## 攻防世界 flag\_universe

# 原创

 方亭子
 □ □ 〒 2022-03-02 09:33:45 修改
 ○ 2344
 ◇ 收藏

 分类专栏:
 # 攻防世界MISC题目
 文章标签:
 安全

 〒 2022-02-24 20:52:46 首次发布
 方莱莱出品

 本文链接:
 https://blog.csdn.net/weixin\_46342884/article/details/123120787

 版权



### <u>攻防世界MISC题目 专栏收录该内容</u>

9 篇文章 0 订阅 订阅专栏 拿到题目,解压后是一个pacpng格式的流量包 使用wireshack打开后追踪tcp数据流。可以看到这是通过PASC上传的图片

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · flag。paap.pcap	-		
PASV 227 Entering Passive Mode (172 17 0 2 82 116)			
LIST -a			
150 Here comes the directory listing. 226 Directory send OK.			
250 Directory successfully changed. PASV			
227 Entering Passive Mode (172,17,0,2,82,111). LIST -a			
150 Here comes the directory listing. 226 Directory send OK.			
227 Entering Passive Mode (172,17,0,2,82,114). RETR /universe.png		- L	
150 Opening BINARY mode data connection for /universe.png (1133535 226 Transfer complete.	bytes)	•	
227 Entering Passive Mode (172,17,0,2,82,115). RETR /universe.png		- 1	
150 Opening BINARY mode data connection for /universe.png (1133535 426 Failure writing network stream.	bytes)	. 1	
分组 86.18 鉴户编 分组、32 照条既 分组、36 turn(s) 点击选择。		· ·	
整个对话(1044 bytes) Show data as ASCII ~		流 0 🌻	
查找:	查		
滤掉此流 打印 另存为… 返回 C1	ose	Help	

继续追踪数据流 在流2里面可以看到上传的文件

drwxrwxrwx	1 ftp	ftp	264 Sep 19 07:52 .
drwxrwxrwx	1 ftp	ftp	264 Sep 19 07:52
-rwxrwxrwx	1 ftp	ftp	41 Sep 19 07:52 flag.txt
-rwxrwxrwx	1 ftp	ftp	1133535 Sep 19 07:51 universe.png

## 在流7里面发现一串base64字符,解码后发现是假的flag

┛ Wireshark · 追踪 TCP 流 (to	:p.stream eq 7) ∙ flag	。paap.pcap			—		(
ZmxhZ3tUaG1zIG1zIGZha2U	gZmxhZyBoYWhhaGF9						
	irn(s).						
整个对话(41 bytes)		✓ Shor	w data as	ASCII	$\sim$	流 🛛 韋	
查找:					1	暨拔下一个( <u>N</u> )	)
	滤掉此流 打	印 另存之	<del>አ</del> …	返回	Close	Help	)

<<< 选择 >>>	
加密	
解码	
退出	
: 解码	
base64解码: ZmxhZ3tUaGlzIGlzIGZha2UgZmxhZyBoYWhhaGF9	
********Decoding complete*******	
: flag{This is fake flag hahaha}	
******	

## 判断flag藏在这些上传的文件中

#### 使用工具networkminer打开流量包,提取图片

注意,需要先用wireshack把流量包另存为格式为pacp的文件,因为pacpng文件需要正式版才可以打开 打开后,可以看到上传的文件

Network	Miner 2.1.1						_	- 0	×
<u>File Too</u>	ls <u>H</u> elp								
 — Select a	network adapter in t	he list —					$\sim$	Start U	Stop
Peremeters	(203) Kermonde Anone	lies						Case Panel	1
Hosts (6)	(100) Reynords Allowe (11es (9) Images (3)	Messages (	Creden	tials (	1) Sessions (	(31) DNS (3	2)	Filename	MD5
Filter keyw	or	Case	sensit	ive E	xactPhrase 🗸	Clea Ap	pl	flag	58079
Frame nr.	Filename	Extension		Size	Source host	S. port	Des		
279	universe[1].png	png	1 133	535 B	172.17.0.2	TCP 21104	172		
420	flag[1].txt	txt		41 B	172.17.0.2	TCP 21102	172		
434	flag[2].txt	txt		41 B	172.17.0.2	TCP 21107	172		
473	flag[1].txt	txt		41 B	172.17.0.2	TCP 21109	172		
529	universe[1].png	png	1 133	535 B	172.17.0.2	TCP 21106	172		
650	new_universe[1].png	png	1 178	630 B	172.17.0.1	TCP 49316	172		
908	flag[3].txt	txt		41 B	172.17.0.2	TCP 21107	172		
924	flag[2].txt	txt		41 B	172.17.0.2	TCP 21108	172		
938	flag[3].txt	txt		881 B	172.17.0.1	TCP 36688	172		
									-
		_						Reload (	Case
Buffered Frames to Parse:									

#### 找到图片

NetworkMiner 2.1.1	_		×
<u>F</u> ile <u>T</u> ools <u>H</u> elp			
Select a network adapter in the list	$\sim$	▶Start (	Stop 🗖
Parameters (203) Keywords Anomalies		Case Pane	1
Hosts (6) Files (9) [Images (3)] Messages Credentials (1) Sessions (31) DNS (32)	)	Filename	MD5
universe[1].png 1200x801, 1 1200x801, 1 1200x801, 1 17		flag Reload	58079
Duffered Formers to Denses			
buffered Frames to Parse:			.:

这里的flag.txt打开后是我们原先解码的假的flag

右键打开图片位置,保存后使用setgsolve查看,没有发现什么线索

放到kali里面使用binwalk查看,也没有发现什么,使用zsteg检查是否有隐藏数据 发现flag

-(root kali-	zxt)-[~/桌面]	1.py Git下载
zsteg <u>new</u>	universe.png	
imagedata	text:	"\n\n\n111???"
b1,r,lsb,xy	text:	"F2&*rq.9Qz"
b1,rgb,lsb,xy	text:	
b3,g,msb,xy	. file:	PGP Secret Sub-key -
b3,b,msb,xy	text:	"zC`)XUWS"
主文件来		

这里推荐一个软件networkminer网络数据分析工具,可以很好的检查流量包文件