bugkuCTF平台逆向题第七道Take the maze题解



9 扁文章 0 订阅 订阅专栏 。<u>我的CTF进阶之路</u> 108 篇文章 18 订阅 订阅专栏

题目链接:

http://123.206.31.85/files/b9e9044c42256306ac9605fffe7aad9b/ConsoleApplication1.exe

tips:

	Take the maze	
	300	
作者: Docupa		
Flag格式 Flag:zsct	f{}	
ConsoleA		

运行截图

·	-	2 · · ·	1.1	
welcome	to z	sctf!		
show me	your	key:11	11111111	11111111
kev erro	or			
请按任音	键继	婕		
H IX IL 10	N BEE SPEC	·		

查壳无壳

入口点: 000588A	2	EP 段:	. text	\triangleright
文件偏移: 00000CA	2	首字节:	E9, D9, A8, OO	\triangleright
连接器版本: 14.0		子系统:	Win32 console	\triangleright
PESniffer: Microsoft	: Visual C++ 8.0	O Debug		\triangleright
PEiDDSCAN: Wicrosoft	: Visual C++ 8.(D [Debug]		\geq
多文件扫描(皿)	查看进程(<u>T</u>)	扩展信息	. 插件	
✓ 总在最前(S)	选项(0)	关于(<u>A</u>)	しし、「退出」	

OD载入

ovsz ecz, byte ptr ds: [eax+0x1381168]	d+1==0123456789
over ecz, bute ptr ds: [eax+0x1381168]	da1xu0123456789
over ecz, byte ptr ds: [eax+0x1381168]	d+1+u0123456789
over env. bute ntr de: [eav+0v1381168]	da1xx0123456789
uth ContoleA 01357E50	hoh wait! Take your ticketh
ash Consolet 01357874	printing ticket In
uth ContoleA 01357E90	printing ticket
ush ConsoleA 01357EAC	printing ticket
ush ContoleA. 01357EC8	printing ticket
ush ConsoleA 01357EE4	printing ticket
uzh ConzoleA 01357F04	printing ticket
ush ConsoleA 01357F24	printing ticket
ush ConzoleA. 01357F44	printing ticket
ush ConsoleA 01357F68	printing ticket
ush ConsoleA. 01357F8C	printing ticket
ush ConsoleA. 01357FB0	printing ticket
ush ConzoleA. 01357FD8	wb
ush ConsoleA.01357FDC	flar.ppr
ush ConzoleA. 01357FE8	print finished view the path to this file, you will get a png file, have a good time\n\n
ush ConsoleA.01358050	pause
ov edx, dword ptr ds:[eax#4+0x1380004]	ñ
ush ConsoleA.01358058	key error\n
ush ConsoleA.01358050	pause
ov_dword_ptr_ds:[eax],ConsoleA.0138117	P
ush ConsoleA.01358068	welcome to rsctf:\n
ush ConsoleA. 01358080	show me your key:
ush ConsoleA. 01358098	Ke
ush ConsoleA.0135809C	done!!!The flag is your input\n
ush ConsoleA. 01358608	Stack area around _alloca memory reserved by this function is corrupted\n
ush ConsoleA. 01358660	\mData: <
ush ConsoleA.0135866C	hAllocation number within this function:
ush ConsoleA.013586A0	InSize:
ush ConsoleA.013586AC	\nAddress: Ox
ush ConsoleA 013586CD	Stack area around _alloca memory reserved by this function is corrupted
ush ConsoleA. 01358718	NSNSNpNsNz dNSN2Ns
ush ConsoleA.01358730	(a
ush ConsoleA. 01358734	
ush ConsoleA 01355/38	RER SPERS
ov cl, byte ptr ds:[eax=0x13580F4]	Stack around the variable
ov edr, ConsoleA. 01358110	was corrupted.
ov eax, consoles, 01358500	Stack Corrupted hear unknown wariable
din contoler 0100000	R. 64

发现程序运行后会生成一个flag.png

那我们就想办法让程序执行这个操作

让程序走到下边这个段

012A3AE0 /> \55 push ebp

012A3ADE	CC	int3	
012A3ADF	CC	int3	
012A3AE0	r> 55	push ebp	
012A3AE1	. SBEC	nov ebp,esp	
012A3AE3	. 81EC CC00000	sub esp,0xCC	
012A3AE9	. 53	push ebx	
012A3AEA	. 56	push esi	ConsoleA. <moduleentrypoint></moduleentrypoint>
012A3AEB	. 57	push edi	ConsoleA. <moduleentrypoint></moduleentrypoint>
012A3AEC	. 8DBD 34FFFFF	<pre>lea edi,[local.51]</pre>	
012A3AF2	. B9 33000000	nov ecx,0x33	
012A3AF7	. B8 CCCCCCCC	nov eax,0xCCCCCCC	
012A3AFC	. F3:AB	rep stos dword ptr es:[edi]	
012A3AFE	. 68 507E3501	push ConsoleA.01357E50	\noh,wait! Take your ticket
012A3B03	. E8 B9AEFFFF	call ConsoleA.0129E9C1	

载入后先单步向下 遇到向上跳转就在下一行按F4

遇到调向失败的就修改z标志位



跳到我们的目标段之后 单步一直向下即可

18F B	•	8364 84	add esp,0x4	
IBFE		68 087F3501	ConsoleA.@1357FD8	wb
10.03		68 DC7F3501	ConsoleA.@1357FDC	flag.png
10.08	Ι.	E8 44961111	call ConsoleA.01290251	
C 00-		83C4 08	add esp. 0x8	
C18	١.	8945 F8	nov [local_2]_eax	
IC13	Ι.	8845 F8	nov eax.[local.2]	
C16		50	push cax	
BC17	١.	68 8A070000	push 0x788	
ETC	Ι.	64 01	public fix1	
IC1E	١.	68 C0093801	ConsoleA.013809C0	
1023	Ι.	E8 8684FFFF	call ConsoleA,0129COAE	
10.28	Ι.	8364 18	add esp. 0x10	
1028	11	8845 F8	now eax,[local.2]	
IC2E	1.	50	perch eax	
9C.2F		E8 5284FFFF	Call Console@.@129C086	
10.34	١.	83Ch 8h	add esp, 0ch	
1037		68 E87F3501	ConsoleA.@1357FE8	print finished, view the path to this file, you will get a png file, have a good ti
1030	١.	E8 BOADFFFF	Call ConsoleA.0129E9C1	
E41		83CA 84	add esp. 0x4	
1044	Ι.	48 50803501	Console4,01358050	pause
-	<u> </u>		and an and a second	
1158-	Con	soleA.01357FE	8 (ASCII 70,"rint finished,view the path	to this file,you will get a png file,have a good time\n\n\n")

welcome to zsctf!				
show me vour key:111111111111111				
done!!!The flag is your input				
oh,wait! Take your ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
printing ticket				
print finished, view the path to this file, you will get a png file, have a good time				
请按任意键继续				



最后可以得到一张二维码图片

(tips: 和程序在一个目录 如果找不到 就用everything搜索)

扫码得到

Congratulations! The flag is your input + "Docupa"

后边觉得没啥可写了

这个写的太全了

https://www.52pojie.cn/forum.php?mod=viewthread&tid=674404&page=1&authorid=666114