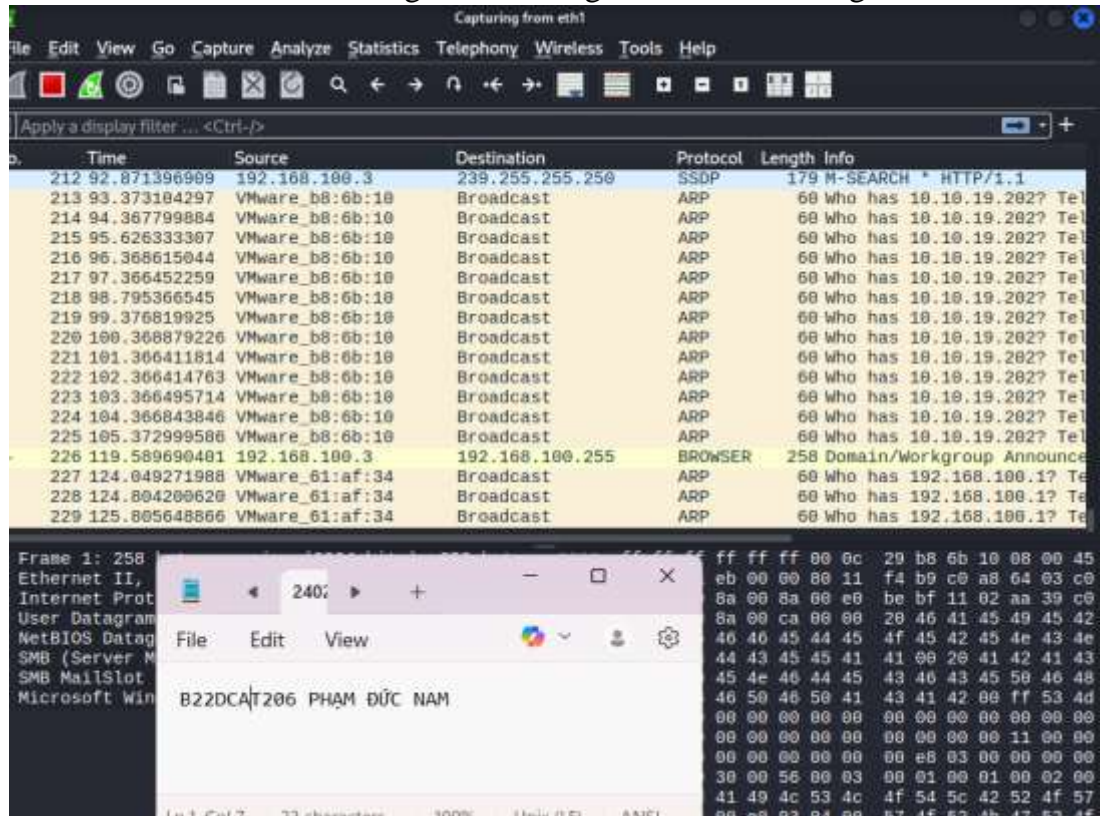


Các dữ liệu đã bắt trên dải External

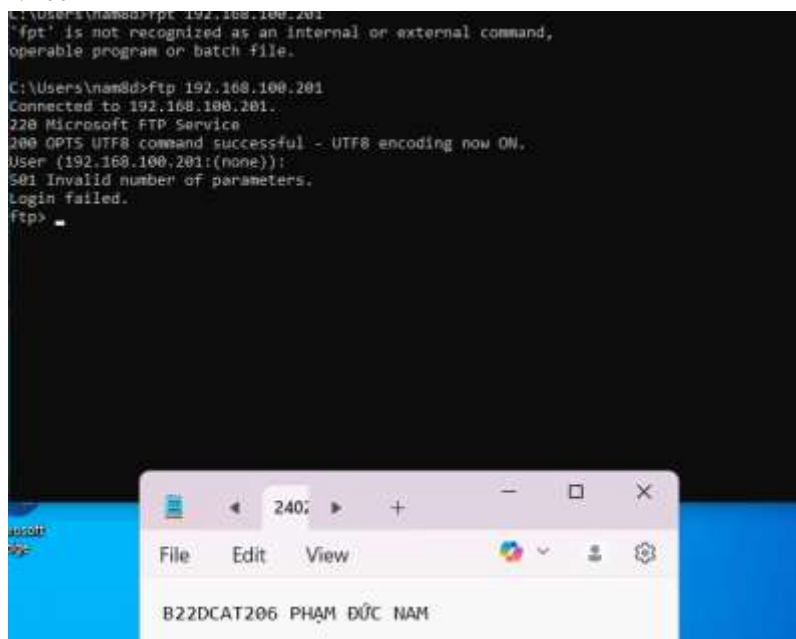
2.2.3. Sử dụng Wireshark để bắt và phân tích các gói tin

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

- Trên máy Linux Sniffer, bật các interfaces eth1, eth2 và khởi động Wireshark. Trong Capture Interfaces chọn Start ở dòng eth1 để bắt gói tin trên dải mạng 192.168.100.0

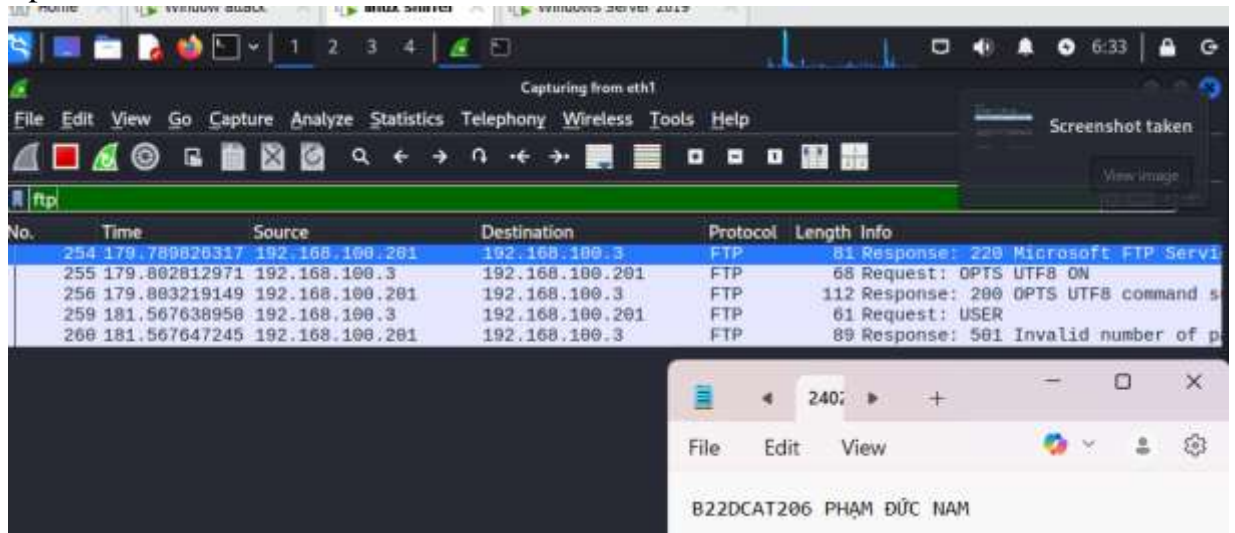


- Trên máy Windows 10 Attack kết nối tới ftp server trên máy Window Server Internal Victim



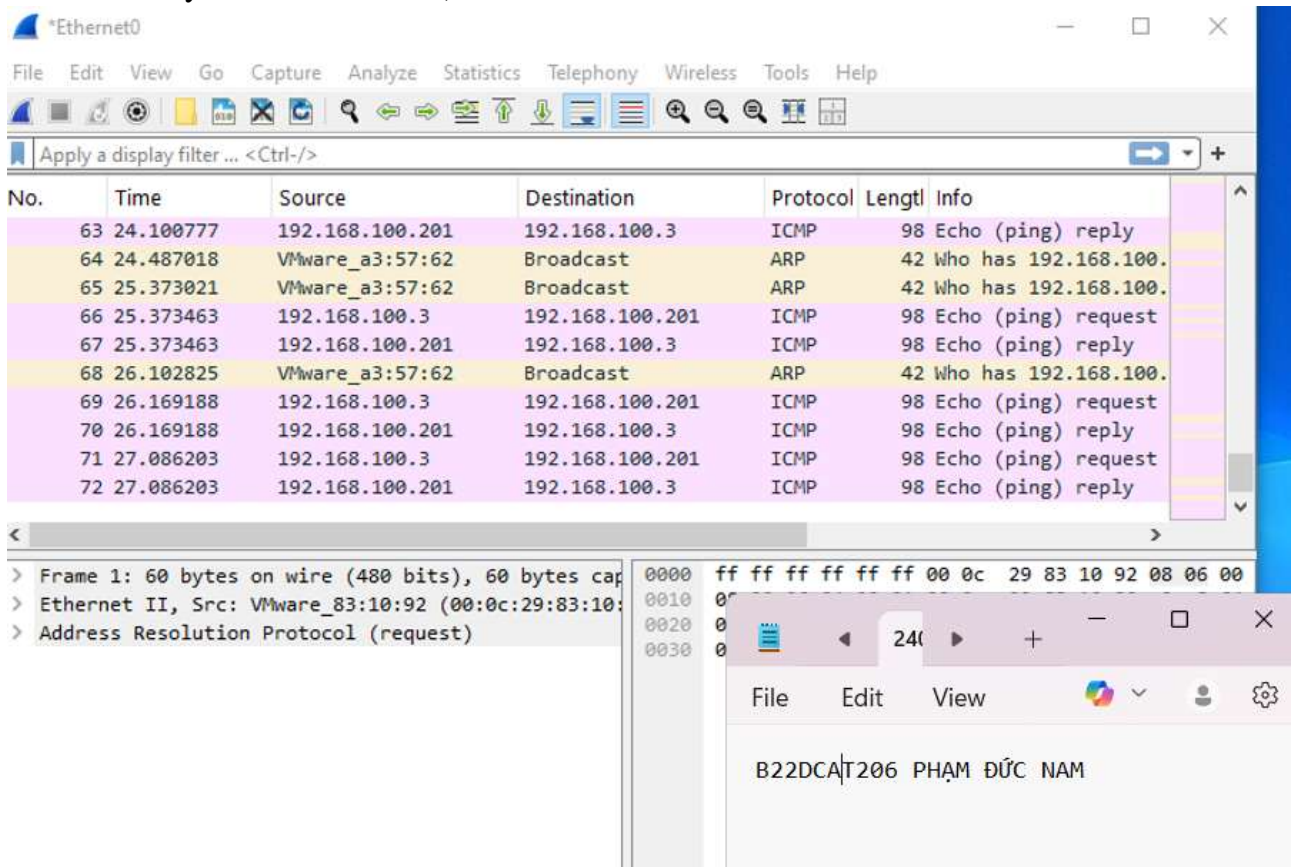
Windows 10 Attack kết nối tới ftp server trên máy Window Server Internal

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



Lọc gói tin theo giao thức ftp

- Trên máy Windows attack (192.168.100.5), trong Capture Interfaces chọn Start ở dòng eth1 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)



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

```

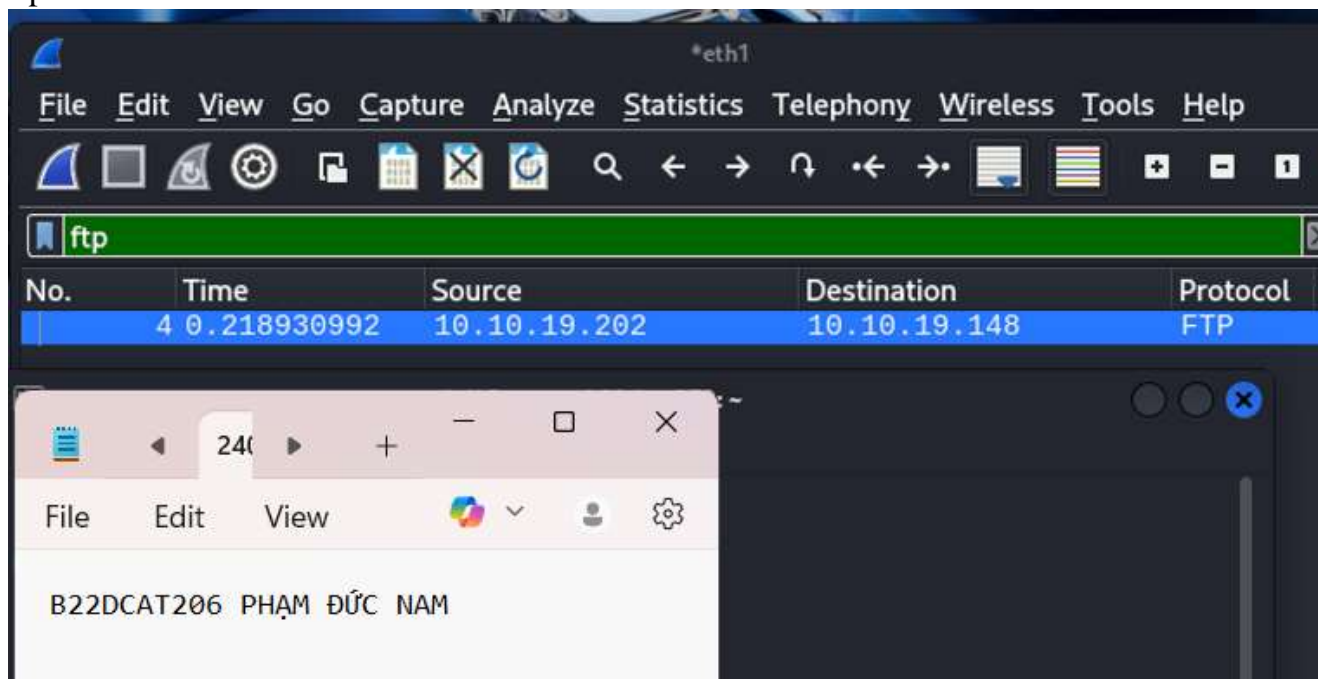
File Actions Edit View Help

(ducnam@ducnam)-[~]
$ ftp 10.10.19.202
Connected to 10.10.19.202.
220 Microsoft FTP Service
Name (10.10.19.202:ducnam): 1
331 Password required
Password:
530 User cannot log in.
ftp: Login failed
ftp>

```

Trên máy Kali Linux External kết nối ftp đến máy Ftp Server

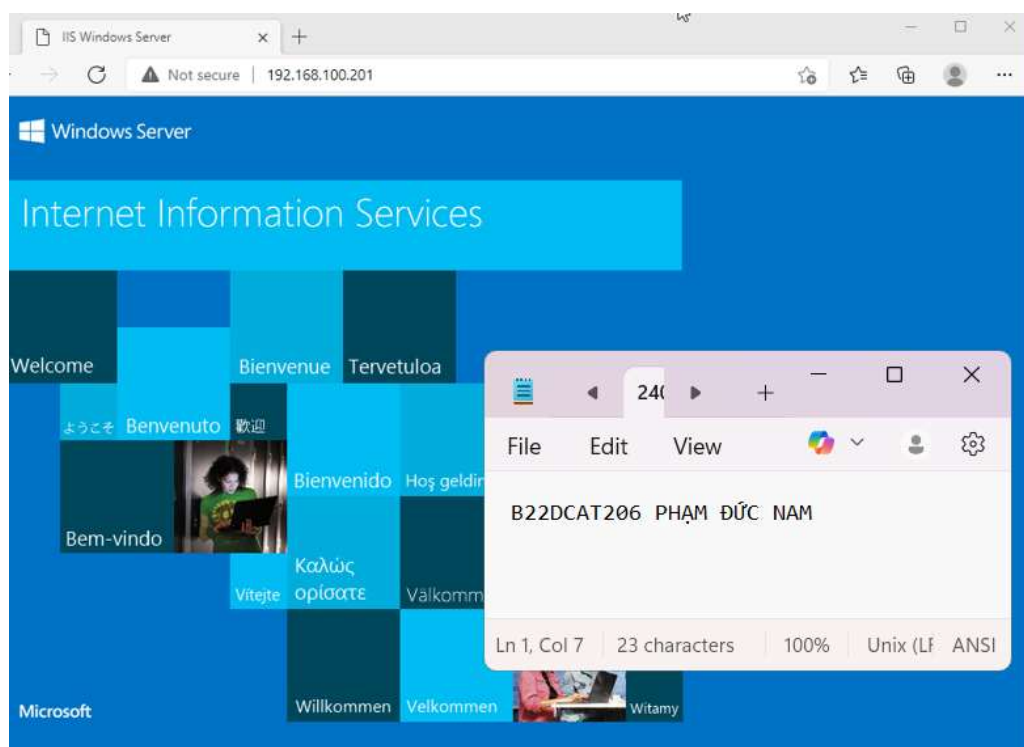
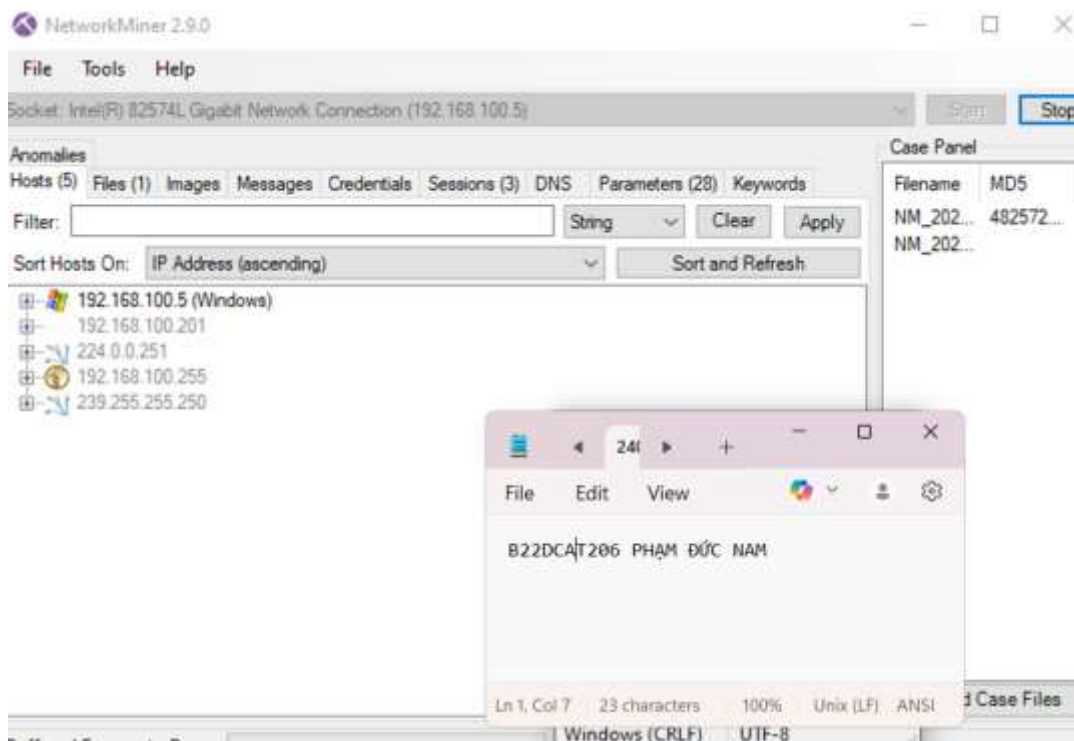
- Trên Linux Sniffer dùng quá trình bắt gói tin và tiến hành lọc gói tin theo giao thức ftp



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

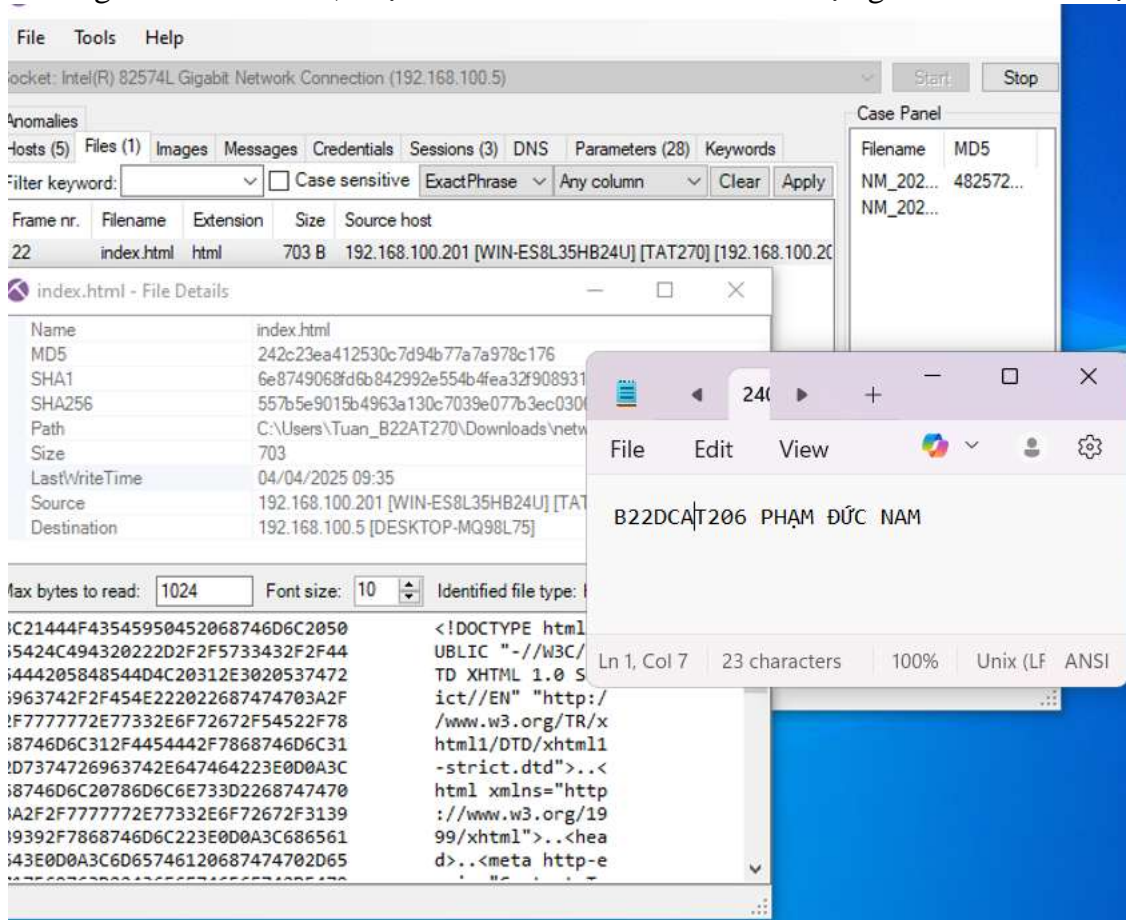
2.2.4. Sử dụng Network Miner để bắt và phân tích các gói tin

- 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 2019 Server Internal Victim: <http://192.168.100.201/>. Sau đó dùng quá trình bắt gói tin.



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.



Chọn File/ index.html để xem dữ liệu gói tin vừa bắt được.

3. Kết luận

- Thu được kết quả bắt gói tin và các file pcap thông qua tcpdump
- Sử dụng Wireshark để bắt và lọc ra được các gói tin ftp, các file pcap tương ứng
- Bắt được các dữ liệu trong file index.html.

4. 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#>