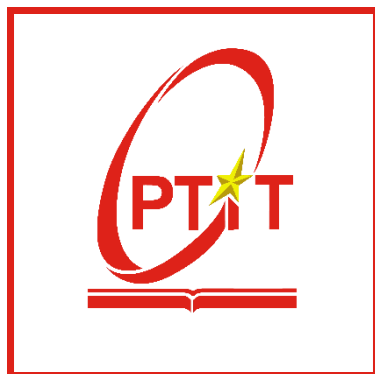


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



THỰC TẬP CƠ SỞ
Bài 8: Bắt dữ liệu mạng

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

Hà Nội – 2024

Môn học Thực tập cơ sở

Bài 8: Bắt dữ liệu mạng

I. Lý thuyết

1. Tìm hiểu về Tcpdump

Tcpdump là công cụ hữu ích được ra đời và phát triển để phục vụ cho mục đích hỗ trợ phân tích các gói dữ liệu mạng theo dòng lệnh đồng thời cho phép khách hàng thực hiện việc chặn, lọc và hiển thị các gói tin TCP/IP được truyền đi hoặc nhận trên một mạng có sự tham gia của máy tính.

Một số lợi ích của tcpdump:

- Hỗ trợ xem các bản tin dump trên terminal
- Capture các bản tin và lưu dưới dạng .pcap(hỗ trợ đọc bởi wireshark)
- Hỗ trợ xem trực tiếp các bản tin điều khiển hệ thống linux thông qua wireshark

Tcpdump là công cụ có khả năng capturing packets mạnh mẽ. Hoạt động trên network layer, tcpdump có thể capture tất cả các gói ra vào máy tính.

Tcpdump sẽ xuất ra màn hình nội dung các gói tin chạy trên card nhà mạng mà máy chủ đang lắng nghe sao cho phù hợp với biểu thức logic chọn lọc mà khách hàng đã sử dụng và nhập vào máy tính. Khách hàng có thể xuất ra các mô tả về gói tin thành một file pcap để phân tích sau dựa trên từng loại tùy chọn khác nhau. Để đọc được nội dung của file pcap này, bạn chỉ cần sử dụng các phần mềm khác như Wireshark hay với option -r của tcpdump

Trong các trường hợp không có tùy chọn nào, tcpdump sẽ vẫn tiếp tục chạy cho đến khi nó nhận được tín hiệu ngắt từ phía khách hàng. Sau khi việc bắt các gói tin kết thúc, tcpdump sẽ đưa ra các báo cáo sau:

Packet capture: Số lượng các gói tin đã bắt được và tiến hành xử lý.

Packet received by filter: Số lượng các gói tin mà bộ lọc nhận được.

Packet dropped by kernel: số lượng packet bị dropped do cơ chế bắt gói tin.

2. Tìm hiểu về Wireshark

Wireshark là một ứng dụng dùng để bắt (capture), phân tích và xác định các vấn đề liên quan đến network như: rò rỉ 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 hiện nay 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, và do đó miễn phí sử dụng, tự do chia sẻ, 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.
- **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.

3. Tìm hiểu về Network Miner

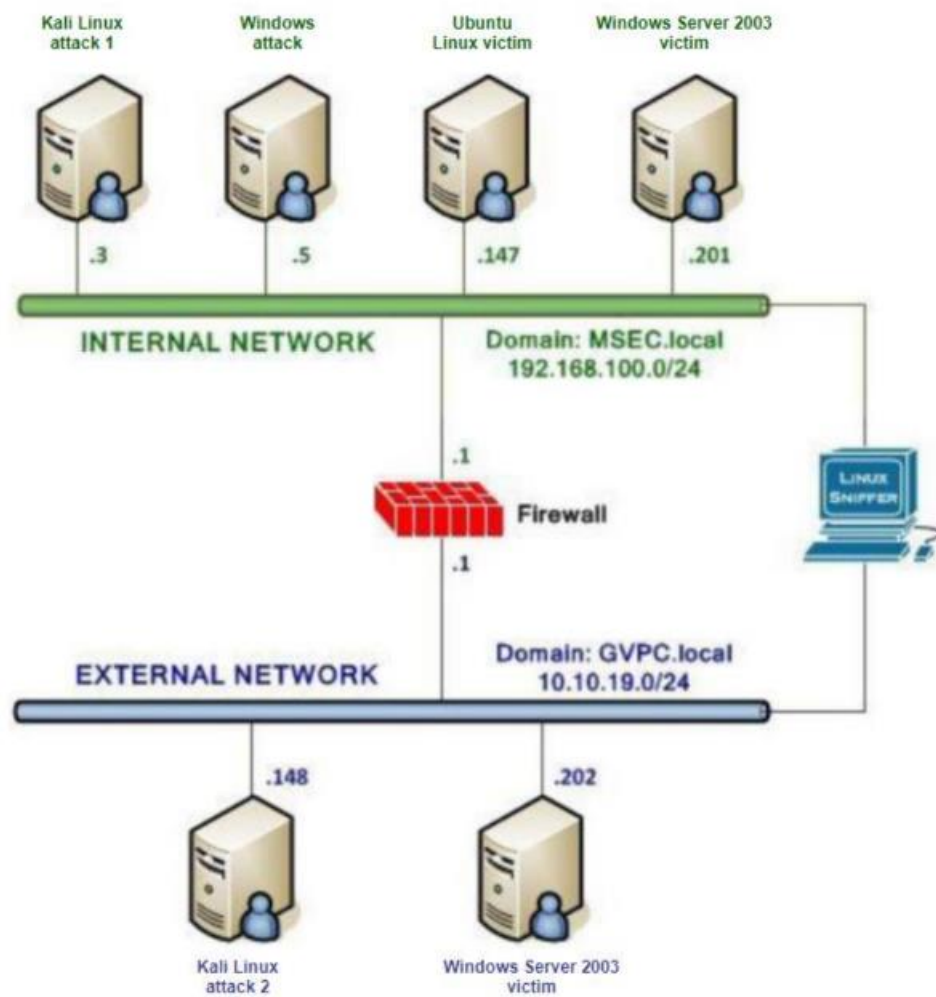
NetworkMiner là công cụ giám sát mạng mã nguồn mở dành cho hệ điều hành Window. Công cụ này cũng được hỗ trợ để cài đặt trên Linux, Mac OS X và FreeBSD. Hiện nay có rất nhiều công cụ giám sát mạng khác nhau, tuy nhiên NetworkMiner vẫn được sử dụng khá phổ biến. Những điểm nổi bật của NetworkMiner phải 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 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.

Nếu bạn đang lo lắng rằng máy tính của mình đang bị kẻ xấu thu thập thông tin từ xa qua các phần mềm gián điệp, ... hãy thử tải và sử dụng NetworkMiner, mọi thiết bị và trang web vừa kết nối thông tin với máy tính của bạn đều sẽ nhanh chóng bị phát hiện.

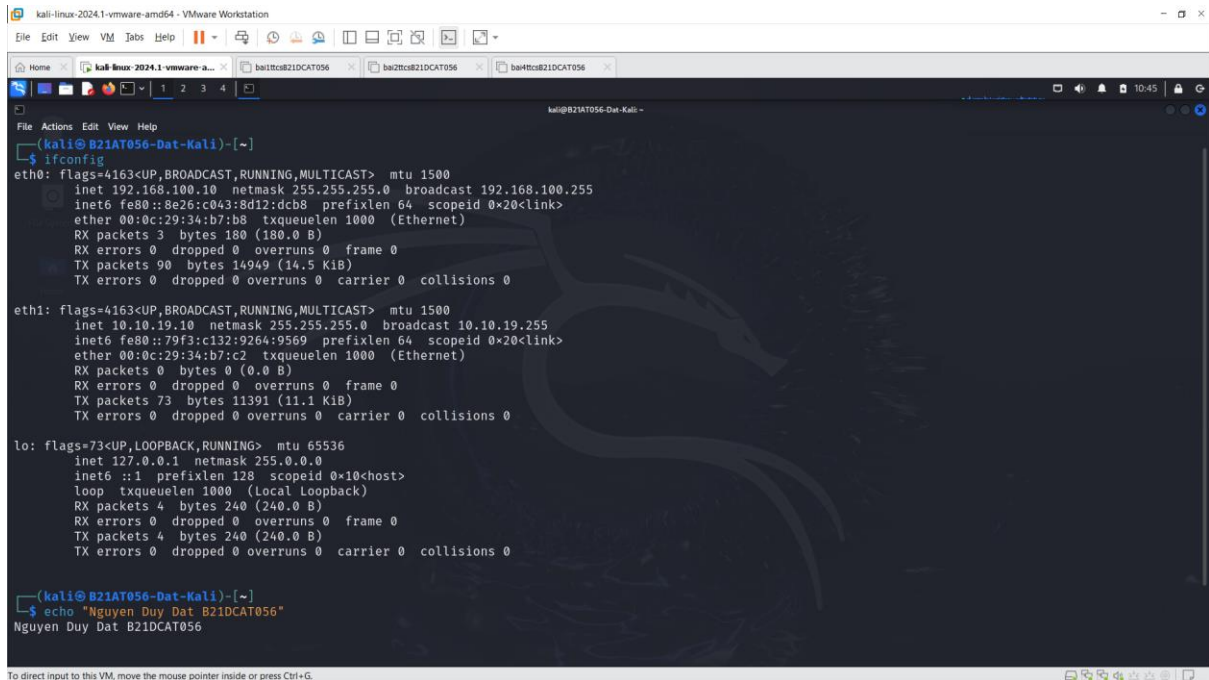
II. Cài đặt

1. Chuẩn bị môi trường



2. Sử dụng tcpdump

- Máy linux sniffer có 2 card mạng:
Eth0 thuộc dải 192.168.100.0/24
Eth1 thuộc dải 10.10.19.0/24



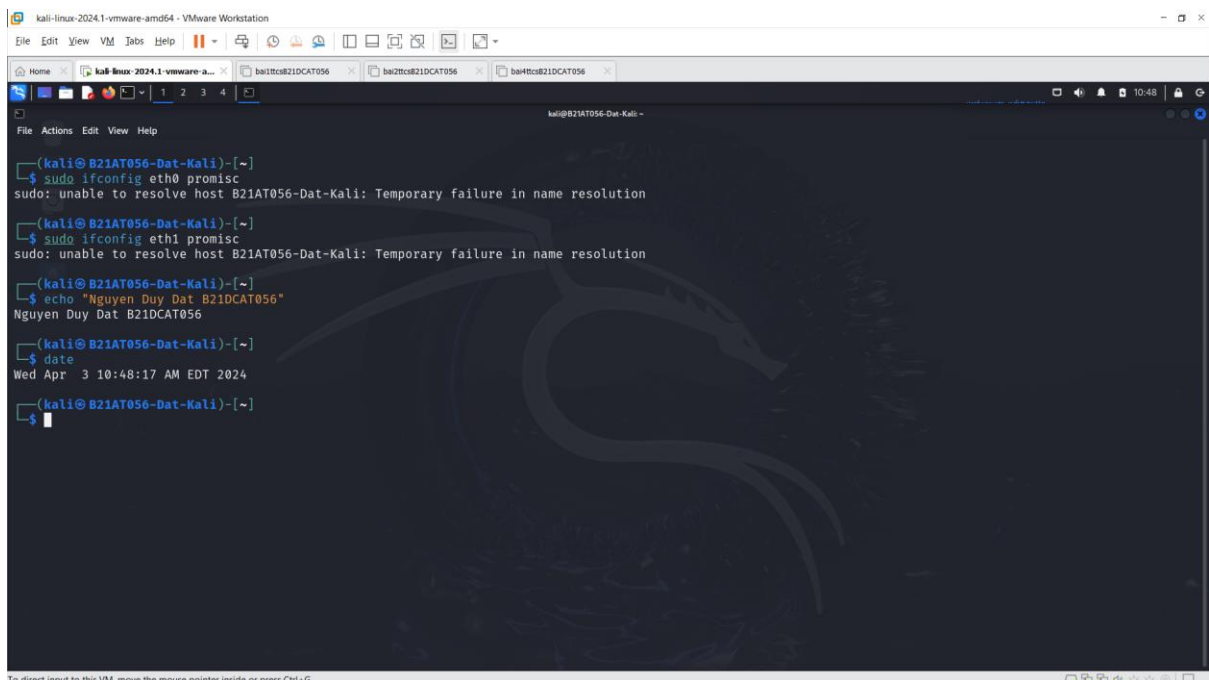
```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.10 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::8e26:c043:8d12:dcb8 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:34:b7:b8 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 180 (180.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 90 bytes 14949 (14.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.10 netmask 255.255.255.0 broadcast 10.10.19.255
    inet6 fe80::79f3:c132:9264:9569 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:34:b7:c2 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 73 bytes 11391 (11.1 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 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
```

- Sử dụng lệnh ifconfig eth0/eth1 promisc để kích hoạt interfaces hoạt động ở chế độ hỗn hợp



```
(kali@kali:~$ sudo ifconfig eth0 promisc
sudo: unable to resolve host kali: Temporary failure in name resolution

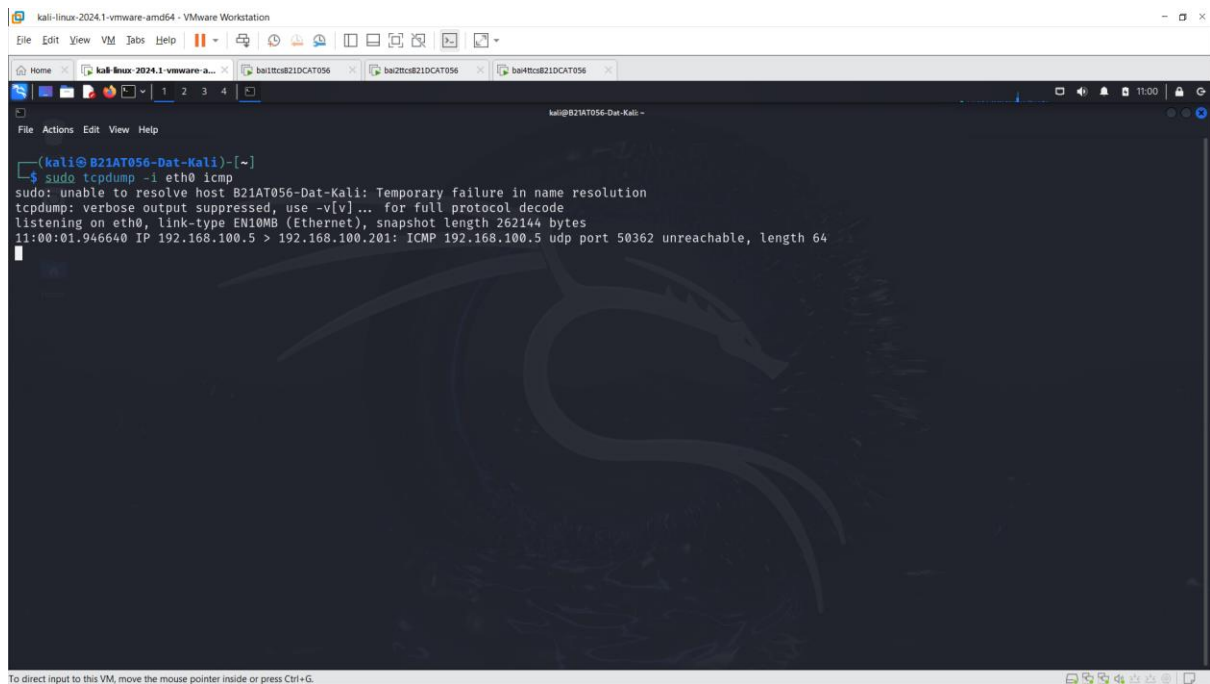
(kali@kali:~$ sudo ifconfig eth1 promisc
sudo: unable to resolve host kali: Temporary failure in name resolution

(kali@kali:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@kali:~$ date
Wed Apr 3 10:48:17 AM EDT 2024

(kali@kali:~$
```

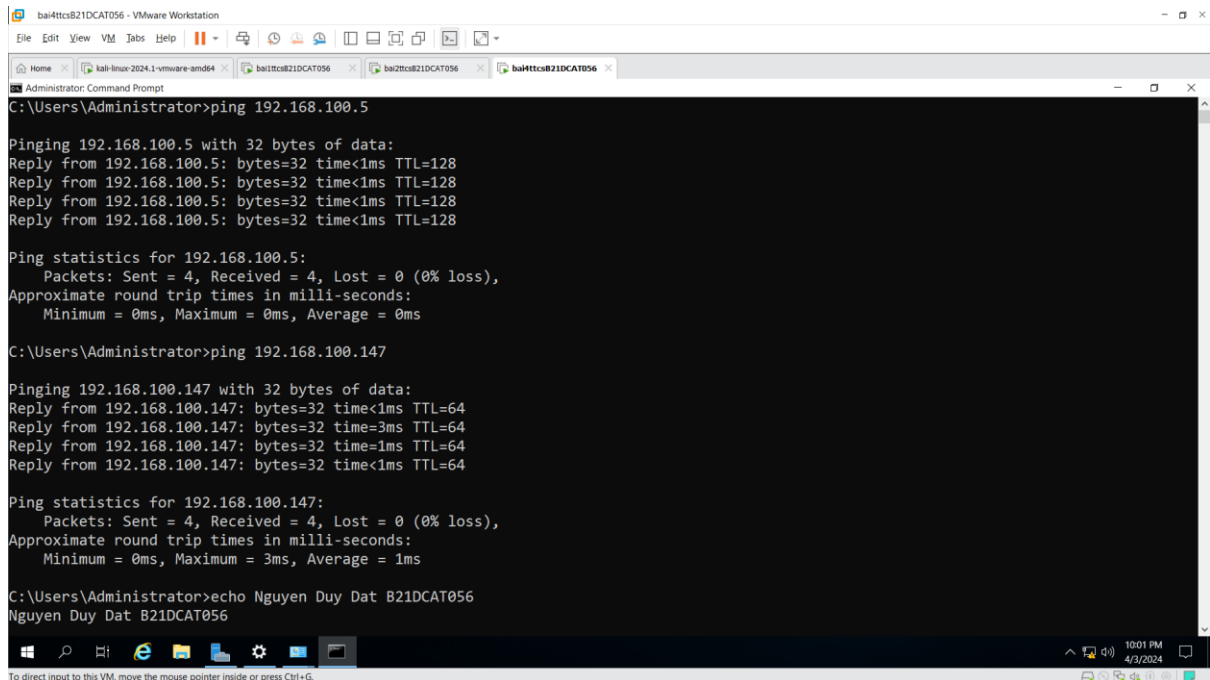
- Sử dụng lệnh `tcpdump -I eth0 icmp` để bắt `tcpdump` bắt gói tin trên dải mạng `192.168.100.0/24`



The screenshot shows a Kali Linux terminal window titled "kali@B21AT056-Dat-Kali". The user has entered the command `sudo tcpdump -i eth0 icmp`. The terminal output shows a message from `tcpdump` indicating it is listening on `eth0` and has captured a packet. The packet details are as follows:

```
11:00:01.946640 IP 192.168.100.5 > 192.168.100.201: ICMP 192.168.100.5 udp port 50362 unreachable, length 64
```

- Trên máy windows server ping tới các mạng trong internal



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The user has entered the command `C:\Users\Administrator>ping 192.168.100.5`. The output shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 128. The ping statistics for 192.168.100.5 are as follows:

```
Ping statistics for 192.168.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The user then enters the command `C:\Users\Administrator>ping 192.168.100.147`. The output shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 64. The ping statistics for 192.168.100.147 are as follows:

```
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 = 3ms, Average = 1ms
```

The user then enters the command `C:\Users\Administrator>echo Nguyen Duy Dat B21DCAT056`. The output is `Nguyen Duy Dat B21DCAT056`.

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 ba11tc821DCAT056 ba27tc821DCAT056 ba44tc821DCAT056
kali@B21AT056-Dat-Kali -
File Actions Edit View Help
(kali@B21AT056-Dat-Kali)-[~]
$ sudo tcpdump -i eth0 icmp
sudo: unable to resolve host B21AT056-Dat-Kali: Temporary failure in name resolution
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
11:00:01.946640 IP 192.168.100.5 > 192.168.100.201: ICMP 192.168.100.5 udp port 50362 unreachable, length 64
11:00:11.915515 IP 192.168.100.5 > 192.168.100.201: ICMP 192.168.100.5 udp port 63347 unreachable, length 80
11:00:34.565342 IP 192.168.100.201 > 192.168.100.5: ICMP echo request, id 1, seq 7, length 40
11:00:34.565786 IP 192.168.100.5 > 192.168.100.201: ICMP echo reply, id 1, seq 7, length 40
11:00:35.587047 IP 192.168.100.201 > 192.168.100.5: ICMP echo request, id 1, seq 8, length 40
11:00:35.587316 IP 192.168.100.5 > 192.168.100.201: ICMP echo reply, id 1, seq 8, length 40
11:00:36.603538 IP 192.168.100.201 > 192.168.100.5: ICMP echo request, id 1, seq 9, length 40
11:00:36.603884 IP 192.168.100.5 > 192.168.100.201: ICMP echo reply, id 1, seq 9, length 40
11:00:37.624179 IP 192.168.100.201 > 192.168.100.5: ICMP echo request, id 1, seq 10, length 40
11:00:37.624180 IP 192.168.100.5 > 192.168.100.201: ICMP echo reply, id 1, seq 10, length 40
11:00:41.617288 IP 192.168.100.201 > 192.168.100.147: ICMP echo request, id 1, seq 11, length 40
11:00:41.617519 IP 192.168.100.147 > 192.168.100.201: ICMP echo reply, id 1, seq 11, length 40
11:00:42.636306 IP 192.168.100.201 > 192.168.100.147: ICMP echo request, id 1, seq 12, length 40
11:00:42.637418 IP 192.168.100.147 > 192.168.100.201: ICMP echo reply, id 1, seq 12, length 40
11:00:43.666160 IP 192.168.100.201 > 192.168.100.147: ICMP echo request, id 1, seq 13, length 40
11:00:43.666959 IP 192.168.100.147 > 192.168.100.201: ICMP echo reply, id 1, seq 13, length 40
11:00:44.681549 IP 192.168.100.201 > 192.168.100.147: ICMP echo request, id 1, seq 14, length 40
11:00:44.681817 IP 192.168.100.147 > 192.168.100.201: ICMP echo reply, id 1, seq 14, length 40
11:01:20.902388 IP 192.168.100.5 > 192.168.100.201: ICMP 192.168.100.5 udp port 54399 unreachable, length 64
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
```

- Tương tự, phía bên external, ping từ windows server
- dùng lệnh Tcpdump -i eth1 icmp để bắt gói tin

```
ba44tc821DCAT056 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2024.1-vmware-amd64 ba11tc821DCAT056 ba27tc821DCAT056 ba44tc821DCAT056 kali-linux-2023.4-vmware-amd64
Administrator: Command Prompt
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 = 1ms, Average = 0ms

C:\Users\Administrator>echo Nguyen Duy Dat B21DCAT056
Nguyen Duy Dat B21DCAT056

C:\Users\Administrator>
```



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home | kali-linux-2024.1-vmware-amd64 | ba11tc8b21dcat056 | ba27tc8b21dcat056 | ba44tc8b21dcat056 | kali-linux-2023.4-vmware-amd64
File Actions Edit View Help
kali@B21AT056-Dat-Kali: ~
kali@B21AT056-Dat-Kali: ~
$ sudo tcpdump -i eth1 icmp
sudo: unable to resolve host B21AT056-Dat-Kali: Temporary failure in name resolution
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:19:01.190989 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 5, length 40
12:19:01.191133 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 5, length 40
12:19:02.199464 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 6, length 40
12:19:02.199738 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 6, length 40
12:19:03.216103 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 7, length 40
12:19:03.216716 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 7, length 40
12:19:04.247496 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 8, length 40
12:19:04.247815 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 8, length 40
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel

kali@B21AT056-Dat-Kali: ~
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@B21AT056-Dat-Kali: ~
$ date
Wed Apr 3 12:19:45 PM EDT 2024

kali@B21AT056-Dat-Kali: ~
$
```

- Để bắt gói tin và lưu vào file pcap sử dụng lệnh:
tcpdump -i eth1 icmp -w datnd_b21dcat056.pcap

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home | kali-linux-2024.1-vmware-amd64 | ba11tc8b21dcat056 | ba27tc8b21dcat056 | ba44tc8b21dcat056 | kali-linux-2023.4-vmware-amd64
File Actions Edit View Help
kali@B21AT056-Dat-Kali: ~
kali@B21AT056-Dat-Kali: ~
$ sudo tcpdump -i eth1 icmp -w datnd_b21dcat056.pcap
sudo: unable to resolve host B21AT056-Dat-Kali: Temporary failure in name resolution
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C8 packets captured
8 packets received by filter
0 packets dropped by kernel

kali@B21AT056-Dat-Kali: ~
$ tcpdump -r datnd_b21dcat056.pcap
reading from file datnd_b21dcat056.pcap, link-type EN10MB (Ethernet), snapshot length 262144
12:21:11.751790 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 9, length 40
12:21:11.752055 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 9, length 40
12:21:12.762922 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 10, length 40
12:21:12.763246 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 10, length 40
12:21:13.794074 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 11, length 40
12:21:13.794388 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 11, length 40
12:21:14.825712 IP 10.10.19.202 > 10.10.19.148: ICMP echo request, id 1, seq 12, length 40
12:21:14.826062 IP 10.10.19.148 > 10.10.19.202: ICMP echo reply, id 1, seq 12, length 40

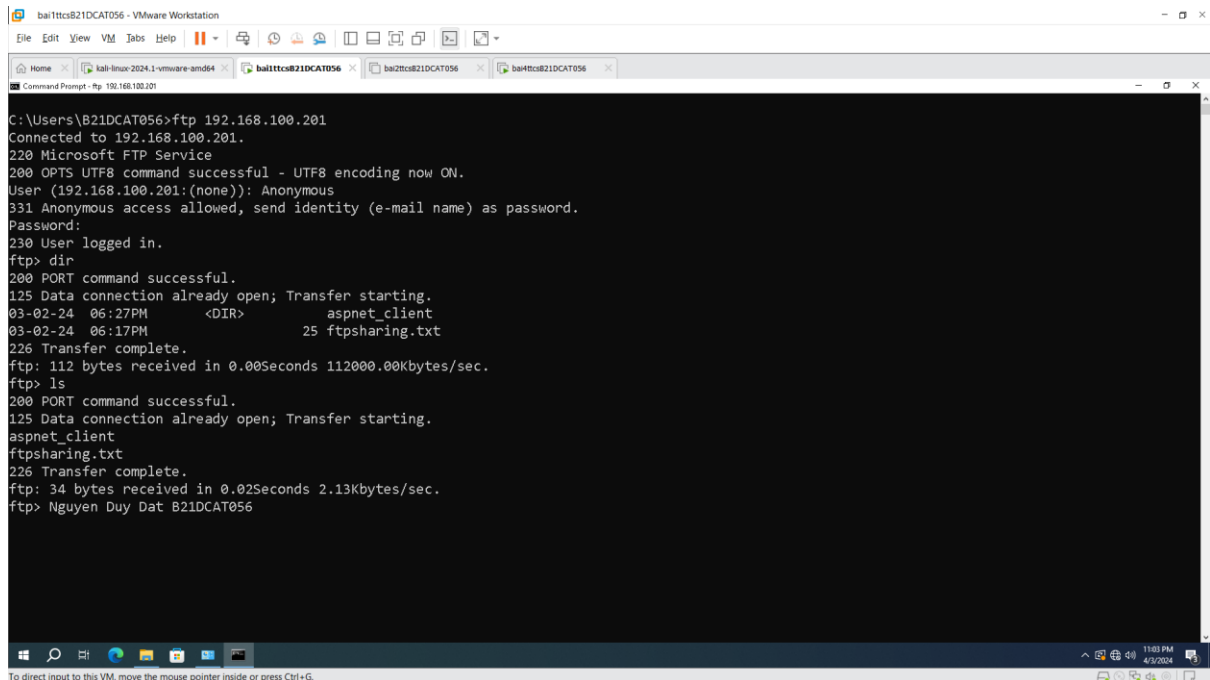
kali@B21AT056-Dat-Kali: ~
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

kali@B21AT056-Dat-Kali: ~
$ date
Wed Apr 3 12:21:39 PM EDT 2024

kali@B21AT056-Dat-Kali: ~
$
```

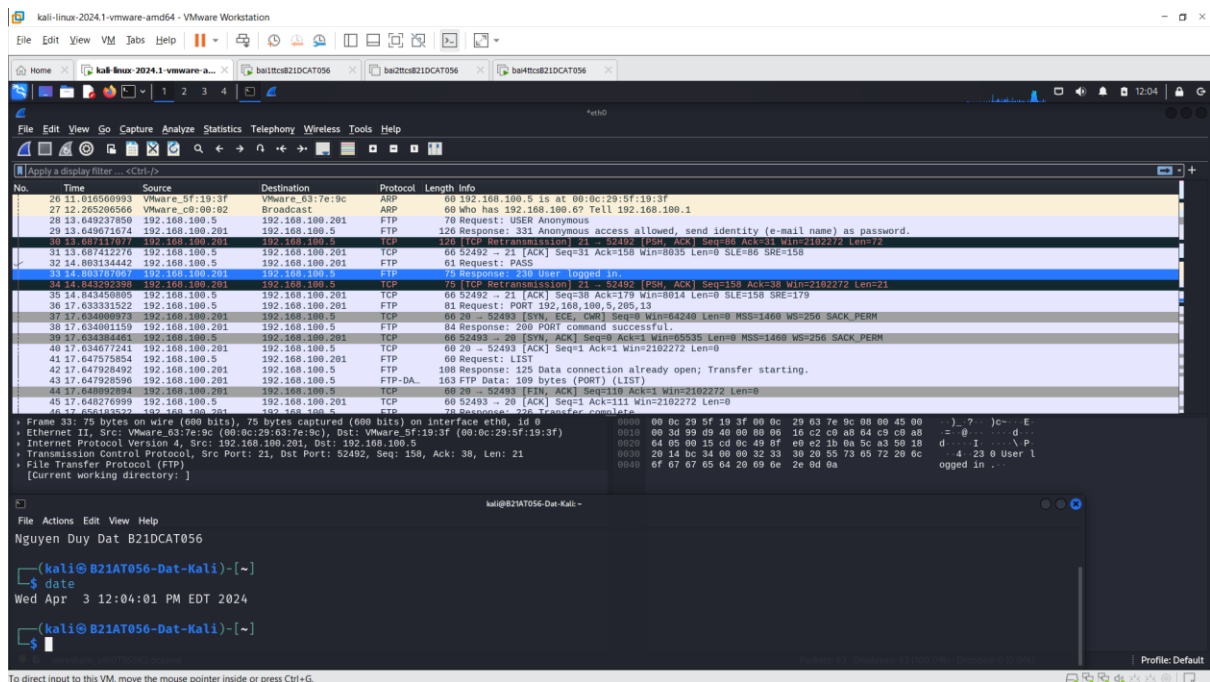

3. Sử dụng Wireshark để bắt và phân tích các gói tin

- Trên windows 10 tiến hành truy cập ftp tới windows server qua ip 192.168.100.201



```
C:\Users\B21DCAT056>ftp 192.168.100.201
Connected to 192.168.100.201.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.100.201:(none)): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-02-24 06:27PM <DIR>          aspnet_client
03-02-24 06:17PM                25 ftpsharing.txt
226 Transfer complete.
ftp: 112 bytes received in 0.00Seconds 112000.00kbytes/sec.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
aspnet_client
ftpsharing.txt
226 Transfer complete.
ftp: 34 bytes received in 0.02Seconds 2.13Kbytes/sec.
ftp> Nguyen Duy Dat B21DCAT056
```

- Trên máy linux sniffer thu được các gói tin ftp



Wireshark packet capture showing an FTP session. The packet list includes:

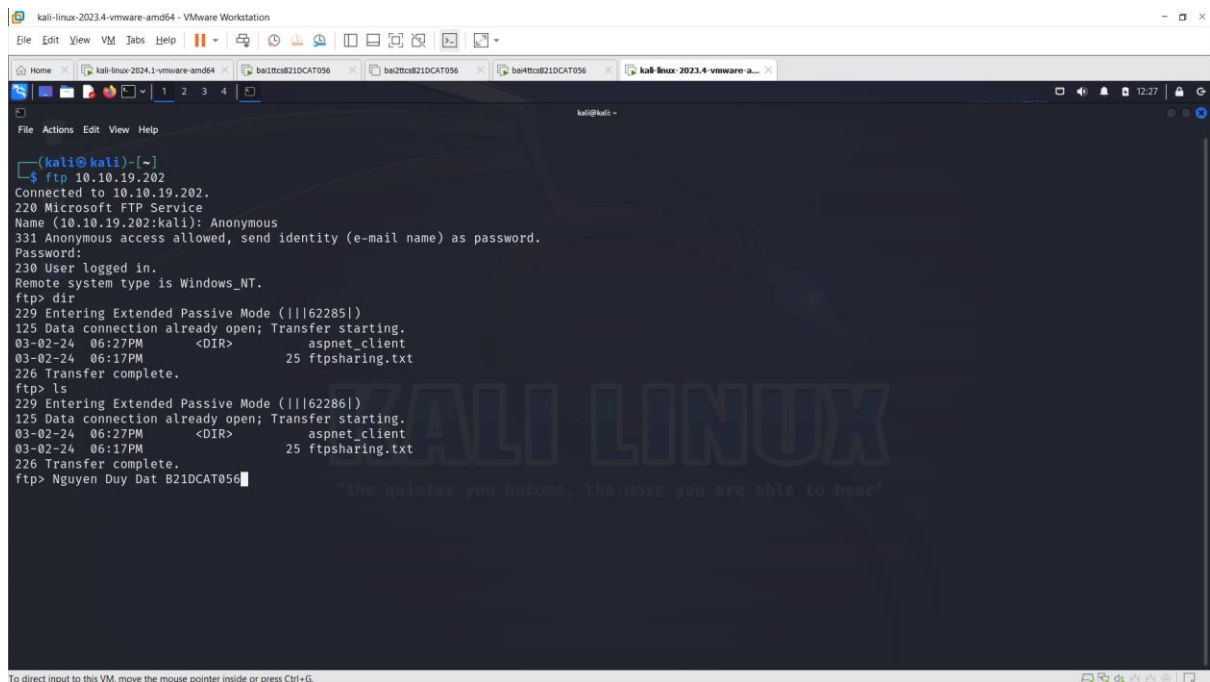
No.	Time	Source	Destination	Protocol	Length	Info
26	11.615569993	Vmware_05f19:3f	Vmware_637e:9c	ARP	60	192.168.100.5 is at 00:0c:29:5f:19:3f
27	12.265296566	Vmware_c000:02	Broadcast	ARP	60	who has 192.168.100.67 Tell 192.168.100.1
28	13.649237850	192.168.100.5	192.168.100.201	FTP	70	Request: USER Anonymous
29	13.649671674	192.168.100.201	192.168.100.5	FTP	120	Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
30	13.64971977	192.168.100.5	192.168.100.201	FTP	70	Request: PORT 192.168.100.5,205,13
31	13.697412276	192.168.100.5	192.168.100.201	TCP	60	52492 -> 21 [ACK] Seq=31 Ack=158 Win=8035 Len=0 SLE=80 SRE=158
32	14.883134442	192.168.100.5	192.168.100.201	FTP	61	Request: PASS
33	14.891217170	192.168.100.201	192.168.100.5	FTP	75	Response: 230 User logged in.
34	14.843292390	192.168.100.201	192.168.100.5	TCP	75	[TCP Retransmission] 21 -> 52492 [PSH, ACK] Seq=158 Ack=38 Win=2102272 Len=21
35	14.843450805	192.168.100.5	192.168.100.201	TCP	60	52492 -> 21 [ACK] Seq=38 Ack=179 Win=8014 Len=0 SLE=158 SRE=179
36	17.633321522	192.168.100.5	192.168.100.201	FTP	81	Request: PORT 192.168.100.5,205,13
37	17.634090973	192.168.100.201	192.168.100.5	TCP	60	20 -> 52493 [SYN, ECE, CWR] Seq=6 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
38	17.634061159	192.168.100.201	192.168.100.5	FTP	84	Response: 200 PORT command successful.
39	17.634040461	192.168.100.5	192.168.100.201	TCP	60	52493 -> 21 [SYN, ACK] Seq=1 Ack=111 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
40	17.634677241	192.168.100.201	192.168.100.5	TCP	60	20 -> 52493 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
41	17.647575854	192.168.100.5	192.168.100.201	FTP	60	Request: LIST
42	17.647820492	192.168.100.201	192.168.100.5	FTP	100	Response: 125 Data connection already open; Transfer starting.
43	17.647928596	192.168.100.201	192.168.100.5	FTP-DA	163	FTP Data: 109 bytes (PORT) (LIST)
44	17.648992894	192.168.100.201	192.168.100.5	TCP	60	20 -> 52493 [FIN, ACK] Seq=119 Ack=3 Win=2102272 Len=0
45	17.648276909	192.168.100.5	192.168.100.201	TCP	60	52493 -> 20 [ACK] Seq=1 Ack=111 Win=2102272 Len=0
46	17.648383322	192.168.100.201	192.168.100.5	FTP	70	Response: 226 Transfer complete.

Below the packet list, a terminal window shows the FTP session output:

```
kali@B21AT056-Dat-Kali:~$ date
Wed Apr 3 12:04:01 PM EDT 2024

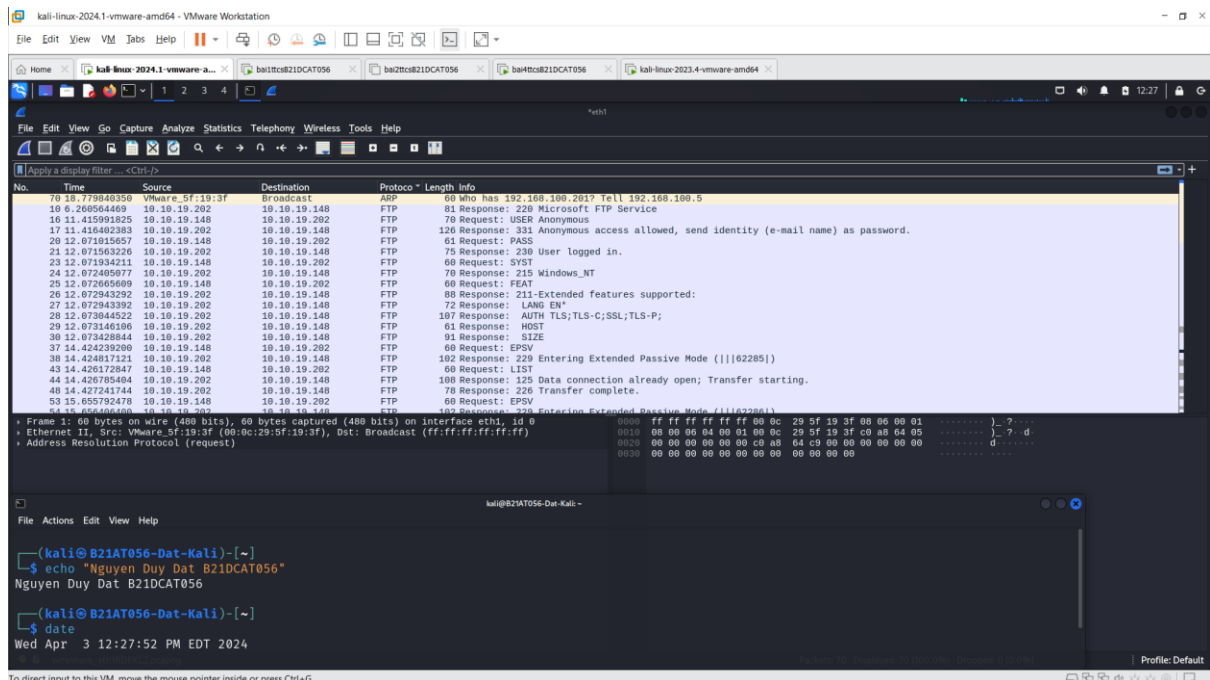
kali@B21AT056-Dat-Kali:~$
```

- Trên máy kali external kết nối ftp tới windows server qua ip 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): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||62285|)
125 Data connection already open; Transfer starting.
03-02-24 06:27PM <DIR> aspnet_client
03-02-24 06:17PM 25 ftpsharing.txt
226 Transfer complete.
ftp> ls
229 Entering Extended Passive Mode (|||62286|)
125 Data connection already open; Transfer starting.
03-02-24 06:27PM <DIR> aspnet_client
03-02-24 06:17PM 25 ftpsharing.txt
226 Transfer complete.
ftp> Nguyen Duy Dat B21DCAT056
```

- Trên máy linux sniffer thu được các gói tin ftp



```
No. Time Source Destination Protocol Length Info
70 18.779840350 VMware 5f:19:3f Broadcast ARP 60 Who has 192.168.100.201? Tell 192.168.100.5
10 6.266564469 10.10.19.202 10.10.19.148 FTP 81 Response: 220 Microsoft FTP Service
10 11.415991325 10.10.19.148 10.10.19.202 FTP 70 Request: USER Anonymous
17 11.416492383 10.10.19.202 10.10.19.148 FTP 126 Response: 331 Anonymous access allowed, send identity (e-mail name) as password.
20 12.071015657 10.10.19.148 10.10.19.202 FTP 61 Request: PASS
21 12.071563226 10.10.19.202 10.10.19.148 FTP 75 Response: 230 User logged in.
23 12.071934211 10.10.19.148 10.10.19.202 FTP 60 Request: SYST
24 12.072405077 10.10.19.202 10.10.19.148 FTP 70 Response: 215 Windows_NT
25 12.072606069 10.10.19.148 10.10.19.202 FTP 60 Request: FEAT
26 12.072943292 10.10.19.202 10.10.19.148 FTP 88 Response: 211-Extended features supported:
27 12.072943392 10.10.19.202 10.10.19.148 FTP 72 Response: LANG EN
28 12.073644522 10.10.19.202 10.10.19.148 FTP 197 Response: AUTH TLS;TLS-C;SSL;TLS-P;
29 12.073146106 10.10.19.202 10.10.19.148 FTP 61 Response: HOST
30 12.073428844 10.10.19.202 10.10.19.148 FTP 91 Response: SIZE
37 14.424239200 10.10.19.148 10.10.19.202 FTP 60 Request: EPSV
38 14.424817121 10.10.19.202 10.10.19.148 FTP 102 Response: 229 Entering Extended Passive Mode (|||62285|)
43 14.426172847 10.10.19.148 10.10.19.202 FTP 60 Request: LIST
44 14.426705404 10.10.19.202 10.10.19.148 FTP 108 Response: 125 Data connection already open; Transfer starting.
48 14.427241744 10.10.19.202 10.10.19.148 FTP 78 Response: 226 Transfer complete.
53 15.655792478 10.10.19.148 10.10.19.202 FTP 60 Request: EPSV
54 15.656496100 10.10.19.202 10.10.19.148 FTP 102 Response: 229 Entering Extended Passive Mode (|||62286|)

+ Frame 1: 60 bytes captured on interface eth1, id 0
+ Ethernet II, Src: VMware 5f:19:3f (00:0c:29:5f:19:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
+ Address Resolution Protocol (request)
0000 ff ff ff ff ff ff ff ff 29 5f 19 3f 00 00 00 01 .....?..
0010 00 00 00 04 01 00 0c 29 5f 19 3f c0 a8 c4 05 .....?..d
0020 00 00 00 00 00 00 c0 a8 c4 c0 00 00 00 00 .....d.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 .....d.....
```

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

