XCTF-MISC-新手区-功夫再高也怕菜刀





87 篇文章 22 订阅 订阅专栏





解题步骤

1、使用binwalk提取文件

C# binw	t <mark>⊗ kal</mark> walk <u>a</u>	i)-[~/桌面] cfff53ce3fa4e2	bbe8654284dfc18e1.pcapng		
DECIMAL	F.SR ML	HEXADECIMAL	DESCRIPTION		
663085		0×A1E2D	xz compressed data		
664045		0×A21ED	xz compressed data		
812025		0×C63F9	xz compressed data		
814001		0×C6BB1	xz compressed data		
1238637		0×12E66D	xz compressed data		
1240937		0×12EF69	xz compressed data		
1391563		0×153BCB	xz compressed data		
1393067		0×1541AB	xz compressed data		
1406647		0×1576B7	xz compressed data		
1412887		0×158F17	xz compressed data		
1422689		0×15B561	Zip archive data, encr	ypted at least v2.0	to extract, compressed si
ze: 52,	uncom	pressed size:	40, name: flag.txt		https://blog.csdn.net/qq_41617034

2、使用foremost分离文件



(root@ kali)-[~/桌面/output] ┃ audit.txt zip

3、该压缩包解压需要密码

🛃 📙 🚽	<u> </u>	提取	zip				- 🗆	×				
+ ±0 ▶ □ 到快复制	共享 道有 ● ● 目 ● 私助	压缩的又件夹工具 至 走方式 移动到 复制到	★ 重	新建项目 新建	∃ •] •	 ☑ 打开 ▼ ☑ 0% 正在提取 	全部选择 C:\Users\1stPea	^ () k\D p\zip\00	002778.zip		- 🗆	×
方问	★ 剪切 剪贴板	* * #	◆ 目织	文件夹 新建		已用时间: 剩余时间:		00:00:02	总大小: 速度:			40
\rightarrow \checkmark \uparrow	_ > zip >			*	ō	又任: 压缩率:	输入	 密码		×		0
🕻 快速访问	^ 名称	^		修改日期	AD.	≝ 正在提取	输入	\密码:				
三 桌面	* 00	002778		2021/6/18 16:43	2	flag.txt						
👆 下载	≠ 00	002778.zip		2021/6/18 16:42	Z	1		見示変码(S)		_		_
🔮 文档	*											
▶ 图片	*							确定	取消			
💻 此电脑	*											
🧧 回收站	*											g_416 <mark>1703</mark>

4、使用wireshark分析该数据包,搜索flag,找到66666.jpg

acfff53ce3fa4e2bbe8654284dfc18e1.pcapng

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(E) 帮助(H)

◢ ■ ∅ ◎ | _ 🗅 🕅 🗙 🖻 | ९ ⇔ ⇔ 🕾 🗿 📃 🗮 ९, ९, ९, म

. É	/用显示过滤器 ··· ⟨Ctrl-/⟩				表达式…	+
	分组字节流 ∨ 宽?	窄 🚽 🗆 区分大	マンション マンド マンド・ション マントレージ マンチャック マンチャップ マンチャッチャップ マンチャッチャップ マンチャップ マンチャッチャッチャップ マンチャップ マンチャッチャッチャッチャッチャッチャッチャッチャッチャッチャッチャッチャッチャッチ	flag	査找 取消	<u>ا</u>
No.	Time	Source	Destination	Protocol	Length Info	^
	1142 49.897175062	219.216.128.25	192.168.25.128	TCP	1434 80 → 58432 [PSH, ACK] Seq=175261	
	1143 49.897215668	192.168.25.128	219.216.128.25	TCP	54 58432 → 80 [ACK] Seq=145 Ack=1766	
+	1144 50.098716397	192.168.43.83	192.168.25.128	HTTP	300 HTTP/1.1 200 OK (text/html)	
	1145 50.098792302	192.168.25.128	192.168.43.83	TCP	54 47856 → 80 [ACK] Seq=205239 Ack=2	
	1146 50.134447510	192.168.25.128	192.168.43.83	TCP	290 47856 → 80 [PSH, ACK] Seq=205239 …	
	1147 50.138633287	192.168.43.83	192.168.25.128	TCP	60 80 → 47856 [ACK] Seq=247 Ack=2054	
-	1148 50.138903657	192.168.25.128	192.168.43.83	HTTP	777 POST /upload/1.php HTTP/1.1 (app	
	1149 50.140816842	192.168.43.83	192.168.25.128	TCP	60 80 → 47856 [ACK] Seq=247 Ack=2061	
	1150 50.147576455	192.168.43.83	192.168.25.128	HTTP	515 HTTP/1.1 200 OK (text/html)	
	1151 50 189982026	192 168 25 128	192 168 /13 83	тср	5/ /7856 → 80 [ACK] Seg=206198 Ack=7	×
	Type: IPv4 (0x080	0)				^
> 1	nternet Protocol Ve	ersion 4, Src: 192.168	3.43.83, Dst: 192.1	168.25.128		
> T	ransmission Control	l Protocol, Src Port:	80, Dst Port: 4785	56, Seq: 247,	, Ack: 206198, Len: 461	
> H	ypertext Transfer F	Protocol				
× L	ine-based text data	a: text/html (7 lines))			
	-> ./\t2017-12-08	11:42:11\t0\t0777\n				
	/\t2017-12-08 1	1:39:10\t4096\t0777\n				
	1.php\t2017-12-08	11:33:16\t33\t0666\n				
	6666.jpg\t2017-12	-08 11:42:11\t102226\	t0666\n			
	flag.txt\t2017-12	-08 11:35:29\t17\t066	6\n			
	hollo zin\+2017 1	2 08 00.22.26/+22//+0	666\n			~
016	0 30 39 36 09 30 3	37 37 37 0a 31 2e 70	68 70 09 32 096	0777 ·1.php	- 2	^
017	0 30 31 37 2d 31 3	32 2d 30 38 20 31 31	3a 33 33 3a 017	-12-0 8 11:33	3:	
018	0 31 36 09 33 33 0	09 30 36 36 36 0a 36	36 36 36 2e 16 :	33-06 66-6666	6.	
019	0 6a /0 6/ 09 32 3	30 31 37 20 31 32 20	30 38 20 31 Jpg	2017 -12-08	1	
01a	0 36 36 36 0a 66 0	5 61 67 2 74 78 74	09 32 30 31 666	$\frac{1102220}{\text{flag}}$	-0 01	
010	0 37 2d 31 32 2d 3	30 38 20 31 31 3a 33	35 3a 32 39 7-12	2-08 11:35.2	29	
01d	0 09 31 37 09 30	36 36 36 0a 68 65 6c	6c 6f 2e 7a · 17	·0666 ·hello.	 .Z	
01e	0 69 70 09 32 30	31 37 2d 31 32 2d 30	38 20 30 39 ip 2	2017- 12-08 0	09	
01f	0 3a 33 32 3a 33 3	36 09 32 32 34 09 30	36 36 36 0a :32	:36.2 24.0666	6 -	
020	0 7c 3c 2d		<-			7034

5、查找6666.jpg

	acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
--	---

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

🔟 🗏 🙆 📙 🔚 🕱 🗳 I 9. 🗢 🗢 🕾 🗿 💆 🚍 🔍 9. 9. 9. 1

	top.	stre	am eq 7										\times		表达式…	• •	+
		分组	字节流 ~ 宽窄	ž v	🗌 区分大小写	字符串	\sim	6666.jpg						查找	取	肖	
1	ło.		Time	Source	Destina	ation		Protocol	Length	Info							^
		884	46.312696198	192.168.25.12	8 192.1	.68.43.83		TCP	4434	47856	→ 80	[ACK]	Seq=24	10 Ack=	1 Wi		
		885	46.312968917	192.168.25.12	8 192.1	.68.43.83		TCP	4434	47856	→ 80	[ACK]	Seq=46	520 Ack	=1 W		
		886	46.314913898	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=24	0 Wi		
		887	46.314950323	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=17	00 W		
		888	46.314956407	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=31	.60 W		
		889	46.314960243	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=46	20 W		
		890	46.314964432	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=60	80 W		
		891	46.314968764	192.168.43.83	192.1	68.25.128		TCP	60	80 → 4	17856	[ACK]	Seq=1	Ack=75	40 W		
		892	46.314972668	192.168.43.83	192.1	68.25.128		TCP	60	80 ÷ 4	17856	[ACK]	Seq=1	Ack=90	00 W		5

> Frame 884: 4434 bytes on wire (35472 bits), 4434 bytes captured (35472 bits) on interface 0

> Ethernet II, Src: Vmware_21:b8:f4 (00:50:56:21:b8:f4), Dst: Vmware_f5:c2:5f (00:50:56:f5:c2:5f)

> Internet Protocol Version 4, Src: 192.168.25.128, Dst: 192.168.43.83

> Transmission Control Protocol, Src Port: 47856, Dst Port: 80, Seq: 240, Ack: 1, Len: 4380

https://blog.csdn.net/qq_41617034

6、追踪TCP流,并将FFD8至FFD9的所有内容复制到010Editor或Winhex中,保存为xx.jpg

POST /upload/1.php HTTP/1.1	^
User-Agent: Java/1.8.0 151	
Host: 192.168.43.83	
Accept: text/html. image/gif. image/ipeg. *: g=.2. */*: g=.2	
Connection: keen-alive	
Content_type: application/x_www_form_uplencoded	
Content Longth: 20/000	
content-Length. 204333	
da-weval.	
(Daseo4_decode(\$_POST[action])); action=Qatdav322AQ01mhpc3b57A172AJ9D3J21	
VJaG80110%2B+C1pUZsKZj11YXNINJK+ZGVJDZKIKCK+UE9TVFs1eJE1XSK/JGM9JF9QT1NUW	
yJ6MiJdOyRjPXN0c19yZXBsYWN1KCJcciIsIiIsJGMpOyRjPXN0c19yZXBsYWN1KCJcbiIsIi	
IsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWN	
vZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXR1KGZvcGVuKCRmLCJ3IiksJGJ1	
Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x	
1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE000104A46494600010101007800780000FFDB00	
4300010101010101010101010101010101010101	
10101010101010101010101010101010101010	
01	
10101010101010101010101010101010101010	
2200021101031101FFC4001F00000105010101010101000000000000000	
708090408FFC40085100002010303020403050504040000017D0102030004110512213141	
061351610722711432819141082342B1C11552D1F02433627282090416171819142526272	
8292034353637383930434445464748494053545556575859546364656667686966737475	
767778797A838/85868788898A92939/95969798999A5546566768996676869566757778	
787777777777777777777777777777777777777	
A0BFFC400B511000201020404030407050404000102770001020311040521310612415107	
61/11322328108144291A1B1C109233352F01562/2D10A162434E125F11/18191A262/282	
92A35363/38393A434445464/48494A535455565/58595A636465666/68696A/3/4/5/6//	
78797A82838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B	
8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8	
F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012B	
CF5E30056C4310192E7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF0096	
4920600CF2966C0C11CF710E22AD6F197C940E9020A971C673D7237790C1D00EC0623170FF	~
分组 883.53 客戶欄 分组,2 服务器 分组,3 turn(s).点击选择。	
整个对话 (206 kB)	-

7、复制粘贴选择ASCII Hex



🏭 WinHex - [未命名]

🏭 文件(F)	编辑(E)	搜索(S)	导航(N)	查看(V)	工具(T)	€₩]	具(I)	选	项(O)	窗](W)	帮助	(H)														
案件数据				06	i 🔒 👙	ء 🔊	7 🛀		5	b C	3 6	BB 10	01-5 10	A	#	HE×	¢,≩ ;	HEX	→ -{	¥ 🔶		3	3 🎖	» 📖	<u>,</u>	<u>ه</u> ا	
文件(L) 编	辑(<u>D</u>)			未命名																							
				Off	set	0	L 2	3	4	5	6 7	8	9	10	11 :	12 1	13 1	4 15		AN	SI A	SCII	~				
				0000	00000	FF D	B FF	E0	00	10 4	A 46	49	46	00	01 (01 0	01 0	0 78	ÿØÿä	à JF	IF	х					
				0000	00016	00 78	3 00	00	FF I	DB 0	0 43	00	01	01	01 (01 0	01 0	1 01	х	ÿΰ C							
				0000	00032	01 0	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	00048	01 0	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	00064	01 03	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	08000	01 03	L 01	01	01 (01 0	1 01	01	FF	DB	00 4	43 0	01 0	1 01			ÿÛ	С					
				0000	00096	01 03	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	00112	01 03	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	00128	01 03	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 0	1 01									
				0000	00144	01 03	L 01	01	01	01 0	1 01	01	01	01	01 (01 0	01 F	F CO				ÿÀ					
				0000	00160	00 1	L 08	01	39	01 E	2 03	01	22	00	02 3	11 0	01 0	3 11		9 â							
				0000	00176	01 FI	5 C4	00	1F (00 0	0 01	05	01	01	01 (01 0	01 0	1 00	ÿÄ								
				0000	00192	00 00	00	00	00	00 0	0 01	02	03	04	05 (06 0	07 0	8 09									
				0000	0208	0A 01	3 FF	C4	00 1	B5 1	0 00	02	01	03	03 (02 0	04 0	3 05	ÿŻ	Åμ							
				0000	00224	05 04	1 04	00	00	01 7	D 01	02	03	00	04 :	11 0	05 1	2 21		}		1					
				0000	00240	31 43	L 06	13	51	61 0	7 22	71	14	32	81 9	91 Z	Al 0	8 23	1A	Qa "	g 2	`i #					
				0000	00256	42 B.	L C1	15	52 1	D1 F	0 24	33	62	72	82 (09 0	DA 1	6 17	B±A	RNð\$:	3br,						
				0000	00272	18 19	9 1A	25	26 :	27 2	8 29	2A	34	35	36 :	37 3	38 3	9 3A	1	\$&'()	*456	789:					
				0000	0288	43 44	45	46	47	48 4	9 4A	. 53	54	55	56 9	57 5	58 5	9 5A	CDEI	FGHIJ:	STUV	WXYZ					
				0000	00304	63 64	1 65	66	67	68 6	9 6A	. 73	74	75	76 '	77 7	78 7	9 7A	cdef	fghij	stuv	wxyz					
				0000	00320	83 84	1 85	86	87	88 8	9 8A	. 92	93	94	95 9	96 9	97 9	8 99	f ,,1	t‡^%S		~тм					
				0000	00336	9A A:	2 A3	A4	A5 1	A6 A	7 A8	A9	AA	B2	B3 I	B4 E	35 B	6 B7	ŝ¢£≯	¤¥¦§"(gas 3	°µ¶ ·					
				0000	00352	B8 B	BA	C2	C3 (C4 C	5 C6	C7	C8	C9	CA 1	D2 I	03 D	4 D5	, 1 ° Z	AAAAÆ	ÇEEE	0000					
				0000	00368	D6 D'	7 D8	D9	DA 1	El E	2 E3	E4	E5	E6	E7 I	E8 E	29 E	A Fl	0רt	JUàâã	ääæç	ėėėñ					
				0000	00384	F2 F:	3 F4	F5	F6 :	F7 F	8 F9	FA	FF	C4	00 :	1F (01 0	0 03	òóôố	öö÷øù	uÿA						

8、解压密码在图片中



9、使用解压密码解密zip文件

🔲 I 🗹 🛄 🕶 I		送収 ²¹	压缩率:		压缩后大小:
文件 主页	共享 查看 压	缩的文件夹工具		+++	
★ 复制 速访问	 □ □ 結贴快速方式 約 約 第 第 約 第 5 第 5 5		正在提取 flag.txt	輸入密码: 輸入密码: 	
$\leftarrow \rightarrow \checkmark \uparrow$	> zip >			确定	取消
	▲ 2段	^			
📌 快速访问	1010				
三 桌面	* 0000277	8		后台(B)	暂停 <mark>(P)</mark>
👆 下载	× 0000277	'8.zip			
🔮 文档	*				

10、解压后的文件中找到flag.txt

zip	> 00002778	ٽ ~	∕○ 搜索"00	002778"							
^	へ 名称	修改日期	类型	大小							
	flag.txt	2017/12/8 17:28	文本文档	1 KB							
	flag.txt - 记事本										
文作	牛(F) 编辑(E) 格式(O) 查看(V) 帮助)(H)									
flag	flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}										