MÔN TRIỂN KHAI AN NINH HỆ THỐNG

TH02 - Lab03 - WireShark

Phúc Lâm - 08/09/2024

I. TÌM HIỂU QUA BỘ TÀI LIỆU

II. Thực hành phân tích gói tin với Wireshark

1. Khởi động ứng dụng Wireshark

The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]	
<u>F</u> ile <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>T</u> ools <u>I</u> nternals <u>H</u> elp	
● ● ▲ ■ ▲ ⊨ ≞ × 2 ٩ ∻ ∻ ⇒ ∓ ± ≡ ≡ ٩ ٩	QE
Filter: 🗸 Expression Cle	ar App
WIRESHARK The World's Most Popular Network Proto Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)	col A
Capture	
Interface List Live list of the capture interfaces (counts incoming packets)	Ē
	Oper
Choose one or more interfaces to capture from, then Start	
June 1 Mare Network Adapter VMnet1	
🔏 Wi-Fi	
Local Area Connection* 2	
Capture Options Start a capture with detailed options	
Capture Help	

- Bước 1: cài đặt WinPcap_4_1_3.exe và Wireshark-win64-1.10.5.exe
- Bước 2: Khởi động Wireshark, chọn loại mạng cần quét. Sau đó nhấn "Start"
- Bước 3: Xem kết quả của việc bắt gói tin

Capturing from Wi-Fi [Wireshark 1.10.5 (SVN Rev 54262 from /true	nk-1.10)]	- 0 X
<u>File Edit View Go Capture Analyze Statistics Telephony</u>	<u>T</u> ools <u>I</u> nternals <u>H</u> elp	
_ ● ● ∡ ■ ∡ ⊨ ≞ x 2 < + + ⇔ 7	। 🛃 🗐 🖬 । 🔍 🔍 🕅 । 🕷	🗹 🍕 ¾ 🗱
Filter:	Expression Clear Apply Save	
No. Time Source Dest	tination Protocol	Length Info
1 0.0000000 192.168.1.89 49.	.213.95.49 TLSv1.2	239 Application Data
2 0.05816600 49.213.95.49 192	2.168.1.89 TLSv1.2	312 Application Data
3 0.10867900 192.168.1.89 49.	.213.95.49 TCP	54 61406 > https [ACK] Seq=186 Ack=259 Win=514 Len=0
4 0.43694200 a4:97:b1:56:97:9b Bro	oadcast ARP	42 who has 192.168.1.5? Tell 192.168.1.35
5 0.4/948800 192.168.1.65 224	4.0.0.251 MDNS	139 Standard query 0x0000 PTR _homekittcp.local, "QM" question PTR _companion-linktcp.local, "
6 0.49392/00 Te80::420:939D:8801:T1a9 TT0	02::TD MDNS	159 standard query 0x0000 PTR _nomexittcp.local, "QM" question PTR _companion-linktcp.local,
7 1.50532200 IntelCor_29:67:60 Bro	oadcast ARP	42 Who has 192.108.1.244? Tell 192.108.1.13
8 1.60481300 192.168.1.117 224	4.0.0.251 MDNS	82 standard query 0x0000 PTR _googlecasttcp.local, _QM question
9 1.60481600 Te80::8015:C352:63/5:99TC TTC	02::TD MDNS	102 standard query 0x0000 PTR _googlecasttcp.local, QM question
10 1.60935800 192.108.1.11/ 224	4.0.0.251 MDN5	102 Standard query 0x0000 PTR _googlecasttcp.local, @M question
11 1.809380001880::8015:0352:8375:9910 110	02::TD MDNS	102 standard query 0x0000 Pik _googlecasttcp.iocai, dM question
12 1.71501000 192.108.1.90 224	02::fb MDNS	122 Standard query 0x0000 PTR_STeep=proxy_upt. Total, om question
14 2 £1028600 £0801140c015228125150££ ££	02fb MDNS	101 standard query 0x0000 - A Br/20077344367 Josal "ON" question
14 2.010200001000;:49C0:Caao:25:0911 110	02::10 MDN5	Of standard query 0x0000 A BR/3077243AF9.10ca1, QM question
15 2.01028/00 Te80::49C0:Caa8:25:09TT TTO	02::1:3 LLMNR	45 Nethership Decent croup 224 0 0 251
10 2.70/10400 192.108.1.141 224	4.0.0.231 IGMPV2	46 Member Ship Report group 224.0.0.251
 Ethernet II, Src: bc:a8:a6:99:df:cc (bc:a8:a6:99:df:cc (bc:a8:a6:99:df:cc (bc:a8:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:a6:39:df:a6:39	:99:8ft:cC), Dst: 60:38:e0:a9:b2; 9(192:168.1.89), Dst: 49.213.95 6(61406), Dst Port: https (443)	3c (60:38:00:49:b2:3c) ,49 (49:12:55:49) , Seq: 1, Ack: 1, Len: 185
0000 60 38 e0 20 b2 3c bc 28 26 99 df cc 08 0	0.45.00 `8 < 5	
$ \begin{array}{c} conto \ ord \ conto \ $	9 31 GS 00	
● Wi-Fi: <live capture="" in="" progress=""> File: C:\Use Packets: 53 · Dis</live>	splayed: 53 (100.0%)	Profile: Default
	Q Search	l 📮 🚱 😑 🧐 📮 🧕 💽 📶 🔷 🔺 🔺 🖉 🖉

- 2. Thực hành phân tích gói tin với Wireshark
- Mục tiêu:
 - Thực nghiệm kiến thức mô hình TCP/IP
 - Hiểu cấu trúc các header cơ bản trường ở gói tin thu thập được
- Công cụ: sử dụng công cụ "Wireshark"
- Các mục chính
 - Phân tích quá trình ping
 - Phân tích quá trình kết nối HTTP
- a) Phân tích quá trình ping
- Bước 1: Mở wireshark và capture ở trên card mạng có kết nối internet
 - Cài đặt và mở wireshark như trên
 - Chọn card mạng "Hợp lý" để capture
 - o Ở đây tôi chọn "Wi-fi"
- Bước 2: vào cmd của máy tính ping 8.8.8.8
 - \circ Ipconfig

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . : fe80::a5dd:e1b3:5530:cfbf%15
IPv4 Address. . . . . . . . : 192.168.1.89
Subnet Mask . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . : 192.168.1.1
```

• Ping 8.8.8.8

Ο

```
C:\WINDOWS\system32\cmd. × + ~
Microsoft Windows [Version 10.0.22631.4037]
(c) Microsoft Corporation. All rights reserved.
C:\Users\y0ns2>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=36ms TTL=55
Reply from 8.8.8.8: bytes=32 time=71ms TTL=55
Reply from 8.8.8.8: bytes=32 time=45ms TTL=55
Reply from 8.8.8.8: bytes=32 time=137ms TTL=55
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 36ms, Maximum = 137ms, Average = 72ms
```

- Bước 3: Stop quá trình capture của wireshark



- Bước 4: Vào thanh filter của wireshark và nhập vào từ khóa "icmp" và ip.addr

• Từ khóa "icmp"

Capturing from Wi-Fi [Wireshark 1.10.5 (SVN Rev 542)	262 from /trunk-1.10)]					-
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp					
0 0 / 1 / b b x 2 9 4	🔿 🗛 🐺 🖳 🗐 🗐 🕀	Q Q 🖭 🌌 🕅 🕵	* 1			
			v.e. e⊡s			
Filter: icmp	 Expression 	Clear Apply Save				
No. Time Source	Destination	Protocol	Length Info			
1865 88.6318580 192.168.1.89	192.168.1.79	ICMP	74 Echo (ping) request	id=0x0001, seq=73/18688, ttl=	=128	
1866 88.6441600 192.168.1.79	192.168.1.89	ICMP	74 Echo (ping) reply	1d=0x0001, seq=73/18688, ttl=	=128 (request in 1865)	
1890 89.0399200 192.108.1.89	192.108.1.79	ICMP	74 Echo (ping) request	id=0x0001, Seq=/4/18944, Lt1=	=128 (reply in 1891)	
1901 90. 6571280 192. 168. 1. 89	192.168.1.79	TCMP	74 Echo (ping) repust	id=0x0001, seq=75/19200, tt]=	=128 (reply in 1902)	
1902 90.6746960 192.168.1.79	192.168.1.89	ICMP	74 Echo (ping) reply	id=0x0001, seg=75/19200, tt]=	=128 (request in 1901)	
1934 91.6723060 192.168.1.89	192.168.1.79	ICMP	74 Echo (ping) request	id=0x0001, seq=76/19456, ttl=	=128 (reply in 1935)	
1935 91.6847220 192.168.1.79	192.168.1.89	ICMP	74 Echo (ping) reply	id=0x0001, seq=76/19456, ttl=	=128 (request in 1934)	
			C:\WINDOWS\syst	tem32\cmd. × + ~	– 🗆 X	
			C:\Users\y0ns2	>ping 192.168.1.79		
			Dinging 102 16	9 1 70 with 22 bytes of d	lata .	
			Pinging 192.10	169 1 70, bytes -22 time-	12mc TTI -129	
			Deply from 192	168 1 70. bytes=32 time=	12ms $11L-120$	
			Repty from 192	160.1.79: Dytes=32 time=	10 ms 11L-120	
			Reply from 192	.168.1.79: Dytes=32 time=	12m- TTL-128	
			Reply From 192	.166.1.79: Dytes=32 time=	12MS 11L=128	
			Ding statistic	- (102 168 1 70.		
			Ping statistic	5 for 192.168.1.79:	-+ - 0 (00, 1)	
			Packets: S	ent = 4, Received = 4, Lo	st = 0 (0% coss),	
			Approximate ro	und trip times in milli-s	econds:	
			Minimum =	10ms, Maximum = 17ms, Ave	rage = 12ms	
4						
⊕ Frame 1865: 74 bytes on wire (592 bit	ts), 74 bytes captured (592	2 bits) on interface	0			
Ethernet II, Src: bc:a8:a6:99:df:cc € Src: bc:a8:a6:99:df:cc € Src: bc:a8:a6:99:df:cc Src: bc:a8:a6:99:df:a8:a6:99:df:cc Src: bc:a8:a6:99:df:cc Src: bc:a8:a	(bc:a8:a6:99:df:cc), Dst: (c:6b:1e:47:b7:7d (cc	::6b:1e:47:b7:7d)			
Internet Protocol Version 4, Src: 194 Internet Control Message Protocol	2.168.1.89 (192.168.1.89),	DST: 192.168.1.79 (1	192.168.1.79)			
Internet control Message Protocol						
0000 cc 6b 1e 47 b7 7d bc a8 a6 99 df	cc 08 00 45 00 .k.g.}	E.				
0010 00 3c e4 ed 00 00 80 01 d1 da c0) a8 01 59 c0 a8 .<	Y				
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71	72 73 74 75 76 ahiik]mr	oparstuv				
0040 77 61 62 63 64 65 66 67 68 69	wabcdefo) hì '				
Win Ein cline capture in program Dile: CAUse De	ckets: 2569 . Displayed: 9 (0.29/)			Des Eler Des	fault	_
WITH SIVE Capture in progress? File: C:\USE Pa	ckets, 2000 · Displayed: 0 (0.5%)			Profile: Det	lauit	

• Ip.addr

3. Mô phỏng tấn công arp qua victim truy cập server, internet phải thông qua attack.



Chuẩn bị: