【原创】实验吧此处无声WP

原创



随笔专栏收录该内容

3篇文章 0 订阅 订阅专栏

实验吧此处无声WP

step1 Get软件 step2 PEID初步分析 step3 OD逆向

step1 Get软件

实验吧下载软件,http://ctf5.shiyanbar.com/crack/5/ Get基本要求:找出nsfocus的正确注册码。

step2 PEID初步分析

先PEID,发现有壳,尝试脱壳失败,大致的流程是启动时先调用LoadLibrary加载kernel32.dll,然后调用GetProcAddress把函数 加载到内存中。

PEiD v0.95 🕍				X
文件: C:\E\sa	mple\CrackMe2.exe			浏览
入口点: 💿	0001579	EP 段:	. Encoded	\square
文件偏移: 0	0001579	首字节:	B8, 7A, E9, 3F	$\overline{\Sigma}$
连接器版本: 6.	0	子系统:	Win32 GUI	\sum
PESniffer: Unk	nown			\ge
PEiDDSCAN: yod	a's Protector v1.02 (.dl	1,.oex) ->.	Ashkbiz Danehk	\sum
多文件扫描 @) 查看进程 (I)	扩展信息	插件	
🗹 总在最前 🛽) 选项 @ ****	关于创	net/tole遇出	188

使用插件查找到OEP地址4027F0



step3 OD逆向

加载OD,下硬件断点he 4027f0,然后F9执行,程序直接停在了EOP,比较欣慰。



用户名输入nsfocus,注册信息testtest,提示失败

Ç	• CrackMe 2011 # 3	对不起	
	-注册信息		ĺ
	用户 nsfoucs		[
	注册 testtest		ł
		确定	C

OD下端口 bp MessageBoxA,并初步分析如下:

1. 先获取用户名并计算长度 EDI0018F648 ASCII "nsfocus"

00401762	E8 3D100000	<pre>call CrackMe2.004027A4</pre>	jmp 到 mfc42.#CWnd::GetWind
00401767	8D4C24 38	<pre>lea ecx,dword ptr ss:[esp+0x38]</pre>	
0040176B	E8 F0010000	call CrackMe2.00401960	
00401770	8DBC24 D400000	<pre>lea edi,dword ptr ss:[esp+0xD4]</pre>	用户名
00401777	83C9 FF	or ecx,-0x1	
0040177A	3300	xor eax,eax	
0040177C	C78424 E001000	<pre>mov dword ptr ss:[esp+0x1E0],0x0</pre>	
00401787	F2:AE	<pre>repne scas byte ptr es:[edi]</pre>	
00401789	F7D1	not ecx	
0040178B	49	dec ecx	用户名长度
0040178C	51	push ecx	
0040178D	8D8C24 D800000	<pre>lea ecx,dword ptr ss:[esp+0xD8]</pre>	https://blog.code.pot/coloc0000
00401794	51	push ecx	nttps://biog.csdn.net/zoleo8088

2. 取注册信息的输入,并判断是否是32字节0~9\A-F之间的数据,判断为MD5。

于是计算nsfocus的MD5填入注册文本框,通过分析把数据内容保存到下面的地址

 0018F648
 42
 39
 42
 37
 44
 43
 34
 32
 31
 45
 30
 30
 35
 42
 B9B7DD1C421E005B

 0018F658
 43
 39
 41
 37
 46
 37
 30
 42
 38
 34
 33
 44
 30
 45
 C9A7F70B848E3D0E

00401700	00 04010000	hasi aviat	
)04017B8	50	push eax	
)04017B9	8D4B 64	<pre>lea ecx,dword ptr ds:[ebx+0x64]</pre>	
)04017BC	E8 E30F0000	call CrackMe2.004027A4	jmp 到 mfc42.#CWnd::GetWindowText
)04017C1	8D8C24 D400000	<pre>lea ecx,dword ptr ss:[esp+0xD4]</pre>	
004017C8	51	push ecx	
)04017C9	8BCB	mov ecx,ebx	
)04017CB	E8 A0000000	call CrackMe2.00401870	判断是否是MD5,且全部大写
)04017D0	8500	test eax,eax	
004017D2	74 54	<mark>je</mark> short CrackMe2.00401828	
)04017D4	8D5424 18	<pre>lea edx,dword ptr ss:[esp+0x18]</pre>	

3. sub4018C0的目的是吧输入的MD5的数据由字符串转换为hex,保存到下面的地址

0018F58C	B9	Β7	DD	1C	42	1E	00	5B	C9	Α7	F7	0B	84	8E	3D	0E	狗?B.[骚?剮=
0018F59C	05	72	87	D9	ED	85	6A	DA	B2	97	CF	63	56	С3	61	8A	r囐韰j诓椣cV胊?

然后比较上面两行是否相同,如果相同则成功。 那么问题来了18F59C的数据怎么来的?

88481713	51	nush ecx	
004017C9	8BCB	mov ecx.ebx	
004017CB	E8 A0000000	call CrackMe2.00401870	判断是否是MD5. 日全部大写
004017D0	8500	test eax.eax	
004017D2	74 54	ie short CrackMe2.00401828	
004017D4	8D5424 18	lea edx.dword ptr ss:[esp+0x18]	
004017D8	56	push esi	
004017D9	8D8424 D800000	<pre>lea eax.dword ptr ss:[esp+0xD8]</pre>	
004017E0	52	push edx	
004017E1	50	push eax	
004017E2	8BCB	mov ecx,ebx	
004017E4	E8 D7000000	call CrackMe2.004018C0	MD5 string to hex
004017E9	8D4C24 0C	<pre>lea ecx,dword ptr ss:[esp+0xC]</pre>	
004017ED	6A 10	push 0x10	
004017EF	51	push ecx	
004017F0	E8 FBF9FFFF	call CrackMe2.004011F0	
004017F5	8D5424 24	<pre>lea edx,dword ptr ss:[esp+0x24]</pre>	
004017F9	8D4424 24	<pre>lea eax,dword ptr ss:[esp+0x24]</pre>	
004017FD	52	push edx	
004017FE	50	push eax	
004017FF	E8 ECFAFFFF	<pre>call CrackMe2.004012F0</pre>	
00401804	83C4 10	add esp,0x10	
00401807	B9 04000000	mov ecx,0x4	
0040180C	8D7C24 1C	<pre>lea edi,dword ptr ss:[esp+0x1C]</pre>	
00401810	8D7424 2C	<pre>lea esi,dword ptr ss:[esp+0x2C]</pre>	
00401814	33D2	xor edx,edx	
00401816	F3:A7	<pre>repe cmps dword ptr es:[edi],dword ptr ds:[esi]</pre>	
00401818	5E	pop esi	0018F58C
00401819 👃	75 OD	<mark>jnz</mark> short CrackMe2.00401828	
0040181B	52	push edx	
0040181C	68 64404000	push CrackMe2.00404064	ASCII "恭喜"
00401821	68 58404000	push CrackMe2.00404058	ASC https: <u>护册</u> 成或.cbsdn.net/zoleo8088
00401826	FB AC	imn short CrackMe2,00401834	

4. 重新跟踪分析发现, sub401AA0把输入的"nsfoucs"进行了MD5,并保存在0018F59C

0040179E	805424 28	lea eux,uwuru ptr ss:[esp+uxz8]	
004017A2	8D4C24 38	<pre>lea ecx,dword ptr ss:[esp+0x38]</pre>	
004017A6	52	push edx	
004017A7	E8 F4020000	call CrackMe2.00401AA0	MD5(nsfocus)
004017AC	8D8424 D400000	<pre>lea eax,dword ptr ss:[esp+0xD4]</pre>	
004017B3	68 04010000	push 0x104	
00401788	50	push eax	
004017B9	8D4B 64	<pre>lea ecx,dword ptr ds:[ebx+0x64]</pre>	

5. 然后才到步骤3,此时18F58C==18F59C

004017E0	52					pust	e	ix											
004017E1	50						i ea	ах											
004017E2	8B(B				mov	eca	c, el	x										
004017E4	E8	D70	000	90		cal]	Cı	racl	<me:< td=""><td>2.00</td><td>940</td><td>18C)</td><td>5]</td><td></td><td></td><td></td><td></td><td>MD5 strin</td><td>g to hex</td></me:<>	2.00	940	18C)	5]					MD5 strin	g to hex
004017E9	8D1	IC24	00			lea	eca	(, di	vori	i pt	tr s	55:	[es]	p + Øx	(C)				
004017ED	6A	10					0)	(10											
004017EF	51						e e	X:											
004017F0	E8	FBF	9FFI	FF		cal]	Ct	racl	<me:< td=""><td>2.01</td><td>940</td><td>11F)</td><td>5]</td><td></td><td></td><td></td><td></td><td></td><td></td></me:<>	2.01	940	11F)	5]						
004017F5	8D5	424	24			lea	eda	e, di	vori	i pi	tr s	55:	[es	p + Øx	(24)]			
004017F9	8D1	424	24			lea	eax	e, di	vori	i pi	tr s	55:	[es	p + Øx	(24)]			
004017FD	52						e e	ix											
004017FE	50					pust	i ea	ax											
004017FF	E8	ECF	AFFI	FF		cal]	Cı	raci	<me:< td=""><td>2.0(</td><td>940</td><td>12F (</td><td>5</td><td></td><td></td><td></td><td></td><td></td><td></td></me:<>	2.0(940	12F (5						
堆板地 = 9918F57C																			
ecx=0000	900E																		
thth	НЕХ ≹	約据														ASCII	*	0018F570	00000001
0018F51C	64 G1	66	ดด	48	F6	18	ពព	86	ពព	3F	76	25	DЦ	5R	հհ	! /H???u2 試力		0018F574	00000000
0018F52C	50 F/	18	ดด	61		ดด	ดด	DR	FD	18	ดด	28	FS	18	ดด	P?.f		0018F578	00000111
0018F53C		18	ดด	4f:	F7	18	ดด	Rń	 Аб	44	76	C.5	21	70	32	亜■_1?_녣Du?12		0018F57C	50824735
0018F54C	FF FF	FF	FF	A6	ดด	3F	76	FF	7F	10	ñD	50	F6	18	ดด	?iiii??u?∎mP?.		0018F580	77858033
0018F55C	ด1 ดเ	า ดด	ดด	D8	FD	18	ดด	E9	17	40	ดด	48	Fő	18	ดด	<i>∔</i> (牛■.?@_H?		0018F584	7A45679A
0018F56C	8C F	18	66	01	00	66	00	00	00	66	00	11	61	66	00	æ∎,£		0018F588	47165C6D
											-			47	1.7			0018F58C	10000700
0018F57C	35 47	82	5C	33	8C	85	77	9A	67	45	78	60	56	10	47	564学る目 W羅』 EZMNIG		00101200	10000709
0018F57C 0018F58C	35 47 B9 B7	82 / 82	5C 1C	33 42	8C 1E	85 00	77 5B	9A C9	67 A7_	45 F7_	7 A ØB	ου 84	50 8E	10 3D	47 ØE	5G1空3具W雒(EZM\■G 狗?B■.「骚?品 =■		0018F590	5B001E42
0018F57C 0018F58C 0018F59C	35 47 B9 B7 B9 B7	82 DD DD	5C 1C 1C	33 42 42	8C 1E 1E	85 00 00	77 5B 5B	9A C9 C9	67 A7 A7	45 F7 F7	7 A 0B 0B	ου 84 84	50 8E 8E	10 3D 3D	47 0E 0E	56位3頁₩₩AEZm\#G 狗?B■.[骚?剮=■ 狗?B■.[骚?剮₩★★://		0018F590	58001E42

6. 当执行sub4012f0时,发现18F58C的内容发生了变化,应该是对MD5(用户名)进行了处理。

004017FD	52	push edx
004017FE	50	push eax
004017FF	E8 ECFAFFFF	call CrackMe2.004012F0
00401804	83C4 10	add esp,0x10
00401807	B9 0400000	mov ecx,0x4
0040180C	8D7C24 1C	<pre>lea edi,dword ptr ss:[esp+0x1C]</pre>
00401810	8D7424 2C	<pre>lea esi,dword ptr ss:[esp+0x2C]</pre>
00401814	33D2	xor edx,edx
00401816	F3:A7	<pre>repe cmps dword ptr es:[edi],dword ptr ds:[</pre>
004012F0=	-CrackMe2.004012F	0
		[
地址	HEX	ASCII
0018F51C	04 01 00 00 48 F	`6 18 00 A6 00 3F 76 25 D4 5B 44 \左H?.??v%款
0018F52C	50 F6 18 00 50 F	6 18 00 01 00 00 00 64 F7 18 00 P?.P?.£d?
0018F53C	D8 FD 18 00 04 0	10 00 00 50 F6 18 00 01 00 00 00 供■. ¦P?. <i>土</i>
0018F54C	64 F7 18 00 D8 F	D 18 00 EC 41 40 00 14 ED 70 33 d?.佚∎.霢@.∎
0018F55C	04 18 40 00 AC 1	9 30 16 8C F5 18 00 7C F5 18 00 📲 0.?0 2 1.
0018F56C	00 00 00 00 01 0	10 00 00 00 00 00 00 11 01 00 00£
0018F57C	35 47 82 5C 33 8	C 85 77 9A 67 45 7A 6D 5C 16 47 5G俓3直w歡Ezi
0018F58C	87 FD 88 07 F7 4	9 94 3B F5 90 44 B4 56 94 67 E5 圐?鳙?魤D碫摄
0018F59C	B9 B7 DD 1C 42 1	E 00 5B C9 A7 F71tBB\$\$60 98 360 00 98 360 00 00 00 00 00 00 00 00 00 00 00 00 0
00405500	00 00 00 00 04 0	o he 47 oo oo eo ee ee oo oo ´´ (#ea翻读

综上,程序大致的意思是把输入的注册信息进行了加密,加密的结果与MD5(用户名)相同即成功获得flag。 那么相反,把MD5(用户名)进行解密的内容就是flag

直接修改汇编指令,让sub4012f0重新执行一次,发现并不能解密出想要的内容,看了一下大佬们的WP, 说是用RC6的算法,(本人目前没有道行如何判断使用哪种算法...),大概调研了一下,不同于AES,RC6虽然是对称加密,但 他的加密和解密的算法不同,无法直接调用sub4012f0来解密。

304017F0	E8 F8F9FFFF	Сапт сраскиег.004011F0
004017F5	8D5424 24	<pre>lea edx,dword ptr ss:[esp+0x24]</pre>
304017F9	8D4424 24	<pre>lea eax,dword ptr ss:[esp+0x24]</pre>
304017FD	52	push edx
304017FE	50	push eax
304017FF	E8 ECFAFFFF	call CrackMe2.004012F0
30401804	83C4 88	add esp,0x8
30401807	^ EB EC	jmp short CrackMe2.004017F5
30401809	90	пор
3040180A	90	nop
3040180B	90	nop
3040180C	8D7C24 1C	<pre>lea edi,dword ptr ss:[esp+0x1C]</pre>
01-01-01	007696 90	100 oci dword ptr cc: $10cp+8y201$

于是找工具进行解密...

密钥(K):	3547825C338C85779A67457A6D5C1647	类型:	RC6	•
明文(M):	F6ADDD6C46EBB644BDA265366E8CA675			*
密文(C):	B9B7DD1C421E005BC9A7F70B848E3D0E			*

收工, 哎, , 不是很完美。

此处无声 分值:50 来源:西普学院 难度:难 参与人数:4871人 	回答 少侠 , 你太 <u>公告天下</u>	正确 棒了!!! 默默牛×
F6ADDD6C46EBB644BDA265366E8CA675		
	https://blog	.csdn.net/zoleo8088