Лабораторная работа: наблюдение за процессом трёхстороннего рукопожатия TCP с помощью программы Wireshark

Топология



Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

• Выберите подходящий интерфейс сетевого адаптера для захвата пакетов.

Часть 2. Захват, поиск и изучение пакетов

- Захватите данные веб-сеанса на узле www.google.com.
- Найдите соответствующие пакеты для веб-сеанса.
- Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

Исходные данные/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, сгенерированных между браузером ПК, где используется HTTP-протокол, и вебсервером, например www.google.com. При первом запуске приложения на узле, например HTTP или FTP, TCP устанавливает связь между двумя узлами с помощью трёхстороннего рукопожатия. Например, при просмотре интернет-страниц через веб-браузер ПК трёхстороннее рукопожатие позволяет установить связь между узловым ПК и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных сеансов TCP с разными веб-сайтами.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

Часть 1: Подготовка программы Wireshark к захвату пакетов

В части 1 вам необходимо запустить программу Wireshark и выбрать подходящие интерфейсы для начала захвата пакетов.

Шаг 1: Узнайте адреса интерфейсов ПК.

Для выполнения лабораторной работы вам нужно узнать IP-адрес своего ПК и физический адрес сетевого адаптера, который также называется МАС-адресом.

а. Откройте окно командной строки, введите ipconfig /all и нажмите клавишу ВВОД.

	_		_			
Physical Address					=	C8-0A-A9-FA-DE-0D
DHCP Enabled					=	Yes
Autoconfiguration Enable	ed					Yes
IPv4 Address					=	192.168.1.130(Preferred)
Subnet Mask	-	-	-	-	-	255.255.255.0
Lease Obtained					=	Saturday, December 01, 2012 1:43:35 PM
Lease Expires					-	Sunday, December 02, 2012 1:43:35 PM
Default Gateway					=	192.168.1.1
DHCP Server					=	192.168.1.1
DNS Servers					=	192.168.1.1
NetBIOS over Tcpip					=	Enabled

b. Запишите IP- и MAC-адреса, связанные с выбранным адаптером Ethernet, поскольку это и есть тот адрес источника, который нужно искать при анализе захваченных пакетов.

IP-адрес узла ПК: __

МАС-адрес узла ПК:

Шаг 2: Запустите программу Wireshark и выберите подходящий интерфейс.

- а. Нажмите кнопку Пуск и дважды нажмите на Wireshark.
- b. Запустив программу Wireshark, нажмите на параметр Interface List (Список интерфейсов).



с. В окне **Wireshark: Capture Interfaces** (Захват интерфейсов) установите флажок напротив интерфейса подключения к вашей локальной сети.

🥖 Wireshark	: Capt	ure Interfaces				- • ×
		Description	IP	Packets	Packets/s	
		Intel(R) PRO/1000 MT Network Connection		19	0	<u>D</u> etails
		Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details
<u>H</u> elp			Start	Stop	<u>O</u> ptions	<u>C</u> lose

Примечание. Если указано несколько интерфейсов и вы не уверены в выборе, нажмите кнопку **Details** (Сведения). Откройте вкладку **802.3 (Ethernet)** и убедитесь в том, что MAC-адрес соответствует тому, что вы записали в шаге 1b. Проверив данные, закройте окно со сведениями об интерфейсе.

Часть 2: Захват, поиск и изучение пакетов

Шаг 1: Нажмите кнопку Start (Старт), чтобы начать захват данных.

a. Откройте веб-сайт www.google.com. Сверните окно Google и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик, как показано на шаге b.

Примечание. Инструктор может предложить вам другой веб-сайт. В этом случае введите название или адрес сайта в соответствующее поле:

b. Теперь окно перехвата данных активно. Найдите столбцы **Source** (Источник), **Destination** (Назначение) и **Protocol** (Протокол).

<u>File Edit V</u> iew	<u>G</u> o <u>C</u> apture <u>A</u> nalyze	<u>Statistics</u> Telephony <u>T</u> oo	ls <u>I</u> nternals <u>H</u>	lelp
001	🔏 📄 🖬 🗶 🥭	् 🗢 🔿 🕹 🖞		€, €, 10, 17 📓 🗵 畅 % 🕱
Filter:			 Expression 	on Clear Apply Save
Time	Source	Destination	Protocol Leng	gth Info
1 0.0000000	00 192.168.1.130	157.55.130.157	ТСР	54 49166 > 40013 [ACK] Seq=1 Ack=1 Win=255 Len=0
2 0.0336960	00 157.55.130.157	192.168.1.130	TCP 1	144 40013 > 49166 [PSH, ACK] Seq=1 Ack=1 Win=83 Len=9(
3 0.0340640	00 192.168.1.130	157.55.130.157	тср	58 49166 > 40013 [PSH, ACK] Seq=1 Ack=91 Win=255 Len=
4 0.0694090	00 157.55.130.157	192.168.1.130	тср	60 40013 > 49166 [ACK] Seq=91 Ack=5 Win=83 Len=0
5 0.0694690	00 192.168.1.130	157.55.130.157	тср	66 49166 > 40013 [PSH, ACK] Seq=5 Ack=91 Win=255 Len=
6 0.1202030	00 157.55.130.157	192.168.1.130	тср	60 40013 > 49166 [ACK] Seq=91 Ack=17 Win=83 Len=0
7 0.1205590	00 157.55.130.157	192.168.1.130	тср	60 40013 > 49166 [PSH, ACK] Seq=91 Ack=17 Win=83 Len=
8 0.3277380	00 192.168.1.130	157.55.130.157	тср	54 49166 > 40013 [ACK] Seq=17 Ack=95 Win=255 Len=0
9 0.3601990	00 157.55.130.157	192.168.1.130	TCP	326 40013 > 49166 [PSH, ACK] Seq=95 Ack=17 Win=83 Len=
10 0.5616150	00 192.168.1.130	157.55.130.157	тср	54 49166 > 40013 [ACK] Seq=17 Ack=367 Win=254 Len=0
11 1.1404590	00 192.168.1.130	192.168.1.1	DNS	74 Standard query Oxded2 A www.google.com
12 1.1552470	00 192.168.1.1	192.168.1.130	DNS 1	154 Standard query response Oxded2 A 74.125.225.209 /
13 1.2325680	00 192.168.1.130	172.17.0.254	SNMP 1	119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.7
14 1.5765950	00 192.168.1.130	74.125.225.209	тср	66 49522 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
15 1.5767540	00 192.168.1.130	74.125.225.209	тср	66 49523 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W
16 1.6112180	00 74.125.225.209	192.168.1.130	тср	66 http > 49523 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=
17 1.6112930	00 192.168.1.130	74.125.225.209	тср	54 49523 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
18 1.6115530	00 74.125.225.209	192.168.1.130	тср	66 http > 49522 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=
•		III		
🕀 Frame 4: 6	50 bytes on wire (48	0 bits), 60 bytes c	aptured (48	0 bits) on interface 0
Ethernet 1	I, Src: Cisco-Li_f6	:84:6e (58:6d:8f:f6	:84:6e), Ds	t: QuantaCo_fa:de:Od (c8:Oa:a9:fa:de:Od)
🗄 Internet 🖡	rotocol Version 4,	Src: 157.55.130.157	(157.55.13	0.157), Dst: 192.168.1.130 (192.168.1.130)

B Transmission Control Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

Шаг 2: Найдите соответствующие пакеты для веб-сеанса.

Если компьютер включён недавно и еще не использовался для доступа к Интернету, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), службу доменных имен (DNS) и трёхстороннее рукопожатие TCP. На экране захвата в части 2, шаг 1 показаны

В данном документе содержится общедоступная информация корпорации Cisco.

все пакеты, которые ПК должен отправить на адрес www.google.com. В данном случае ПК уже имел запись ARP для шлюза по умолчанию, поэтому первым делом он создал DNS-запрос для преобразования www.google.com.

a. В кадре 11 показан DNS-запрос от ПК к DNS-серверу, призванный преобразовать доменное имя www.google.com в IP-адрес веб-сервера. ПК должен знать IP-адрес до отправления первого пакета на веб-сервер.

Назовите IP-адрес DNS-сервера, запрошенного компьютером.

- b. Кадр 12 показывает ответ DNS-сервера, содержащий IP-адрес www.google.com.
- с. Найдите соответствующий пакет, чтобы запустить процедуру трёхстороннего рукопожатия. В данном примере кадр 15 показывает начало трёхстороннего рукопожатия TCP.

Назовите IP-адрес веб-сервера Google.

d. Если вы получили много пакетов, связанных с TCP-соединением, воспользуйтесь фильтрами программы Wireshark. В поле фильтра программы Wireshark введите tcp и нажмите клавишу ВВОД.

<u>F</u> ile	<u>E</u> di	it <u>V</u> ie	w <u>G</u> o	<u>C</u> apt	ure <u>A</u> i	nalyze	<u>S</u> tatistics	Telepho	n <u>y T</u> ools	Internals	<u>H</u> elp									
0	۲				<u>.</u>	82	୍ଦ୍	• 🛸 🗳	₩ 🕹		⊕ ∈	20		¥) 🖪 :	% D	1			
File	r: to	cp								 Express 	ion C	lear	Apply	Save						
No.		ine in		Source	e		Destinati	on	Protoco	l Length	Info									
	1 0.	. 0000	00000) 192.	168.1	.130	157.55	.130.15	57 TCP	5	4 4916	б>	40013	[ACK]	Seq=	1 Ack≓	1 Win=	255 Len	=0	
	20.	. 0336	96000) 157.	55.13	0.157	192.16	8.1.130) TCP	14	4 4001	3 >	49166	[PSH,	ACK]	Seq=1	Ack=1	Win=83	Len=	90
	30.	.0340	64000) 192.	168.1	.130	157.55	.130.15	57 TCP	5	8 4916	6 >	40013	[PSH,	ACK]	Seq=1	Ack=9	1 Win=2	55 Le	n=4
	4 0.	. 0694	09000) 157.	55.13	0.157	192.16	8.1.130) TCP	6	0 4001	3 >	49166	[ACK]	Seq=	91 Ack	=5 Win	=83 Len	=0	
	50.	.0694	69000) 192.	168.1	.130	157.55	.130.15	57 TCP	6	6 4916	6 >	40013	[PSH,	ACK]	Seq=5	Ack=9	1 Win=2	55 Le	n=12
	60.	.1202	03000) 157.	55.13	0.157	192.16	8.1.130) TCP	6	0 4001	3 >	49166	[ACK]	Seq=	91 Ack	=17 Wi	n=83 Le	n=0	
	70.	.1205	59000	157.	55.13	0.157	192.16	8.1.130) TCP	6	0 4001	3 >	49166	[PSH,	ACK]	Seq=9	1 Ack=	17 Win=	83 Le	n=4
	80.	. 3277	38000) 192.	168.1	.130	157.55	.130.15	57 ТСР	5	4 4916	6 >	40013	[ACK]	Seq=	17 Ack	=95 Wi	n=255 L	en=0	
	90.	. 3601	.99000) 157.	55.13	0.157	192.16	8.1.130) TCP	32	6 4001	3 >	49166	[PSH,	ACK]	Seq=9	5 Ack=	17 Win=	83 Le	n=272
1	00.	.5616	515000) 192.	168.1	.130	157.55	.130.15	57 ТСР	5	4 4916	6 >	40013	[ACK]	Seq=	17 Ack	=367 W	in=254	Len=0	
1	41.	. 5765	95000) 192.	168.1	.130	74.125	.225.20)9 TCP	6	6 4952	2 >	http	[SYN]	seq=0	Win=8	192 Le	n=0 MSS	=1460	WS=4 SA
1	51.	.5767	54000) 192.	168.1	.130	74.125	.225.20)9 тср	6	6 4952	3 >	http	[SYN]	seq=0	Win=8	192 Le	n=0 MSS	=1460	WS=4 SA
1	61.	. 6112	18000	74.1	25.22	5.209	192.16	8.1.130) TCP	6	6 http	> 4	9523	[SYN, /	ACK]	Seq=0	۸ck=1 ۱	vin=143	00 Le	n=0 MSS=
1	71.	.6112	93000) 192.	168.1	.130	74.125	.225.20)9 тср	5	4 4952	3 >	http	[ACK]	seq=1	Ack=1	Win=6	5780 Le	n=0	
1	81.	. 6115	53000	74.1	25.22	5.209	192.16	8.1.130) TCP	6	6 http	> 4	9522	[SYN, /	ACK]	Seq=0	۸ck=1 ۱	vin=143	00 Le	n=0 MSS=
1	91.	.6116	514000) 192.	168.1	.130	74.125	.225.20)9 TCP	5	4 4952	2 >	http	[ACK]	seq=1	Ack=1	Win=6	5780 Le	n=0	
2	01.	.6136	646000) 192.	168.1	.130	74.125	.225.20)9 HTTP	61	9 GET	/ нт	TP/1.	1						
2	11.	.6516	62000	74.1	25.22	5.209	192.16	8.1.130) TCP	6	0 http	> 4	9523	[ACK] :	Seq=1	Ack=5	66 Win	=15488	Len=0	
٠ [
⊕ F	rame	e 4:	60 by	tes o	n wir	e (48	30 bits). 60 b	vtes can	tured (4	80 bit	s) (on int	erface	0					
₽ E	the	rnet	II. S	Src: 0	isco-	Li_f	5:84:6e	(58:6d	:8f:f6:8	4:6e). D	st: Ou	anta	aCo_fa	:de:0d	(c8:	0a:a9:	fa:de:	(b0		

■ Internet Protocol Version 4, Src: 157.55.130.157 (157.55.130.157), Dst: 192.168.1.130 (192.168.1.130) ■ Transmission Control Protocol, Src Port: 40013 (40013), Dst Port: 49166 (49166), Seq: 91, Ack: 5, Len: 0

Шаг 3: Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления ТСР.

- а. В нашем примере кадр 15 показывает начало трёхстороннего рукопожатия между ПК и вебсервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена зашифрованная информация из пакета в двух нижних панелях. Проверьте данные ТСР в панели сведений о пакетах (средний раздел основного окна).
- b. На панели нажмите на значок + слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.
- Слева от флажков нажмите на значок +. Обратите внимание на порты источника и назначения. С а также на установленные флажки.

Примечание. Чтобы отобразить все необходимые данные, скорректируйте размеры окон программы Wireshark.

File Edit View Go Capture Analyze Statistics Telephony Iools Internals Help
● ● 🗶 📕 🧟 🖻 📇 🗶 😂 🔍 💠 🗢 😽 💆 🗐 🗐 Q, Q, Q, 🖸 👹 🗹 🥵 % 🤮
Filter. tcp Expression Clear Apply Save
to: Time Source Destination Protocol Length Info Tore Source Log State Stat
14.1.576595000 102,168,1.130 74.125,225,200 TCP 66.49522 > http [SYN] 560=0 win=81.92 Len=0 MSS-1460 MS=4 SACK_PERM=1
151.370734000 192:106:1:130 74:123:223:209 TCP 064923 > TCC1p [STM] SeqPo WinBel22 CellWinS=1400 WSS=1540C WSS=1540 KSS=1540 KSS=
17 1.611293000 192.168.1.130 74.125.225.209 TCP 54 49523 > http [Ack] seq=1 Ack=1 win=65780 Len=0 18 1.611553000 74.125.225.209 192.168.1.130 TCP 66 http > 49522 [SvN, Ack] seq=0 Ack=1 win=1430 Len=0 MS5=1430 SACK_PERM=1 wS=64
□ Transmission Control Protocol, Src Port: 49523 (49523), Dst Port: http (80), Seq: 0, Len: 0 Source port: 49523 (49523) Destination port: http (80) [Stream index: 2] Sequence number: 0 (relative sequence number) Header length: 32 bytes □ □ 000
0000 58 66 57 68 66 57 68 66 57 68 66 57 68 66 57 68 66 57 68 57 68 56 57 68 58 56 58 56 57 58 58 57 57 58 57 57 58 57 57 58 57 5
M Frame (frame), 66 bytes Packets: 178 Displayed: 170 Marked: 0 Load time: 0:00.046 Profile: Default
Назовите номер порта источника ТСР
Как бы вы классифицировали порт источника?
Назовите номер порта назначения ТСР.
Как бы вы классифицировали порт назначения?
Какие установлены флажки?
На какое значение настроен относительный последовательный номер?

d. Чтобы выбрать следующий кадр в трёхстороннем рукопожатии, в меню программы Wireshark выберите параметр Go (Перейти), а затем Next Packet In Conversation (Следующий пакет коммуникации). В данном примере это кадр 16. Это ответ веб-сервера Google на исходный запрос

<u>File Edit View G</u> o	Capture Analyze Statistics	Telephony <u>T</u> ools <u>I</u> nter	nals <u>H</u> elp							
00 🖌 🔳 🙇	🖹 🛅 💥 🛃 🔍 🗢	🁒 🥥 ዥ 👱 🗐		0, 🖭 👹 🔟	🚯 🎇	Ħ				
Filter: tcp		• 1	xpression Clea	r Apply Save						
No. Time	Source	Destination	Protocol Ler	igth Info						
10 0.5616150	00 192.168.1.130	157.55.130.157	тср	54 49166 > 40	013 [ACK	(] Seq=17 Ack	=367 Win=2	254 Len=0		
14 1.5/65950	00 192.168.1.130	/4.125.225.209	тср	66 49522 > ht	p [SYN]	Seq=0 Win=8	3192 Len=0	MSS=1460 WS=	4 SACK_PERM=1	
15 1.5/6/540	00 192.168.1.130	/4.125.225.209	TCP	6649523 > MC	D SYN	Seq=0 Win=a	Ack-1 Win-	MSS=1460 WS=	4 SACK_PERM=1	DEDM-1 NC-64
10 1.0112180	00 74.125.225.209	74 125 225 200	TCP	54 40522 > bt	23 LSYN,	ACK Seq=0	ACK=1 WIN=	=14300 Len=0	M55=1430 SACK	_PERM=1 WS=64
18 1 6115530	00 74 125 225 209	192 168 1 130	TCP	66 http > 495	2 ESVN	ACK1 Sec-0	Ack-1 Win-	-14300 Len=0 L	MSS-1/130 SACK	PEPM-1 WS-64
(00 74.125.225.205	152.100.1.150		00 1100 2 455	.2 [314,	Acky beq-0	ACK-1 WITH	-14500 Een-0 1		
Transmission Co	ntrol Protocol, Src P	Port: http (80), Ds	t Port: 4952	23 (49523), Seq	: 0, Acl	k: 1, Len: 0				
Source port:	http (80)									
Destination p	ort: 49523 (49523)									
[Stream index	: 2]									
Sequence numb	er: 0 (relative se	equence number)								
Acknowledgmer	t number: 1 (relat	tive ack number)								
Header length	: 32 bytes									
■ Flags: 0x012	(SYN, ACK)									
000	= Reserved: Not s	set								
	- Condection Win	low Reduced (CWR):	Not set							
0	= ECN-Echo: Not	set	NOU SEC							
	= Urgent: Not set	t								
1 .	= Acknowledgment	Set								
C	= Push: Not set									
	0 = Reset: Not set									
···· ·	.1. = Syn: Set									
	0 = Fin: Not set									
Window size v	alue: 14300									
[Calculated w	indow size: 14300]									
E Checksum: 0xb	aes (validation disal	pled								
0000 c8 0a a9 fa 0010 00 34 49 cc 0020 01 82 00 50 0030 37 dc ba e5 0040 03 06	de 0d 58 6d 8f f6 8 00 00 33 06 4f 5f 4 c1 73 a2 e5 5b 91 3 00 00 02 04 05 96 0	4 6e 08 00 45 20 a 7d e1 d1 c0 a8 b 89 92 21 80 12 1 01 04 02 01 03	Xm .4I3. 0_ P.S [. 7	.nE J} ;!						

Назовите значения портов источника и назначения.

для начала сеанса.

Какие установлены флажки?

На какие значения настроены относительный последовательный номер и номер подтверждения?

 И, наконец, изучите третий пакет трёхстороннего рукопожатия в данном примере. Нажав на кадр 17 в верхнем окне, вы увидите следующую информацию в данном примере:

Eile Edit Yiew Go Capture Analyze Statistics Telephony Iools Internals Help
● ● 🖌 📕 🧟 🗁 📇 🗶 😂 🔍 💠 🜩 🖓 7 👱 🗐 🗐 Q. Q. Q. [2] 👪 🗵 🥦 💥 13
Filter Expression Clear Apply Save
Vo. Time Source Destination Protocol Length Info
12 1.155247000 192.168.1.1 192.168.1.130 DNS 154 Standard guery response 0xded2 A 74.125.225.209 A 74.125.225.210 A 74.125.225.212
13 1.232568000 192.168.1.130 172.17.0.254 SNMP 119 get-request 1.3.6.1.2.1.25.3.2.1.5.1 1.3.6.1.2.1.25.3.5.1.1.1 1.3.6.1.2.1.25.3.5.1
14 1.576595000 192.168.1.130 74.125.225.209 TCP 66 49522 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
15 1.576754000 192.168.1.130 74.125.225.209 TCP 66 49523 > http [SYN] seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16 1.611218000 74.125.225.209 192.168.1.130 TCP 66 http > 49523 [SYN, ACK] Seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
17 1.611293000 192.168.1.130 74.125.225.209 TCP 54 49523 > http [ACK] seq=1 Ack=1 win=65780 Len=0
18 1.611553000 74.125.225.209 192.168.1.130 TCP 66 http > 49522 [SYN, ACK] seq=0 Ack=1 win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
٠
In administer port: 49523 (49523) District fittp (60), Seq. 1, Ack. 1, Len. 0 Source port: 49523 (49523) Destination port: (1 (relative sequence number) Acknowledgment number: 1 (relative ack number) Header length: 20 bytes Flags: NOID (Ack) 000 Reserved: NOT set
0010 00 28 20 38 40 00 80 06 00 00 c0 a8 01 82 4a 7d . (8%

Изучите третий и последний пакет рукопожатия.

Какие установлены флажки?

Для относительного последовательного номера и номера подтверждения в качестве исходного значения выбрана единица. Соединение TCP настроено. Теперь можно начать передачу данных между ПК источника и веб-сервером.

f. Закройте программу Wireshark.

Вопросы на закрепление

- 1. В программе Wireshark доступны сотни фильтров. В большой сети может быть множество фильтров и различных типов трафика. Какие три фильтра в списке будут наиболее полезны для сетевого администратора?
- 2. Как ещё можно использовать программу Wireshark в производственной сети?