

Khoa: Công Nghệ Thông Tin



LAB REPORT TH GK Phân tích gói tin

Student's ID:Student's name: Phúc LâmSubject: Triển khai an ninh hệ thốngInstructor: Đỗ Hà PhươngFaculty: Công Nghệ Thông TinCompleted Date: / /2024

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẫN

 ••••••
 ••••••
 ••••••

Điểm lab report:

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 -1 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 11.03963	60 192.168.10.2	192.168.10.128	ICMP	120 Destination unreachable
	15 13.55872	70 192.168.10.200	192.168.10.255	BROWSER	243 Host Announcement SERVE
	16 15.63072	00 192.168.10.128	192.168.10.255	NBNS	92 Name query NB ATTACK<1c
	17 16.37278	20 192.168.10.128	192.168.10.255	NBNS	92 Name query NB ATTACK<1c
	18 17.13759	10 192.168.10.128	192.168.10.255	NBNS	92 Name query NB ATTACK<1c
	19 46.86033	30 fe80::e002:4fa0:6e	e ff02::1:2	DHCPv6	148 Solicit XID: 0x2ef144 C
	20 46.92469	20 192.168.10.1	192.168.10.128	IPv4	1514 Fragmented IP protocol
	21 46.92469	20192.168.10.1	192.168.10.128	IPv4	1514 Fragmented IP protocol
	22 46.92469	30Dhân1thành	116 matanh	IPv4	1514 Fragmented IP protocol
	23 46.92471	20192.468.10.1	192.168.10.128	IPv4	1514 Fragmented IP protocol
	24 46.92471	20 192.168.10.1	192.168.10.128	IPv4	1514 Fragmented IP protocol
	25 46.92471	20 192.168.10.1	192.168.10.128	ICMP	642 Echo (ping) request id

Lab Report / @tailieuitiuh

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

Giải thích:

Kích thước gói ping: 8000 bytes + 8 (đầu ICMP) = 8008 Tính số Frame: 8008/1480 = 5,41 => cần 6 Frame Frame 1: 1480 + 20 (IP header) + 14 (Ethernet header) + 4 = 1518 bytes Frame 2: 1480 + 20 + 14 + 4 = 1518 bytes Frame 3: 1480 + 20 + 14 + 4 = 1518 bytes Frame 4: 1480 + 20 + 14 + 4 = 1518 bytes Frame 5: 1480 + 20 + 14 + 4 = 1518 bytes Frame 6: 8008 - (1480 * 5) = 608 bytes $\Rightarrow 608 + 20 + 14 = 642$ 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 bytes

Frame 2: 1480 + 20 + 14 = 1514 bytes

Frame 3: 966 + 20 + 14 = 1000 bytes

Tổng kích thước tất cả các Frame: 1514 +1514 +1000 = 4028 bytes

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

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

IX.		ại bàng cách bà	it got till.		
lo.	Time	Source	Destination	Protocol	Length Info
	10.00000	000 192.168.10.1	192.168.10.128	IPv4	1514 Fragmented C:\Users\COMPUTER>ping 192.168.10.128 -1 3918 -n 1
	2 0.00000	100 192.168.10.1	192.168.10.128	IPv4	1514 Fragmented
	3 0.00000	100 192.168.10.1	192.168.10.128	ICMP	1000 Echo (ping)Pinging 192.168.10.128 with 3918 bytes of data:
	4 0.00016	300 Vmware_d4:0a:79	Broadcast	ARP	42 Who has 192 Reply from 192.168.10.128: bytes=3918 time<1ms TTL=128
	5 0.00025	500 Vmware_c0:00:08	Vmware_d4:0a:79	ARP	60 192.168.10.
	6 0.00026	600 192.168.10.128	192.168.10.1	ICMP	1514 Echo (ping)Ping statistics for 192.168.10.128:
	7 0.00026	900 192.168.10.128	192.168.10.1	IPv4	1514 Fragmented Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
	8 0.00027	100 192.168.10.128	192.168.10.1	IPv4	1000 Fragmented Approximate round trip times in milli-seconds:
	9 4.80720	000 ⁽ Vmware_c0:00:08	Vmware_d4:0a:79	ARP	60 Who has 192 Minimum = Oms, Maximum = Oms, Average = Oms
	10 4.80722	100 Vmware_d4:0a:79	Vmware_c0:00:08	ARP	42 192.168.10.
	11 11.5071	370 192.168.10.128	192.168.10.255	BROWSE	R 243 Local MasteC:\Users\COMPUTER>

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



a. Tấn công ARP

Kiểm tra lại bằng cách bắt gói tin.

- Kẻ tấn công ngồi ở PC4 và tấn công PC1, khi pc1 gửi arp ra tới pc5 mà pc4 đã gửi ARP rely 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 cấp 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:

- 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.
- 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-inthe-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:

- 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	v victim	
C:\Users\COMPUTER>arp -	a	
Interface: 192.168.254.1	1 0x4	
Internet Address	Physical Address	Туре
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	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	Туре
192.168.1.1	60-38-e0-a9-b2-3c	dynamic
192.168.1.255	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-7t-tt-ta	static
255.255.255.255	++-++-++-++-++	static
Interface, 102 160 10 1	Out	
Interface. 192.108.10.1	Physical Address	Tuno
102 168 10 128	00-0c-20-d4-0a-70	dynamic
192.168.10.200	00-0c-29-c6-47-8d	dynamic
192.168.10.255	++-++-++-++	static
224.0.0.2 Ser	VCF5e-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 adminitrator 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



- 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.



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
 Ping statistics for 192.168.10.200:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
     Minimum = Oms, Maximum = Oms, Average = Oms
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 ACTTACK 192.168.10.128 đã bắt được gói tin và chuyển tiếp gói tin.

<u>F</u> ile <u>E</u> dit <u>V</u> iew V <u>M</u> <u>T</u> abs <u>H</u> elp ↓ → ⊕				
🕞 ATTACK 🗙 🕞 SERVER 🛛				
Capturing from Local Area Connection [Wireshark 1.10.	0.5 (SVN Rev 54262 from /trunk-1.10)]			×
File Edit View Go Canture Analyze Statistics Telen	phony Tools Internals Help			
Ene gan yew go gaptare Branyze gatastics herep	phony Tools Internals Help	n de l Ca		
		18 % I		
Filter	 Expression Clear 	Apply Save		
No. Time Source Dest	tination Protocol Le	nath Info		
1 0.00000000 192.168.10.1 192	2.168.10.200 IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=), ID=2ad2) [Reassembled in #6]	
2 0.00000100 192.168.10.1 192	2.168.10.200 IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1	480, ID=2ad2) [Reassembled in #6]	
3 0.00000100(192.168.10.1 192	2.168.10.200 IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=2	960, ID=2ad2) [Reassembled in #6]	
4 0.00001400(192.168.10.1 192	2.168.10.200 IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=4	440, ID=2ad2) [Reassembled in #6]	
5 0.00001500(192.168.10.1 192	2.168.10.200 IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=	920, ID=2ad2) [Reassembled in #6]	
6 0.00001500(192.168.10.1 192	2.168.10.200 ICMP	642 Echo (ping) request id=0x0001, seq=2617/14	1602, tt]=128	
7 0.00013400\Vmware_d4:0a:79 Bro	oadcast ARP	42 Who has 192.168.10.1? Tell 192.168.10.128		
8 0.00020700\Vmware_d4:0a:79 Bro	oadcast ARP	42 Who has 192.168.10.200? Tell 192.168.10.12	8	
9 0.00024300\Vmware_c0:00:08 Vmw	ware_d4:0a:79 ARP	60 192.168.10.1 is at 00:50:56:c0:00:08		
10 0.00025400 192.168.10.128 192	2.168.10.1 ICMP	1514 Redirect (Redirect for network)		
11 0.00025800 192.168.10.128 192	2.168.10.1 IPv4	62 Fragmented IP protocol (proto=ICMP 1, off=)	480, ID=3408)	
12 0.00034400/Vmware_c6:47:8d Vmw	ware_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	2.168.10.200 IPv4	642 Fragmented IP protocol (proto=ICMP 1, off=)	400, ID=2ad2)	
14 2.79555600 fe80::e002:4fa0:6ee ff0	02::1:2 DHCPv6	148 Solicit XID: 0xa13730 CID: 000100012e8aa842	2000c29d40a79	
15 5.11298600\Vmware_c6:47:8d Bro	oadcast ARP	60 Who has 192.168.10.2? Tell 192.168.10.200		
16 5.11306000\Vmware_e7:66:be Vmw	ware_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	5.251.194.224 DNS	74 Standard query 0x388f SOA SERVER.abc.com		
18 5.11324000 192.168.10.128 192	2.168.10.200 ICMP	102 Redirect (Redirect for network)		
19 5.11341500 Vmware_d4:0a:79 Bro	oadcast ARP	42 Who has 192.168.10.2? Tell 192.168.10.128		
20 5.11360900\Vmware_e7:66:be Vmw	ware_d4:0a:79 ARP	60 192.168.10.2 is at 00:50:56:e7:66:be	Administrator: Windows Powe × + v	
21 5.11361600(192.168.10.200 205	5.251.194.224 DNS	74 Standard query 0x388f SOA SERVER.abc.com		
22 5.16211600 205.251.194.224 192	2.168.10.200 DNS	152 Standard query response 0x388f No such name	PS C:\Users\COMPUTER> ping 192.168.10.200 -l 8000 -n 1	
23 5.16211/00/205.251.194.224 192	2.168.10.200 DNS	152 Standard query response 0x388f No such name		
24 5.16219000/205.251.194.224 192	2.168.10.200 DNS	152 Standard query response 0x388f No such name	Pinging 192.168.10.200 with 8000 bytes of data:	
<		III	Request timed out	
B Frame 1: 1514 bytes on wire (12112 bit	s), 1514 bytes captured (1	L2112 bits) on interface 0	Request ermed out.	
B Ethernet II, Src: Vmware_c0:00:08 (00:	50:56:c0:00:08), Dst: Vmwa	are_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)	Ping statistics for 192.108.10.200:	
- Data (1400 butac)	00 00 00 45 00 >> 0		Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),	
10000 00 0C 29 d4 0a 79 00 50 56 C0 00	08 08 00 45 00)y.P	VE.	PS C:\Users\COMPUTER>	
0020 0a c8 08 00 e1 bb 00 01 0a 39 61	62 63 64 65 66	.9abcdef		
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71	72 73 74 75 76 ghijklmn	opgrstuv		
● M Local Area Connection: live captur Packets: 102 · D	Displayed: 102 (100.0%)	a ta da a	Profile: Default	
📀 🦾 📜 💽 🚺			∽ ilo R ₂ 1 29/09/2	PM 2024
To direct input to this VM, move the mouse pointer inside or	press Ctrl+G.		📮 🛇 🔂 🖶 🦛 🎯	
			405 DA	4
		Q Search 🧮 📮 💽 🔮 🙋	🔊 🕒 🛀 💹 🔷 🖓 🆢 40.0 PM	4

- n ×

4.2. Mô phỏng tấn công DHCP

Máy SERVER cấp IP cho máy VICTIM có Option Defalt 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

🕞 ATTACK × 🕼 SERVER ×		
Administrator		
ФОНСР		
File Action View Help		
	DHCP	
E server.abc.com	Contents of DHCP	Status
Server Options	server.abc.com	
^E New Scope Wizard		
Scope Name You have to prov providing a descri	ide an identifying scope name. You also have the op ption.	ption of
Type a name and how the scope is	description for this scope. This information helps yo to be used on your network.	u quickly identify
Name:	192.168.10.100	
Description:		

 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

Ф DHCP		_O×
File Action View Help		
🗢 🔿 📅 🗈 🔽 🖬 🗆	1	
Р рнср	DHCP	
E Prv4	Contents of DHCP Status	
New Scope Wizard		
IP Address Range You define the scope addresses.	address range by identifying a set of consecutive IP	
Enter the range of add	resses that the scope distributes.	
Start IP address:	192.168.10.100	
End IP address:	192.168.10.150	
A subnet mask define IDs and how many bit length or as an IP add	how many bits of an IP address to use for the network/subnet to use for the host ID. You can specify the subnet mask by ess.	
Length:	24	
Subnet mask:	255 . 255 . 255 . 0	
Pequete		
Recycle	< Back Next > Cancel	

Lab Report / @tailieuitiuh

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



	, , ,
-	Tiếp theo là cấu hình DNS là địa chỉ 192.168.10.200

Ф DHCP			
File Action View Help			
🗢 🔿 🔰 📷 🛛 🕰 🖬 🛛	چې		
PHCP S	cope Options		
E server.abc.com	ption Name	V	/endor
🖃 🧰 Scope [192.168.10.0] 1	003 Router	5	Standard
Address Pool			
Address Leases Reservations			
Scope Options			
Scope Options			<u>? ×</u>
General Advanced			
			1
Available Options		D	escription 🔺
		A	vray of time
✓ 005 Name Servers		A	vray of rout
U 007 Log Servers		A	may of MIT 🚽
•			
Data entry			
Server name:			
		F	Resolve
IP address:			
Recycle Bin 192 . 168 . 10 . 2	00 Add	1	
	Remove	1	
		-	
	Up		
	Down		
oxit Reader			
	ОК	Cancel	Apply

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 trỏ 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 thông qua máy ATTACK mới truy cập ra internet bên phải ngoài



4.3. Mô phỏng tấn công DNSCài đặt role DNS

_ _

Cấu hình và tạo ra miền Zone: abc.com _

t 🛔 DNS Manager		_ 🗆 ×
File Action View Help		
SERVER Global Logs Forward Lookup Zones Reverse Lookup Zones Conditional Forwarders	Add a New Zone w Zone Wizard Cone Name What is the name of the new zone? The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com). The zone name is not the name of the DNS server. Zone name: abc.com	
	< Back Next > Cancel	
St DNS Manager File Action View Help DNS DNS SERVER Global Logs DNS Events Forward Lookup Z abc.com Conditional Forwar Conditional Forwar	Name Type D New Host × Name (uses parent domain name if blank): server Fully qualified domain name (FQDN): server.abc.com. IP address: 192.168.10.200 Create associated pointer (PTR) record Add Host Cancel	ata :: si /ei

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

a Dis Hanager					
Hie Action view Help	1 mm				
B DNS	Name	Туре	Data		
 SERVER Global Logs DNS Events Porward Lookup Zones Reverse Lookup Zones Conditional Forwarders 	Image: Construct of the second server Alias (CNAME) Alias (CNAME) Alias (CNAME) Alias name (uses parent domain i www Fully qualified domain name (FQD) www.abc.com. Fully qualified domain name (FQD)	Start of Authority (SOA) Name Server (NS) Host (A) fleft blank): N) for target host:	[1], server.abc.com., hostm server.abc.com. 192.168.10.200 Browse Look in: Records: Name server. Selection: Record types:	abc.com Type Host (A)	Data Timestamp 192. 168. 10 Iases (A and CNAME Records)
Bin					OK Cancel
7		ок	Cancel		

-

Cấu hình trang web, thiết lập trang Defalt



ao trang htm					U
	Name 🔺	▼ Date modified ▼	Туре	▼ Size ▼	Tags
	Default.html.txt	9/29/2024 4:50 PM	Text Document	1 KB	
	🕖 iisstart.htm	9/29/2024 1:50 PM	HTML Document	1 KB	
	Nelcome.png	9/29/2024 1:50 PM	PNG Image	181 KB	
Default.html.txt - Notep	ad				
File Edit Format View He	lp				
This is my website!	Hello world				
		Tao tyt y	và đổi t	hành l	ntm
			va uur t		IUI

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



:)

Tiếp tục, cấu hình địa chỉ DNS, cấu hình card Vmnet 8 SERV **⊡** າ -Eile Edit View VM Iabs Help 📙 - 🖧 😳 🕰 🚇 🔲 🗖 🗗 💽 🖉 -File Insert Draw De Lavout References Mail Q Tell n 🕞 ATTACK 🛛 💦 SERVER Times New Roman i≡ • i≡ • ¹5₁ • € → **A** Q Server Taget B I U v alas X₂ X² 🏘 = = = = 📰 🐲 -Styles Editing tt × ork and Sharing Ce Add-ins 🔄 Network Connection ⇐ C Search Network Connections 🔎 h .htm Computer 👔 Recycl VMnet8 Status ange settings of this connection 8: • 🔳 🕜 00 Organize 🔻 Disable this network device Diagnose this c VMnet8 Propertie General Ethern VMware Network Adapter VMnet1 Bluetooth Network Connection Networking Sharing 🕘 Organi Connec Network Network Internet Explorer Control Panel Recycle Bin Not con Netwo × * Trang 21 × IPv4 Con Bluetooth Device (Personal Area .. Killer E Co Favorite Lir IPv6 Con Internet Protocol Version 4 (TCP/IPv4) Properties × Wi-Fi Docume Pictures Media St Wifi-H62-5GHz Wifti-H62-5GHz Killer(R) Wi-Fi 6 AX1650i 160MHz ... General Duration Music More Speed: You can get IP settings assigned automatically if your network supp this capability. Otherwise, you need to ask your network administra for the appropriate IP settings. Th 6 Detai Folders E Des Obtain an IP address automatically Ad Activity O Use the following IP address: Pul Pul R Co Co IP address: 192 . 168 . 10 . 1 Subnet mask: 255 . 255 . 255 . 0 Bytes: Default gateway: @ % -- **(** 🐤 Proper ain DNS server address automatically Oht O Use the following DNS server addresses: Preferred DNS server: Alternate DNS server: 2 Validate settings upon exi Advanced... 1 item selected 5 items OK Cancel 📻 🎴 🤮 🤩 📾 au hinh địa chi DNS, câu hinh card Vmnet 8 ОК ø 🎊 Start 📋 🚠 📰 🏈 💋 🗍 🌈 IIS 7.0 Detailed Error - 4.. # E Fo To direct input to this VM, move the mouse pointer inside or press Ctrl+G. Page 22 of 22 . + 80% COA 🔮 💩 Q Search C Ð w >___ <u>0</u>/2

_

Cấu hình DNS cho card mạng VMnet8 trên máy VICTIM

agnose this conne	VMnet8 Status	ection	Change settings of this connec	tion 🗄 🔹 🔲 🔇						
Ethernet Network ca Killer E2600	General	VMnet8 Properties	Pv4) Properties							
	Connection	Networking Sharing	General Alternate Configuration							
	IPv4 Connectivity:	Connect using:	utomatically if your network supports							
	IPv6 Connectivity:	🚽 VMware Virtual Ethernet A	this capability. Otherwise, you need to ask your network add for the appropriate IP settings.							
	Media State:									
	Duration:		Obtain an IP address automa	tically						
	Speed:	This connection uses the followi	O Use the following IP address:							
	Details	Client for Microsoft Net	IP address:							
		VMware Bridge Protoco	Subpat mach							
		 Internet Protocol Versio 	Subher mask.	* * *						
	Activity	🗌 🔟 Microsoft Network Ada	Default gateway:	A						
		Microsoft LLDP Protoco								
	Sent —	Internet Protocol Versio	Obtain DNS server address a	utomatically						
	Deckster 192		O Use the following DNS server	addresses:						
	Packets. 183	Install Un	Preferred DNS server:	192 . 168 . 10 . 200						
	Duranting Direkte	Description	Alternate DNS server:	· · · ·						
		Transmission Control Protocol wide area network protocol th across diverse interconnected	Validate settings upon exit	Advanced						

- Sau đó truy cập <u>http://www.abc.com/</u> 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 xả DNS ở máy VICTIM bằng lệnh ipconfig /flushdns với quyền Adminitrator trên CMD.



- 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 <u>www.abc.com</u> tại máy chủ SERVER thì bị tấn công DNS - thay đổi đi 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 mền Wireshark để bắt gói tin. Chọn Capture Option chọn bộ lọc
 TCP. Và nhấn Start

SERVER	× 🕞 ATTACK ×			
煮 The Wirer		4.40\3		_ @ %
Eile Edit V	Wireshark: Capture Options			
0 0 🖌 1	Capture			
Filter:	Capture Interface Link-layer header Prom. Me	de Snaplen [B] Buffer [MiB] Capture Filter		
	Local Area Connection Ethernet enable	default 2 tcp		
WIRE	192.168.1.131		=	
_			-	
Test	4		Þ	
•	☑ Capture on all interfaces		Manage Interfaces	
(cour	Ise promiscuous mode on all interfaces		indiage incitaces	
	E ose <u>p</u> romocious mode on an interfaces			
🖉 Sta	Capture Filter: tcp		 Compile selected BPFs 	d)
Choc		Wireshark: Canture Filter - Profile: Default		-/
🖅 Local A	Capture Files	Edit Capture Filter	Display Options	
	File:	Browse	✓ Update list of packets in real time	ble
C -	Ilse multiple files	IPX only		
⊚ Ca	e ose peap-ing tormat	New TCP only	Automatically scroll during live capture	
Start	Next file every 1 megabyte(s)	UDP only		
	Next file every 1 👘 minute(s) 💌	TCP or UDP port 80 (HTTP)	☑ <u>H</u> ide capture info dialog	
	Ring buffer with 2 files	HTTP TCP port (80)	Name Resolution	
	Stop capture after 1 file(s)	No ARP and no DNS	R Baraha MAC addamaa	
		Delete	Resolve MAC addresses	
💧 Ho	Stop Capture Automatically After	< III +	Resolve network-layer names	
Step	1 packet(s)	Properties		
No			Resolve transport-layer name	
	I v megabyte(s)	Filter name: TCP only		
Ether	1 minute(s)	Filter string: tcp	Use external network name resolver	
	Halp	Help OK Cancel	Start Class	
Ready to log	Пер		<u>Start</u> <u>Close</u>	
Ready to loa			II.	1,28 DM
1	2 📃 🔍 🚺 📶			1:28 PM 05/10/2024

- ở máy VICTIM PC thì truy cập trang web <u>http://www.abc.com</u>. Để cho Wireshark bắt gói tin

rồi sau đó nhấn stop capture

SEF	IVER ×	🕞 АТТАСК 🗵																			
🔏 Cap	turing from	Local Area Connection ((tcp) [Wires	hark 1.10.5 (SVN Rev 54	262 from /tru	ink-1.10)]															a ×
<u>F</u> ile <u>E</u>	dit <u>V</u> iew	<u>Go</u> <u>C</u> apture <u>A</u> nalyze	Statistics Te	elephony <u>T</u> ools <u>I</u> nter	nals <u>H</u> elp																
0 0	a 🔳 🔬	🖹 🖹 X 🖉 🔍	🌞 🏟 🥥 🖥	<u>.</u>	Q 🗹 🗃	¥ 🗹 🍕 %	Ħ														
Filte	n			 Expre 	ssion Cle	ear Ap	ply	Sa	ave												
No.	Time	Source	0	Destination	Protocol	I Length Ir	fo														-
	5 0.0002	28100 192.168.1.2	100 1	192.168.1.1	TCP	66 [TCP	Keep-	Alive	ACK]	http > 6	4751	[ACK] Seq	=1 Ack=2	Win=256	Len=0 SLI	E=1 SRE	=2			
	7 5 0718	3300192.168.1.2	. 00	192.108.1.1	HTTP	706.6		нттр	A11Ve	ACK	nttp > c	94731	LACKJ SEQ	=1 ACK=2	win=250	Len=0 SLI	E=I SKE	:=2			
	8 5.0720	2100 192.168.1.1		192.168.1.200	НТТР	706 [TCP	Retra	nsmiss	sionl	GET / HT	TP/1.3	1								
	9 5.0722	20800 192.168.1.2	00	192.168.1.1	тср	66 h	ttp	> 647	84 [A0	CK] Se	eq=1 Ack=	653 W	in=252 Le	1=0 SLE=1	SRE=653	3					
1	LO 5.0722	23200192.168.1.2	:00	192.168.1.1	TCP	66 [ТСР	Dup A	CK 9#1	1] htt	:p > 6478	4 [ACI	<] Seq=1	Ack=653 W	in=252 L	.en=0 SLE:	=1 SRE=	=653			
1	1 5.0722	29700 192.168.1.2	100 1	192.168.1.1	HTTP	241 H	TTP/	1.1 3	04 No1	t Modi	ified	1. 100	udu 540								
-		29700 192.168.1.1 20200 102 168 1 2		192.168.1.200		241	4/84	> nt	tp LAG	CKJ Se	2q=053 AC	.K=188	W1N=512	_en=0							
	4 5.072	30400 192.168.1.1	.00 .	192.168.1.200	ТСР	54 [TCP	Dup A	CK 12	#11 64	1784 > ht	$\frac{1}{10}$	CK1 Sea=6	53 Ack=18	8 Win=51	2 en=0					
	15 5.072	34800 192.168.1.1		192.168.1.200	ТСР	66 [ТСР	Dup A	CK 12	#2] 64	1784 > ht	tp [A	CK] Seq=6	53 Ack=18	8 Win=51	.2 Len=0 :	SLE=1 S	RE=18	8		
1	16 5.0723	35100192.168.1.1	. 1	192.168.1.200	TCP	66 [ТСР	Dup A	CK 12#	#3] 64	1784 > ht	tp [A	CK] Seq=6	53 Ack=18	8 Win=51	.2 Len=0 !	SLE=1 S	GRE=18	8		
1	17 9.0949	8300 192.168.1.1	. 1	192.168.1.200	TCP	60 [ТСР	segme	nt of	a rea	assembled	PDU]			54.0						
		4500 192.168.1.1	00	192.168.1.200	ТСР	55 [TCP	Keep-	Alive		0 > nttp	LACK	Seq=1 A	CK=1 Win=	512 Len=	=1					
-		20500 192.168.1.2	200 1	192.108.1.1	ТСР	66 [тср	> 04/ Keen-	Alive		q=1 ACK=	2 WIN	=230 Len=	-1 Ack = 2	KE=2 Win=256	Len-0 SLI	E-1 SDE	-2			
	21 9.0954	0800 192.168.1.2	00	192.168.1.1	ТСР	66 [TCP	Keep-	Alive	ACK]	http > 6	4750	[ACK] Seq	=1 Ack=2	Win=256	Len=0 SLI	E=1 SRE	=2			
	22 9.0954	1500 192.168.1.2	00	192.168.1.1	ТСР	66 [ТСР	Keep-	Alive	ACK]	http > 6	4750	[ACK] Seq	=1 Ack=2	Win=256	Len=0 SLI	E=1 SRE	=2			
	23 34.272	25630 192.168.1.1	. 1	192.168.1.200	TCP	60 [тср	segme	nt of	a rea	assembled	PDU]									
	24 34.272	27060 192.168.1.1	. 1	192.168.1.200	тср	55 [тср	Keep-	Alive	1 6478	35 > http	ACK	∣ Sea=1 A	ck=1 Win=	4100 Ler	1=1					
	25 34.272	27480 192.168.1.2	200 1	192.168.1.1	TCP	66 r	~	0	abc.com			×	+						_		×
	20 34.2/2	2//20/192.108.1.2	00	192.108.1.1		66															
	28 34.27	32410 192.108.1.2	200 1	192.168.1.1	ТСР	66	~	\rightarrow	a		nông bảo m	it also					~		<u>_</u>	1.0	. :
< □							~	-	0		iong bao ma	and and					Ж	-		1.4	•
- Erai	ne 1 · 60	hytes on wire ((480 hits)	60 bytes cant	ured (480	hits) or	m 1 -														
B Eth	ernet II	, Src: Vmware_c0	:00:08 (0	0:50:56:c0:00:0	8), Dst: \	Vmware_c6	1 his	is my	websi	te: Hel	to world										
🗄 Inte	ernet Pr	otocol Version 4	, Src: 19	2.168.1.1 (192.)	168.1.1),	Dst: 192															
0000	00.06.7	o control Dustac		0 08 08 00 AE 0	C1) De+ 1	Dont. htt															
0010	00 29 2	4 a1 40 00 80 06	5 52 14 0	10 08 08 00 43 0 10 a8 01 01 c0 a	8 .)\$.@																
0020	01 c8 f	c ef 00 50 b4 ff	F 9F 34 6	50 48 02 e2 50 1	0	P4`H															
0030	02 01 /	5 1a 00 00 00 00	00 00 0	00 00	u	• • • • • • • • •															
🔵 💆 Lo	cal Area Co	nnection: <live capture<="" td=""><td>Packets: 28 -</td><td>Displayed: 28 (100.0%)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></live>	Packets: 28 -	Displayed: 28 (100.0%)																	
	\bigotimes		0																		
e mouse p	ointer insid	e or press Ctrl+G.																	-		
				Q Searc	h	190		. (2	، 🌮	Zalo 🛛	ø					^	\$ \$	•	1:31 10/5/2	РМ 024 Д

- Sau đó ở máy ATTACK bấm dừng capture và nhấp chọn Protocol vào phần HTTP

	SERVI	er $ imes$ is attack $ imes$														
ĺ	🚄 *Loca	I Area Connection (tcp)	[Wireshark 1.10.5 (S	VN Rev 54262 fro	om /trunk-1.10)]											
	<u>File</u> <u>E</u> dit	t <u>V</u> iew <u>G</u> o <u>C</u> apture	Analyze Statistics	Telephony Tool	ls <u>I</u> nternals <u>H</u>	elp										
	0 0 /	(🔳 🔬 🖻 🛅 🗙 (2 🔍 🔶 🔿	7 ⊻ 🗐 🖬		- I I I I I I I I I I I I I I I I I I I	🖲 💥 🖾									
					.											
	Filter:				Expression	Clear	Apply	Save								
	No.	Time Source		Destination	Pr	otocol Len	gth Info									
	1	0.000000000192.1	.68.1.1	192.168.1.2	200 T	СР	60 [TCP	segment	of a reasser	mbled PDU]						
J	2	0.00017400192.1	.68.1.1	192.168.1.	200 T	СР	55 [TCP	Keep-Ali	ve] 64751 >	http [ACK	<] Seq=1	L Ack=1	Win=513 L	_en=1		
- L	3	3 0.00021800 192.1	.68.1.200	192.168.1.1	1 т	СР	66 http	> 64751	[ACK] Seq=1	Ack=2 Win	1=256 L€	en=0 SLE	=1 SRE=2			
	4	0.00022700 192.1	.68.1.200	192.168.1.	<u>1 T</u>	СР	66 LTCP	Keep-Ali	ve ACK] http	p > 64751	[ACK] S	Seq=1 Ac	k=2 Win=2	256 Len=0	SLE=1 SRE	E=2
	5	50.00028100192.1	.68.1.200	192.168.1.1	1 т	СР	66 [TCP	Keep-Ali	ve ACK] http	p > 64751	[ACK] S	Seq=1 Ac	k=2 Win=2	256 Len=0	SLE=1 SRE	E=2
J	6	50.00028600192.1	.68.1.200	192.168.1.1	1 т	CP	66 [TCP	Keep-Ali	ve ACK] http	p > 64751	[ACK] S	Seq=1 Ac	k=2 Win=2	256 Len=0	SLE=1 SRE	E=2
	7	5.07183300 192.1	.68.1.1	192.168.1.	200 Н	ТТР	706 GET ,	/ HTTP/1.	1							
J	8	35.07202100192.1	.68.1.1	192.168.1.	200 Н	ТТР	706 [TCP	Retransm	ission] GET	/ HTTP/1.	.1					
	9	5.07220800192.1	.68.1.200	192.168.1.3	1 т	CP	66 http	> 64784	[ACK] Seq=1	Ack=653 W	Vin=252	Len=0 S	LE=1 SRE=	=653		
J	10	5.07223200 192.1	.68.1.200	192.168.1.1	1 т	СР	66 [TCP	Dup ACK	9#1] http >	64784 [AC	[K] Seq=	=1 Ack=6	53 Win=25	52 Len=0 :	SLE=1 SRE=	=653
	11	5.07229700192.1	.68.1.200	192.168.1.3	1 н	ТТР	241 HTTP,	/1.1 304	Not Modified	d						
	12	2 5.07229700 192.1	.68.1.1	192.168.1.2	200 T	СР	60 6478	4 > http	[ACK] Seq=6	53 Ack=188	3 Win=51	L2 Len=0)			
	13	3 5.07230300 192.1	.68.1.200	192.168.1.3	1 н	TTP	241 [TCP	Retransm	ission] HTTP	P/1.1 304	Not Mod	dified				
	14	5.07230400 192.1	.68.1.1	192.168.1.	200 T	СР	54 [TCP	Dup ACK	12#1] 64784	> http [A	ACK] Sec	q=653 Ac	<u>k=188 Wir</u>	1=512 Len:	=0	
	15	5.07234800192.1	.68.1.1	192.168.1.	200 T	CP	66 [TCP	Dup АСК	12#2] 64784	> http [A	ACK] Sec	q=653 Ac	k=188 Wir	n=512 Len:	=0 SLE=1 9	SRE=188
	16	5.07235100 192.1	.68.1.1	192.168.1.	200 T	СР	66 [TCP	Dup ACK	12#3] 64784	> http [A	ACK] Sec	q=653 Ac	:k=188 Wir	1=512 Len:	=0 SLE=1 9	SRE=188
	17	9.09498300192.1	.68.1.1	192.168.1.2	200 T	CP	60 [TCP	segment	of a reasser	mbled PDU]						
	18	39.09514500192.1	.68.1.1	192.168.1.	200 T	СР	55 [TCP	Keep-Ali	ve] 64750 >	http [ACK	<] Seq=1	L Ack=1	Win=512 L	_en=1		
	19	9.09518500192.1	68.1.200	192.168.1.1	1 T	CP	66 http	> 64750	[ACK] Seg=1	Ack=2 Win	1=256 Le	en=0 SLE	=1 SRF=2			

- Coi phần get HTTP từ server tới Máy VICTIM

SERVI	er \times [] attack \times								
📕 📶 *Loca	Area Connection (tcp) [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-	-1.10)]						
<u>F</u> ile <u>E</u> di	t <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics	Telephony <u>T</u> ools <u>I</u> ntern	als <u>H</u> elp						
0 0 /	🕻 🔳 🔬 🗁 📇 🗶 🍠 🔍 🗢 🌳 🍛	7 ⊻ 🗐 🗐 🔍 Q	0, 🖭 🛛 👹	🗵 畅 💥 💢					
Filter:		Expres	sion Clea	r AlaaA	Save				
No	Time Source	Destination	Protocol	Length Info					
1	0.00000000192.168.1.1	192.168.1.200	TCP	60 [TCP	segment	of a reas	sembled PD	U]	
2	2 0.00017400 192.168.1.1	192.168.1.200	ТСР	55 [TCP	Keep-Al	ive] 64751	. > http [AG	CK] Seq=1 A	ck=1 Win=513
3	0.00021800 192.168.1.200	192.168.1.1	ТСР	66 http	> 64751	[ACK] Seq	=1 Ack=2 W	in=256 Len=(0 SLE=1 SRE=2
4	0.00022/00192.168.1.200	192.168.1.1	TCP	66 [TCP	Keep-Al	ive ACK] h	ttp > 64751	1 [ACK] Seq	=1 Ack=2 Win=
 	0.00028100192.108.1.200	192.108.1.1			Keep-Al	ive ACK] n	ttp > 6475	I [ACK] Seq	=1 ACK=2 WIN= -1 Ack=2 Win=
7	5.07183300 192.168.1.1	192,168,1,200	HTTP	706 GET /	/ HTTP/1.	.1		I [ACK] JC4-	-1 ACK-2 WIII-
8	5.0/202100/192.168.1.1	192.108.1.200	нттр	700 LICP	Retransi	nission] G	ET / HTTP/I	1.1	
9	5.07220800 192.168.1.200	192.168.1.1	TCP	66 http	> 64784	[ACK] Seq	=1 Ack=653	Win=252 Ler	n=0 SLE=1 SRE
10	5.07223200 192.168.1.200	192.168.1.1	TCP	66 [TCP	Dup ACK	9#1] http	> 64784 [/	ACK] Seq=1 /	Ack=653 Win=2
11	5.07229700192.168.1.200	192.168.1.1	HTTP	241 HTTP/	$(1.1 \ 304)$	NOT MODIT	1ed	99 Win_517 I	on_0
13	5 07230300 192 168 1 200	192.108.1.200	НТТР	241 TCP	Retransi	lack J Seq	=0.000 ACK=10	4 Not Modif	ied
14				- · · · · · · · ·			,		1-
14									
14	4 7 5.071833000 192.168.1.1 192.168.1.20	0 HTTP 706 GET / HTTP/1.1	•						
14 15 16	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706	bytes cap	tured (5648	bits) or	n interfac	e 0		
14 15 16 17	 7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Interpet Protocol Version 	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4 Src: 192 168 1	bytes cap c0:00:08)	tured (5648 , Dst: Vmwar 8 1 1) Dst:	bits) or re_c6:47	n interfac :8d (00:0c 8 1 200 (1	e 0 :29:c6:47:8	8d)	
14 15 16 17 18	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col. Src Port: 647	bytes capt c0:00:08) 1 (192.168 84 (64784)	tured (5648 , Dst: Vmwar 8.1.1), Dst:). Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80). Seg:	e 0 :29:c6:47:8 92.168.1.20 1. Ack: 1.	8d) 00) Len: 652	
14 15 16 17 18 19 20	 7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Protocol Hypertext Transfer Protocol 	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1	bytes cap c0:00:08) 1 (192.168 84 (64784)	tured (5648 , Dst: Vmwan 8.1.1), Dst:), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80), Seq:	e 0 :29:c6:47:8 92.168.1.20 1, Ack: 1,	8d) 00) Len: 652	
14 15 16 17 18 19 20 21	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1	bytes cap c0:00:08) 1 (192.164 84 (64784)	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80), Seq:	e 0 :29:c6:47:8 92.168.1.20 1, Ack: 1,	8d) 00) Len: 652	
14 15 16 17 18 19 20 21 22	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1	bytes cap c0:00:08) 1 (192.168 84 (64784)	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80), Seq:	e 0 :29:c6:47:8 92.168.1.2(1, Ack: 1,	8d) 00) Len: 652	
14 15 16 17 18 19 20 21 21 22 23 23	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r'	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1	bytes cap c0:00:08) 1 (192.168 84 (64784)	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80), Seq:	e 0 :29:c6:47:6 92.168.1.2(1, Ack: 1,	8d) 00) Len: 652	
14 15 16 17 18 19 20 21 22 23 24	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0' Ungrade-Trsecure-Request	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 (n (n (n (n) (n) (n) (n) (n) (n) (n) (n	bytes cap c0:00:08) 1 (192.164 84 (64784)	tured (5648 , Dst: Vmwar 8.1.1), Dst), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 80), Seq:	e 0 :29:c6:47:8 92.168.1.20 1, Ack: 1,	8d) 00) Len: 652	
14 15 16 17 18 19 20 21 22 23 24 4	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n \n xr\n s: 1\r\n (Windows NT 10.0; \)	bytes cap c0:00:08) 1 (192.164 84 (64784) win64; x64	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port:	bits) or re_c6:47 : 192.168 : http (8	n interfac :8d (00:0c 8.1.200 (1 30), Seq: 16 (KHTML,	e 0 :29:c6:47:{ 92.168.1.2(1, Ack: 1,]ike Gecko	8d) 00) Len: 652 0) Chrome/12	29.0.0.0
14 15 16 17 18 19 20 21 22 23 24 < □ ⊕ Frame ⊕ Frame	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept: text/html,applica	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 (n xr\n s: 1\r\n (windows NT 10.0; V ation/xhtml+xml,app	bytes cap c0:00:08) 1 (192.164 84 (64784) win64; x64 plication/	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: A) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 : it/537.3 mage/avi	n interfac :8d (00:0c 8.1.200 (1 30), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:t 92.168.1.2(1, Ack: 1, like Geckœ ebp,image/a	8d) 00) Len: 652 0) Chrome/12 upng,*/*;q=0	29.0.0.0 0.8, app1i
14 15 16 17 18 19 20 21 22 23 24 ∢ 	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept: text/html,applict Accept-Encoding: gzip, do	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n yr\n s: 1\r\n (windows NT 10.0; V ation/xhtml+xml,app eflate\r\n	bytes cap c0:00:08) 1 (192.164 84 (64784, 44 (64784, win64; x64 plication/	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: 4) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 : http (8 : it/537.3 mage/avi	n interfac :8d (00:0c 8.1.200 (1 30), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:t 92.168.1.20 1, Ack: 1, like Gecko ebp,image/a	8d) 00) Len: 652 0) Chrome/12 ppng,*/*;q=0	29.0.00 ().8, app1i
14 15 16 17 18 19 20 21 22 23 24 ∢ □ ⊕ Frame ⊕ Ether ⊕ Inter ⊕ Inter	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept: text/html,applict Accept-Language: vi-VN,v	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n \n \n \n \s: 1\r\n (windows NT 10.0; \u03e4 dion/xhtml+xml,app eflate\r\n i;q=0.9,en;q=0.8\r'	bytes cap c0:00:08) 1 (192.164 84 (64784, win64; x64 plication/ \n	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: 4) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 : it/537.3 mage/avi	n interfac :8d (00:0c 3.1.200 (1 30), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:t 92.168.1.20 1, Ack: 1, like Gecko ebp,image/a	8d) 00) Len: 652 0) Chrome/12 ppng,*/*;q=0	29.0.0.0 0.8, app1i
14 15 16 17 18 19 20 21 22 23 24 ✓ E Frame E Ether Inter 00000 (0 0010 (0	7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Proto Hypertext Transfer Protoco GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept: text/html,applic: Accept-Language: vi-VN,vr	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n \r\n s: 1\r\n (Windows NT 10.0; V ation/xhtml+xml,app eflate\r\n i;q=0.9,en;q=0.8\r'	bytes cap c0:00:08) 1 (192.164 84 (64784, win64; x64 plication/ \n	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: 4) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 : it/537.3 mage/avi	n interfac :8d (00:0c 8.1.200 (1 30), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:t 92.168.1.20 1, Ack: 1, like Gecko ebp,image/a	8d) 00) Len: 652 0) Chrome/12 ppng,*/*;q=0	29.0.0.0 0.8, appli
14 15 16 17 18 19 20 21 22 23 24 ← Ether ■ Ether ■ Ether 0000 (0010 (0020 (7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Protoc GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept: text/html,applica Accept-Language: vi-VN,vi Control: 02 by 24 cb 40 00 50	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n \r\n s: 1\r\n (windows NT 10.0; N ation/xhtml+xml,app eflate\r\n i;q=0.9,en;q=0.8\r' 	bytes cap c0:00:08) 1 (192.16) 84 (64784) win64; x64 plication/ \n 00 45 00 01 c0 28	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: 4) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 : it/537.3 mage/avi	n interfac :8d (00:0c 8.1.200 (1 80), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:: 92.168.1.2(1, Ack: 1, like Gecko ebp,image/a	8d) 00) Len: 652 0) Chrome/12 upng,*/*;q=0	29.0.0.0 0.8, appli
14 15 16 17 18 19 20 21 22 23 24 ← Ether ■ Frame ■ Ether ■ Inter 0000 (0010 (0020 (0030 (0040 (<pre>7 5.071833000 192.168.1.1 192.168.1.20 Frame 7: 706 bytes on wire Ethernet II, Src: Vmware_c Internet Protocol Version Transmission Control Protoc GET / HTTP/1.1\r\n Host: www.abc.com\r\n Connection: keep-alive\r' Cache-Control: max-age=0 Upgrade-Insecure-Request: User-Agent: Mozilla/5.0 Accept-Encoding: gzip, d Accept-Language: vi-VN,vi Control 00 00 c2 9 c6 47 8d 00 5 0010 02 b4 24 ab 40 00 80 0 0020 01 c8 fd 10 00 50 77</pre>	0 HTTP 706 GET / HTTP/1.1 (5648 bits), 706 0:00:08 (00:50:56: 4, Src: 192.168.1. col, Src Port: 647 1 \n \r\n s: 1\r\n (Windows NT 10.0; \n ation/xhtml+xml,app eflate\r\n i;q=0.9,en;q=0.8\r' \n 0 56 c0 00 08 08 26 4f 7f c0 a8 01 1 755 1a a8 dc	bytes cap c0:00:08) 1 (192.16) 84 (64784) win64; x64 plication/ \n 00 45 00 01 c0 a8 e4 50 18	tured (5648 , Dst: Vmwar 8.1.1), Dst:), Dst Port: 1) ApplewebK (xml;q=0.9,i	bits) or re_c6:47 : 192.168 : http (8 :it/537.3 mage/avi vE. 0	n interfac :8d (00:0c 8.1.200 (1 80), Seq: 66 (KHTML, f,image/we	e 0 :29:c6:47:: 92.168.1.2(1, Ack: 1, like Geckα ebp,image/a	8d) 00) Len: 652 0) Chrome/12 upng,*/*;q=0	29.0.0.0 0.8, appli

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

*Local Area Connection (tcp) [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.1	0)
Eile Edit View Go Capture Analyze Statistics Telephony Tools Internals	Help
Filter:	n Clear Apply Save
No. Time Source Destination	Protocol Length Info
19 23.33318/0192.168.1.200 192.168.1.1 20 23 3332010102 168 1 200 102 168 1 1	ICP bb http > b4919 [ACK] Seq=1 AcK=b34 Win=254 Len=0 SLE=2 SRE=b34
20 23. 3335910(192.108.1.200 192.108.1.1	ICP OO [ICP Dup Ack 1991] IIC[P > 04919 [ACK] Set[1 ACK=034 WIT=234 Lett=0 SLE=2 SKE=034 HTTP 377 HTTP/1 1 200 0K (text/html)
22 23.3336010/192.168.1.200 192.168.1.1	
23 23.3336640 192.168.1.1 192.168.1.200	21 23.333591000 192.168.1.200 192.168.1.1 HTTP 327 HTTP/1.1 200 OK (text/html)
24 23.3336710192.168.1.1 192.168.1.200	Frame 21: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) 🖕 Len=0 SLE=1 SRE=274
25 25.21925/0192.168.1.1 192.168.1.200 26 25 2104260.102 168 1 1 102 168 1 200	Ethernet II, Src: Vmware_c6:47:8d (00:0c:29:c6:47:8d), Dst: Vmware_c0:00:
27 25 2196780(192,168,1,200) 192,168,1,1	Transmission Control Protocol Sec Dort: http://doi.org/10.00110/00100000000000000000000000000
28 25.2197180/192.168.1.200 192.168.1.1	Hypertext Transfer Protocol
29 25.2200860 192.168.1.200 192.168.1.1	Line-based text data: text/html
30 25.2201120 192.168.1.200 192.168.1.1	This is my testing website! I am testing wireshark
31 25.2201660/192.168.1.1 192.168.1.200	=462 2 Lon 2 CLE 274 CDE 463
33 29.0259960(192.168.1.200 192.168.1.131	SACK PERM=1
34 29.0261540192.168.1.131 192.168.1.200	L460 WS=256 SACK_PERM=1
35 29.0266580 192.168.1.200 192.168.1.131	
36 29.0268390 192.168.1.131 192.168.1.200	
<	0000 00 50 56 c0 00 08 00 0c 29 c6 47 8d 08 00 45 00 PV) c
🖲 Frame 21: 327 bytes on wire (2616 bits), 327 bytes cap	0010 01 39 08 65 40 00 80 06 6d 40 c0 a8 01 c8 c0 a8 .9.e@ m@
<pre> Ethernet II, Src: Vmware_c6:47:8d (00:0c:29:c6:47:8d),</pre>	0020 01 01 00 50 fd 97 7f 91 78 08 b1 7a 06 3f 50 18P xz.?
Internet Protocol Version 4, Src: 192.168.1.200 (192.1 Transmission Control Protocol Snc Parts http://www.protocol.com/ 192.168.1.200 (192.1	
Hypertext Transfer Protocol	(14919) (04919), Seq. 1, ACK. 034, Left. 275
■ Line-based text data: text/html	
0000 00 50 56 c0 00 08 00 0c 29 c6 47 8d 08 00 45 00	.PV).GE
0020 01 01 00 50 fd 97 7f 91 78 08 b1 7a 06 3f 50 18	
0030 00 fe 32 95 00 00 48 54 54 50 2f 31 2e 31 20 32	2HT TP/1.1 2
● ∑ File: "C:\Users\win7\AppData\Loca Packets: 74 · Displayed: 74 (100.0%) · D	ropped: 0 (0.0%) Profile: Default
	1:51 PM
	- 🕕 🍺 🤯 05/10/2024

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

Internet Information Services (11S) Ma	anager	_ & ×
G G ♥ + SERVER +		🖬 🖂 🔂 I 🕢 🔹
File View Help		
Connections	SERVER Home Group by: Area II II Compression Compres	Actions Open Feature Manage Server Pestart Start Start Start View Application Pools View Mapplication Pools View
Reauy	formation -	
💦 Start 🛛 🌚 💻 🦷 🛯 📢 Internet In	iformation	🧠 🔐 🛒 🔁 1:54 PM

- Chọn phần Authentication, Phần Anoymous chọn Disabled và Enabled mục Bacsic

💐 Internet Information Services (IIS) Ma	anager			
G 🕥 🧐 🕨 SERVER 🔸				
File View Help				
Connections		n •		
BRVER (SERVER\Administrator)	Name A	Status	Response Type	
STP Sites	Anonymous Authentication	Disabled		1
E Sites	Basic Authentication	Enabled	HTTP 401 Challenge	

Sau đó, mở lại wireshark trên ATTACK và truy cập trang web <u>www.abc.com</u> trên VICTIM
 và nhập tài khoản mật của WIN VICTIM

~	S abc.com	×	+			_	×
÷	\rightarrow G	() abc.com		☆	٩	≏	:
		Đăng nhập http://www.abc.c Kết nối của bạn t Tên người dùng Mật khẩu	om ới trang web này không ở chế độ riêng tư adminitrastor ••• Đăng nhập Huỷ				

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

Server × 🕞 Attack ×	
*Local Area Connection (tcp) [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]	- @ X
Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals Help	
● ● ∡ ≢ ∡ ⊟ 🗄 ೫ 🐉 ! ९, ♦ ♦ 🗣 💈 ! 🗐 🗐 ! ९, ९, ९, 🗉 ! 👪 🛛 🥵 ೫ छ	
Filter: Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	A
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$	131328 Len=0 SLE=1479 SRE=2939 131328 Len=0 SLE=2939 SRE=2957 131328 Len=0 SLE=1479 SRE=2957 Lan=1 Len=1 Len=1 5 Len=0 SLE=0 SRE=1 36 Len=0 SLE=0 SRE=1 16 Len=0 SLE=0 SRE=1 16 Len=0 SLE=0 SRE=1
a 51 54.501095000 192.106.1.1 192.106.1.200 HTP /34 GET / HTP/LT	
© Ethernet II, Src: Vmare_c0:00:08 (00:50:56:c0:00:08), Dst: Vmare_c6:47:8d (00:0c:29:c6:47:8d)	Â
B Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.200 (192.168.1.200)	
Transmission Control Protocol, Src Port: 64952 (64952), Dst Port: http (80), Seq: 1354, Ack: 2957, Len: 700	
	=======================================
□ [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]	
Request Method: GET	
Request VRI: / Perust Version: HTTP/1 1	
Host: www.abc.com/r/n	
Connection: keep-alive\r\n	
Cache-Control max-age=0\r\n	
Authorization: Basic YWRtaW5pc3RyYXRvcjphQDE=\r\n	
United and the second s	.
0080 6d 61 78 2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f max-ago 0 Autho	
2 0090 72 69 7a 61 74 69 6f 6e 3a 04 26 173 69 63 20 rization : Basic	<u>^</u>
00a0 59 57 52 74 61 57 35 70 63 33 52 79 59 58 52 76 00b0 63 6a 70 68 51 44 45 3d 0d 0a 55 70 67 72 61 64 cjphQDE=Upgrad	-

- Kết thúc phân tích mật khẩu

- 5.2. Phân tích FTP

-	Ở máy	SERVER	tiếp tục	mở IIS	và chọn	chạy F7	TP sites
---	-------	--------	----------	--------	---------	---------	-----------------

Internet Information Services	(IIS) 6.0 Manage	r		
🔰 File Action View Window F	Help			
Internet Information Services		lama	Path	Status
🖃 🗊 SERVER (local computer)	Ė	ionne	- Fuur	100000
🗉 🔂 FTP Sites 🗊 🚱 Default FTP Site (Stoppe	ക			
	Explore			
	Open			
	Browse			
	Start			
	Stop Pause			
	New All Tasks	>		
	View New Window fro	► om Here		
	Delete			
	Rename			
	Refresh			
	Export List			
	Properties			
liep tục cấp hình FTP				
The Action View Wind	tow Help			
File Action View Wind	dow Help	▶ ■ II		
Image: File Action View Wind	dow Help	▶ ■ II Name	[Path
Image: File Action View Wine	dow Help P I P P pes r)	Name		Path
File Action View Wind Internet Information Service Internet Information Service Internet FTP Sites Polault FTP Sites	dow Help E I I I I I ces r)	Name		Path
 File Action View Wind File Action View Wind File Provide SERVER (local compute FTP Sites Default FTP Site 	dow Help ses r) roperties	Name		Path
File Action View Wind File Action View Wind Thermet Information Service SERVER (local compute FTP Sites Toefault FTP Site P Default FTP Site P	dow Help	Name		Path
File Action View Wind File Action View Wind Thernet Information Service SERVER (local compute FTP Sites Default FTP Site FTP Site Security	dow Help ses r) roperties Accounts Messa	Bes Home Directory	Directory Security	Path
File Action View Wink File Action View Wink The content of the security The content for the security The content for the security	dow Help ses r) roperties Accounts Messa his resource shoul	Bes Home Directory	Directory Security	Path
File Action View Wink File Action View Wink The content Information Service SERVER (local compute FTP Sites Default FTP Site FTP Site Security The content for the	dow Help	Name Name Iges Home Directory d come from: located on this compu	Directory Security	Path
File Action View Wink File Action View Wink The content information Service SERVER (local compute FTP Sites Default FTP Site FTP Site Security The content for the formation the	dow Help	Bes Home Directory	Directory Security Iter imputer	Path
File Action View Wink File Action Service File Action S	dow Help	Bes Home Directory d come from: located on this compu- located on another co	Directory Security Iter Imputer	Path
File Action View Wink File Action View Wink FIP Site File Action Service FIP Site Ac	tow Help	Mame Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security Iter Imputer Browse	Path
File Action View Wink File Action View Wink The content Information Service SERVER (local compute FTP Sites Default FTP Site FTP Site Security The content for the Local path:	tow Help	Bes Home Directory d come from: located on this compu- located on another co	Directory Security Iter Imputer Browse	Path
File Action View Wink File Action View Wink The content Information Service SERVER (local compute FTP Sites Default FTP Site FTP Site Security The content for the Local path:	tow Help	Bes Home Directory d come from: located on this compu- located on another co	Directory Security Iter Imputer Browse	Path
File Action View Wink File Action View Wink FIP Site File Action Service FIP Site Action Service FIP Service Action Service FIP Service Action Service FIP Service Action Service FIP Service Action Service FIP Service FIP Servi	tow Help	Bes Home Directory d come from: located on this compu- located on another co	Directory Security Iter Imputer Browse	Path
File Action View Wine File Action View Wine Thermet Information Service FTP Sites FTP Site FTP Site FTP Site FTP Site FTP Site Security The content for the Local path: Local path:	tow Help	Bes Home Directory	Directory Security	Path
File Action View Wine File Action View Wine File Action View Wine File Action View Wine File Action Service File File File File Security File Security The content for the Con	tow Help	Name Name Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Name Name Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Name Name Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind File Action Service File Action Service File Action Service File Action Service File Action Service File Action Service File Action Service File	tow Help	Name Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Name Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Name Name Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Name Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security	Path
File Action View Wind	tow Help	Mame Name Iges Home Directory d come from: located on this compu- located on another co	Directory Security	Path

- Cấu hình Security và tắt Allow anonymous connections

🔰 Internet Information Services (IIS) 6.0 Manag	ger						
🐚 File Action View Window Help							
Internet Information Services	Name	Path		Status	;		
□ server (local computer) □ ⇒ FTP Sites							There
😰 Default FTP Site							
Default FTP Site Properties		? ×					
FTP Site Security Accounts Message	s Home Directory Direc	tory Security					
Allow anonymous connections							
Use the following Windows user ad	ccount for anonymous acc	ess:					
User name: IUSR_SERVER		Browse					
Password:							
Allow only anonyn	nous connections						
IIS6 Manager		×					
Č máy VICTIM mở <u>ftp://192.168.1.</u>	In you have selected resu nitted over the network wit tempting to compromise ; tocol analyzer to examine uthentication process. For sult the online help. This SSL) connections. continue? No Help .200 hoặc ftp://v	Its in hout data your system e user more detail on varning does					
✓ S abc.com	+				_		×
\leftarrow \rightarrow C \triangle Không bảo mật abc.co	ym		☆	٩	Ď	(:
This is my testing websi Mở Microsoft I	Edge?	nàv					
	Mở	Microsoft Edge	Huý				

-

O 192.168.1.200 O 192.110 O 192.1	n 6	1		192.168.1.2	00		_		\times		
Sign in to access this site Authorization required by http://192.168.1.200 Your connection to this site is not secure Username administrator Password Sign in Cancel Éu không duryce thì Test trên máy ATTACK Mô Internet Explore Vev Favorites Now Attack Image: State trên máy ATTACK. Mô Internet Explore Image: State trên Máy ATTACK. Mô Image: State trên State trên Image: State trên State trên trên trên trên trên trên trên trên	\leftarrow (C ()	192.168.1.2	200	\$	¢	C D				
Authorization required by http://192.168.1.200 Your connection to this site is not secure Username dministrator Password Sign in Cancel étu không được thì Test trên máy ATTACK. Mở Internet Explore và truy c tru://www.abc.com và đăng nhập mật khâu. Để kiểm tra bắt gói tin ftp: SERVER ATTACK X C ATTACK X C Internet Explorer MSN X e Edit View Favorites Tools Help To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: Atter you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel			Sign in to	access this sit	e						
+ Username administrator Password Sign in Cancel éu không dược thì Test trên máy ATTACK. Mớ Internet Explore và truy c tp://www.abc.com và dăng nhập mật khẩu. Để kiểm tra bắt gói tin fp SERVER ATTACK MSN K E dit View Favorites Tools Help Toteg on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: After you log on, you can add this server to your Favorites and return to it easily. I tog on gnonymously Log on Cancel	8		Authorizatio Your conne	on required by htt ction to this site is	p://192.168. not secure	1.200					
Password Sign in Cancel éu không được thì Test trên máy ATTACK. Mở Internet Explore và truy c tp://www.abc.com và dăng nhập mật khẩu. Đẻ kiểm tra bắt gói tin ftp SERVER ATTACK Image: Attack X	+		Username	administrator							
Sign in Cancel Éu không được thì Test trên máy ATTACK. Mở Internet Explore và truy c tự://www.abc.com và đăng nhập mật khẩu. Để kiểm tra bắt gói tin ftp: SERVER I TATACK Image:			Password								
éu không được thì Test trên máy ATTACK. Mở Internet Explore và truy c tp://www.abc.com và đăng nhập mật khẩu. Để kiểm tra bắt gói tin ftp. SERVER ➤ ► ▲ TTACK ➤ C SERVER ➤ ► ▲ TTACK ➤ C MIN					Sign in	Cance	I				
éu không được thì Test trên máy ATTACK. Mở Internet Explore và truy c tp://www.abc.com và dăng nhập mật khẩu. Để kiểm tra bắt gói tin ftp SERVER ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲			_			-					
 không được thì Test trên máy ATTACK. Mở Internet Explore và truy c server ATTACK ATTACK ATTACK ATTACK ATTACK ATTACK ATTACK ATTACK Internet Explorer To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: Internet: administrator <l< td=""><th></th><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></l<>											
e Edit View Favorites Tools Help Thernet Explorer Vi-vn?pc=UE09&cocid=UE09DHP MSN × e Edit View Favorites Tools Help To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on gnonymously Log on Cancel											
SERVER X TTACK X SERVER X TTACK X MSN X e Edit View Favorites Tools Help Internet Explorer To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: After you log on, you can add this server to your Favorites and return to it easily. Log on gnonymously Log on Cancel	lán lihên	a trans t	h) Tost (tuân máy Ar	FT A CV	Må I	at a ma	t Ex	n 1ana	và tenu	
Image: bit	lếu khôr ttp://www	ng được tỉ w.abc.com v	hì Test và đăng nh	trên máy A nâp mât khẩu.	ΓΤΑCK. Để kiểm	Mở I tra bắt	nterne gói tii	et Ex	plore	và truy	cậ
https://www.msn.com/vi-vn?pc=UE09&ocid=UE09DHP MSN x e Edit View Favorites Tools Help Internet Explorer To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on Cancel	lếu khôn ttp://www ▶ server	ng được tỉ w.abc.com v	hì Test t ∕à đăng nh ĸ ×	trên máy A' 1ập mật khẩu.	ΓΤΑCK. Để kiểm	Mở I tra bắt	nterne gói tii	et Ex 1 ftp	plore	và truy	cậ
MSN × e Edit View Favorites Tools Help Internet Explorer Image: Tool og on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel	éu khôr ttp://www server	ng được tỉ w.abc.com v × Граттас	hì Test t /à đăng nh ĸ ×	trên máy A' 1ập mật khẩu.	ITACK. Để kiểm	Mở I tra bắt	nterno gói tii	et Ex 1 ftp	plore	và truy	câ
e Edit View Favorites Tools Help Internet Explorer Image: Second	lếu khôr ttp://www server	ng được tỉ w.abc.com v X I Trac	hì Test t /à đăng nh ĸ × w.msn.com/vi	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc	ITACK. Để kiểm id=UE09DH	Mở I tra bắt	nterne gói tii	et Ex	plore	và truy	cậ
Internet Explorer Image: To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: ••••• After you log on, you can add this server to your Favorites and return to it easily. Image: Log on gnonymously Log on Cancel	lếu khôr ttp://www server	ng được tỉ w.abc.com v C Trac	hì Test t 7à đăng nh K × w.msn.com/vi	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc	ITACK. Để kiểm id=UE09DH	Mở I tra bắt P	nterno gói tii	et Ex 1 ftp	plore	và truy	cậ
Internet Explorer Image: To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: Password: After you log on, you can add this server to your Favorites and return to it easily. Log on gnonymously Log on Cancel	lếu khôr ttp://www server	ng được tả w.abc.com v X I C ATTAC	hì Test t /à đăng nh ĸ × w.msn.com/vi × tools He	trên máy A nập mật khẩu. i-vn?pc=UE09&oc elp	ΓΤΑCK. Để kiểm id=UE09DH	Mở I tra bắt P	nterno gói tii	et Ex	plore	và truy	Ċậ
To log on to this FTP server, type a user name and password. FTP server: www.abc.com User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously	éu khôr tp://www server	ng được tả v.abc.com v X I ATTAC	hì Test t zà đăng nh ĸ × w.msn.com/vi x tools He	trên máy A nập mật khẩu. i-vn?pc=UE09&oc elp	ΓΤΑCΚ. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tin	et Ex	plore	và truy	cậj
FTP server: www.abc.com User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel	éu khôr tp://www server MSN le Edit V	ng được tỉ <u>v.abc.com</u> v Граттас https://www /iew Favorites et Explorer	hì Test t /à đăng nh K × w.msn.com/vi X 1 5 Tools He	trên máy A nập mật khẩu. i-vn?pc=UE09&oc elp	ΓΤΑCK. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tii	et Ex n ftp	plore	và truy	cậ
User name: administrator Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel	éu khôr tp://www server MSN e Edit V	ng được tỉ v.abc.com v To log on to t	hì Test trà đăng nh k × w.msn.com/vi x 1 s Tools He this FTP server,	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name an	TTACK. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tii	et Ex	plore	và truy	cậ
Password: •••• After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel	féu khôr ttp://www server MSN le Edit V	ng được tỉ v.abc.com v Trace ATTAC ATTAC ATTAC ATTAC ATTAC To log on to to FTP server:	hì Test trà đăng nh k × w.msn.com/vi x 1 s Tools He this FTP server, www.abc.co	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar	TTACK. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tii	et Ex	plore	và truy	Ċ Cậ
After you log on, you can add this server to your Favorites and return to it easily. Log on anonymously Log on Cancel	éu khôr tp://www server	ng được tỉ v.abc.com v Trace ATTAC ATTAC ATTAC ATTAC ATTAC To log on to t FTP server: User name:	hì Test trà đăng nh xà đăng nh x × w.msn.com/vi x tria transferences this FTP server, www.abc.com administrat	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar om	TTACK. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tin	et Ex	plore	và truy	cậ
Log on <u>a</u> nonymously	éu khôr ttp://www server	ng được ti v.abc.com v Trace Attace	hì Test trà đăng nh xà đăng nh x × w.msn.com/vi x 1 s Tools He chis FTP server, www.abc.co administrat •••••	trên máy Ar nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar om	TTACK. Để kiểm id=UE09DH	Mở I tra bắt	nterno gói tii	et Ex	plore	và truy	cậj
Log on Cancel	éu khôr ttp://www server MSN le Edit V	ng được tí v.abc.com v icom v icom v ng được tí ntrac After you log	hì Test tr và đăng nh k × w.msn.com/vi x 1 s Tools He this FTP server, www.abc.co administrat •••••	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar om tor	Favorites and	Mở I tra bắt	nterno gói tin	et Ex	plore	và truy	cậj
	Iếu khôr ttp://www SERVER	ng được the second seco	hì Test tr và đăng nh k × w.msn.com/vi x 1 s Tools He chis FTP server, www.abc.co administrat on, you can ad onymously	trên máy Ar nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar om tor	Favorites and	Mở I tra bắt	nterno gói tin	et Ex	plore	và truy	cậ
	Iếu khôr ttp://www server	ng được tí v.abc.com v ir attac https://www /iew Favorites et Explorer To log on to t FTP server: User name: Password: After you log Log on an	hì Test tr /à đăng nh k × w.msn.com/vi × 1 s Tools He this FTP server, www.abc.co administrat on, you can ad onymously	trên máy A' nập mật khẩu. i-vn?pc=UE09&oc elp , type a user name ar om tor Id this server to your	TTACK. Để kiểm id=UE09DH nd password. Favorites and Log on	Mở I tra bắt	nterno gói tin	et Ex	plore	và truy	Ċ Ċ

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

	Search Or A + A
FTB root at www.abc.com	
File Edit View Favorites Tools Help	
FTD post at your abo com	
r i r root at www.adc.com	
To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer .	
10/05/2024 02:12PM 24 <u>data.txt</u>	
	€ 125% ▼
	▲ 🕕 😼 🔁 2:21 PM ● 👘 🌄 05/10/2024

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

^LO	ocal Area Con	nection [Wireshark 1.	.10.5 (SVN Rev 54262 from	/trunk-1.10)]			
ile <u>E</u>	dit <u>V</u> iew (<u>Go</u> <u>C</u> apture <u>A</u> nalyze	e <u>S</u> tatistics Telephony <u>T</u> e	ools <u>I</u> nternals <u>H</u> elp)		
DO	<u>í</u>	🗀 🛅 🗙 🔁 🔍	. 🖗 🔿 주 🕹 🗐	I Q Q Q 🗹	🗃 🗹 🕵 %		
Eil+.	er ftp			Evoression	Clear An	oply Save	
THO	ei. Itp			Expression	Ciedi Ap	pply Save	
0.	Time	Source	Destination	Prote	ocol Length In	nfo	
	47 14.938	8890 192.168.1.	200 192.168.1	131 FTP	81 R	Response: 220	Microsoft FTP Service
	49 14.939	0330 192.168.1.	131 192.168.1	200 FTP	74 R	Request: USER	administrator
	50 14.939	1640 192.168.1.	200 192.168.1	131 FTP	96 R	Response: 331	Password required for administrator.
	52 14.939	2690 192.168.1.	131 192.168.1	200 FTP	64 R	Request: PASS	a@1
	53 14.941	1940 192.168.1.	200 192.168.1	.131 FTP	89 R	Response: 230	User administrator logged in.
	55 14.941	3730 192.168.1.	131 192.168.1	200 FTP	61 R	Request: CWD	/
	56 14.941	5390 192.168.1.	200 192,168,1	.131 FTP	83 R	Response: 250	CWD command successful.
	58 14, 941	6900(192,168,1,	131 192,168,1	.200 ETP	62 R	Request: TYPE	Α
	59 14 941	7960 192 168 1	200 192 168 1	131 FTP	74 R	Response: 200	Type set to A
	61 14 942	2040/192 168 1	131 192 168 1	200 FTP	60 R	Request: PASV	
	62 14 942	3750/102 168 1	200 192 168 1	131 FTD	105 P	Asnonse: 227	Entering Passive Mode (102 168 1 200 102 37)
	67 14 043	2260/102 168 1	131 102 168 1	200 ETD	105 K		Encering rassive mode (152,100,1,200,152,57).
	69 14 042	6420/102 162 1	200 102 168 1	121 FTP	109 0	locnonco: 125	Data connection already open: Transfer starting
	75 14 043	0400 192.100.1.	200 192.108.1		100 K	kesponse: 123	Tara connection an eauy open, fransfer starting.
	/5 14.943	9000/192.168.1.	200 192.168.1		/8 R	kesponse: 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

🕼 server 🗵	Г <mark>р</mark> аттаск ×					
🔍 Services						
File Action View	Help					
) 📑 🛛 🖬 🕨 🔳 🕪					
🤹 Services (Local)	🔍 Services (Local)	_				
	Telnet	Name 👻	Description	Status	Startup Type	Log On As
		Services	Enables ac		Automatic (D	Local Serv
	Stop the service	🔍 TP VC Gateway Service	ThinPrint		Manual	Local Syst
	Pause the service	🔍 TP AutoConnect Service	ThinPrint		Manual	Local Syst
	Kestart une service	🔍 Thread Ordering Server Provides			Manual	Local Serv
		🔍 Themes	Provides u		Disabled	Local Syst
	Description:	🔍 Terminal Services UserMode Port Redirector	Allows the r		Manual	Local Syst
	Enables a remote user to log on	🔍 Terminal Services Configuration	Terminal S		Manual	Local Syst
	programs, and supports various	Carterminal Services	Allows user	Started	Automatic	Network S
	TCP/IP Telnet clients, including	🖏 Telnet	Enables a r	Started	Automatic (D	Local Serv
	UNIX-based and Windows-	Sa Telephony	Provides T		Manua <mark>Start</mark>	
	is stopped, remote user access	🔍 TCP/IP NetBIOS Helper	Provides s	Started	Autom Stop	ł
	to programs might be	🔍 Task Scheduler	Enables a u	Started	Autom Paus	e
	unavailable. If this service is	System Event Notification Service	Monitors s	Started	Autom Resu	me
	disabled, any services that	Superfetch	Maintains a		Disable Rest	art
	start	SSDP Discovery	Discovers		Disable All Ta	isks 🕨 🛄
		Special Administration Console Helper	Allows admi		Manual	
		Software Licensing	Enables th	Started	Autom Refre	sh j
		SNMP Trap	Receives tr		Manual Prop	perties '
		Smart Card Removal Policy	Allows the		Manual	
		Smart Card	Manages a		Manual Help	·····
	1	👒 SL UI Notification Service	Provides S		Manual	Local Serv

- Tương tự cài ở máy ATTACK, Telnet client



Lab Report / @tailieuitiuh

- Chay Service ở máy ATTACK client



- Kiểm tra 2 máy đã ping nhau chưa



- Tạo user trên SERVER

SERVER ×	
🚘 Server Manager	
File Action View Help	
🗢 🔿 🖄 💼 🙆 📑 👔	
🔚 Server Manager (SERVER)	Users 3 User(s)
🗉 🚏 Roles	Name Full Name Description
🗉 🚮 Features	Built-in account for administe
Diagnostics	🐼 Guest Built-in account for guest ac
E In Configuration	STUSR_SER Internet Guest Acco Built-in account for anonym
	New User ? ×
Services	
📹 WMI Control	Username: HPL
🗉 🌆 Local Users and Group	Ha Dhual am
Users	
Groups	Description:
E E Storage	,
	Password:
	Confirm password:
	Licer must change password at next logen
	Coser cannot change password
	Password never expires
	Count is disabled
	Help Create Close
	1

- Add user vừa tạo vào group TelnetClients

	к ×		
File Action View Help	?		
Server Manager (SERVER) Roles Role	Groups 19 Group(s) Name Administrators Carptographic Op Cryptographic Op Performance Log Performance Log Performance Moni Power Users Print Operators Remote Desktop Cryptographic Desktop Cryptographic Op Cryptographic	Description Administrators have complet Backup Operators can overl Members of this group are all Members are allowed to laun Members are allowed to laun Members of this group can r Guests have the same acces Built-in group used by Intern. Members of this group can A Members of this group can A Members of this group can a Power Users are included for Members in this group are gr Supports file replication in a Users are prevented from m Members who have view-onl Members of this group have	Select Users General Select this object type: Description: Member system. Members: Select the ebject mes to select (axamples): SERVER Advanced OK Add Remove OK Cancel Apply Help

- Mở Wireshark coi các cổng protoco TELNET trên máy ATTACK client
- Ở máy client bật cmd và nhập lệnh "telnet"

q	
	ATTACK Google
	Administrator: C:\Windows\system32\cmd.exe
	Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.
	C:\Users\win7>ping 192.168.1.200
	Pinging 192.168.1.200 with 32 bytes of data:
	Reply from 192.168.1.200: bytes=32 time<1ms TTL=128 Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
1.1000	Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
	Reply from 192.168.1.200: bytes=32 time<1ms TTL=128
	Ping statistics for 192.168.1.200: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms
I	C:\Users\win7>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 cổng protoco TELNET và chọn follow TCP Stream

Icoal Area Connection [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]									
Eile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>I</u> ools <u>I</u> nternals <u>H</u> elp									
◉ ◉ 🛋 🔳 🔬 🖻 🛅 💥 😂 🗢 🛸 🗳) 77 👱 🗖 🗐 🔍 Q Q	. 🖭 👪 🖻	1 🕵 🔆 💢						
Filter: tcp.stream eq 0	Expression	n Clear	Apply Save						
No. Time Source 23 16.7615750192.168.1.131 24 16.7620770192.168.1.200 25 16.7621450192.168.1.131	Destination 192.168.1.200 192.168.1.131 192.168.1.200	Protocol Le TCP TCP TCP	ength Info 66 49162 > telnet [: 66 telnet > 49162 [: 54 49162 > telnet [/	5YN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 5YN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 ACK] Seq=1 Ack=1 Win=65536 Len=0					
28 16.7789190192.168.1.200 29 16.7792910192.168.1.131 30 16.7799670192.168.1.131 31 16.7799670192.168.1.131 32 16.7799740192.168.1.200 33 16.9867950192.168.1.200 33 16.9867950192.168.1.131 34 18.6533020192.168.1.200 36 18.653310192.168.1.131 37 18.8528420192.168.1.131 39 18.85580100192.168.1.131 41 21.8383490192.168.1.131 41 21.8383490192.168.1.131 42 21.8390180192.168.1.131 42 21.3390180192.168.1.131 43 22.4138610192.168.1.131 44 22.1388610192.168.1.131 44 22.1389810192.168.1.131 45 22.1398880192.168.1.200 46 22.2328820192.168.1.200 47 22.4174670192.168.1.131 47 22.4174670192.168.1.131 48 22.4174670192.168.1.131 48 22.4174670192.168.1.200 49 22.4174670192.168.1.131 40 22.4174670192.168.1.200 40 22.4174670192.168.1.200 41	$192.168.1.200\\192.168.1.200\\192.168.1.21\\192.168.1.200\\192.168.1.131\\192.168.1.200\\192.168.1.131\\192.168.1.200\\192.168.1.131\\192.168.1.200\\192.168.1.131\\192.168.1.200\\192.168.1.131\\192.168.1.200\\1$	TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET TELNET	As For Isos' Pheter Mark Packet (toggle) Ignore Packet (toggle) © Set Time Reference (toggle © Time Shift Packet Comment Manually Resolve Address Apply as Filter Prepare a Filter Colorize Conversation SCTP Follow TCP Stream Follow UDP Stream Follow UDP Stream Follow UDP Stream Follow SL Stream	<pre>ieq=31 Ack=65 Win=65536 Len=0 ieq=262 Ack=133 Win=65536 Len=0 ieq=594 Ack=453 Win=65024 Len=0 eq=595 Ack=454 Win=65024 Len=0 ieq=596 Ack=455 Win=65024 Len=0 ieq=596 Ack=55 Win=65024 Len=500 ieq=596 Ack=550 Ack=55</pre>					
© Frame 28: 75 bytes on wire (600 b © Ethernet II, Src: Vmware_c6:47:8d © Internet Protocol Version 4, Src:	its), 75 bytes captur (00:0c:29:c6:47:8d), 192.168.1.200 (192.1	ed (600 b Dst: Vmw 68.1.200)	Decode As Print Show Packet in New Windo	w Ja:79)					

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 cấp bởi bên thứ ba.

🕼 SERVER 🛛 🕞 ATTACK 🗡							
*Local Area Connection [Wireshark 1.10.	5 (SVN Rev 54262 from /trunk-1.10)]						- Ø S
<u>File E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u>	tatistics Telephony <u>T</u> ools Interna	als <u>H</u> elp					
o o ք 🖩 🔬 🖻 🛅 💥 🔁 🔍 🭕	• 🔅 🤪 7 👱 🗐 🗐 🔍 Q	🔍 🖸 👪 🗹 🕵 %	1.				
Filter: tcp.stream eq 0	Express	ion Clear App	bly Save				
 Time Source 23 16.7615750192.168.1.13 24 16.7620770192.168.1.20 25 16.7621450192.168.1.13 28 16.7789190192.168.1.20 	Destination 1 192.168.1.200 0 192.168.1.131 1 192.168.1.200 0 192.168.1.231	Protocol Length Inf TCP 66 49 TCP 66 te TCP 54 49 TCP 54 49 TELNET 75 Te	o 162 > telnet [SYM 10et > 49162 [SYM 162 > telnet [ACM 10et Data] Seq=0 Win=8192 Len= , ACK] Seq=0 Ack=1 Wi] Seq=1 Ack=1 Win=655	0 MSS=1460 WS=256 SACK_PE n=8192 Len=0 MSS=1460 WS= 36 Len=0	RM=1 256 SACK_PERM=1	
Follow TCP Stream							
	S	<pre>''''''''''''''''''''''''''''''''''''</pre>	SFUTLNTVER.SFUT S.E.R.V.E.R onsole 5.7 	NTMODE%(S.E.R.V.E.RS.E.R. (C.ISi. ISi. AWr.	NTLMSSPS.E.R.V.E.Ra	1. b. c c. o. m S. I	E.R.V.E.R
password: a@1 Server. \HPL> [14;1H.[K.[15;1H.[K.[16;1H.	H* [К. [17;1н. [К. [18;1н. [К. [.[3;1) 19;1H.[K.[20;1H.[I	l* . [5;1Н. [К. [6; <. [21;1Н. [К. [22;1	 LH. [K. [7;1Н. [K. [8;1Н. [I. [K. [23;1Н. [K. [24;1Н.	.[2;1HMicrosoft Telnet K.[9;1H.[K.[10;1H.[K.[11; [K.[25;1H.[K.[4;14H	= .[1н.[К.[12;1н.[К.[13	4;1HC:\User ;1H.[K.
Entire conversation (1648 bytes)							
Eind	ave <u>A</u> s <u>P</u> rint	ASCII	© EBCDIC	🖱 Hex Dum	p 🗇 C Arrays	Raw	
Help						Filter Out This Stream	Close
🚱 🥭 📜 🛛						- 🕩 🔂 🖞	7:13 PM

- Login: hpl
- Password a@1

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