从CTF比赛真题中学习压缩包伪加密与图片隐写术



先讲个笑话,刚刚打完 MAR DASCTF明御攻防赛,一如往常,很轻松便拿到了两个 flag (签到与问卷),哈哈,一个脑细胞都不 用消耗

参赛模式: 团队 参	家赛题目总数: 22 题 靶机数量: 0 个 竞赛设置阶段: 准备竞赛 竞赛状态: ● 已结束
609 个 实际参与数	MAR DASCTF明御攻防赛(竞赛编号:MATCH-20210326-u3Ccl) MAR DASCTF明御攻防赛
A 创建账号: root	⑤ 创建时间: 2021-03-26 17:06:13 ⑤ 竞赛起止时间: 2021-03:27:10:00:00 cm; 2021-03:27:10:00:00 cm; 2021-03:27.14:90:00 cm; 2021-03:27.14:14:90:00 cm; 2021-03:27.14:14:90:00 cm; 2021-03:27.14:14:14:14:14:14:14:14:14:14:14:14:14:1

好了下面通过其中的一道misc题,一起学习一下伪加密与图片隐写的破解

本文知识点:

- 遇到加密压缩文件怎么办? 需要哪些工具
- 遇到图片隐写怎么办? 需要哪些工具
- 十六进制数据还原文件

大佬就不用看了,全是小白操作

压缩包类的解题思路

如遇加密压缩包,在没有密码提示的情况下,先判断是不是伪加密 最简单的方法就是看十六进制数据,第一行如果有 09 多半就是了

🎊 简单的png陶	急写的附件.zip		- • ×	🚟 www.zip			- 0 ×
Offset	0 1 2 3 4 5 6 7 8 9	10 11 12 13 14 15 ANSI AS	CII 🔨	Offset	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	ANSI ASCII 🔺
00000000	50 4B 03 04 14 00 09 00 08 00	44 90 77 50 E7 C0 PK D w	PçÀ	00000000	50 4B 03 04 14 00 00 00	00 00 CB A3 5C 52 00 00	PK ˣ\R
00000016	8E 6D EA 2E 02 00 1B 31 02 00	08 00 00 00 66 6C Žmê. 1	fl	00000016	00 00 00 00 00 00 00 00	00 00 04 00 00 00 77 77	ww
00000032	61 67 2E 6A 70 67 9C FD 75 54	5C 4F F0 F0 0D DE ag.jpg∞ýuT\0ð	ðÞ	00000032	77 2F 50 4B 03 04 14 00	09 00 08 00 E0 99 5C 52	w/PK à™\R
00000048	61 80 C1 82 05 12 20 68 18 82	13 3C D8 60 09 32 a€Á, h, <ø	`2	00000048	74 55 B0 E5 78 02 00 00	48 08 00 00 0D 00 00 00	tU°åx H
00000064	10 DC 35 38 01 82 3B 04 18 20	10 20 B8 BB BB BB U58 ,;	»»»	00000064	77 77 77 2F 61 64 6D 69	6E 2E 70 68 70 F1 8F 49	www/admin.phpñ I
00000080	43 20 E8 E0 EE 24 B8 43 70 97	CD F7 F7 BE CF DA C èàî\$ Cp-Í÷÷	%ïÚ	00000080	B0 8F E1 A8 77 46 4D 66	E6 F6 87 16 4D 81 DD 14	° á wFMfæö‡ M Ý
00000096	FB EC 39 BB DB 73 EA 9F B9 F7	DC E9 9A EE 5B F5 ûì9»Ûsꟹ÷Üéš	î[ő	00000096	47 9C FE OC AF 44 6E 29	CD BC 39 11 6E 92 94 6D	Goeb [Dn) 149 n' "m
00000112	A9 EE EA EE A7 B9 A7 15 00 5F	46 12 2E 09 80 40 ©îêî§¹§ F .	€0	00000112	DE BC 11 AB 3A E3 93 AB	2A 73 31 E9 73 5A B4 81	Þ4 «:㔫*slés7′

点击查找十六进制数值搜索 504B,最后如果有 09 那基本就是了,改为 00 完活

	- to						
🇱 文件(F)	编辑(E) 搜索(S)	导航(N) 查看(V)	工具(T) 专业工具(l) 选项(O) 窗	읍囗(W) 帮助(H	ł)	
🗅 👅 🗐 🍣) 📚 😭 📑 👘	📴 📴 🔂 📴 1012	👫 🏘 🙀 🎲 🙀	→ + <u>₩</u> 🗲 →	i 🍐 🕹 🧼	🔳 🔎 🦚 💒 🥮 🗌	88 🖬 🖌 🕨 🛛 🧇
位置管理器((全部)			讲制数值			
Offset 🔺	搜索结果			ניונים			
0	504B			2021/03/28	1		
22F10	504B			2021/03/28	1		
2743F	504B			2021/03/28	1		
287C6	504B			2021/03/28	1		
32D2A	504B			2021/03/28	1		
32D84	504B			2021/03/28	1		
32DDE	504B			2021/03/28	1		

Offset	0	1	2	3	4	5	6	7	8	9	Α	в	С	D	Е	F	�≡ ANSI ASCII ∧
00032D00	1A	17	9F	\mathbf{FC}	F1	BF	9F	EE	FF	\mathbf{CF}	AF	FE	F7	87	FF	$\mathbf{F}\mathbf{F}$	Ÿüñ;Ÿîÿϯþ÷‡ÿÿ
00032D10	FD	70	EΒ	D1	2E	56	2D	4D	20	6F	64	40	D0	D5	59	14	ýpëÑ.V-M od@ĐÕY
00032D20	7F	2F	2D	0C	7F	AB	EΒ	FD	FF	00	50	4B	01	02	1F	00	/- «ëýÿ <mark>PK</mark>
00032D30	14	00	09	00	08	00	44	90	77	50	E7	C0	8E	6D	ΕA	2E	D wPçÀŽmê.
00032D40	02	00	1B	31	02	00	80	00	24	00	00	00	00	00	00	00	1 \$
00032D50	20	00	00	00	00	00	00	00	66	6C	61	67	2E	6A	70	67	flag.jpg
00032D60	0A	00	20	00	00	00	00	00	01	00	18	00	56	41	в7	1D	VA ·
00032D70	FA	00	D6	01	7A	89	29	1A	03	01	D6	01	BD	E1	37	16	ú Ö z‰) Ö ½á7
00032D80	03	01	D6	01	5 <mark>0</mark>	4B	01	02	1F	00	14	00	09	00	80	00	ÖPK
00032D90	C5	8D	77	50	22	C2	EΒ	BE	F4	$\mathbf{F}\mathbf{D}$	00	00	FF	1F	01	00	Å wP"Âë¾ôý ÿ
00032DA0	08	00	24	00	00	00	00	00	00	00	20	00	00	00	10	2F	\$ /
00032DB0	02	00	68	69	6E	74	2E	70	6E	67	0A	00	20	00	00	00	hint.png
00032DC0	00	00	01	00	18	00	AF	в2	03	E2	F7	00	D6	01	79	80	[−] ² â÷ Ö y€
00032DD0	D0	16	03	01	D6	01	$^{\rm CD}$	93	37	16	03	01	D6	01	50	4B	Ð ÖÍ"7 Ö <mark>PK</mark>
00032DE0	05	06	00	00	00	00	02	00	02	00	в4	00	00	00	2A	2D	· *-
00032DF0	03	00	00	00													
	1																

伪加密破解

比如这道misc题,结合了压缩包伪加密与图片隐写技术,我们就以它为例学习一下这两种常见技术的解决方法



就是这个压缩文件,后面带*说明需要密码,但是题中没有任何密码提示,ctf中不可能让你无脑爆破,因为时间是有限的,但也 有可能是弱口令,反正无从下手先爆破一下试试呗

ARC	HPR 4.50	- 2%				_ □	×			
☆(生(F)	恢复(R)	±2,0 非助(山)					~			
	. R		٢	-	?					
打开	开始!	停止	基准	购买	帮助	关于	退出			
已加密的 ZIP/RAR/ACE/ARJ-文件 碳解类型										
C:\Use	rs\XuanJian	Desktop\简单	的png隐	暴力			\sim			
范围	长度 字	四典 纯文本	自动保存	字 选项	高级					
一密码也	6度选项—									
		最小?	密码长度 =	1 🔹	个字符					
		最大?	密码长度 =	6 🌲	个字符					
一状态窗	·D		1							
2021/3	/27 14:05:4	4 - 密码未找3 1 - 文件℃・\□	ēlj sers\Xuan īk	an\Deskton	简单的nng	陷空的附供	zin"			
包打开	•		ser s your si	unpeskop	(Ie) U)Pri 9	66-94 JH JH JH				
2021/3	/27 14:08:2	8 - 开始暴力	波解				*			
当前密码 逝去时间 密码长度	}: E]: 2 夏=6, 总计	GrhzA 25s : 19,770,609),664, 已处	平均速度 剩余时间 理: 430,1	: 3: : 10 49,305	1,465,057p/ Om 14s	's			
			2	%						
ARCHPR V	version 4.50	(c) 1997-2008	B ElcomSoft	Co. Ltd.	dn.net/w	eixin_45	728978			

当时我也想到了伪加密,用 WinHex 打开压缩包,将全局方位标记中的 09 改为 00 保存即可解除密码限制,这里有两个文件所以 要改两处,但提示我试用版超过200kb不能保存,怎么回事,我记得是破解的啊

)2	90	D3	70	FE	FF	5C	9E	8ø8\$ïž`pò ópþÿ\ž						
-8	F.4	IA	40	21	00	81	09							
31	FE	P												
)8	\mathbf{FF}	e vv	INHe	ex				X						
75	\mathbf{DF}	5												
A	86	With this evaluation version you cannot save files												
:A	E3													
)E	DO	that are larger than 200 KB. However, you can												
52	4A	1	Ŀ		cre	eate	back	ups of such files at any time for future						
56	FE	Γ						use with the full version.						
10	F7	A												
C	BC	F						OK						
δF	5D	Γ												
19	85	L-	50	10	00	CD	110	wield o amono i						
B	СВ	AB	EB	9в	DB	FF	F4	í ݽ™Ó°ó<Ë≪ë>Ûÿô						
3D	08	FE	E9	85	82	8A	0A	`Đỹ*ỹ [≯ þé…, šlog.osdn.nel/weixin_4572897						

比赛结束后我才找到破解伪加密的工具—— ZipCenOp

命令 java -jar ZipCenOp伪加密破解.jar r 简单的png隐写的附件.zip





图片隐写破解

图片隐写的方式很多样,用到的工具也多,文件名已经提示的很明显了,是png隐写,所以朝着这方面想就行了



binwalk 和 Stegsolve 都没能找到什么有用的东西

(<mark>root⊙kal</mark> ∟# binwalk <u>f</u>	i)-[~/桌面] lag.jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	JPEG image data, JFIF standard 1.01
[<mark>root⊕kal</mark> [# binwalk <u>h</u>	i)-[~/桌面] int.png	
DECIMAL	HEXADECIMAL	DESCRIPTION - TATE
0 26973 主文件夹	0×0 0×695D	PNG image, 1654 x 485, 8-bit/color RGBA, non-interlayed Zlib compressed data, defaultocompression https://blog.csdn.net/weixin_45728976

所以百度一下,当当当,学到两个新工具 pngcheck 和 TweakPNG

png隐写							Ó	百度	王一下	
Q 网页	■资讯	▶视频	■图片	⑦知道	□文库	贴贴吧	⊘地图	位采购	更多	
 百度为您找到相关结果约879,000个										
) tdoom	inglhlog (⇒ idat				

<u> MUG图片限与IDAI 万竹(3) LUCOTIING DIOG-CODIN 時谷 LUAL</u>



png隐写zlib nga f5隐写 图片隐写 png图片 github

PNG隐写model.png(1) tdcoming'blog-CSDN博客 png隐写

A Peopletic L3 by Concert	
In States into	
The local division of	
Thata Contracts	
darangent Later	
Frank Browner	
Incase Continued	

2018年8月8日 这只是一道png的隐写题目,当看到png的图片进行隐写的 时候,我们要去考虑IHDR隐写,和Isb的隐写。 0X00准备 实验工具Stegsol ve 0X01实验操作 ...

🎬 CSDN技术社区 💿 百度快照

Misc 总结 --- 隐写术之图片隐写(二) - 先知社区



23条回复 - 发帖时间: 2017年12月24日 2017年12月24日 我们这里重点先了解一下,png图片文件头数据块以及pn g图片IDAT块,这次的隐写也是以这两个地方位基础的。 png... xz.aliyun.com/t/1... ◎ 百度快照

<u> 隐写技巧——PNG文件中的LSB隐写 - 知乎</u>



2016年12月2日本文分别介绍如何通过Python和C++实现对PNG文件的L SB隐写,参照文中的分析思路也可对常见的LSB隐写数据进行提取分析。 注:修改好的PNG_stego工程已上传至github: githu... → 知乎 ○ 百度快照 https://blog.csdn.net/

它们的功能是差不多的,只不过一个是命令行模式一个是图形化界面,但 pngcheck 可以识别多个图像类型,而另一个只能 是 png格式

pngcheck

Hacking Tools 1.31k 阅读

描述: 通过检查CRC和解压缩图像数据来验证PNG、JNG和MNG文件的完整性。

复制一张 hint.png 然后用 TweakPNG 打开,可以看到两个 IDAT块,正常的图片应该只有一条IDAT数据不同,而这里有两条不一样的,可以判断是两张图片

	🛃 hint.png (D:\工作区\ctf\DASCTF\misc\简单的png隐写的附件\) - TweakPNG											
	File Edit	t Insert	Options	Tools Help								
	Chunk	Length	CRC	Attributes	Contents							
I	IHDR	13	c897c20b	critical	PNG image header: 1654×485, 8 bits/sample, truecolor+alpha, noninterlaced							
	IDAT	8192	d6af059d	critical	PNG image data							
	IDAT	8192	94ad4d	critical	PNG image data							

IDAT	8192	3bdf9286	critical	PNG image data
IDAT	2308	0a1c4eff	critical	PNG image data
IDAT	8192	9a8af608	critical	PNG image data
IDAT	8192	4cc3dd	critical	PNG image data
IDAT	8192	87f56ea9	critical	PNG image data
IDAT	8192	295ab40f	critical	PNG image data
IDAT	8192	9bf751fc	critical	PNG image data
IDAT	5718	948b8d	critical	PNG image data
IEND	0	ae426082	critical	end-of-image marker

https://blog.csdn.net/weixin_45728976

右键将上面四条 Delete, 然后 Ctrl+s 保存

File Ed	dit Insert	Options	Tools	Help		
Chunk	Length	CRC	Attribut	tes		Contents
IHDR	13	c897c20b	critical			PNG image header: 1654×4
IDAT	8192	d6af059d	critical			DNC losses data
IDAT	8192	94ad4d	critical			Edit Chunk
IDAT	8192	3bdf9286	critical			Delete
IDAT	2308	0a1c4eff	critical			Move Up
IDAT	8192	9a8af608	critical	_		Move Down
IDAT	8192	4cc3dd	critical			Cut
IDAT	8192	87f56ea9	critical			Сору
IDAT	8192	295ab40f	critical			Paste
IDAT	8192	9bf751fc	critical		_	PING Image data
IDAT	5718	948b8d	critical			PNG image data
IEND	0	ae426082	critical			end-of-image marker

这样隐藏的图片就出来了,这句意思是你可以用89504E猜出旗子在哪里



89504E 应该是个密码,而需要密码解图片隐写的工具有很多,如: steghide 和 stegpy ,然而都没用,看了大佬的wp才知道用 的是 outguess ,又学了一个工具



这个kali里是没有的,输入 apt install outguess 安装即可



用命令 outguess -k 89504E -r flag.jpg -t output.txt 导出加密内容



里面有一行编码字符,看着像 Base64

6	/root/桌面/output.txt - Mousepad					-	•	×
文件(F)	编辑(E)	搜索(S)	视图(V)	文档(D)	帮助(H)			
警告: 您正在使用 root 帐户。有可能会损害您的系统。								
MUY4QjA4	AMDg5MTg	wNzg1RTA	wMDM2NjZ	DNjE2NzJ	FNzQ30Dc0MDA0QkNCNDk0Q0FGMzZCM	IDMwMz(QØR	DM

十六进制数据还原文件

解密得到一串好像十六进制的东西



十六进制再转字符串发现有个 flag.txt 字样,有经验的已经想到了,这可能是个压缩文件,那怎样将十六进制数据变成文件 呢? 大神用的Python导出成文件,那咱这种菜鸡不会,只能用笨办法喽



打开 WinHex 点击左上角新建

	VinHex						
File	Edit Search	Navigation	View	T			
D	New	C	trl+N				
5	Open	C	trl+O				
	Save	(Ctrl+S				
	Save As						
4	Create Disk In	nage	Alt+C				
	Restore Imag	e					
	Backup Mana	ger	F12				
	Execute	(Ctrl+E				
1	Print	(Ctrl+P				
r	Properties.log.csdn.nel/weixin_Al						

输入4个字符,OK

Create New File			\times
fla	Sizo:	Puton y	
. Ine	Size.	Dytes	×
<u>O</u> K	C <u>a</u> ncel		

将十六进制字符粘贴进去,选择第三个





然后保存到桌面即可,其实现在这个文件可以用压缩软件直接打开





看完你会发现其实这道题没有多难,只是很多工具我们不知道,没见过罢了,总之还是要多学多看,不要做井底之蛙 文章提到的工具都已打包,公众号回复"CTF"获取下载链接

参考文章:

- zip伪加密原理及操作
- [MAR DASCTF明御攻防赛] 个人(or团队) writeup

欢迎关注公众号,原创不易,转载请注明来源【爱国小白帽】 🗆



</article>