xctf攻防世界 MISC高手进阶区 János-the-Ripper



68 篇文章 2 订阅 订阅专栏

1. 打开环境,下载附件

是一个misc100无后缀的文件,用vscode打开后发现是一堆乱码,但其中包含flag.txt,如图:



2. 问题分析

1. 使用winhex打开文件

🗅 👗 🔚 🗳) 📚	Ê			5	圔	4	G	B 01	0	Ê	à 🌶	HE:	24	B HEX		- → - 🕅 📢	🗕 🔶 🕴 🤹
misc100																		
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F		ANSI ASCII
00000000	50	4B	03	04	14	00	03	00	08	00	0E	Α2	77	44	44	D4	PK	¢wDDÔ
00000010	88	77	27	00	00	00	19	00	00	00	08	00	00	00	66	6C	°₩'	fl
00000020	61	67	2E	74	78	74	00	10	01	4B	93	FF	03	EE	9C	FA	ag.txt	K"ÿ îœú
00000030	D3	12	83	Al	57	88	57	8C	BF	41	AA	41	87	16	F6	85	ó f¦₩^	ö ‡AªA; ƊW
00000040	FE	40	02	DA	73	CA	1F	AC	16	97	89	44	ЗA	50	4B	01	þ@ ÚsÊ	-, -%D:PK
00000050	02	14	00	14	00	03	00	08	00	0E	Α2	77	44	44	D4	88		¢wDDÔ^
00000060	77	27	00	00	00	19	00	00	00	08	00	00	00	00	00	00	w'	
00000070	00	01	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E		flag.
00000080	74	78	74	50	4B	05	06	00	00	00	00	01	00	01	00	36	txtPK	6
00000090	00	00	00	4D	00	00	00	00	00								М	
															(CSE	N @18	947943

我们可以看到文件的开头为 504B, PK开头的文件, 我们知道这个开头的标识是zip文件, 详见: 各类文件的文件头标志

改为zip文件

 ● misc100.zip - Bandizip (Standard) 文件(F) 編輯(E) 查找(I) 选项(O) 视图(V) 工具(T) 帮助(H) ◆ 「論 ◆ 「書 ● 「書 ● 「● ● ● ● ● ● ● ● ● ● ● ● ● ●			现需要解压密码,如图:	成zip结尾的,发现	我们将文件修改成
文件(F) 编辑(E) 查找(F) 选项(O) 视图(Y) 工具(T) 帮助(H)	- 🗆 X		ard)	ip - Bandizip (Standa	🔇 misc100.zip
近す 「日本」」) 视图(V) 工具(T) 帮助(H)	(E) 查找(I) 选项(O)	文件(F) 编辑(E)
打开 解压 State State State State Ea 代码页 論 misc100.zip 輸入密码 X 原始大小 美 39 25 文 輸入密码 「 小加密文件的密码。 39 25 文 輸入密码 「 協力 39 25 文 39 25 文		<i>7</i> 🛞 🗄			→ ×
★ misc100.zip ★ 新入加密文件的密码。 第 和人密码 第 和人图 第 和	目 代码页		☆C2卦 沃hn 血llA.	解压	打开
 輸入加密文件的密码。 39 25 文 輸入密码 □显示密码 ◎ 密码管理器 确定 取消 	原始大小 类型	~ 后大小		p	😭 misc100.zip
· □ □ 显示密码 密码管理器 确定 取消	25 文本文档	39	輸入加密文件的密码。		
輸入密码 「□显示密码 密码管理器 确定 取消					
輸入密码 □显示密码 密码管理器 确定 取消	A				
	1		输入密码		
□显示密码 密码管理器 确定 取消	8	~			
·····································					
显示密码 密码管理器 确定 取消	c				
□显示密码 密码管理器 确定 取消					
密码管理器 确定 取消					
密码管理器 确定 取消					
		确定取消	密码管理器		
	1				
	0				
	* の 価縮文体大水 158 安节 つ	□ □ □ □ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	`		

winhex中并没有伪加密,说明需要我们进行暴力破解。

掏出ARCHPR

附带工具下载链接: https://zhangfa.lanzouw.com/iQmy8yq3tuh

或者GitHub上下载: https://github.com/cnsuhao/Advanced-Archive-Password-Recovery-Professional-Edition

直接使用ARCHPR压缩包破解工具,如图,得到解压码'fish',如图:

ARCHPR 4.54 Professio	onal Edition			_	×					
文件(E) 恢复(R) 帮助(H)										
🗳 . 移 🕅	3	-	2		-					
打开 开始! 停山	基准测试	升级	帮助	关于	退出					
加密的 ZIP/RAR/ACE/ARJ 文件 攻击类型										
C:\Users\ ktop\misc100.zip 暴力										
范围 长度 字典 明 暴力范围选项	文 自动保存	选项	高级							
☑ 所有大写拉丁文(A - Z) 开始于: ▼ ☑ 所有小写拉丁文(a - z) 「 「 □ 所有为字(0 - 9) 结束于: ▼										
□ 所有特殊符号(!@)		掩码:			N					
 □ 空格 □ 所有可打印字符 				用户定义	<mark>8</mark> ₿					
状态窗口										
2022/1/13 15:48:47 - 自动保存路径选择被取消,自动保存现在已禁用										
2022/1/13 15: 8:48 - 口令日 2022/1/13 15: 8:48 - 'fish' 责	2成功恢复! 是这个文件的——	个有效口	÷		~					
当前口令: 已用时间: 进度指示器		平均速度 剩余时间	度: 司:							
	0%	6								
ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd. CSDN @18947943										

我们将zip解压,得到flag.txt。最终的答案为: flag{ev3n::y0u::bru7us?!}