# CTF 内涵的软件 stage1

# 原创

 艺博东
 ● ± 2020-10-06 18:00:14 发布
 ● 10113
 ◆ 收藏 5

 分类专栏:
 网络攻防
 文章标签: CTF
 CTF

 版权声明:
 本文为博主原创文章,遵循
 CC 4.0 BY-SA
 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 https://blog.csdn.net/HYD696/article/details/108906098
 版权



网络攻防专栏收录该内容

24 篇文章 17 订阅 订阅专栏

文章目录

一、内涵的软件

<u></u>\_∖ stage1

## 一、内涵的软件

题目描述: 图片有内涵, exe也可以有内涵, 也许你等不到答案, 赶快行动起来吧!!!(答案为flag{形式, 提交{}内内容即可) 题目附件: 附件1

1、附件1

链接: https://pan.baidu.com/s/1BzQc84cvoE0rA7pddlQrDw 提取码: pxxw

**2**、文件



3、用逆向工具包打开程序查看源代码—>ollydbg



**4、**打开



5、文件名—>打开

2345着图王	Cisco Packet	EVCapture	✓ exe逆向.e	xe
文件名(N):	exe逆向.exe			打开(O)
文件类型(T):	可执行文件 (*.exe)		~	取消
参数:		http:	s://blog.esic	

6、慢慢找

■ 育樓 < 0.1.1.y.D.b.g > - exe(世内.exe - [VII	P - 土我程, 倶吠 - exe逆问]		BP P VB 记事本 计算器 资源	管理器 CMD命令 退出	
☑ 収件(F) 賃着(V) 調試(D) 插件(P) 選具(1)	廖口(W) 常助(H) ⊥具 設査API町邸>			Carter and a second second	- 8 ×
			E U A 🚥 🕙 🔤 I 2 3 4 5		
0040105C . B9 13000000 mov ecx,0x	(13			~ 落	F存器 (FP 🔗 ↓ 128 KB/s
00401061 . B8 CCCCCCCC mov eax,0x	<00000000			E	AX 0019FFCC
00401066 . F3:AB rep stos d	lword ptr es:[edi]			E	CX 00401240 exe逆向. <modu< th=""></modu<>
00401068 . C745 FC 0500 mov [local	.1], 0x5			E	DX 00401240 exej逆向. <modu< th=""></modu<>
0040100F . C745 F8 18514 MOV [10Cal	.2],exe)归口.00425118	H2C11	25caad81232130F3d2eDFad}"	E	BX 003B7000
				E	SP 0019FF74
00401078 2 8045 FC FNO eax,				E	BP 0019FF80
8848187F 8945 FC DOU LOCA	al.11.eax			E	SI 00401240 exe <sub>过</sub> 问, <modu< th=""></modu<>
00401081 > 837D FC 00 + cmp [loca	1.1],0×0			E	DI 00401240 exe <u>(</u> )].(Houu
00401085 ., 7C 18 11 Xexe进	亩。0040109F			E	IP 00401240 exe逆向. <modu< th=""></modu<>
00401087 . 8B4D FC mov ecx,	local.1]			c	A FS AA2B 32位 A(FFFFFF
0040108A . 51 push ecx				Р	1 CS 0023 32位 0(FFFFFF
00401088 . 68 <u>EC504200</u> push exej	英向-004250EC			A	Ø SS ØØ2B 32位 Ø(FFFFFF
00401090 . E8 EB000000 <mark>call</mark> exej	<b>逆向 - 00401180</b>			z	1 DS 002B 32位 0(FFFFF
00401095 . 83C4 08 add esp,				S	0 FS 0053 321 3BA000(F
eeledeeleen ^ ED DO	<u> 씨</u> 미,-0040100H 光白, 00101070			Т	0 GS 002B 32位 0(FFFFF
60401090 . ED 09 Cjiip Aexe	四月,00401078			~ D	
00425118=exei逆向,00425118(ASCII "DB	APP{49d3c93df25caad81232130f3d	2ebfad}")		0	Ø LASTERR ERROR_SUCCES
				E	FL 00000246 (NO,NB,E,BE <mark>,N</mark>
地址 HEX 数据	ASCII	∧ 0019FF	C 0000000		^
00401000 CC CC CC CC CC E9 46 00 00	00 E9 01 00 00 00 CC 烫烫涕F	.?? 0019FFd			
00401010 55 8B EC 83 EC 44 53 56 57	8D 7D BC B9 11 00 00 U要该DSUW	悟脊■ 0019FF0	4 00000000		
00401020 00 B8 CC CC CC CC F3 AB C7	45 FC 00 00 00 00 81 - 柑烫腆	E?? 0019FF0			
00401030 /D FC 00 65 CD 1D /D 08 88	45 FC 83 CU U1 89 45 }?e?} mat	信?I荒 法子》新》而。	6 66666666		
00401040 FL EB EL SF SE SB 88 ES SV 00401050 55 98 EC 93 EC 4C 53 56 57		1曲與·與··· 唐·······························	4 7777F989 仮回到 kernel32.777	7F989	
	45 FC 05 00 00 00 C7 田汤睡	F2 2 0019FF	8 00387000		
00401070 45 F8 18 51 42 00 EB 09 8B	45 FC 83 E8 01 89 45 E?0B.?婨身	据?!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!	C 7777F970 kerne132.BaseThread	InitThunk	
00401080 FC 83 7D FC 00 7C 18 8B 4D	FC 51 68 EC 50 42 00 番}?I■琴摩	⊈h霞B. 0019FF8	0 C 0019FFDC		
00401090 E8 EB 00 00 00 83 C4 08 E8	6D FF FF FF EB D9 68 桦	灌ÿÿÿÿ胭h 0019FF8	4  77B97084 返回到 ntdl1.77B9708	84	
004010A0 88 50 42 00 E8 D7 00 00 00	83 C4 04 C6 45 F4 01 先B. 枳	兡 施? 0019FF8	18 003B7000		
004010B0 8D 55 F4 52 68 84 50 42 00	E8 62 00 00 00 83 C4 峌艄h凱B.	鑒····兡 0019FF8			
004010C0 08 0F BE 45 F4 83 F8 59 75	14 68 <u>54 50 42 00</u> E8 ■ 編集) 鴻u	TPB.?	0 0000000		
004010D0 AC 00 00 00 83 C4 04 E8 2E	FF FF FF EB 2F 0F BE ? 翹 ?ÿÿ	0019FF9	00387000		
004010E0 40 F4 83 F9 4E 75 14 68 34	58 42 88 E8 8F 88 88 間前計画は開始	DB·肇·· A019FF9			
004010F0 00 63 C4 04 E8 11 FF FF FF	EB 12 08 16 50 42 00 - 現 ?? UUU? ED EE EE EE EE EE SE SE 盤 話 噏	所211 ^r ¥ 0019FF6	0 0000000	htt	ps://blog.csdn.net/HYD69

#### 7、**OK**

DBAPP{49d3c93df25caad81232130f3d2ebfad}

49d3c93df25caad81232130f3d2ebfad

# <u></u> \_ ∖ stage1

**难度系数: ★★** 题目来源: XCTF 3rd-GCTF-2017 题目附件: 附件1

#### 1、附件1

链接: https://pan.baidu.com/s/1FoDs-U4c-Ac5mjTpXmn\_Mw 提取码: thyl

### **2、**文件



3、用进 Stegsolve打开



然后出现了二维码

4、微信扫一扫

# 

https://blog.csdn.net/HYD696

#### 5、放入 WinHext 中,发现如下信息,将文件保存为.pyc 格式

5.1 Edit—>Clipboard Data—>Paste Into New File



#### 5.2 ASCII Hex->OK

ADOLL NEX	

5.3 之后,提示是.pyt 文件—>是 python文件的编译文件,保存为 666.pyc 文件

Case Data	U 🤊 🖬 🤅	ii 🤜 🖏	1 📘		-) 8		LB.	B 010		9 P	HE:	< 斗	HEX	:	-	1			9	Si Smi	, 🎟 🗡
Fi <u>l</u> e E <u>d</u> it	noname																				
	Offset	0	1 2	3	4 :	56	7	8 9	10	11	12	13	14	15		1	ANSI	A 1	SCII	T	
	00000000	03 F	3 0D	OA I	B6 2	6 6A	57	63 00	00	00	00	00	00	00	ó	<b>4</b> 8	j₩c			T	
	00000016	00 0	1 00	00	00 40	0 00	00	00 73	0D	00	00	00	64	00		e	2	3	d		
	00000032	00 8	4 00	00	5A 0(	0 00	64	01 00	53	28	02	00	00	00		Z	d	S (			
	00000048	63 0	0 00	00	00 03	3 00	00	00 08	00	00	00	43	00	00	с				С		
	00000064	00 7	3 4E	00	00 00	0 64	01	00 64	02	00	64	03	00	64	sN		d o	d d	d d		
	00000080	04 0	0 64	05	00 64	4 06	00	64 05	00	64	07	00	67	08	d	d	d	d	g		
	00000096	00 7	D 00	00	64 08	8 00	7D	01 00	78	1E	00	7C	00	00	}	d	}	х	1		
	00000112	44 5	D 16	00	7D 02	2 00	7C	01 00	74	00	00	7C	02	00	D]	}	1	t	1		
	00000128	83 0	1 00	37	7D 01	1 00	71	2B 00	57	7C	01	00	47	48	f	7}	q+	W	GH		
	00000144	64 0	0 00	53	28 09	9 00	00	00 4E	69	41	00	00	00	69	d i	5 (	1	liA	i		
	00000160	6C 0	0 00	00	69 70	0 00	00	00 69	68	00	00	00	69	61	1	ip	j	ih	ia		
	00000176	00 0	00 0	69	4C 0(	0 00	00	69 62	00	00	00	74	00	00		ίL	ik	5	t		
	00000192	00 0	0 28	01	00 00	0 00	74	03 00	00	00	63	68	72	28	(		t		chr (		
	00000208	03 0	00 0	00	74 03	3 00	00	00 73	74	72	74	04	00	00		t	5	stri	t		
	00000224	00 6	6 6C	61	67 74	4 01	00	00 00	69	28	00	00	00	00	fl	agt		i(			
	00000240	28 0	0 00	00	00 73	3 07	00	00 00	74	65	73	74	2E	70	(	s		te	st.p		
	00000256	79 5	2 03	00	00 00	0 01	00	00 00	73	0A	00	00	00	00	уR			s			
	00000272	01 1	E 01	06	01 01	D 01	14	01 4E	28	01	00	00	00	52			1	A (	R		
	00000288	03 0	0 00	00	28 00	0 00	00	00 28	00	00	00	00	28	00		(		(	(		
	00000304	00 0	0 00	73	07 00	0 00	00	74 65	73	74	2E	70	79	74		3	te	est	.pyt		
	00000320	08 0	0 00	00	3C 61	D 6F	64	75 6C	65	3E	01	00	00	00	<module></module>						
	00000336	73 0	0 00	00	00																
																				et/HY	
																				L	

## 6、反编译

在线工具: https://tool.lu/pyc/



7、获得python脚本代码



8、 python 环境运行得到flag





AlphaLab