



BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP HỒ CHÍ MINH

Khoa: Công Nghệ Thông Tin



LAB REPORT

TH GK Phân tích gói tin

Student's ID :
Student's name : Phúc Lâm
Subject : Triển khai an ninh hệ thống
Instructor : Đỗ Hà Phương
Faculty : Công Nghệ Thông Tin
Completed Date : / /2024

LAB GIỮA KÌ 2023

1. Kết quả phân mảnh khi thực hiện lệnh Ping IPx -l 8000

2. Tính lượng dữ liệu gửi lệnh Ping khi nhận được các mảnh: Frame1: 1514 Frame2: 1514 Frame3: 1000

3. Trình bày mục đích, cách thức tấn công ARP, DHCP, DNS

4. Mô phỏng tấn công ARP, DHCP, DNS

5. Mô phỏng bắt và phân tích mật khẩu gói tin truy cập Web, FTP, Telnet

Máy thật làm máy victim và 1 winserver và 1 pc win 7 làm attack

THỰC HIỆN

Câu 1: Kết quả phân mảnh khi thực hiện lệnh Ping IPx -l 8000

Thực hiện các bước:

1. PC – Victim 192.168.10.1 ping tới máy Attack 192.168.1.128
2. Lệnh ping 192.168.10.128 -l 8000 -n 1
3. Ở máy Attack bật Wireshark để bắt gói tin

Kết quả:

20	46.9246920	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=942e) [Reassembled in #25]
21	46.9246920	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=942e) [Reassembled in #25]
22	46.9246930	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=942e) [Reassembled in #25]
23	46.9247120	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=942e) [Reassembled in #25]
24	46.9247120	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=942e) [Reassembled in #25]
25	46.9247120	192.168.10.1	192.168.10.128	ICMP	642	Echo (ping) request id=0x0001, seq=2591/7946, ttl=128 (reply in 28)
26	46.9248290	VMware_d4:0a:79	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.128
27	46.9249610	VMware_c0:00:08	VMware_d4:0a:79	ARP	60	192.168.10.1 is at 00:50:56:c0:00:08
28	46.9249740	192.168.10.128	192.168.10.1	ICMP	1514	Echo (ping) reply id=0x0001, seq=2591/7946, ttl=128 (request in 25)
29	46.9249770	192.168.10.128	192.168.10.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=31e8)
30	46.9249790	192.168.10.128	192.168.10.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=31e8)
31	46.9249800	192.168.10.128	192.168.10.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=31e8)
32	46.9249810	192.168.10.128	192.168.10.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=31e8)
33	46.9249820	192.168.10.128	192.168.10.1	IPv4	642	Fragmented IP protocol (proto=ICMP 1, off=7400, ID=31e8)

No.	Time	Source	Destination	Protocol	Length	Info
14	11.0396360	192.168.10.2	192.168.10.128	ICMP	120	Destination unreachable
15	13.5587270	192.168.10.200	192.168.10.255	BROWSER	243	Host Announcement SERVE
16	15.6307200	192.168.10.128	192.168.10.255	NBNS	92	Name query NB ATTACK<1c
17	16.3727820	192.168.10.128	192.168.10.255	NBNS	92	Name query NB ATTACK<1c
18	17.1375910	192.168.10.128	192.168.10.255	NBNS	92	Name query NB ATTACK<1c
19	46.8603330	fe80::e002:4fa0:6ee	ff02::1:2	DHCPv6	148	Solicit XID: 0x2ef144 c
20	46.9246920	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol
21	46.9246920	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol
22	46.9246930	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol
23	46.9247120	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol
24	46.9247120	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented IP protocol
25	46.9247120	192.168.10.1	192.168.10.128	ICMP	642	Echo (ping) request id

Khi thực hiện ping 8000 thì sẽ chia gói tin phân thành 6 mảnh

Giải thích:

Kích thước gói ping: $8000 \text{ bytes} + 8 \text{ (đầu ICMP)} = 8008$

Tính số Frame: $8008/1480 = 5,41 \Rightarrow$ cần 6 Frame

Frame 1: $1480 + 20 \text{ (IP header)} + 14 \text{ (Ethernet header)} + 4 = 1518 \text{ bytes}$

Frame 2: $1480 + 20 + 14 + 4 = 1518 \text{ bytes}$

Frame 3: $1480 + 20 + 14 + 4 = 1518 \text{ bytes}$

Frame 4: $1480 + 20 + 14 + 4 = 1518 \text{ bytes}$

Frame 5: $1480 + 20 + 14 + 4 = 1518 \text{ bytes}$

Frame 6: $8008 - (1480 * 5) = 608 \text{ bytes}$

$\Rightarrow 608 + 20 + 14 = 642 \text{ bytes}$

FRAME	Size	MF	OFFSET	Total Lenght	Head Lenght
1	1514	1	0	1500	20
2	1514	1	1480	1500	20
3	1514	1	2960	1500	20
4	1514	1	4440	1500	20
5	1514	1	5920	1500	20
6	642	0	7400	628	20

Câu 2: Tính lượng dữ liệu gửi lệnh Ping khi nhận được các mảnh: Frame1: 1514 Frame2: 1514 Frame3: 1000

Xác định kích thước dữ liệu:

Frame 1: $1480 + 20 + 14 = 1514 \text{ bytes}$

Frame 2: $1480 + 20 + 14 = 1514 \text{ bytes}$

Frame 3: $966 + 20 + 14 = 1000 \text{ bytes}$

Tổng kích thước tất cả các Frame: $1514 + 1514 + 1000 = 4028 \text{ bytes}$

Trong mỗi Frame, tổng kích thước header (IP, Ethernet) chiếm: $20 + 14 = 34 \text{ bytes}$

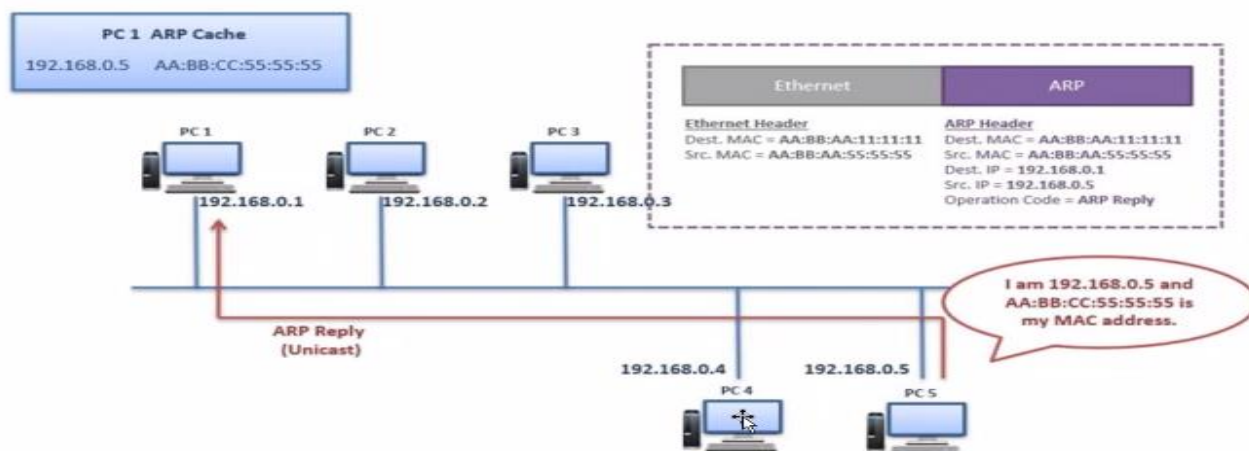
Tổng kích thước dữ liệu khi gửi đi là: $4028 - (34 * 3) - 8 = 3918 \text{ bytes}$

Kiểm tra lại bằng cách bắt gói tin:

Io.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented
2	0.00000100	192.168.10.1	192.168.10.128	IPv4	1514	Fragmented
3	0.00000100	192.168.10.1	192.168.10.128	ICMP	1000	Echo (ping)
4	0.00016300	Vmware_d4:0a:79	Broadcast	ARP	42	who has 192.168.10.1
5	0.00025500	Vmware_c0:00:08	Vmware_d4:0a:79	ARP	60	192.168.10.1
6	0.00026600	192.168.10.128	192.168.10.1	ICMP	1514	Echo (ping)
7	0.00026900	192.168.10.128	192.168.10.1	IPv4	1514	Fragmented
8	0.00027100	192.168.10.128	192.168.10.1	IPv4	1000	Fragmented
9	4.80720000	Vmware_c0:00:08	Vmware_d4:0a:79	ARP	60	who has 192.168.10.1
10	4.80722100	Vmware_d4:0a:79	Vmware_c0:00:08	ARP	42	192.168.10.1
11	11.50713700	192.168.10.128	192.168.10.255	BROWSER	243	Local Master

```
Select C:\Windows\system32\cmd.exe
C:\Users\COMPUTER>ping 192.168.10.128 -l 3918 -n 1
Pinging 192.168.10.128 with 3918 bytes of data:
Reply from 192.168.10.128: bytes=3918 time<1ms TTL=128
Ping statistics for 192.168.10.128:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\COMPUTER>
```

Câu 3: Trình bày mục đích, cách thức tấn công ARP, DHCP, DNS



a. Tấn công ARP

- Kẻ tấn công ngồi ở PC4 và tấn công PC1, khi pc1 gửi arp ra tới pc5 mà pc4 đã gửi ARP reply trước PC5
- Pc1 gửi cho PC5 mà PC4 đã lấy được.(bẻ lái đường truyền, ăn cắp thông tin)
- Giả sử pc5 kết nối cổng ra internet, pc4 giả mạo mac của pc5 làm cho pc1 gửi nhầm sang pc4 và sau đó pc4 gửi sang pc5 để ra cổng internet

b. Tấn công DHCP server

- DHCP server cấp ip, subnet, mask cho các máy, kẻ tấn công tiến hành cướp hoặc sửa thông tin ip, mac.

c. Tấn công DNS

- Pc1 muốn truy cập internet thì phải truy cập pc3 để phân giải miền dns,
- pc4 tiến hành truy cập vào cơ sở dữ liệu của pc3 để sửa hoặc làm cho khi truy cập vào miền máy chủ khác, giả mạo nhằm đánh cắp thông tin đăng nhập,v.v

3.1. Tấn công ARP (ARP Spoofing)

Mục đích:

- Tấn công ARP (ARP Spoofing) nhằm giả mạo địa chỉ MAC của kẻ tấn công thành địa chỉ MAC của một thiết bị khác trong mạng, từ đó chặn hoặc điều hướng lưu lượng mạng đến thiết bị của kẻ tấn công.
- Kẻ tấn công có thể nghe trộm thông tin (Man-in-the-Middle attack), đánh cắp dữ liệu, thông tin đăng nhập hoặc thực hiện các cuộc tấn công từ chối dịch vụ (DoS).

Cách thức tấn công:

1. Kẻ tấn công gửi các gói tin ARP giả mạo (spoofed ARP replies) đến bảng ARP của máy nạn nhân, lừa nạn nhân tin rằng địa chỉ IP của một thiết bị trong mạng (ví dụ: gateway hoặc một thiết bị khác) thuộc về địa chỉ MAC của kẻ tấn công.
2. Khi nạn nhân cập nhật bảng ARP với thông tin giả mạo, tất cả lưu lượng gửi tới địa chỉ IP giả sẽ được chuyển đến máy của kẻ tấn công.
3. Kẻ tấn công có thể xem, sửa đổi, hoặc chuyển tiếp các gói tin mà không bị phát hiện.

3.2. Tấn công DHCP (DHCP Spoofing)

Mục đích:

- Tấn công DHCP nhằm đánh cắp thông tin cấu hình mạng của nạn nhân hoặc ngăn không cho nạn nhân kết nối được với mạng. Điều này có thể dẫn đến các cuộc tấn công Man-in-the-Middle hoặc DoS.
- Kẻ tấn công có thể kiểm soát thiết bị mạng của nạn nhân hoặc điều khiển cấu hình mạng để chuyển hướng lưu lượng qua thiết bị của mình.

Cách thức tấn công:

1. Kẻ tấn công thiết lập một máy chủ DHCP giả trong mạng để phát gói tin DHCP Offer với thông tin cấu hình giả (IP, gateway, DNS, v.v.).
2. Khi nạn nhân yêu cầu địa chỉ IP từ máy chủ DHCP (thông qua DHCP Discover), máy chủ giả mạo sẽ gửi phản hồi trước khi máy chủ DHCP hợp lệ phản hồi, khiến nạn nhân nhận địa chỉ IP từ máy chủ giả.
3. Sau khi nhận cấu hình từ máy chủ giả, lưu lượng của nạn nhân sẽ được chuyển qua máy của kẻ tấn công, cho phép kẻ tấn công kiểm soát hoặc ngăn chặn truy cập mạng.

3.3. Tấn công DNS (DNS Spoofing/DNS Cache Poisoning)

Mục đích:

- Tấn công DNS nhằm chuyển hướng người dùng đến các trang web giả mạo hoặc máy chủ độc hại thay vì trang web hợp pháp. Điều này giúp kẻ tấn công đánh cắp thông tin cá nhân, thông tin đăng nhập, hoặc phát tán phần mềm độc hại.
- Các trang web ngân hàng, mạng xã hội, hoặc dịch vụ email thường là mục tiêu của các cuộc tấn công DNS.

Cách thức tấn công:

1. Kẻ tấn công lợi dụng lỗ hổng trong hệ thống DNS để gửi các gói tin DNS giả mạo (fake DNS responses) đến nạn nhân hoặc máy chủ DNS đích.
2. Khi nạn nhân yêu cầu phân giải tên miền (ví dụ: từ google.com sang địa chỉ IP), kẻ tấn công gửi kết quả giả, trỏ tên miền đến một máy chủ do kẻ tấn công kiểm soát.
3. Khi nạn nhân truy cập trang web giả mạo, dữ liệu đăng nhập hoặc thông tin nhạy cảm có thể bị đánh cắp hoặc người dùng có thể bị tải xuống phần mềm độc hại.

Câu 4: Mô phỏng tấn công ARP, DHCP, DNS

4.1. Mô phỏng tấn công ARP

- Kiểm tra ping victim tới máy server với IP 192.168.10.200
- Kiểm tra arp -a trên máy victim

```
C:\Users\COMPUTER>arp -a

Interface: 192.168.254.1 --- 0x4
    Internet Address      Physical Address      Type
    192.168.254.132       00-0c-29-c6-47-97     dynamic
    192.168.254.133       00-0c-29-2a-cc-5c     dynamic
    192.168.254.255       ff-ff-ff-ff-ff-ff     static
    224.0.0.2             01-00-5e-00-00-02     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    224.0.0.252           01-00-5e-00-00-fc     static
    239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.1.90 --- 0x8
    Internet Address      Physical Address      Type
    192.168.1.1           60-38-e0-a9-b2-3c     dynamic
    192.168.1.255         ff-ff-ff-ff-ff-ff     static
    224.0.0.2             01-00-5e-00-00-02     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    224.0.0.252           01-00-5e-00-00-fc     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
    255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.10.1 --- 0xb
    Internet Address      Physical Address      Type
    192.168.10.128        00-0c-29-d4-0a-79     dynamic
    192.168.10.200        00-0c-29-c6-47-8d     dynamic
    192.168.10.255        ff-ff-ff-ff-ff-ff     static
    224.0.0.2             01-00-5e-00-00-02     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    224.0.0.252           01-00-5e-00-00-fc     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
```

-
- Tiến hành lái địa chỉ vật lý của Server 192.168.10.200 chuyển thành địa chỉ vật lý của máy ATTACK 192.168.10.128
- Lệnh arp -d 192.168.10.200 với quyền administrator trên CMD của máy VICTIM để xóa arp
- Sau đó thêm địa chỉ vật lý của Máy ATTACK 192.168.10.128 vào Card mạng “Vmnet8” vào địa chỉ mạng của máy SERVER 192.168.10.200.
- netsh interface ipv4 add neighbors “Vmnet8” 192.168.10.200 00-0c-29-d4-0a-79


```

Interface: 192.168.10.1 --- 0xb
Internet Address      Physical Address      Type
192.168.10.128        00-0c-29-d4-0a-79     dynamic
192.168.10.200        00-0c-29-c6-47-8d     dynamic
192.168.10.255        ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\Users\COMPUTER> arp -d 192.168.10.200
PS C:\Users\COMPUTER> netsh interface ipv4 add neighbors "VMnet8" 192.168.10.200 00-0c-29-d4-0a-79
PS C:\Users\COMPUTER> |

```

- Tiến hành kiểm tra, máy VICTIM ping tới máy SERVER 192.168.10.200 và kết quả là không ping được.

```

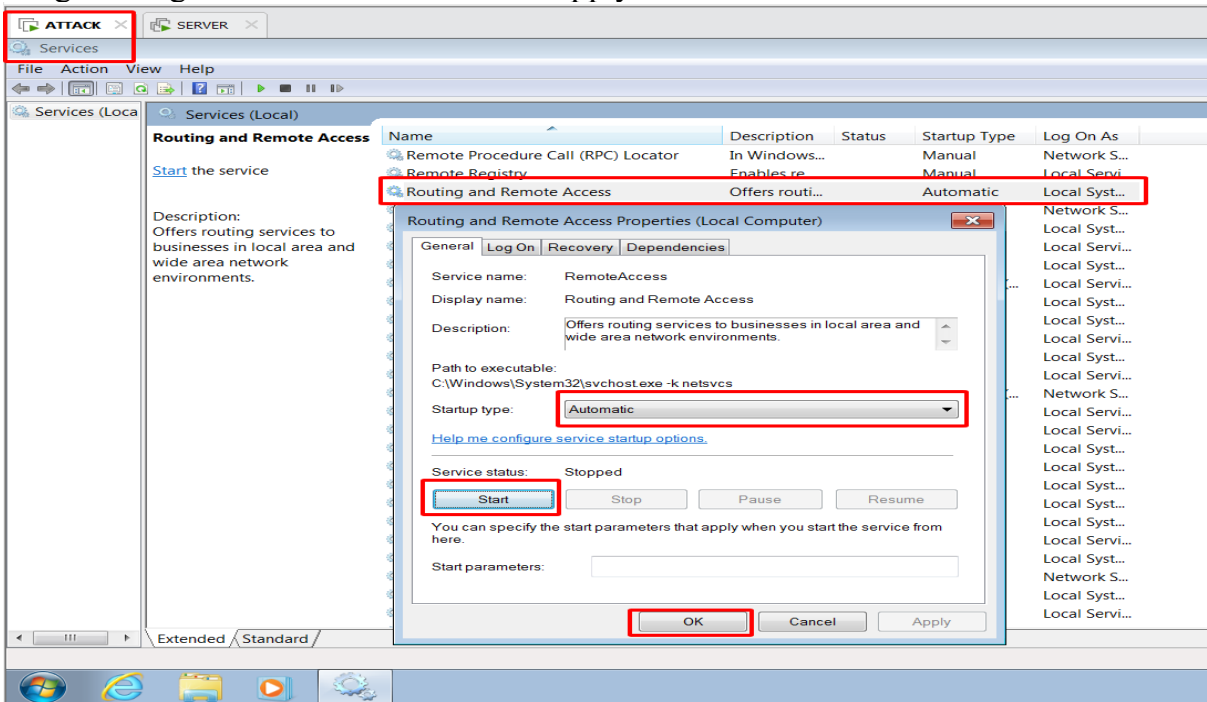
PS C:\Users\COMPUTER> ping 192.168.10.200

Pinging 192.168.10.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\COMPUTER> |

```

- Tiến hành bật cấu hình mở chuyển tiếp trong Máy ATTACK thì máy VICTIM mới thấy được. Ở máy ATTACK mở Services tìm mục **Routing and Remote Access**. Chọn chế độ khởi động tự động "Automatic" sau đó nhấn apply -> nhấn start -> nhấn OK.



- Tiến hành ping lại máy VICTIM ping tới máy Server.

```
PS C:\Users\COMPUTER> ping 192.168.10.200

Pinging 192.168.10.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\COMPUTER> ping 192.168.10.200

Pinging 192.168.10.200 with 32 bytes of data:
Reply from 192.168.10.200: bytes=32 time<1ms TTL=128
Reply from 192.168.10.200: bytes=32 time<1ms TTL=128
Reply from 192.168.10.200: bytes=32 time<1ms TTL=128
Reply from 192.168.10.200: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\COMPUTER>
```

- Khi tấn công ARP thì quá trình ping của VICTIM sẽ phải thông qua máy ATTACK mới đến được máy SERVER. Kết quả sau khi thực hiện tấn công ARP. Máy VICTIM 192.168.10.1 ping gói tin tới máy SERVER 192.168.10.200 nhưng máy ATTACK 192.168.10.128 đã bắt được gói tin và chuyển tiếp gói tin.

The screenshot displays a VMware Workstation environment with two virtual machines: ATTACK and SERVER. The ATTACK VM is running Windows, and the SERVER VM is running Linux. A network capture is being performed on the ATTACK VM using Wireshark, showing traffic between 192.168.10.1 (ATTACK) and 192.168.10.200 (SERVER). The capture shows an ARP request from 192.168.10.1 to 192.168.10.200, which is then redirected to 192.168.10.128. The Windows command prompt shows a successful ping from 192.168.10.1 to 192.168.10.200 with 8000 bytes of data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.10.1	192.168.10.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2ad2) [Reassembled in #6]
2	0.00000100	192.168.10.1	192.168.10.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=2ad2) [Reassembled in #6]
3	0.00000100	192.168.10.1	192.168.10.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=4440, ID=2ad2) [Reassembled in #6]
4	0.00000100	192.168.10.1	192.168.10.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=5920, ID=2ad2) [Reassembled in #6]
5	0.00000100	192.168.10.1	192.168.10.200	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=7400, ID=2ad2) [Reassembled in #6]
6	0.00000100	192.168.10.1	192.168.10.200	ICMP	64	Echo (ping) request id=0x0001, seq=2617/14602, ttl=128
7	0.00013400	Vmware_d4:0a:79	Broadcast	ARP	42	who has 192.168.10.1? Tell 192.168.10.128
8	0.00020700	Vmware_d4:0a:79	Broadcast	ARP	60	192.168.10.1 is at 00:50:56:c0:00:08
9	0.00024300	Vmware_c0:00:08	192.168.10.1	ICMP	1514	Redirect (Redirect for network)
10	0.00025400	192.168.10.128	192.168.10.1	IPv4	62	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3408)
11	0.00025800	192.168.10.128	192.168.10.1	IPv4	62	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3408)
12	0.00034400	Vmware_c6:47:8d	Vmware_d4:0a:79	ARP	60	192.168.10.200 is at 00:0c:29:c6:47:8d
13	0.00034800	192.168.10.1	192.168.10.200	IPv4	642	Fragmented IP protocol (proto=ICMP 1, off=7400, ID=2ad2)
14	2.79555600	fe80::e002:4fa0:6ee	ff02::1:2	DHCPv6	148	Solicit XID: 0x13730 CID: 000100012e8aa84200c29d40a79
15	5.11298600	Vmware_c6:47:8d	Broadcast	ARP	60	who has 192.168.10.2? Tell 192.168.10.200
16	5.11306000	Vmware_e7:66:be	Vmware_c6:47:8d	ARP	60	192.168.10.2 is at 00:50:56:e7:66:be
17	5.11318100	192.168.10.200	205.251.194.224	DNS	74	Standard query 0x388f SOA SERVER.abc.com
18	5.11324000	192.168.10.128	192.168.10.200	ICMP	102	Redirect (Redirect for network)
19	5.11341500	Vmware_d4:0a:79	Broadcast	ARP	42	who has 192.168.10.2? Tell 192.168.10.128
20	5.11360900	Vmware_e7:66:be	Vmware_d4:0a:79	ARP	60	192.168.10.2 is at 00:50:56:e7:66:be
21	5.11361600	192.168.10.200	205.251.194.224	DNS	74	Standard query 0x388f SOA SERVER.abc.com
22	5.16211600	205.251.194.224	192.168.10.200	DNS	152	Standard query response 0x388f No such name
23	5.16211700	205.251.194.224	192.168.10.200	DNS	152	Standard query response 0x388f No such name
24	5.16219000	205.251.194.224	192.168.10.200	DNS	152	Standard query response 0x388f No such name

Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_d4:0a:79 (00:0c:29:d4:0a:79)
Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.200 (192.168.10.200)

```
PS C:\Users\COMPUTER> ping 192.168.10.200 -l 8000 -n 1

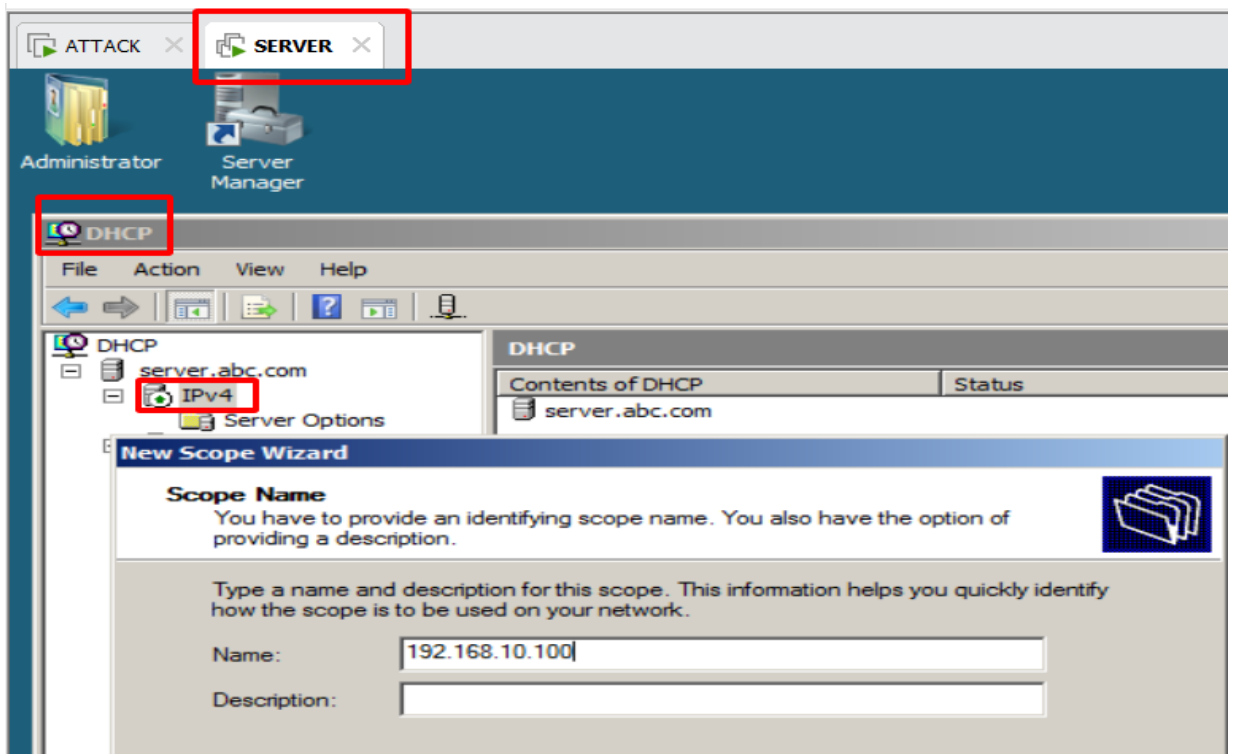
Pinging 192.168.10.200 with 8000 bytes of data:
Request timed out.

Ping statistics for 192.168.10.200:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
PS C:\Users\COMPUTER>
```

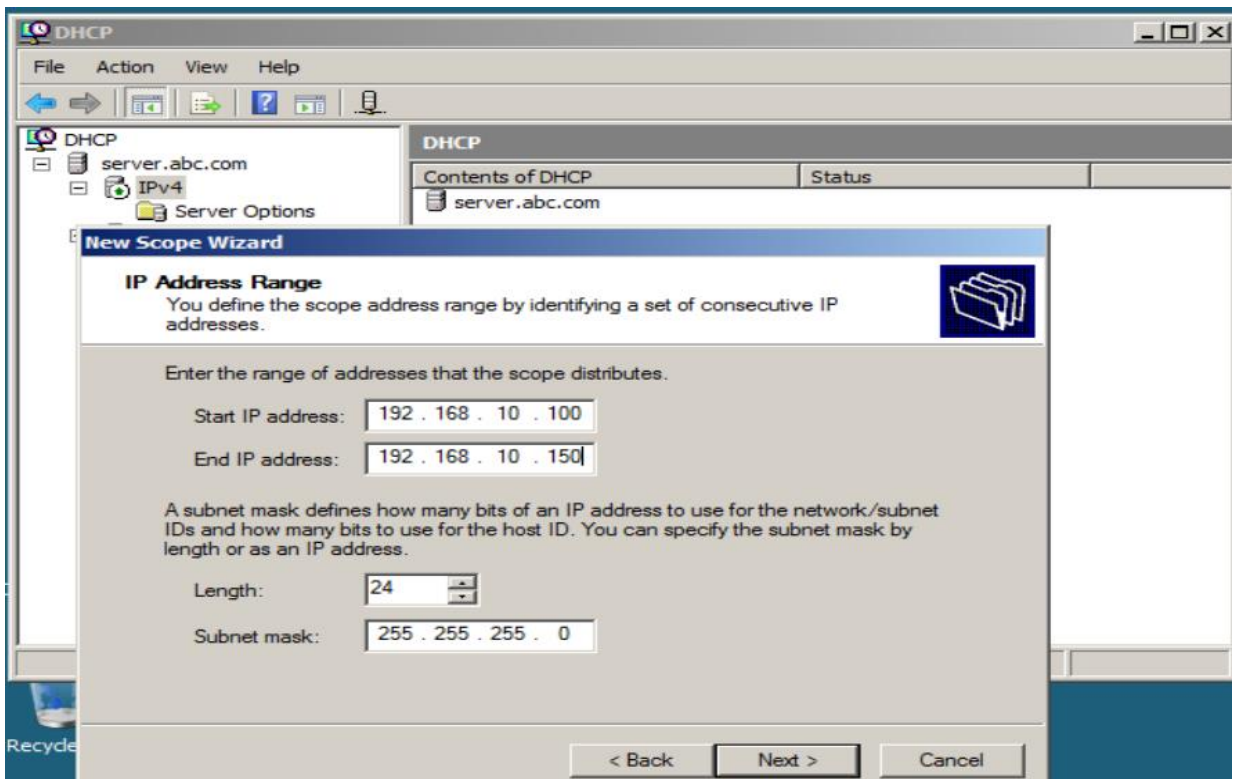
4.2. Mô phỏng tấn công DHCP

Máy SERVER cấp IP cho máy VICTIM có Option Default Gateway là IP máy ATTACK

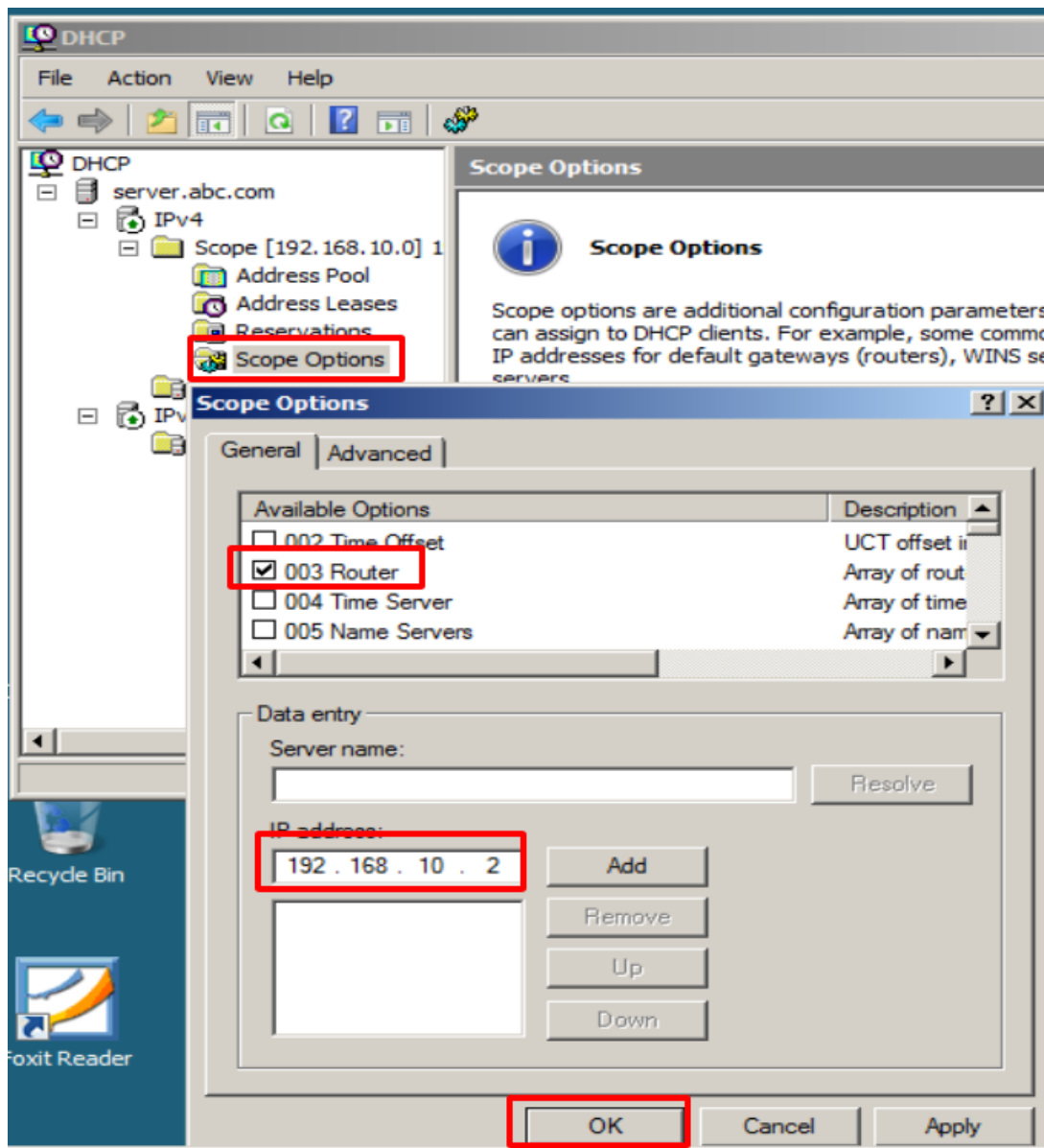
- Mở DHCP ở máy SERVER, tạo thêm mới New Scope ở phần Ipv4 có tên là 192.168.10.100



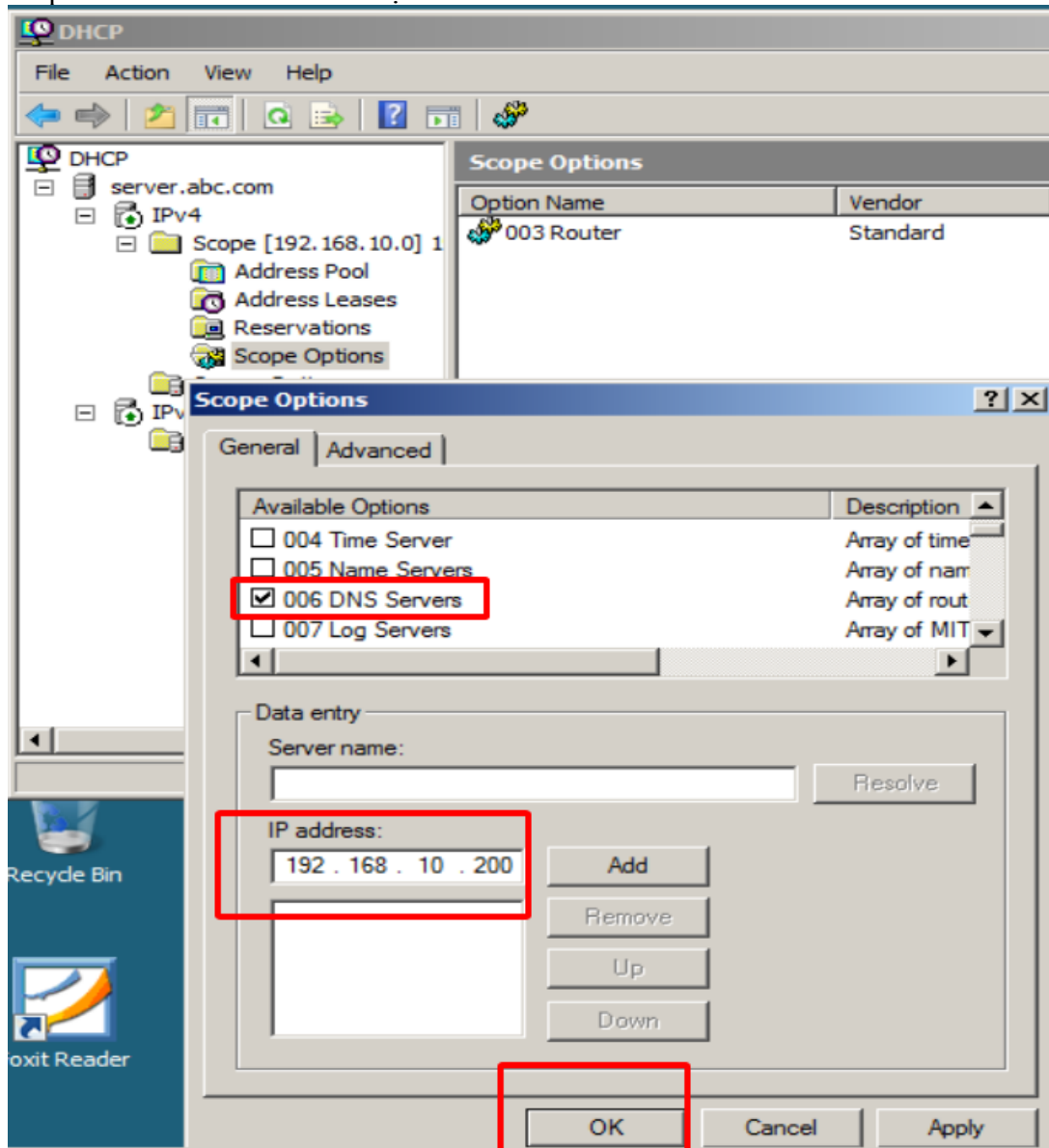
- Cài đặt vùng cấp IP là từ 192.168.10.100 đến 192.168.10.150 là vùng cấp phát IP. Sau đó nhấn Next đến Finish



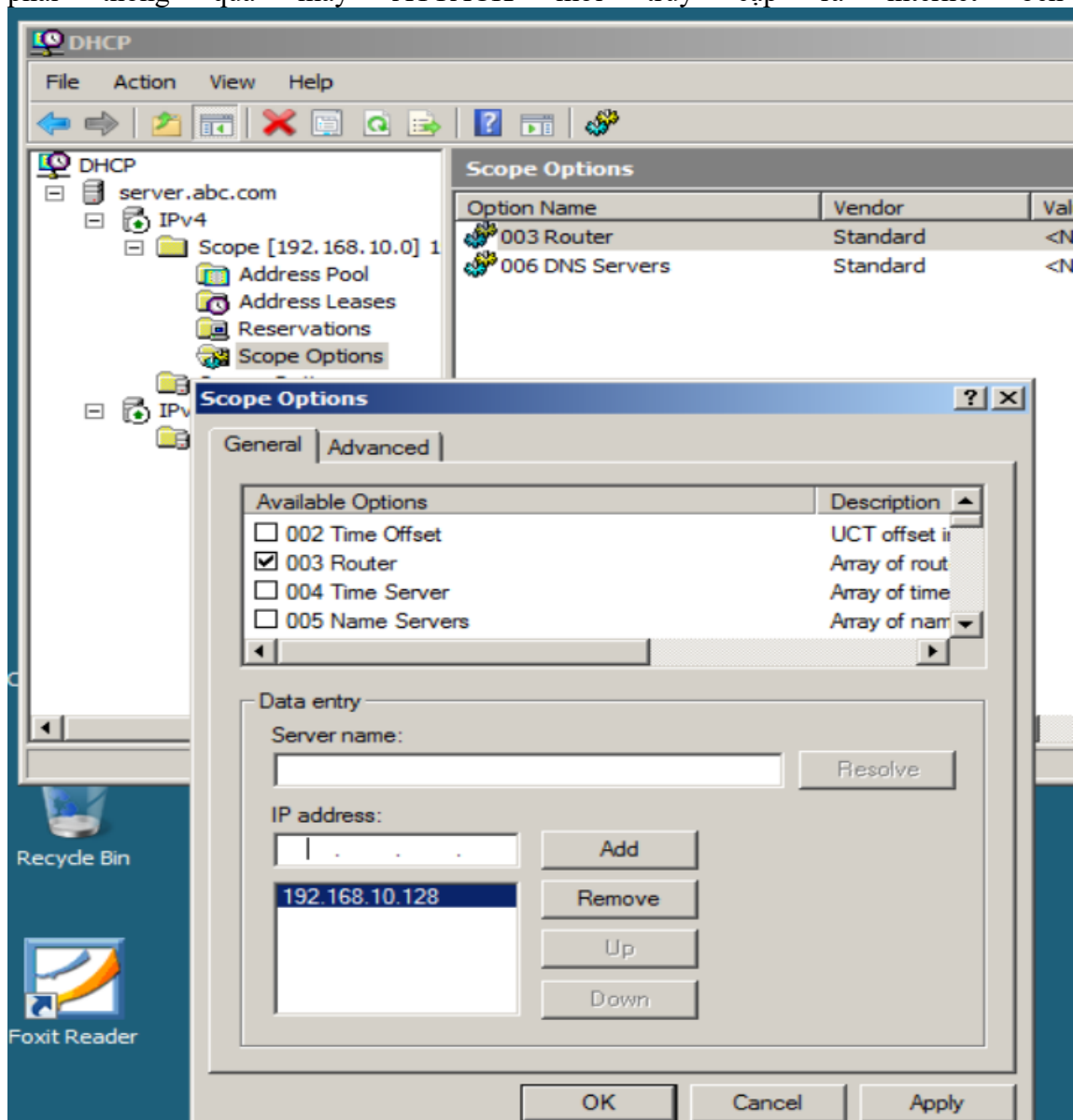
- Sau đó, cấp hình cho Scope Option, chọn Cấu hình 003 Router với địa chỉ IP address là 192.168.10.2 (Default Gateway)



- Tiếp theo là cấu hình DNS là địa chỉ 192.168.10.200

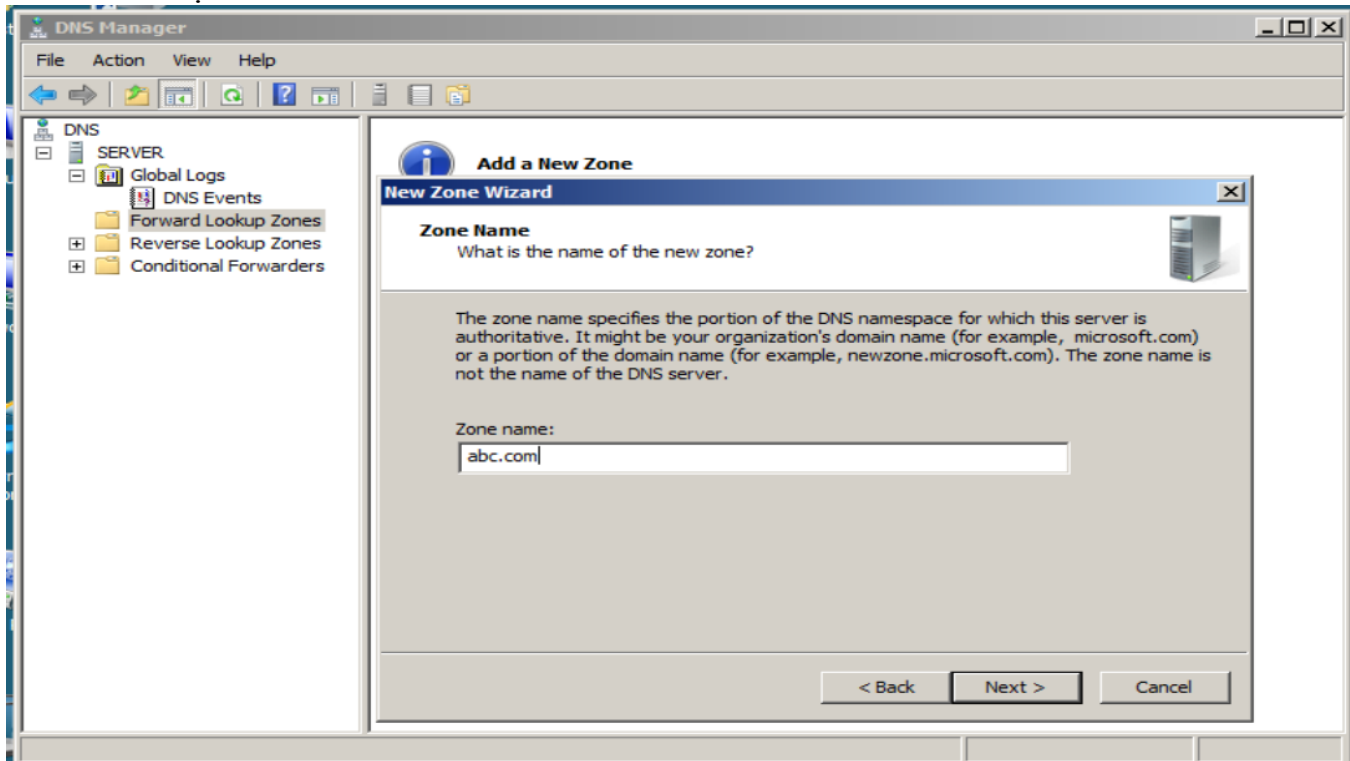


- Giả sử tấn công DHCP, thì khi kẻ tấn công ATTACK chiếm được quyền điều khiển máy chủ DHCP và điều chỉnh địa chỉ Router thành địa chỉ IP trở về IP của máy ATTACK 192.168.10.128. Sau đó, khi đó Máy chủ DHCP cấp IP cho Client (máy VICTIM) thì sẽ cái cổng Defalt Gateway sẽ chuyển thành máy IP máy ATTACK. Từ đó khi Client truy cập internet thì phải thông qua máy ATTACK mới truy cập ra internet bên ngoài

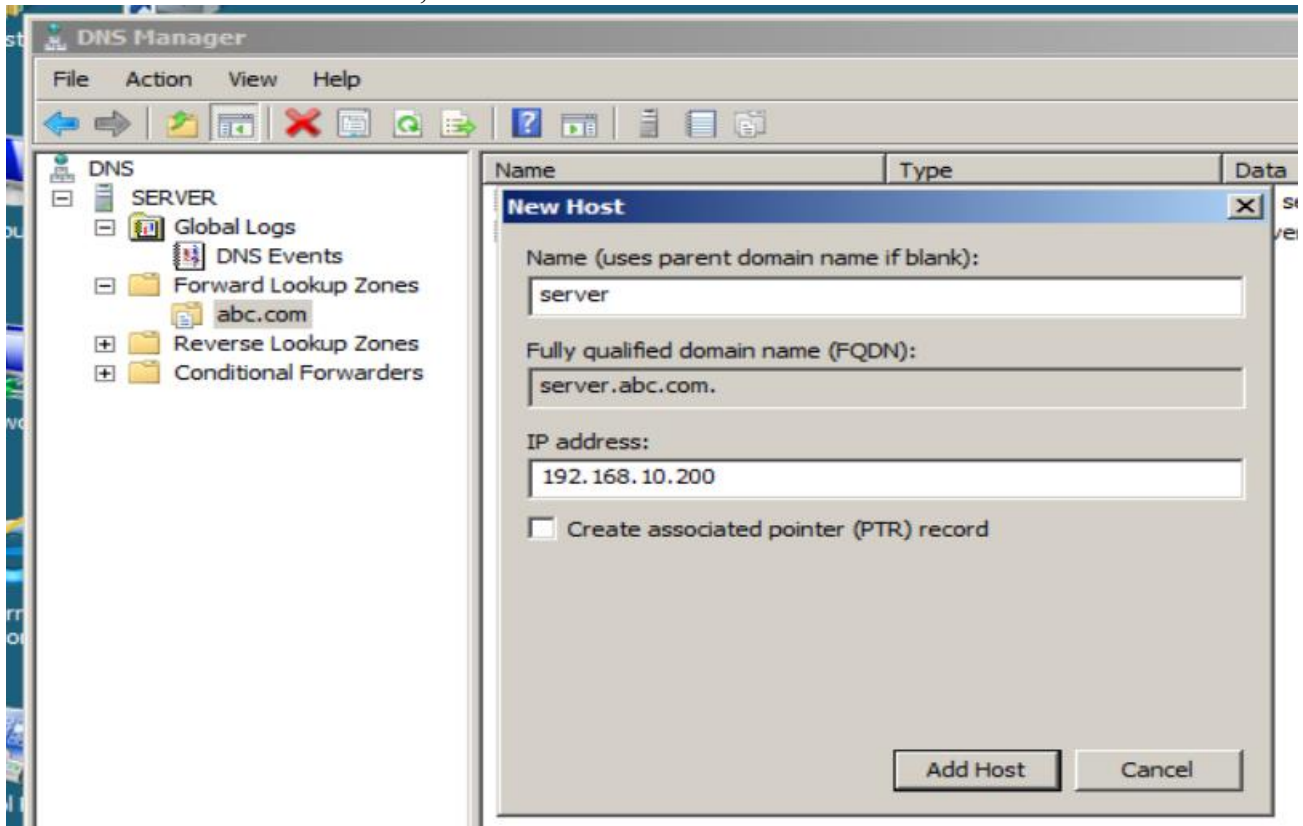


4.3. Mô phỏng tấn công DNS

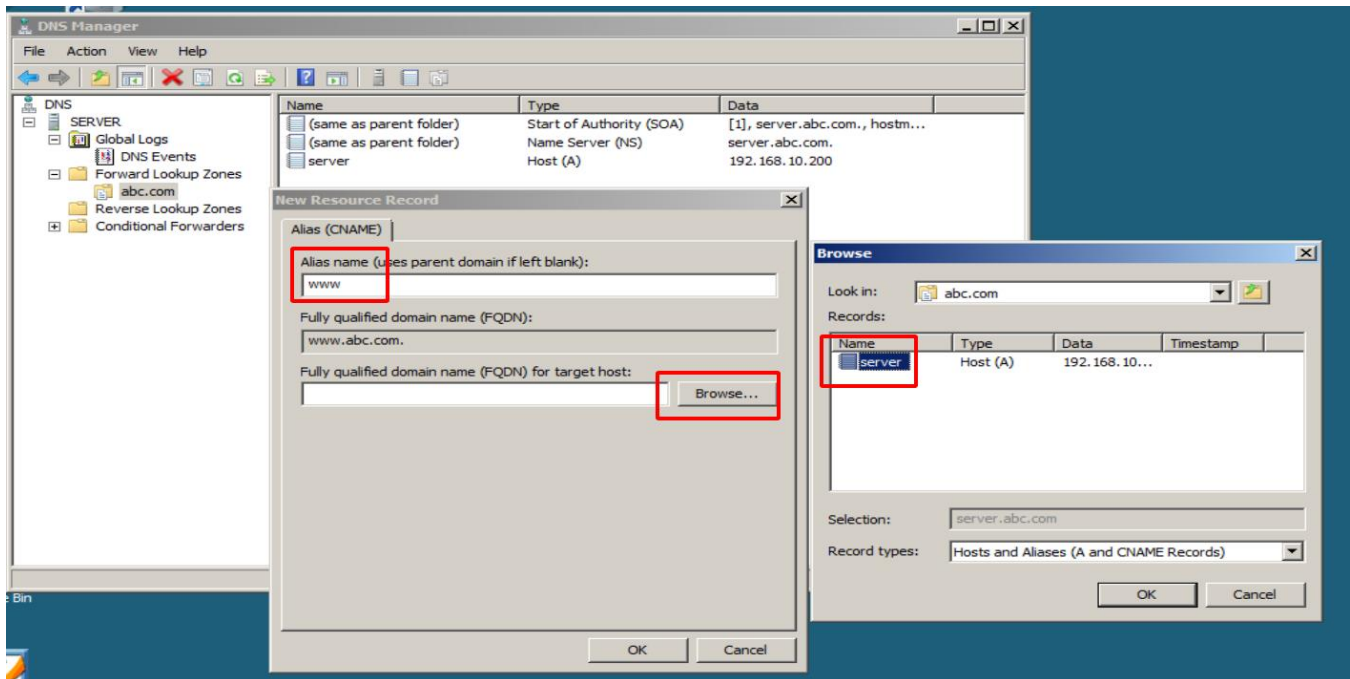
- Cài đặt role DNS
- Cấu hình và tạo ra miền Zone: abc.com



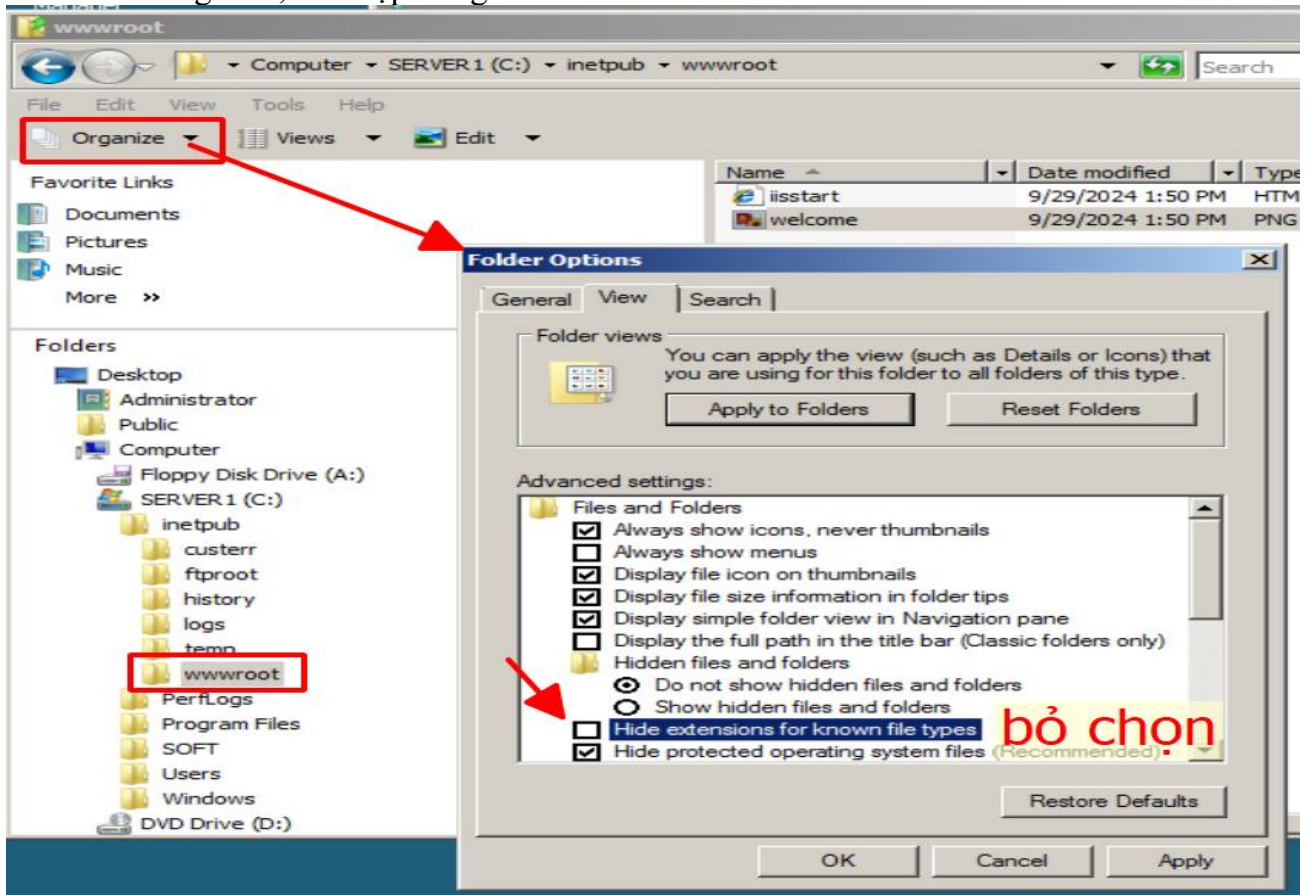
- New Host với name = Server, IP= 192.168.10.200



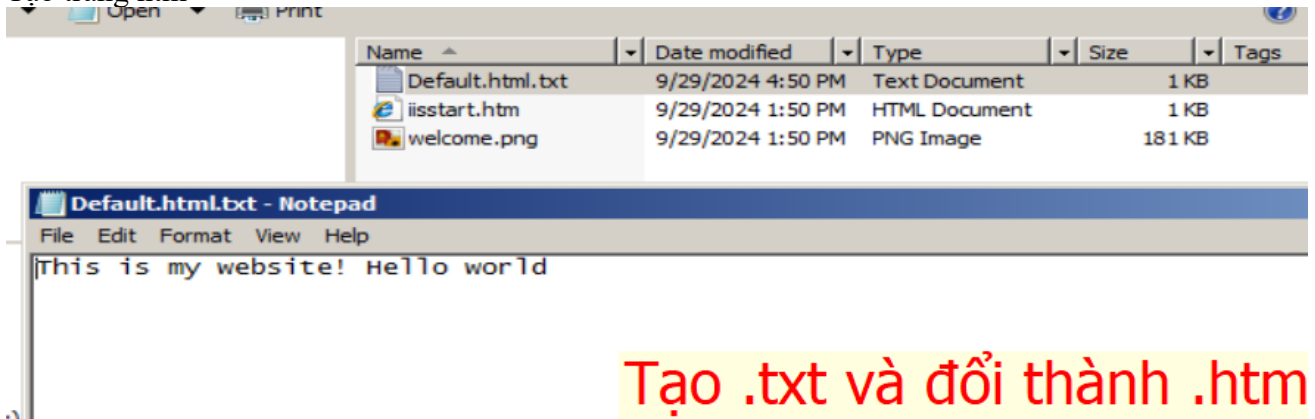
- Tạo 1 Alias cho máy chủ web server, Alias name = www; sau đó browse tới server có miền abc



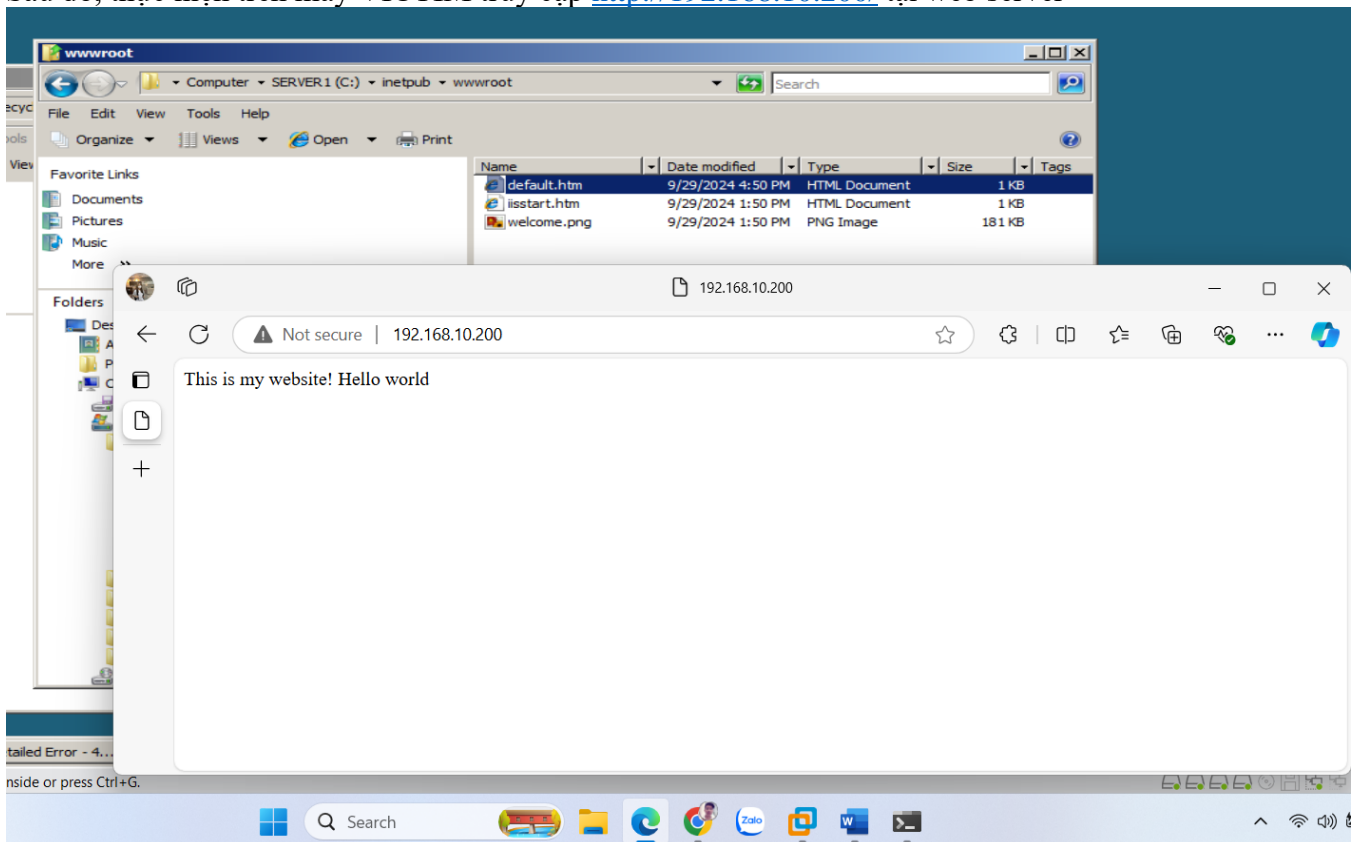
- Cấu hình trang web, thiết lập trang Default



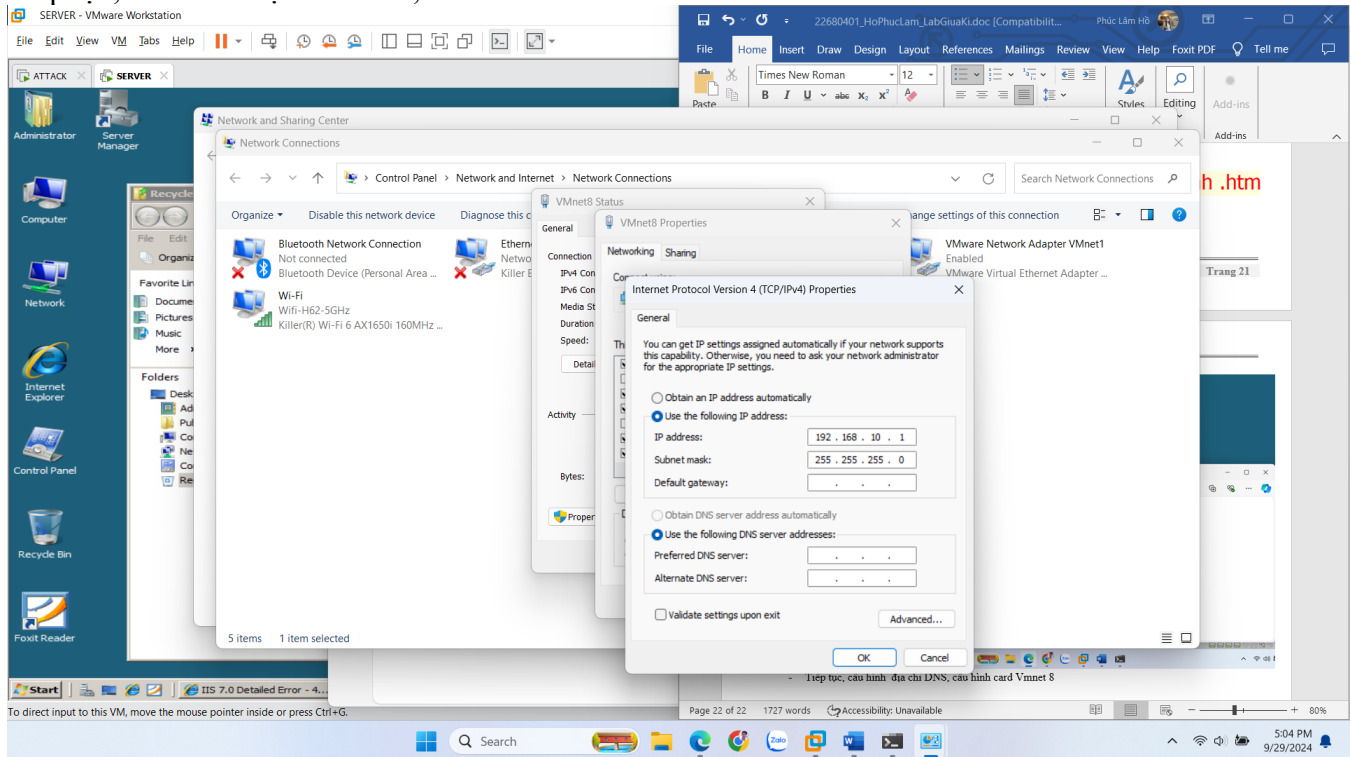
- Tạo trang htm



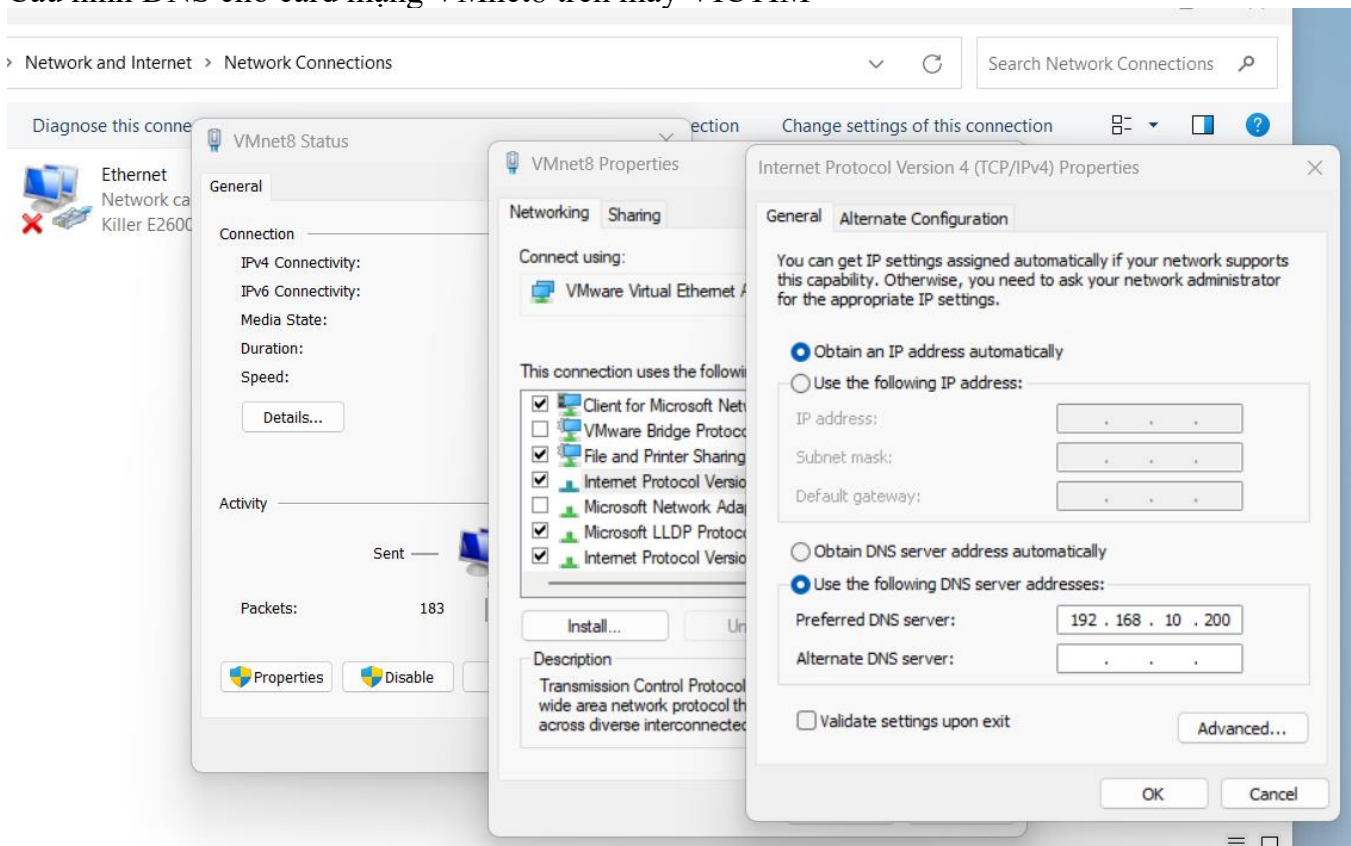
- Sau đó, thực hiện trên máy VICTIM truy cập <http://192.168.10.200/> tại web server



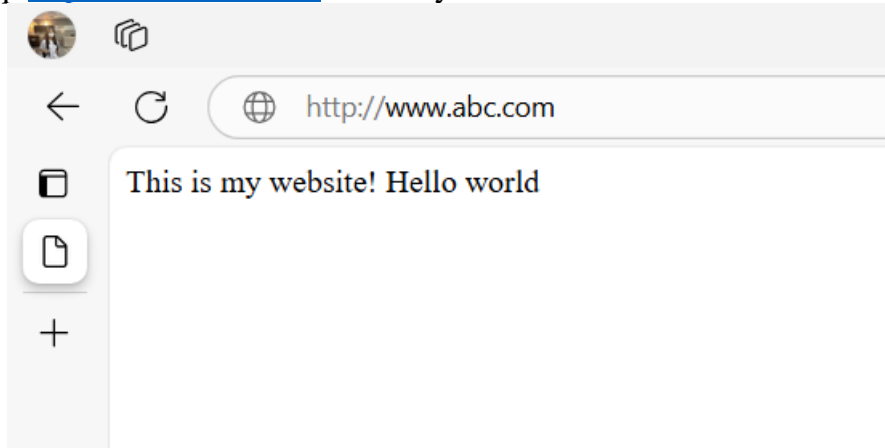
- Tiếp tục, cấu hình địa chỉ DNS, cấu hình card Vmnet 8



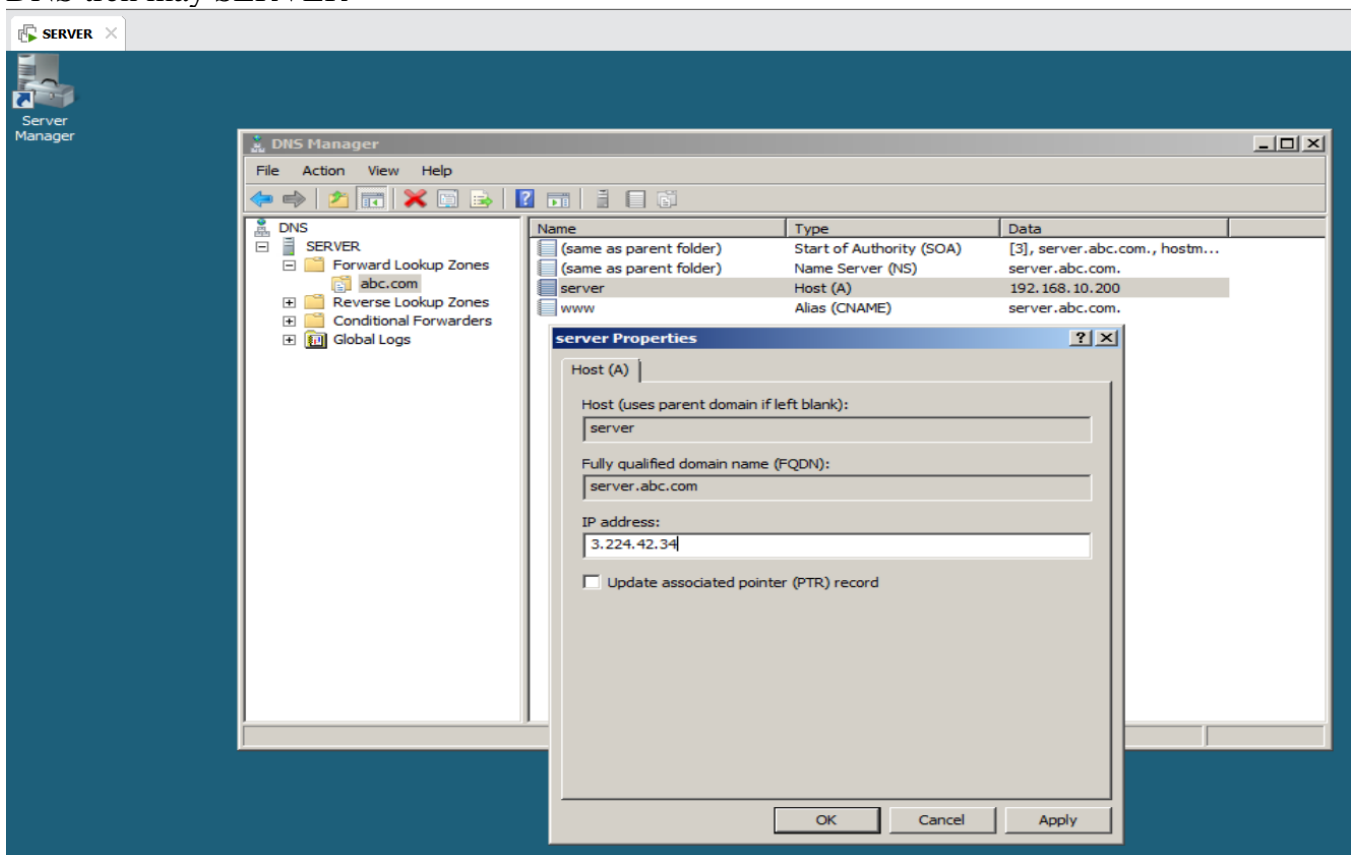
- Cấu hình DNS cho card mạng VMnet8 trên máy VICTIM



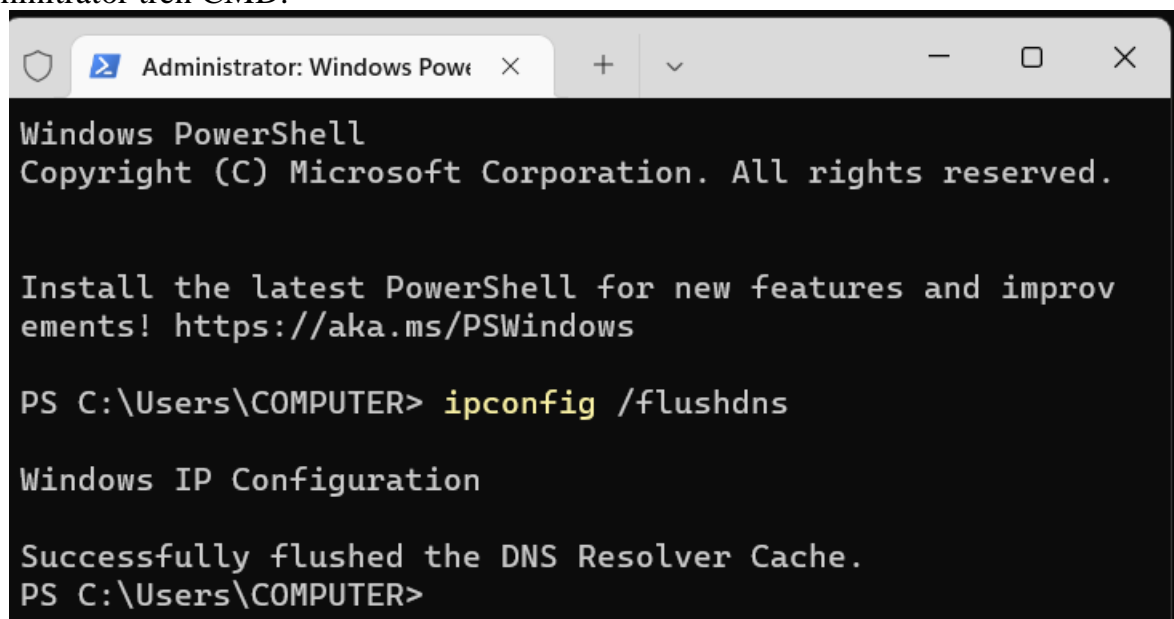
- Sau đó truy cập <http://www.abc.com/> trên máy VICTIM



- Tiến hành tấn công DNS, thực hiện chiếm quyền quản lý DNS và chỉnh sửa phần IP của DNS trên máy SERVER



- Sau đó tiến hành xóa DNS ở máy VICTIM bằng lệnh `ipconfig /flushdns` với quyền Administrator trên CMD.



```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

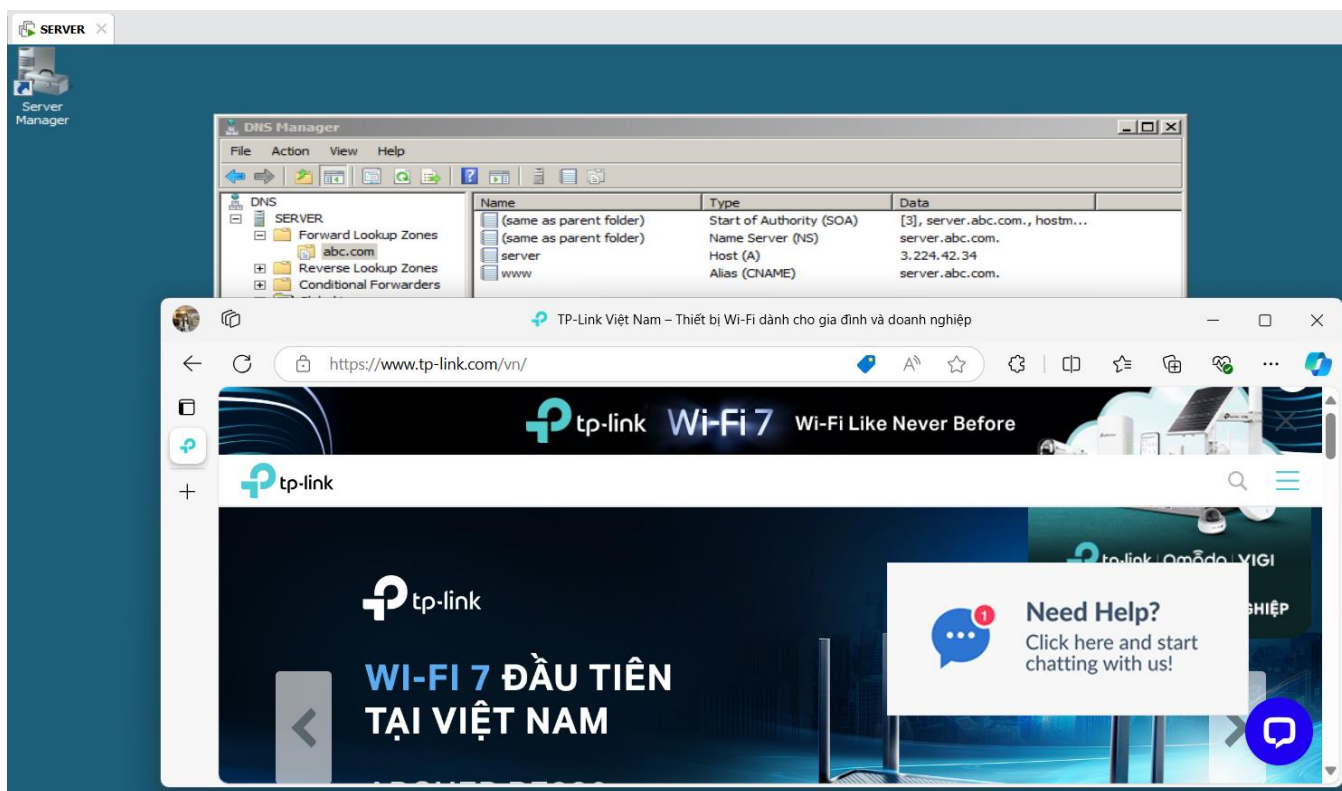
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\COMPUTER> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Users\COMPUTER>
```

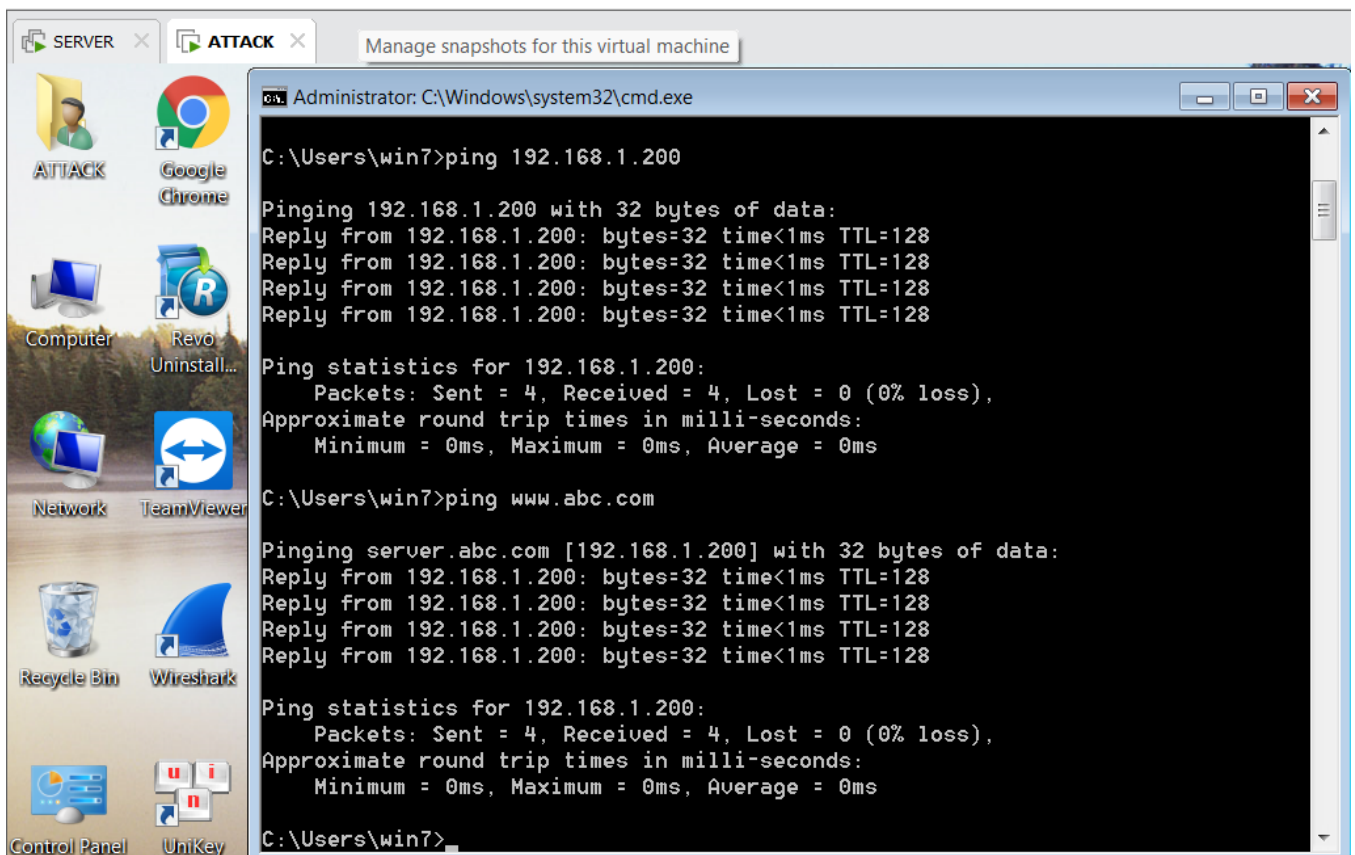
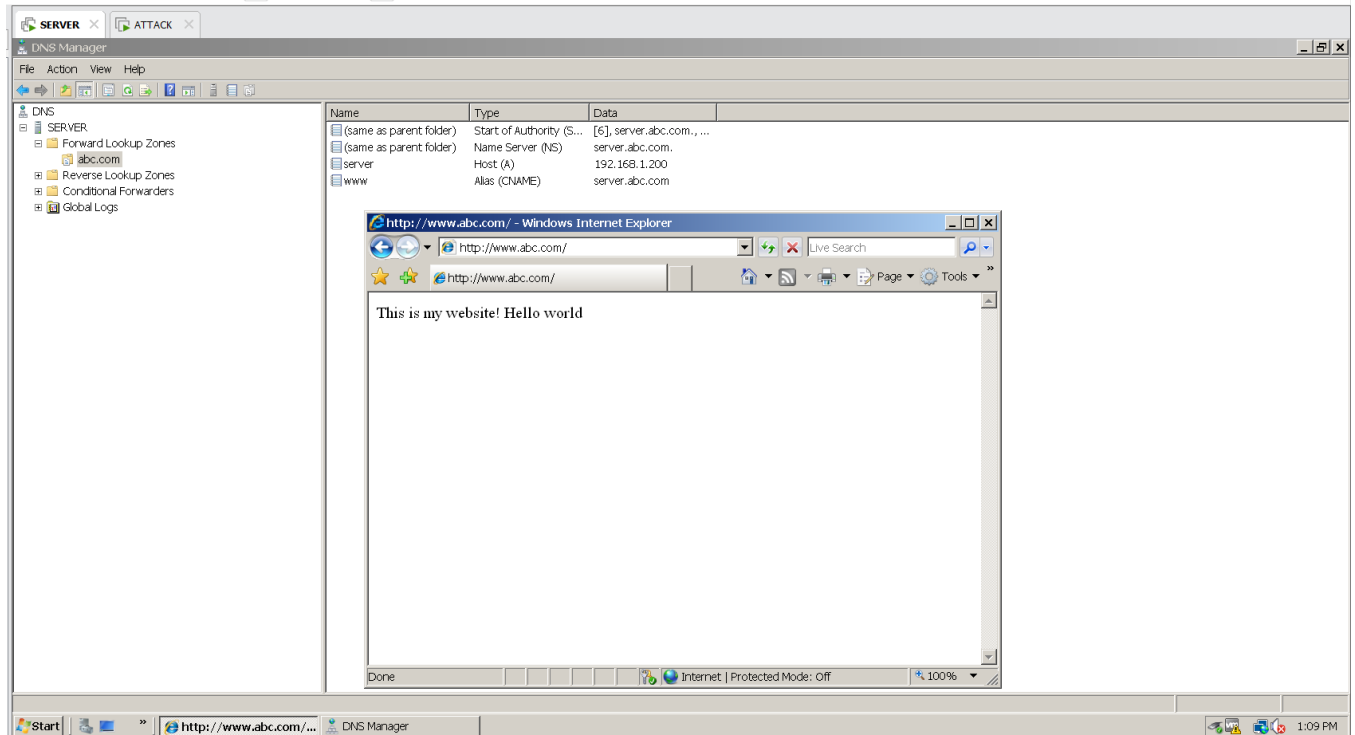
- Tiếp theo, truy cập lại <http://www.abc.com> và xem kết quả: bị chuyển sang 1 trang web khác



- Tóm lại, khi tấn công DNS thì máy VICTIM truy cập trang web www.abc.com tại máy chủ SERVER thì bị tấn công DNS - thay đổi địa chỉ DNS và làm cho SERVER trả về truy cập tại một IP khác (ở đây là 3.224.42.32 – tp-link.com).

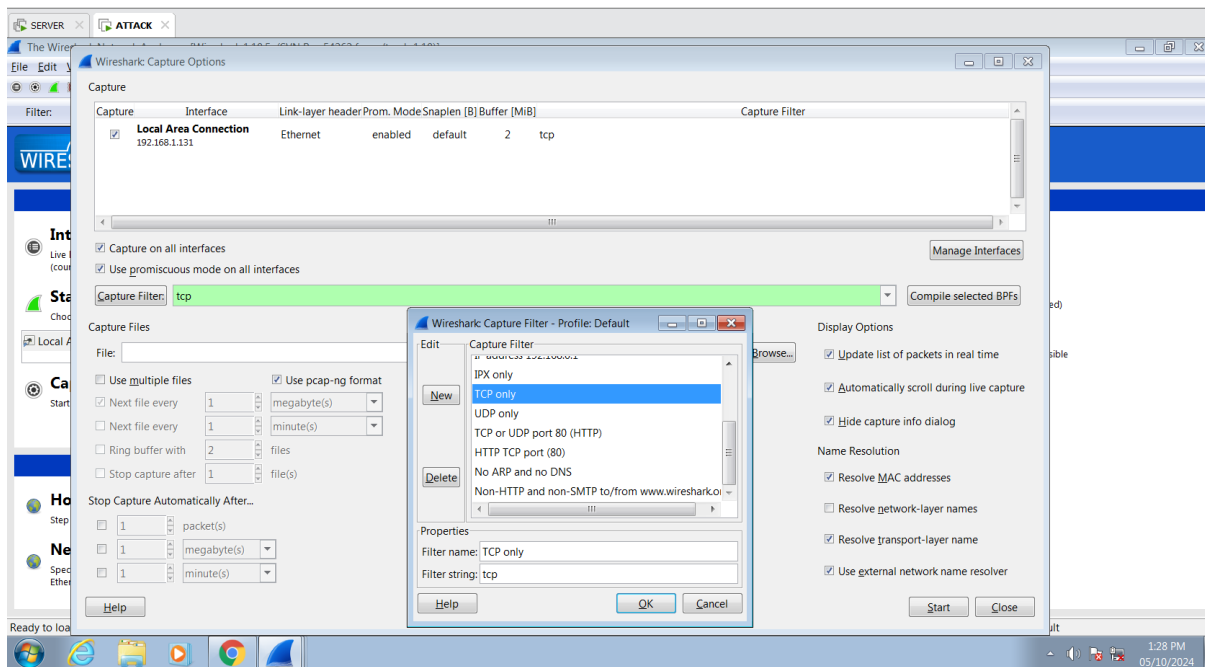
5. Mô phỏng bắt và phân tích mật khẩu gói tin truy cập Web, FTP, Telnet

Tiến hành Cài lại địa chỉ IP của máy SERVER

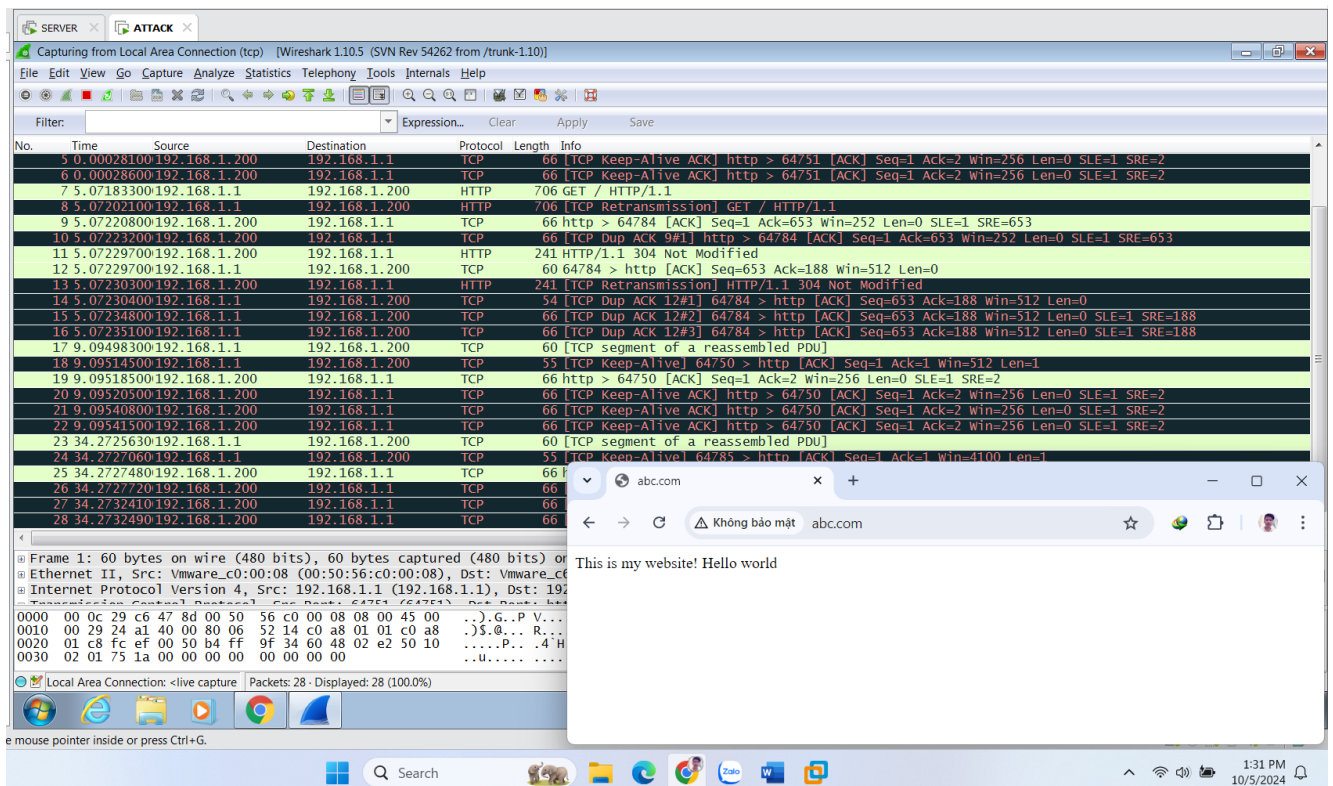


5.1. WEB

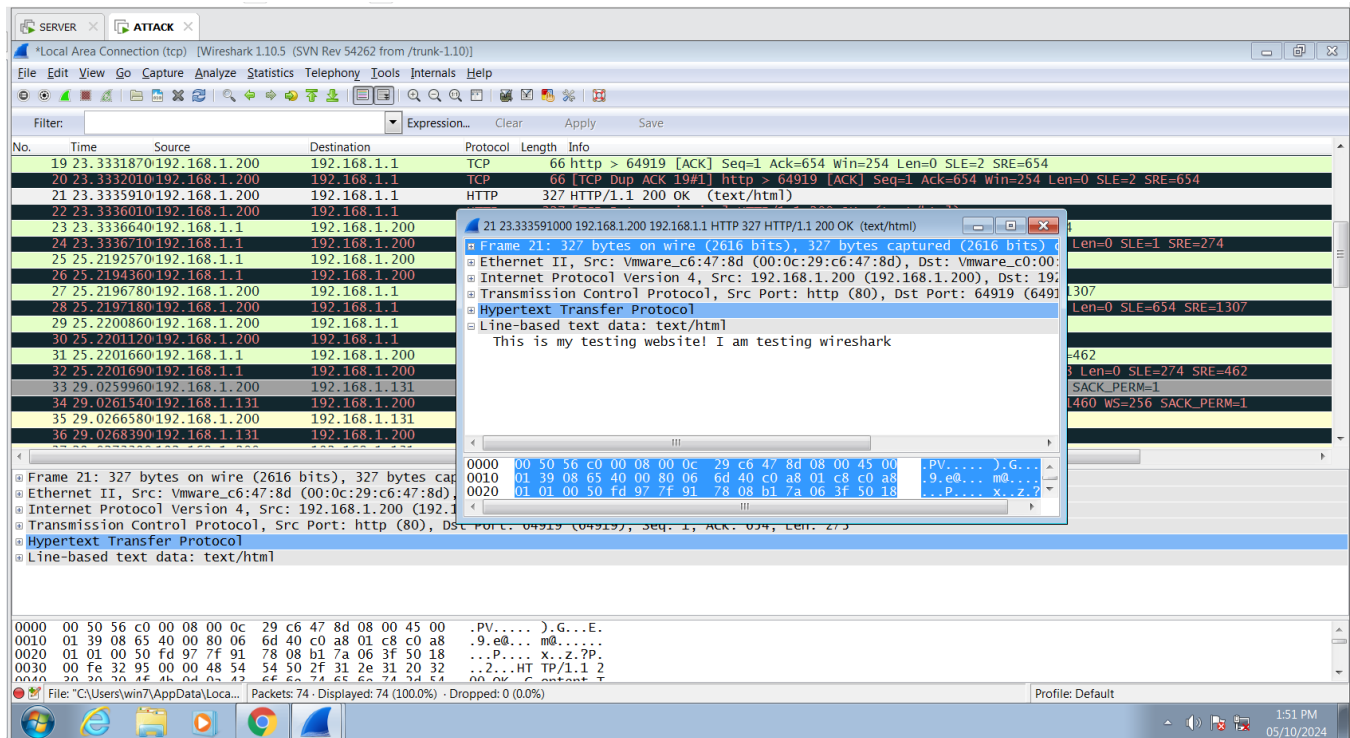
- ở máy ATTACK mở phần mềm Wireshark để bắt gói tin. Chọn Capture Option chọn bộ lọc TCP. Và nhấn Start



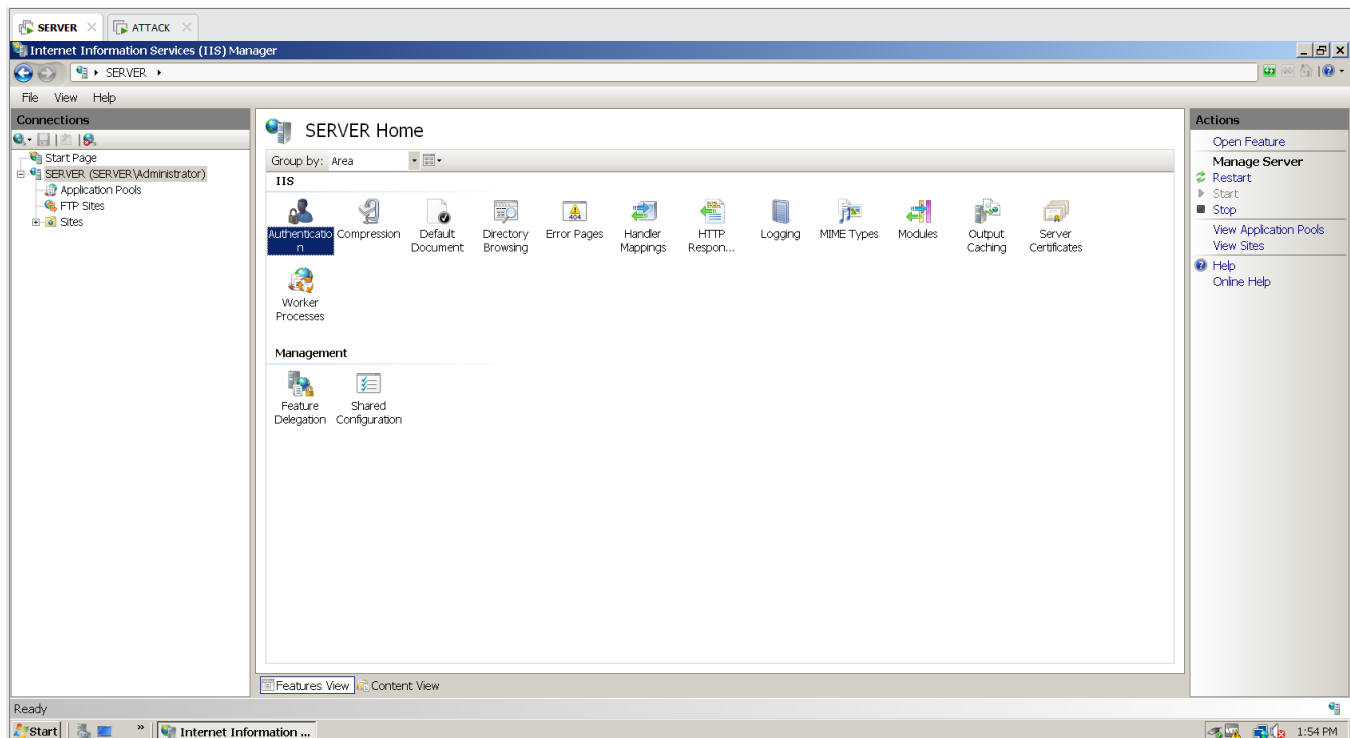
- ở máy VICTIM PC thì truy cập trang web <http://www.abc.com>. Để cho Wireshark bắt gói tin rồi sau đó nhấn stop capture



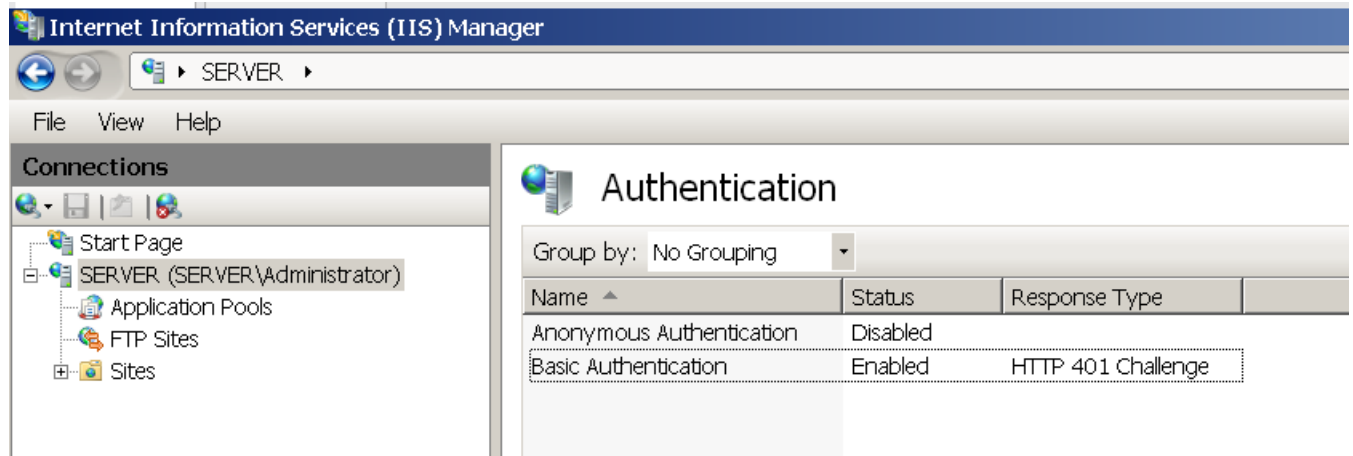
- Ở máy VICTIM khi truy cập trang web <http://www.abc.com> và truy cập tới SERVER và trả về cái dữ liệu, và ở đây có thể đọc được dữ liệu html



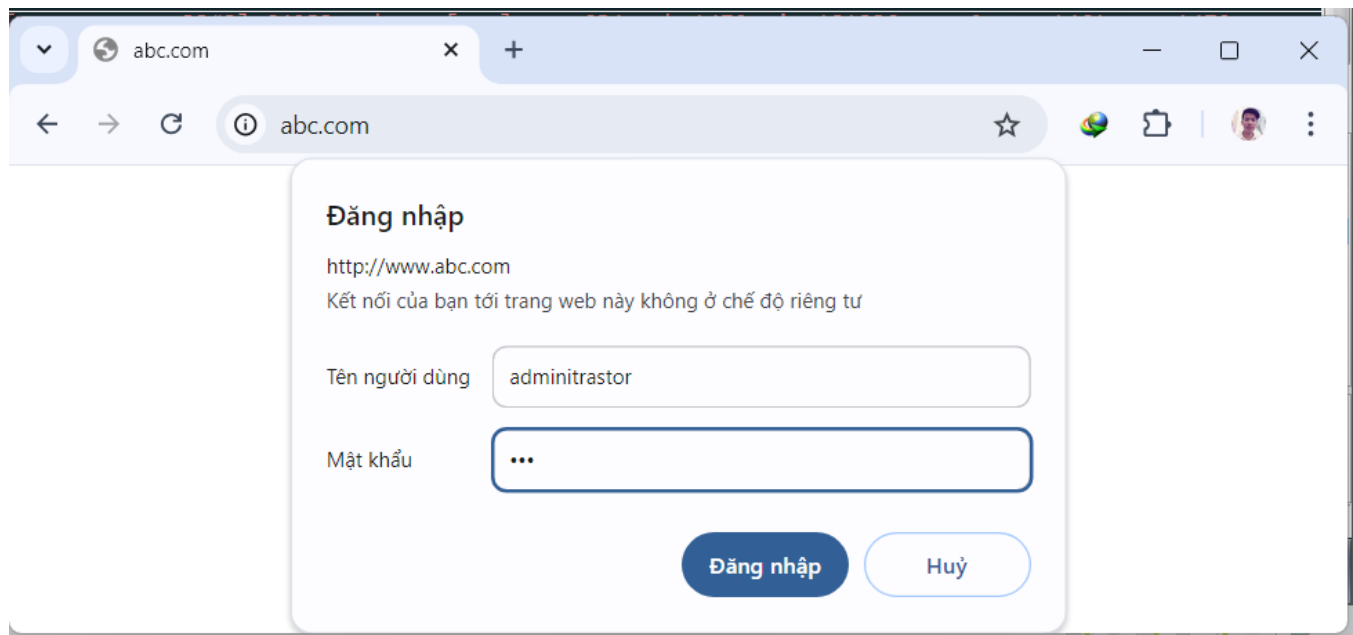
- Tiếp theo, làm nâng cấp xác thực cho trang web trên SERVER. Cấu hình trên IIS



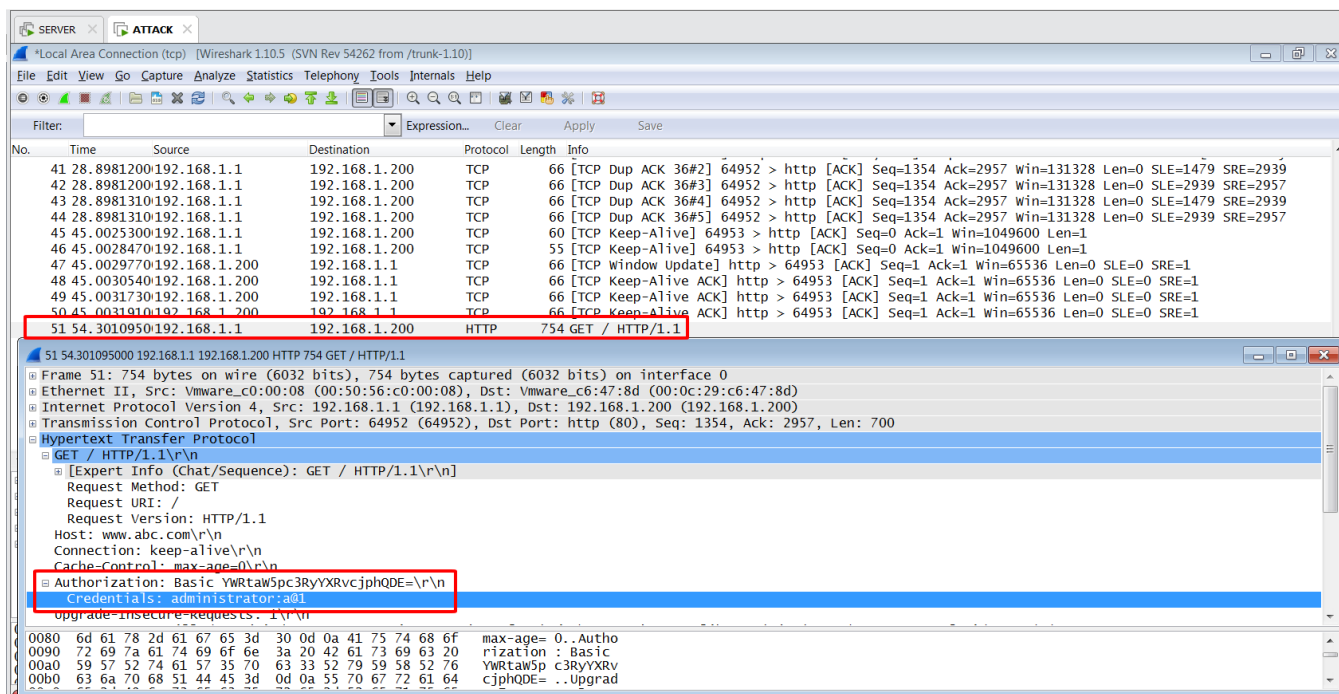
- Chọn phần Authentication, Phần Anonymous chọn Disabled và Enabled mục Basic



- Sau đó, mở lại Wireshark trên ATTACK và truy cập trang web www.abc.com trên VICTIM và nhập tài khoản mật của WIN VICTIM



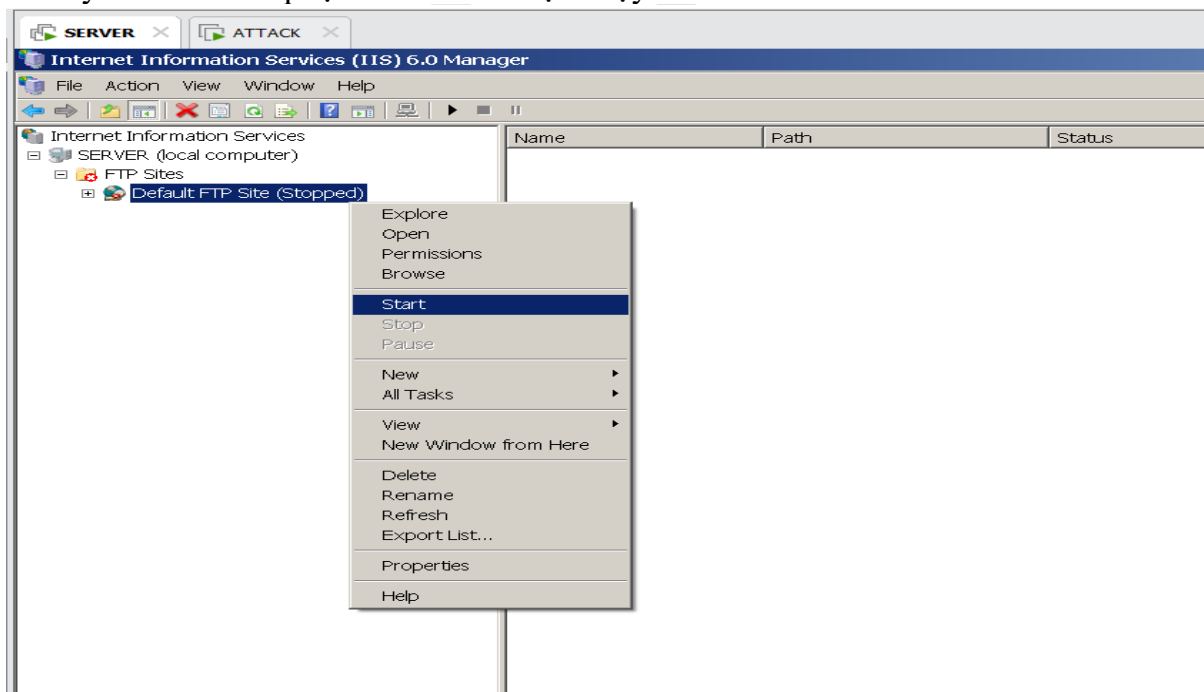
- Kiểm tra phần HTTP gửi từ VICTIM đến máy SERVER. Chúng ta đọc phần xác thực thì thấy được đoạn dữ liệu text (chứa tài khoản mật khẩu) mà VICTIM đã gửi lên cho SERVER để xác thực



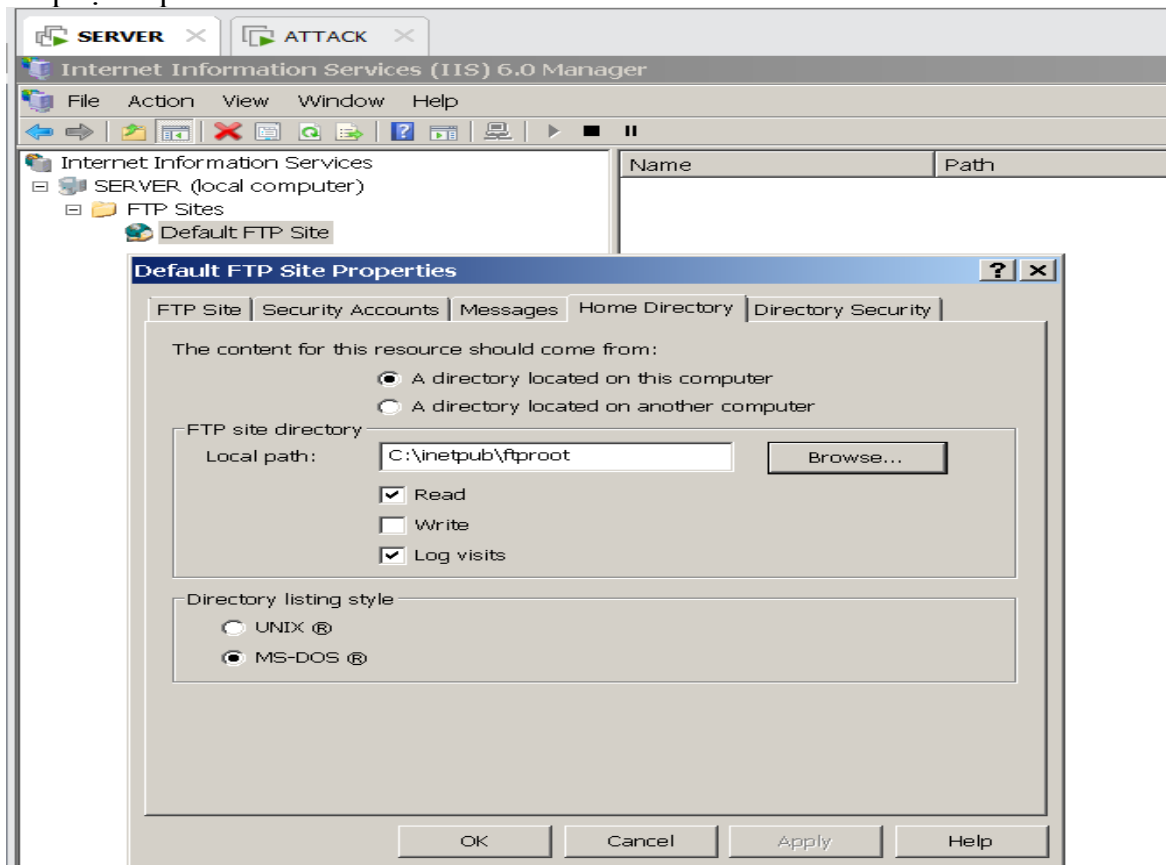
- Kết thúc phân tích mật khẩu

- 5.2. Phân tích FTP

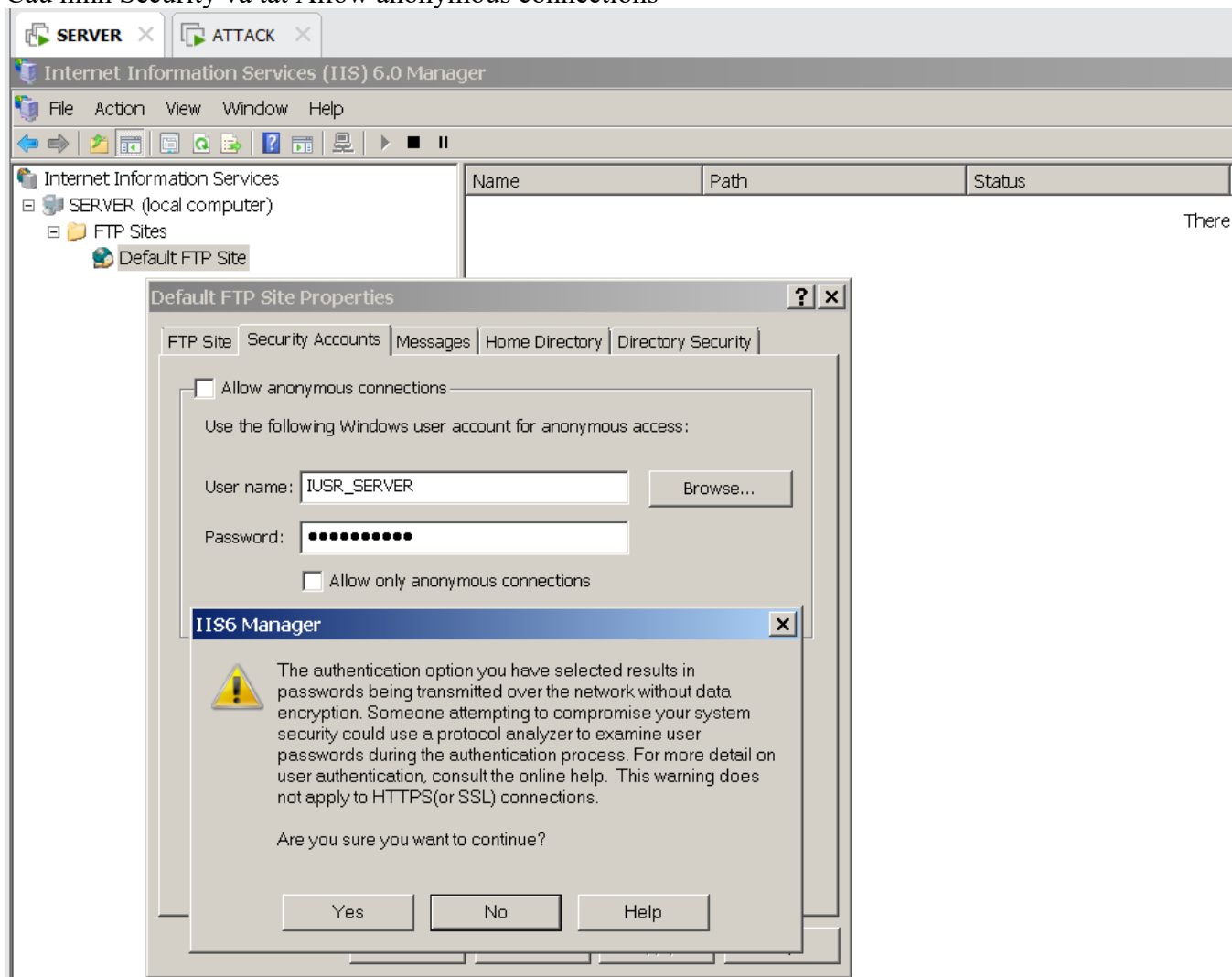
- Ở máy SERVER tiếp tục mở IIS và chọn chạy FTP sites



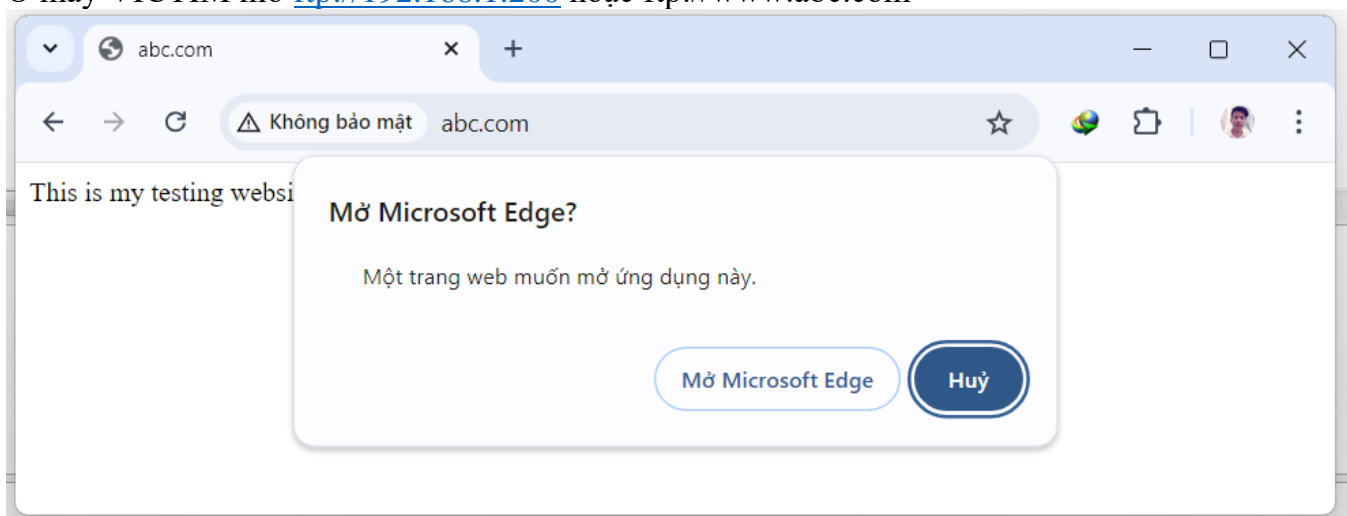
- Tiếp tục cập hình FTP

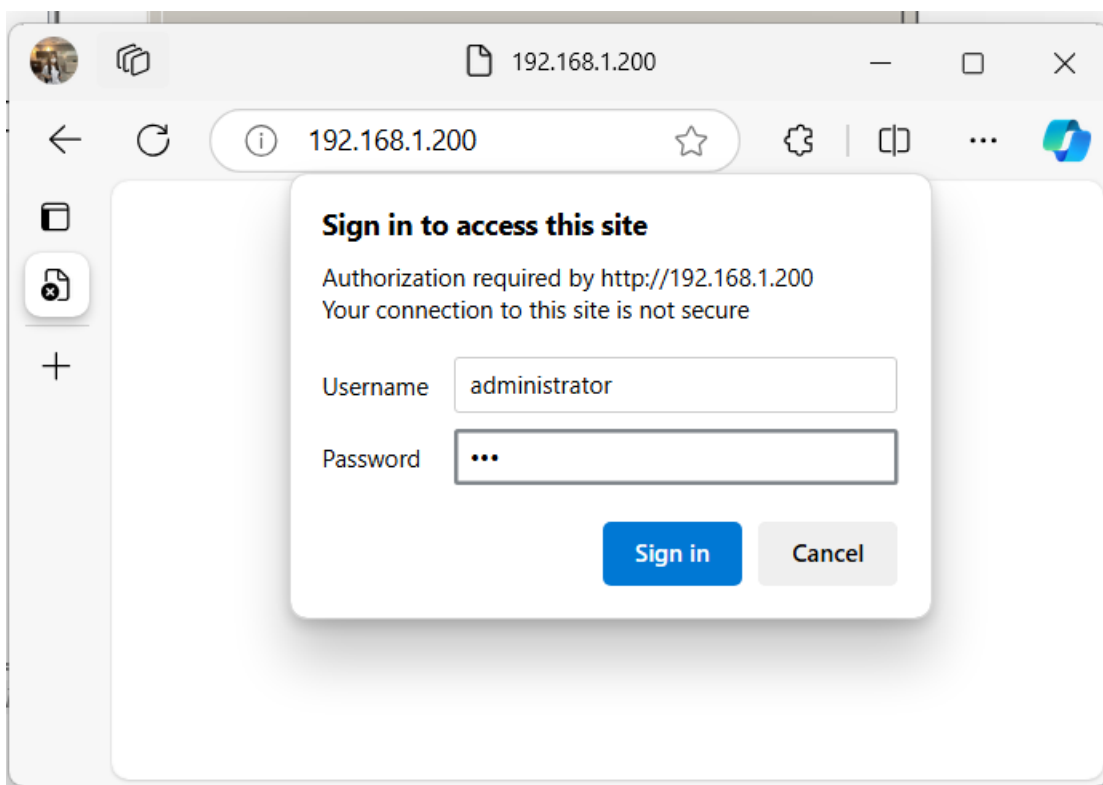


- Cấu hình Security và tắt Allow anonymous connections

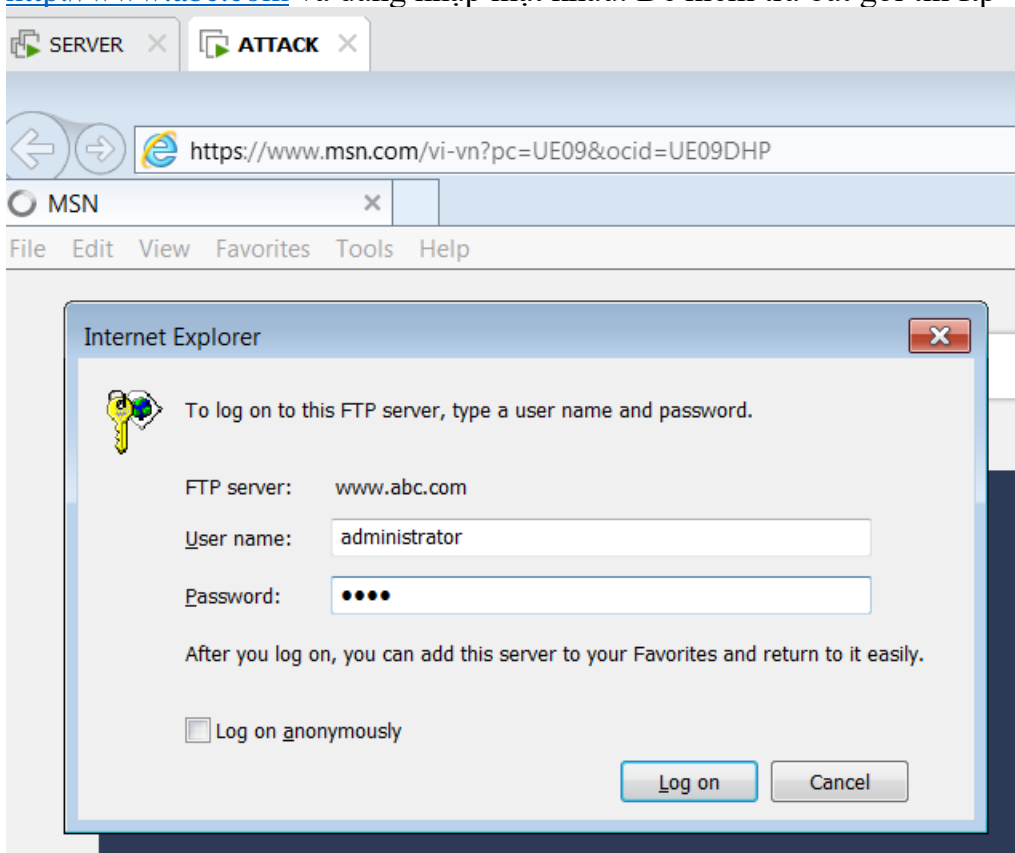


- Ở máy VICTIM mở <ftp://192.168.1.200> hoặc <ftp://www.abc.com>

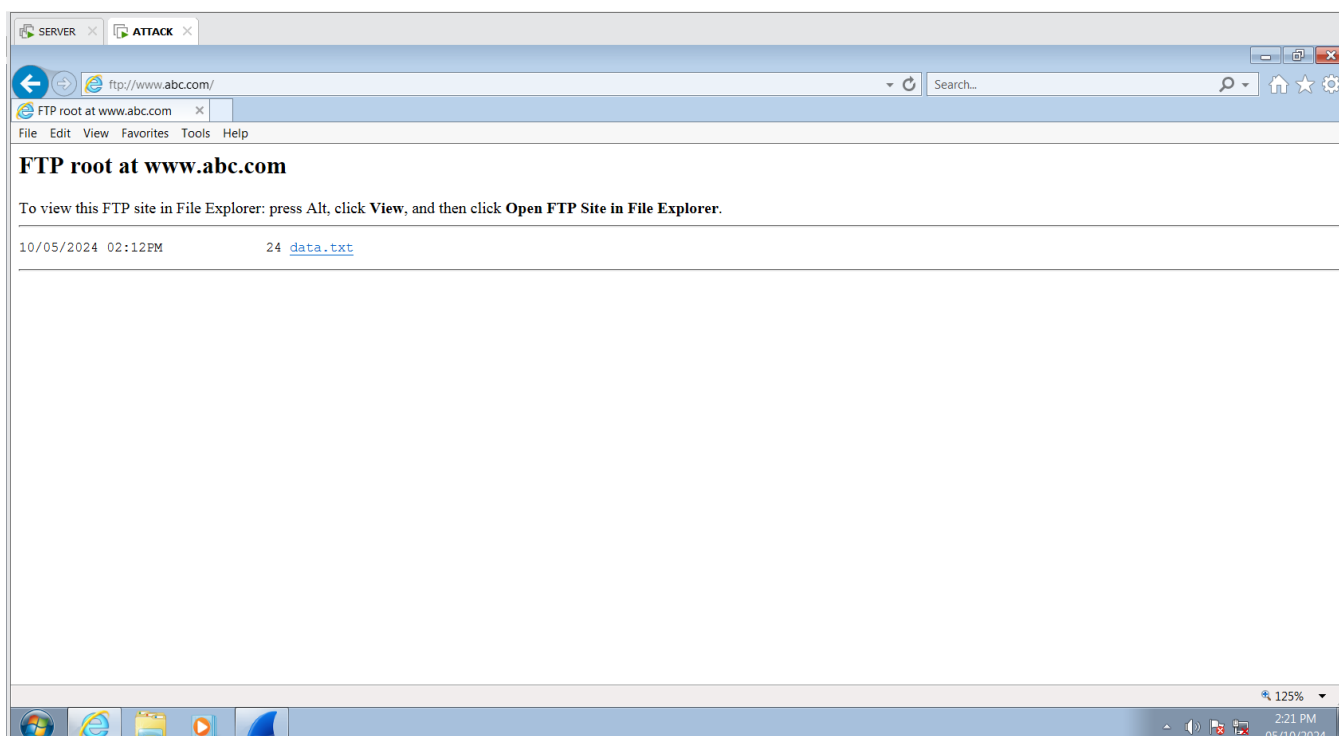




- Nếu không được thì Test trên máy ATTACK. Mở Internet Explore và truy cập <http://www.abc.com> và đăng nhập mật khẩu. Để kiểm tra bắt gói tin ftp



- Sau khi đăng nhập thành công thì sẽ được giao diện như sau

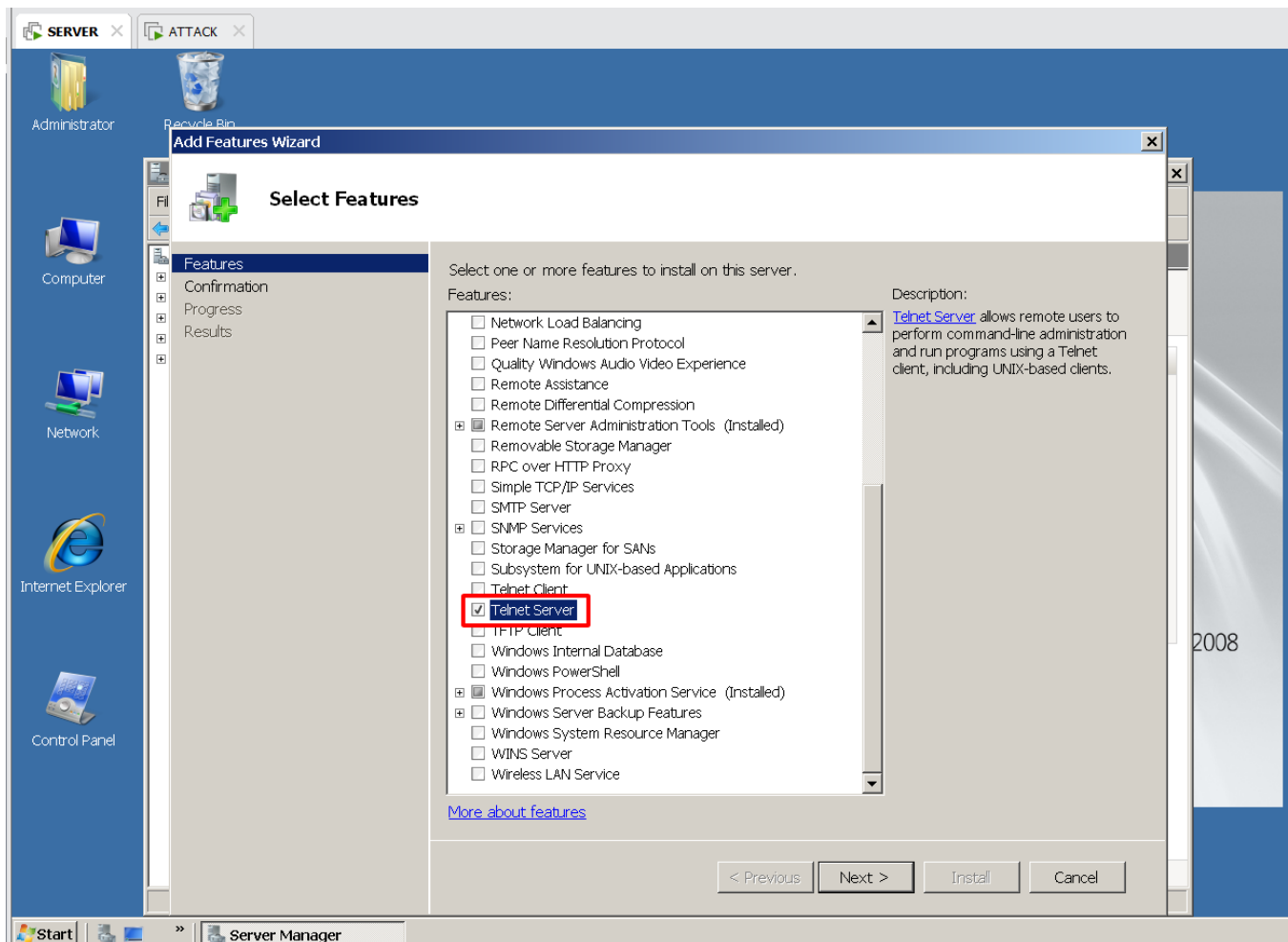


- Tìm trong wireshark và lọc ra phần ftp và thấy được username và password của tài khoản đã login

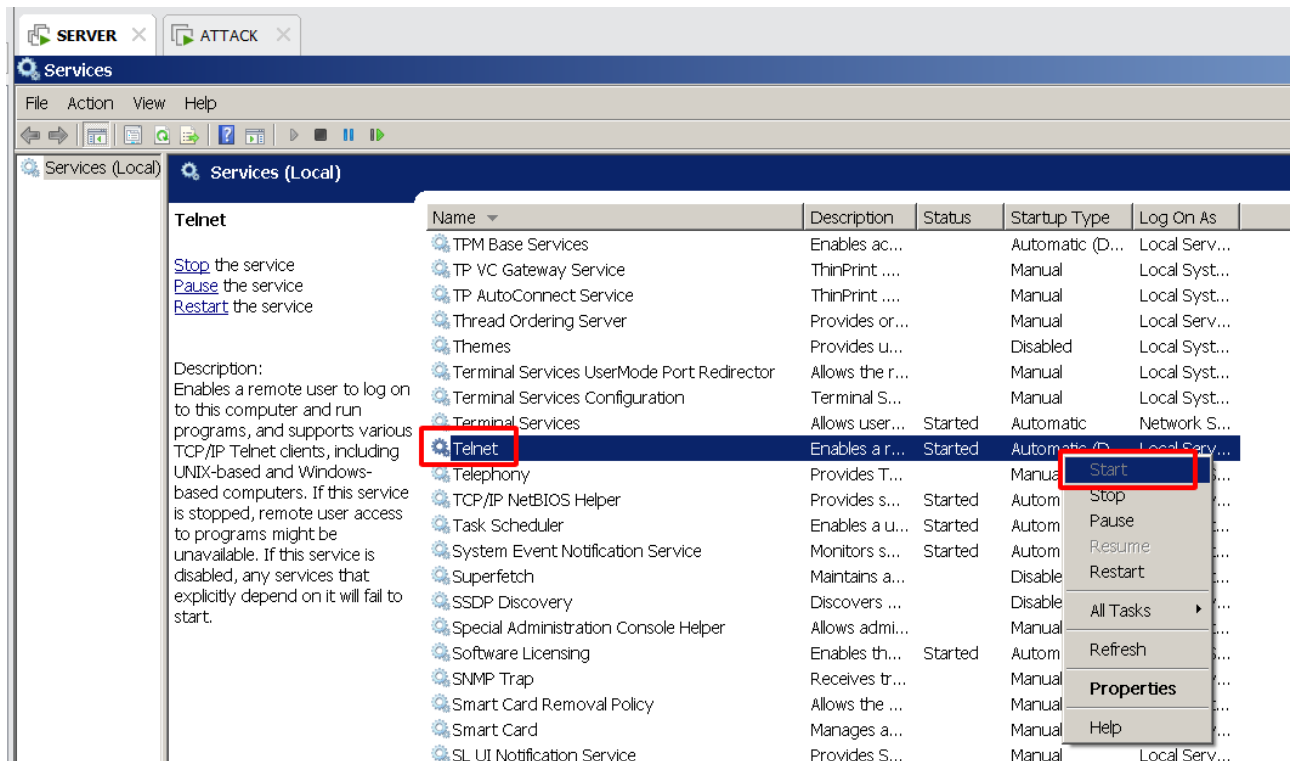
No.	Time	Source	Destination	Protocol	Length	Info
47	14.9388890	192.168.1.200	192.168.1.131	FTP	81	Response: 220 Microsoft FTP Service
49	14.9390330	192.168.1.131	192.168.1.200	FTP	74	Request: USER administrator
50	14.9391640	192.168.1.200	192.168.1.131	FTP	96	Response: 331 Password required for administrator.
52	14.9392690	192.168.1.131	192.168.1.200	FTP	64	Request: PASS a01
53	14.9411940	192.168.1.200	192.168.1.131	FTP	89	Response: 230 User administrator logged in.
55	14.9413730	192.168.1.131	192.168.1.200	FTP	61	Request: CWD /
56	14.9415390	192.168.1.200	192.168.1.131	FTP	83	Response: 250 CWD command successful.
58	14.9416900	192.168.1.131	192.168.1.200	FTP	62	Request: TYPE A
59	14.9417960	192.168.1.200	192.168.1.131	FTP	74	Response: 200 Type set to A.
61	14.9422040	192.168.1.131	192.168.1.200	FTP	60	Request: PASV
62	14.9423750	192.168.1.200	192.168.1.131	FTP	105	Response: 227 Entering Passive Mode (192,168,1,200,192,37).
67	14.9432260	192.168.1.131	192.168.1.200	FTP	60	Request: LIST
68	14.9436480	192.168.1.200	192.168.1.131	FTP	108	Response: 125 Data connection already open; Transfer starting.
75	14.9439000	192.168.1.200	192.168.1.131	FTP	78	Response: 226 Transfer complete.

5.3. Telnet - khái niệm Telnet là gì?

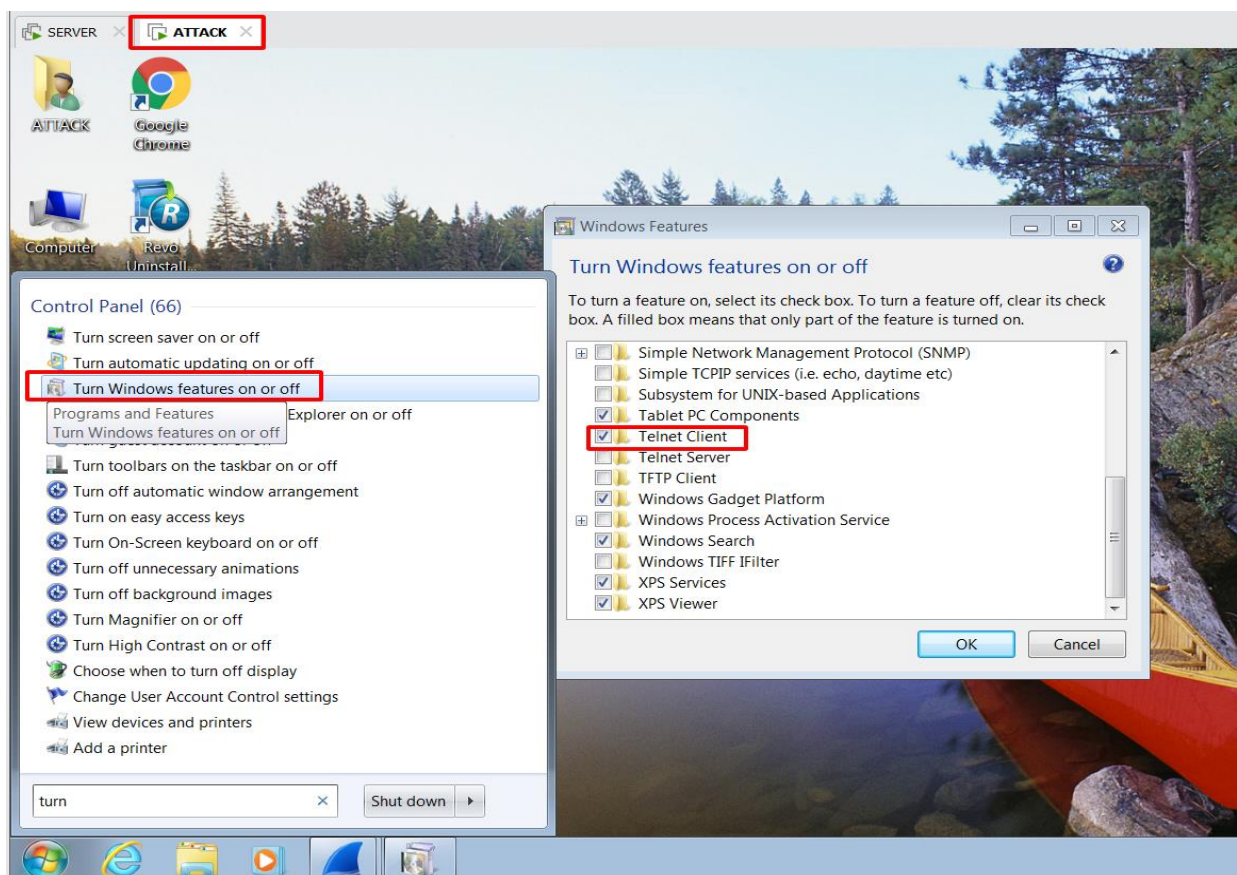
- Telnet (Terminal network) là một giao thức mạng tiêu chuẩn được sử dụng để thiết lập và quản lý kết nối từ xa giữa các máy tính.
 - Giao thức này cho phép người dùng điều khiển và truy cập vào một máy tính từ xa thông qua mạng, cung cấp khả năng gửi và nhận dữ liệu qua một kết nối TCP/IP.
 - Telnet hoạt động dựa trên cơ chế client-server, trong đó máy tính điều khiển được gọi là Telnet client và máy tính được điều khiển là Telnet server. Và khi một kết nối Telnet được thiết lập, người dùng có thể nhập lệnh và truyền dữ liệu từ máy tính client đến máy tính server.
-
- Cài đặt Telnet Server ở máy SERVER



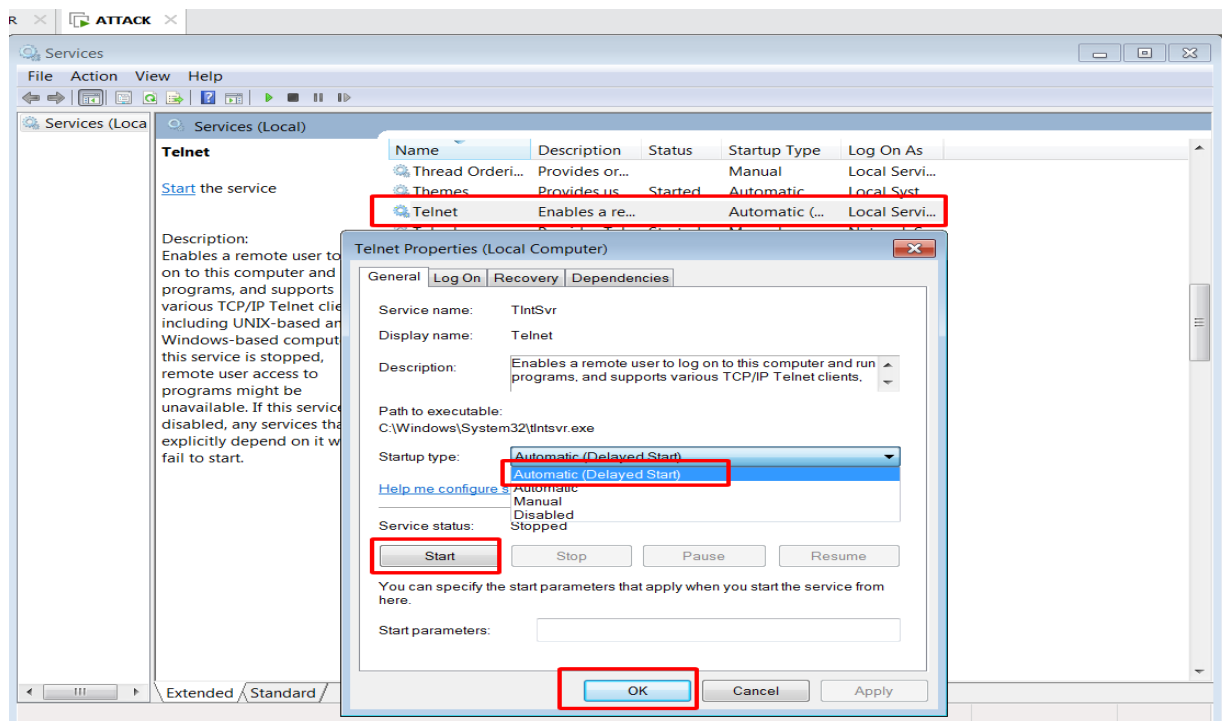
- Ở SERVER mở Service, và bật Telnet và bật automatic và start



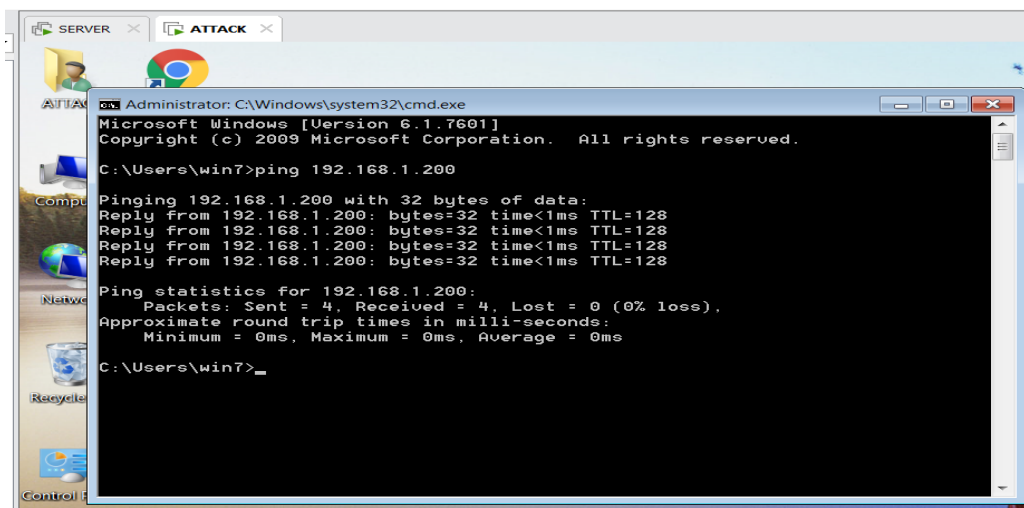
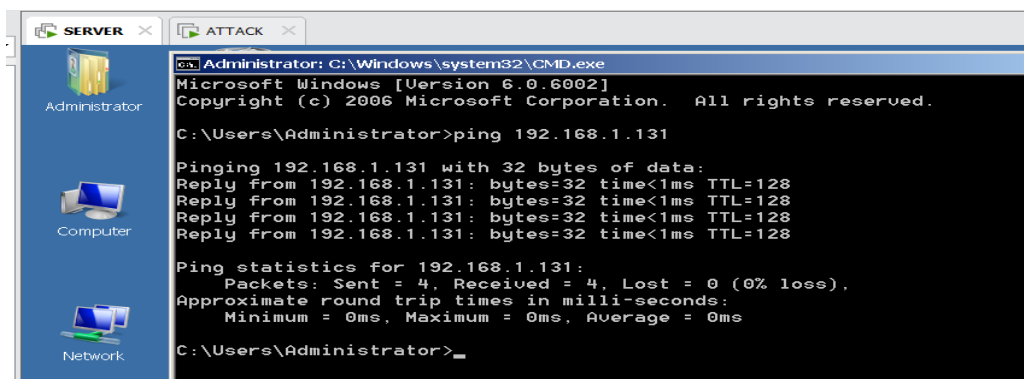
- Tương tự cài ở máy ATTACK, Telnet client



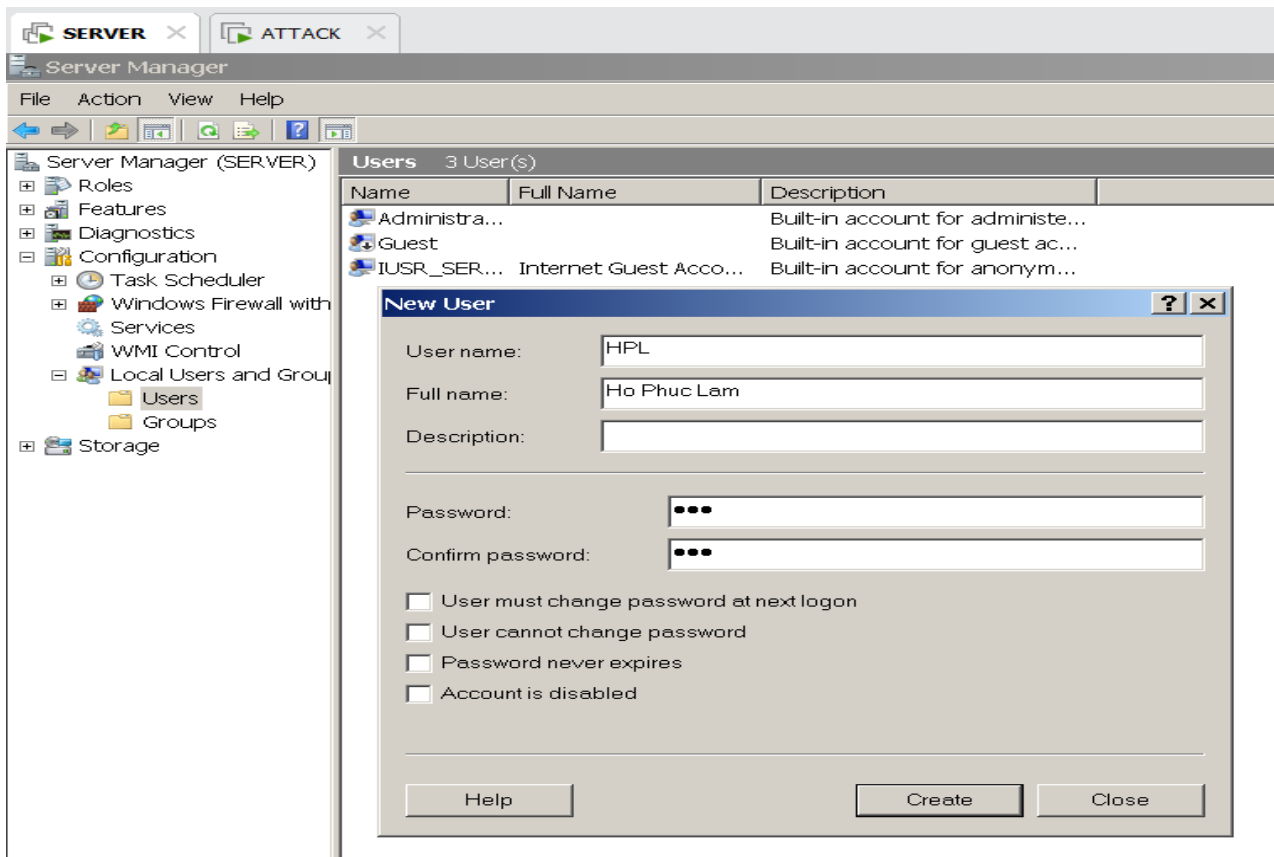
- Chạy Service ở máy ATTACK client



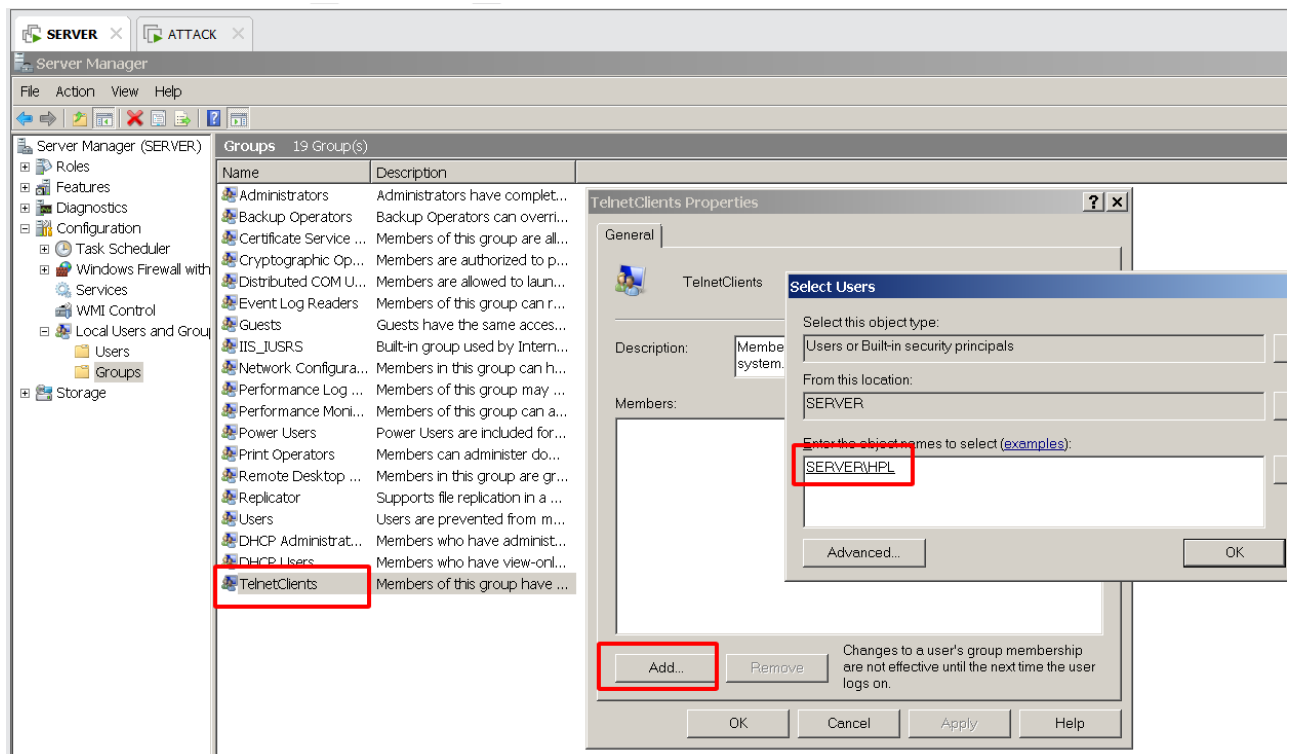
- Kiểm tra 2 máy đã ping nhau chưa



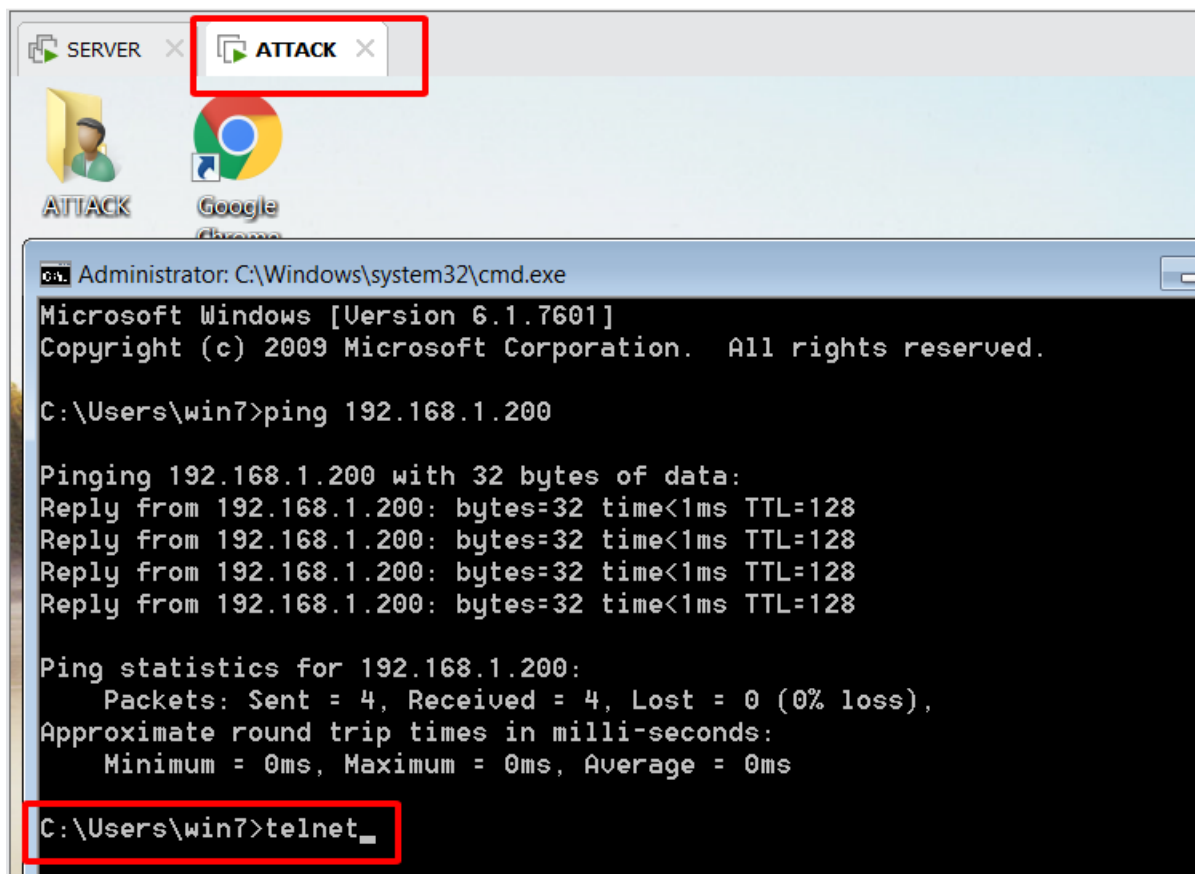
- Tạo user trên SERVER



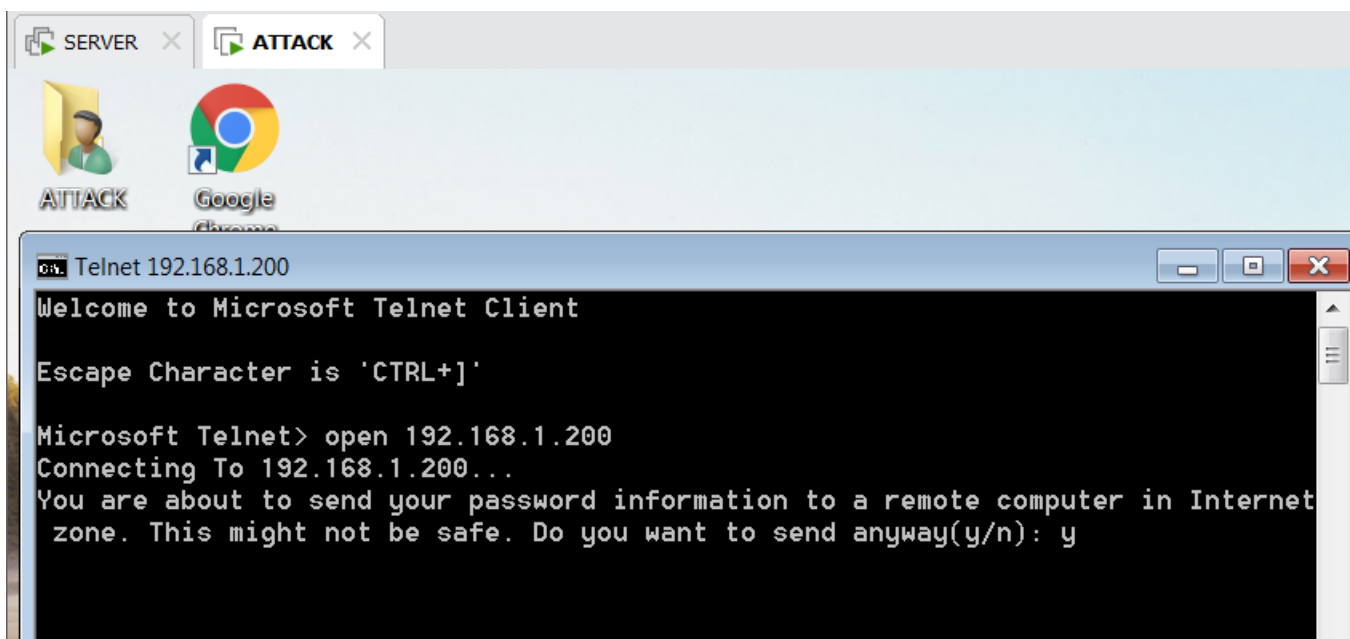
- Add user vừa tạo vào group TelnetClients



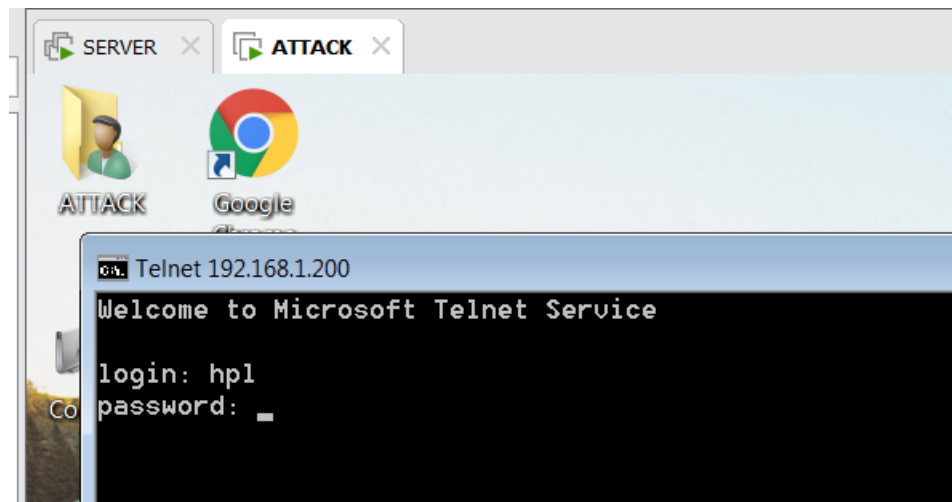
- Mở Wireshark coi các cổng proto TELNET trên máy ATTACK - client
- Ở máy client bật cmd và nhập lệnh “telnet”



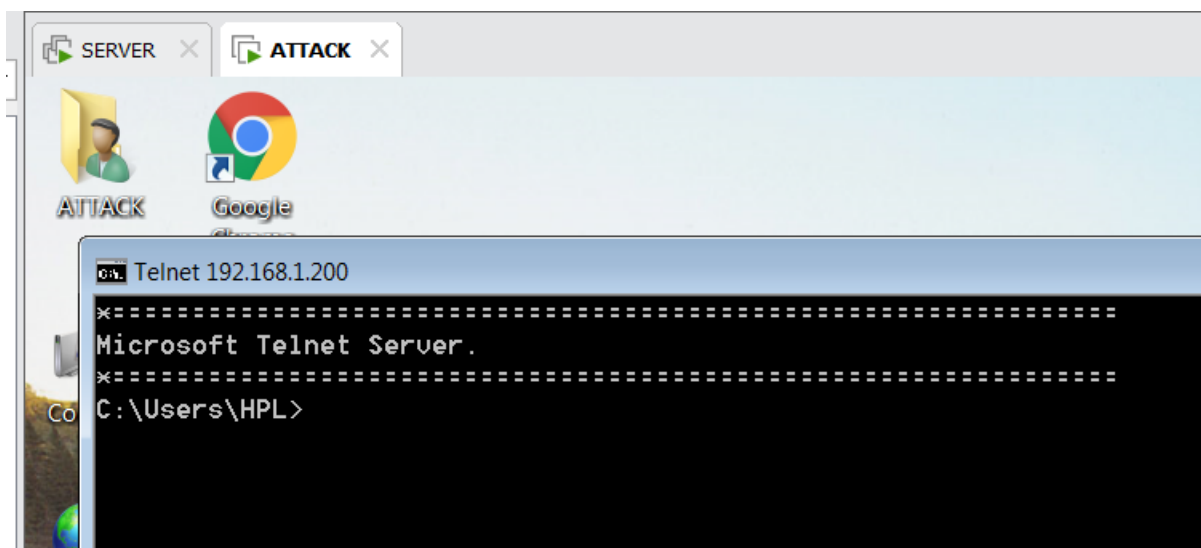
- Tiếp theo chọn open 192.168.1.200 để mở cổng port tới máy SERVER



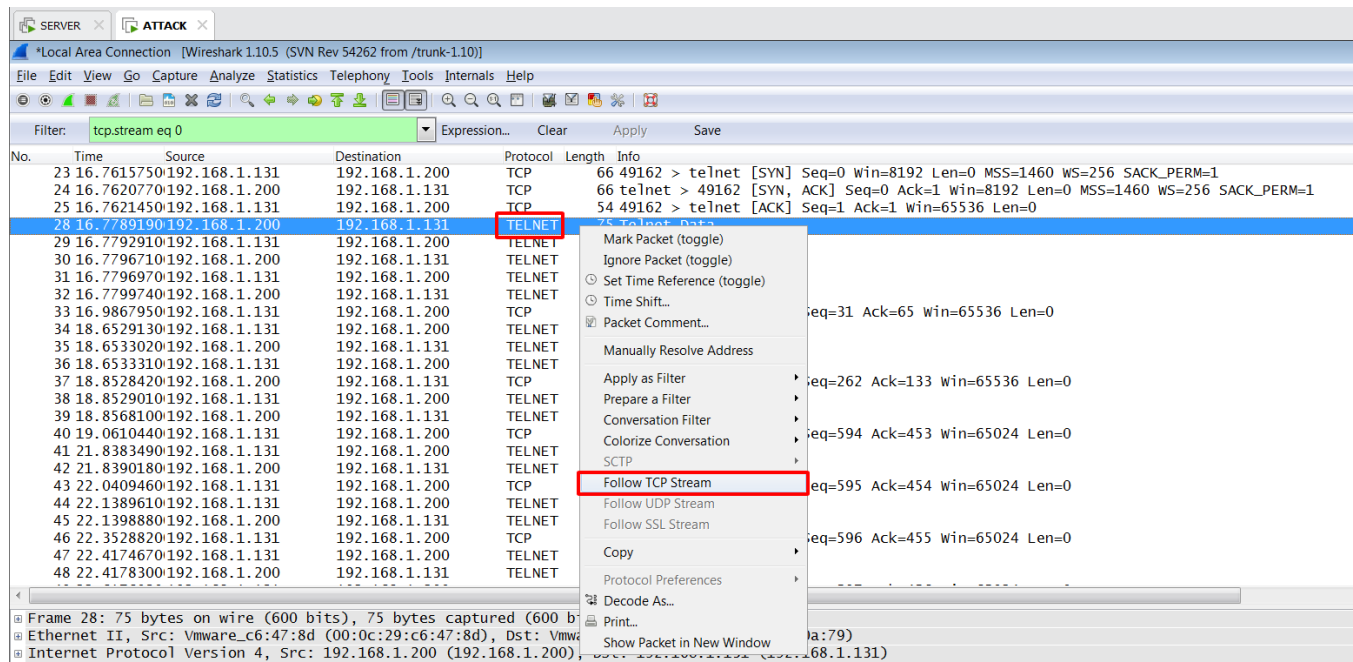
- Login với tài khoản user SERVER/HPL đã tạo trước đó và đã được thêm vào nhóm Telnet Client



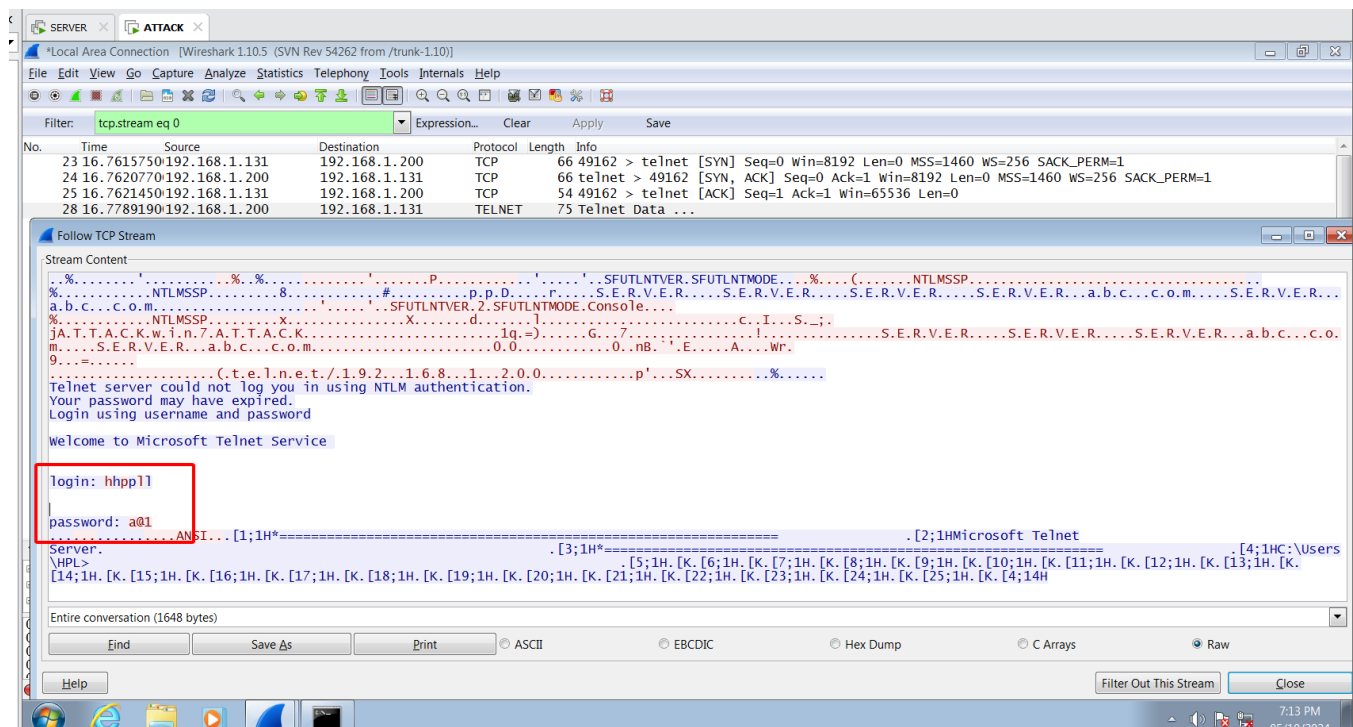
- Giao diện sau khi đăng nhập thành công



- Mở Wireshark coi các công proto TELNET và chọn follow TCP Stream



- **Kết quả:** xem được tài khoản mật khẩu của User khi đăng nhập vào Telnet do giao thức Telnet không mã hóa dữ liệu truyền đi nên dễ bị đánh cắp bởi bên thứ ba.



- Login: hpl
- Password a@1

--- Kết thúc phân tích gói tin trên telnet ---