xctf攻防世界 MISC高手进阶区 flag_universe

原创

Ⅰ8947943 ● 于 2022-01-17 20:26:10 发布 ● 5579 ☆ 收藏 1
 分类专栏: <u>攻防世界misc之路</u> 文章标签: <u>misc</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/l8947943/article/details/122547543</u>
 版权



<u>攻防世界misc之路 专栏收录该内容</u>

68 篇文章 2 订阅

订阅专栏

1. 进入环境,下载附件

下载后,给的是pcapng文件,果断使用wireshark打开,在其中搜索关键词flag,发现如下:

	flag_universe.pcapng					– 🗆 X
文件	(F) 编辑(E) 视图(V)	跳转(G) 捕获(C)	分析(<u>A</u>) 统计(<u>S</u>) 电话(<u>Y</u>)	无线(<u>W)</u> 工具(<u>T</u>) 帮助(<u>H</u>)		
	🔳 🖉 💿 📙 🛅 🗙	🔄 🍳 👄 🔿 🕯	🛎 T 🕹 🥃 🔳 Q Q	€. Ⅲ		
t	cp.stream eq 16					+
	 分组字节流 ~		✓ □ 区分大小写 字符	串 flag		查找 取消
No.	Time	Source	Destination	Protocol Leng	th Info	
	733 71.14325557	1 172.17.0.1	172.17.0.2	2 TCP	74 53670 → 21109	[SYN] Seq=0 Win=29
	735 71.14328265	1 172.17.0.2	172.17.0.1	ТСР	74 21109 → 53670	[SYN, ACK] Seq=0 A
	737 71.14330747	1 172.17.0.1	172.17.0.2	2 TCP	66 53670 → 21109	[ACK] Seq=1 Ack=1
	744 71.14407188	9 172.17.0.2	172.17.0.1	L FTP-DA 3	95 FTP Data: 329	bytes (PASV) (LIST
	745 71.14409462	9 172.17.0.1	172.17.0.2	2 TCP	66 53670 → 21109	[ACK] Seq=1 Ack=33
	746 71.14412958	9 172.17.0.2	172.17.0.1	L TCP	66 21109 → 53670	[FIN, ACK] Seq=330
<						>
	Command: LIST -a]					1
	ommand frame: 739					
[Current working d	lirectory: /]				
✓ L	ine-based text da	ta (5 lines)				
	drwxrwxrwx 1	ftp ftp	384 Sep 19	07:55 .\r\n		
	drwxrwxrwx 1	ftp ftp	384 Sep 19	07:55\r\n		
1	-rwxrwxrwx 1	ftp ftp	41 Sep 19	07:52 flag.txt\r\n		
<u> </u>	-rwxrwxrwx 1	ftp ftp	1178630 Sep 19	07:55 new_universe.png	g\r\n	×
001	0 37 3a 35 35 20) 2e 2e 0d 0a	2d 72 77 78 72 77 7	8 7:55rwxrwx		1
000	0 72 77 78 20 20	0 20 20 31 20	66 74 70 20 20 20 2	0 rwx 1 ftp		
000	0 20 20 66 74 70	0 20 20 20 20	20 20 20 20 20 20 20 2	0 ftp		
000	20 34 31 20 53	3 65 70 20 31 7 2- 74 78 74	39 20 30 37 3a 35 3	2 41 Sep 19 0/:52		
001	20 00 0C 01 07	2 E 7 E 7 E 7 E 7 E 7 E 7 E 7 E 7 E 7 E	31 20 66 74 70 20 2	2 Hiag. LX L····rwxr		
011	0 20 20 20 20 66	5 20 20 20 20 5 74 70 20 20	20 20 20 20 20 20 31 3	1 ftn 11		
012	37 38 36 33 30	20 53 65 70	20 31 39 20 30 37 3	a 78630 Sep 19 07:		
013	35 35 20 6e 65	5 77 5f 75 6e	69 76 65 72 73 65 2	e 55 new_u niverse.		
014	10 70 6e 67 0d 0a	a 2d 72 77 78	72 77 78 72 77 78 2	0 png··-rw xrwxrwx		
015	0 20 20 20 31 20	0 66 74 70 20	20 20 20 20 20 66 7	4 1 ftp ft		
016	70 20 20 20 20 20	20 20 20 31	31 33 33 35 33 35 2	0 p 1133535		
0	🝸 字节 325-394: Text	t item (text)			分组: 1012 · 已显;	r: 806.1941 (1983) 147943

2. 问题分析

追踪流

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 16) · flag_universe.pcapng	_	×

	drwxrwxrwx drwxrwxrwx - rwxrwxrwx - rwxrwxrwx - rwxrwxrwx	1 ftp 1 ftp 1 ftp 1 ftp 1 ftp	ftp ftp ftp ftp	384 384 41 1178630 1133535	Sep 19 Sep 19 Sep 19 Sep 19 Sep 19	07:55 07:55 07:52 07:55 07:55	flag.txt new_univ universe	t verse.p e.png	ong	3
0	客户端 分组, 1 服务制	# 分組, 0 turn(s).								
3	整个对话(329 byte	s)		\sim	Show d	ata as A	SCII	~ 流	16 🌻	
갵	ē找:							查找下	$-\uparrow(\underline{N})$	
		滤掉此流	打印	另存为…	Ì	20	Close CSDN @	н. 1894	1p 7943::	

可以看到,采用的ftp协议,对文件flag.txt、new_uniberse.png和universe.png文件进行了上传,因此,解题关键是把上传的 图片给还原出来。

找到new_uniberse.png

如图:

📕 📕	niverse.pcapng —	οx				
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(T) 帮助(H)					
	(🐵 📙 🛅 🕱 🖆 🍳 👄 🗢 🕾 🕢 👲 🚍 🔍 Q. Q. Q. X.					
ftp-d	ta	+				
	Destination Protocol Length Info	^				
0.1	172.17.0.2 FTP-DA 3184 FTP Data: 3118 bytes (PASV) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA 59434 FTP Data: 59368 bytes (PASV) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA… 55090 FTP Data: 55024 bytes (PASV) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA… 10202 FTP Data: 10136 bytes (PASV) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA… 8754 FTP Data: 8688 bytes (PASV) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA… 56538 FTP Data: 56472 bytes (PA <mark>S</mark> V) (STOR /new_universe.png)					
0.1	172.17.0.2 FTP-DA 37714 FTP Data: 37648 bvtes (PASV) (STOR /new universe.png)	,=*(
> Inte	net Protocol Version 4, Src: 1/2.1/.0.1, Ust: 1/2.1/.0.2	^				
Tran	mission Control Protocol, Src Port: 49316, Dst Port: 21103, Seq: 11/5513, Ack: 1, Len: 3118	_				
	aca (Silo Dytes data)					
	ip method: PASV1					
	and: STOR /new universe nng]					
Com	ind frame: 650					
[Cur	ent working directory:]	~				
0000	2 42 oc 11 60 62 62 42 f2 67 df 33 68 60 45 60					
0010	$c_{12} = c_{11} = c_{12} = c_{12} = c_{12} = c_{13} = c$					
0020	00 02 c0 a4 52 6f 53 b5 ab b3 2b b5 b9 ff 80 19 ····RoS···+····					
0030	00 e5 64 7a 00 00 01 01 08 0a 24 c6 9c eb b1 9f ···dz·····\$·····					
0040	:d f7 ed 3c b9 d3 27 67 4d a8 5e bd fa 55 ee d2 ···<··'g M·^··U··					
0050	57 9f 7d 7a 7b 7d 1b 2a 1f 97 71 bb db 9c 9c 9c g·}z{}·* ··q····					
0060	A4 1c et ee ee /c /0 e3 d1 a4 aa 43 ec d2 ae dd ····· p····C····					
0070	א איט פט כי סט סט סט איט א מע 40 מי 40 מי 40 מי 00 איט פע כי סט סט סט איט סט פט א סט 40 מי 40 מי 40 מי 40 מי 40 או 30 אוא איז איז איז איז איז איז איז איז איז אי					
0090	a = a = a = a = a = a = a = a = a = a =					
00a0	06 f7 55 22 ea aa f2 6d 1b b7 db 6d ce 60 6b c0 ···U"····m ····m·`k·					
0060	ie e6 10 52 08 70 dd 51 8c 79 b3 de a2 ca ab 52 ^R·p·Q -yR					
00c0	ef 62 b1 b8 ba ba da ed 76 88 dc c6 18 2f 2e 2e ·b····· v···/	~				
0 🗹	○ 2 flag_universe. poapng 分组: 1012 · 已显示: 254①终□》》(觀點9 準預4日月3:					

把找到的上传图片追踪流导出来,在这里推荐使用工具用NetworkMiner打开流量包,他妈的电脑安装后缺少什么dll文件, 人麻了,手工导出吧。

追踪流,复制原始数据,到winhex中建立10MB的文件并粘贴进去,最终以为png文件命名。如图:



CSDN @18947943

使用zstag隐写发现

先安装工具,参考博客: https://www.cnblogs.com/lzkalislw/p/12831430.html 使用命令进行分离,如图:



得到最终的答案: flag{Plate_err_klaus_Mail_Life}

StegSolve发现隐写

ш.

如图,该工具也可以找到隐写:

	– 🗆 X
Extract Preview	
666cc61677b506cc61 74655f6572725f6b flag{Pla te_err_k 6c6175735f4d6169 6c5f4c6966657d0a laus Mai 1 Life}. db71b91c4954aa56 a49131b6e38e3724 .q.IT.V .17\$ 49256a56ab562e49 1b71b71c71c71b91 I%jV.V.I .qq b6e38dc6e48e36dc 8e392471c7239249 69\$q.#.1 1b8db7239238db6d b8e39247248db6e4 #.8.mG\$ 8e48e37246e48e39 1c6dc9248e48dc71 .H.rF9 .m.\$.H.q b72471c8db924924 8e47247236db6e36 .\$qI\$.G\$r6.n6 e48db8e36dc71c8e 36e392371c6db8dc m 67.m. 71b8e48e36dc8e47 246e491b6e471b91 q	
Bit Planes	Order settings Extract By Row Column
Red 7 6 5 4 3 2 1 2 0	Bit Order 💿 MSB First 🔾 LSB First
Green 7 6 5 4 3 2 1 ν 0 Blue 7 6 5 4 3 2 1 ν 0	Bit Plane Order RGB GRB
Preview Settings Include Hex Dump In Preview 🖌	 ○ RBG ○ GBR ○ BGR

Preview Save Text	Save Bin Cancel	CSDN @18947943

3. 总结

- 隐写工具使用(第一次接触zstag。。。)
- 追踪流并得到传输文件

这个题学到东西了,欢迎交流~~~