

xctf攻防世界simple-unpack writeup

原创

qq_112419837

于 2020-11-04 10:17:48 发布

104

收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/qq_42983283/article/details/109484979

版权

simple-unpack 19 最佳Writeup由 **中老年划水爱好者2** · 只是看看提供

难度系数: ★★★★★ 3.0

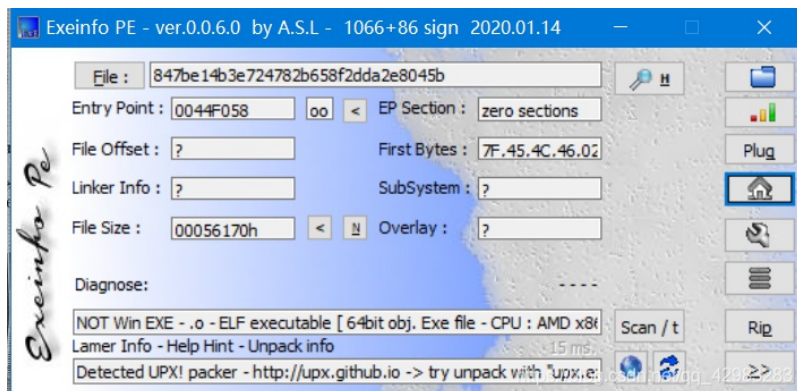
题目来源: 暂无

题目描述: 菜鸡拿到了一个被加壳的二进制文件

题目场景: 暂无

题目附件: 附件1 https://blog.csdn.net/qq_42983283

下载附件查看，发现upx:



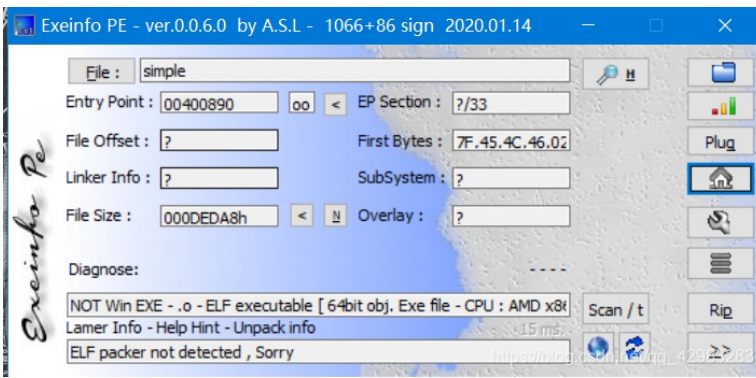
010editor搜索flag发现:

49	92	24	00	00	00	40	FF	B8	1C	00	00	6C	02	00	00	I'\$....@y,...l...
08	00	00	00	36	72	98	F2	E0	B9	6C	00	0F	00	BA	E8	...6r~òà¹l...è
1F	E4	36	F2	FB	70	09	40	0F	F0	05	40	1F	C0	83	3D	.ä6òùp.@.ò.@.Àf=
0A	D8	01	B1	6C	1D	07	B4	14	B0	01	B3	95	F6	E4	64	.ò.±l...°.°.*òad
76	86	02	4F	06	03	0F	16	26	E4	E4	E4	E4	36	46	56	vt.O...&àààà6FV
66	21	DA	E4	E4	76	86	01	FF	FF	FF	FF	66	6C	61	67	f!Ûääv†.ÿÿÿÿflag
7B	55	70	78	5F	31	73	5F	6E	30	74	5F	61	5F	64	33	{Upx_ls_n0t_a_d3
6C	69	76	33	72	5F	63	30	6D	70	34	6E	86	DF	B3	DB	liv3r_c0mp4ntß°Ù
79	7D	51	08	0D	D8	15	4A	0F	80	C1	9F	C0	F0	83	F6	y}Q..ò.J.eAYÀòfò
A1	6C	BF	86	20	AD	FB	D5	26	38	C5	52	01	20	A3	0F	¡l¿† -ûò&8ÀR. f.
02	8B	1C	B6	DD	1F	FF	01	3F	D0	C5	2F	69	2B	D8	43	.<.¶Y.ÿ.?ðÀ/i+ØC
E0	A1	6C	CB	01	54	B5	01	ED	40	22	4A	6F	01	A0	63	à¡lÈ.Tm.í@"Jo. c
62	38	40	1F	6F	84	3F	11	AA	14	2F	40	A5	CF	59	C8	b8@.o,,?..@/¶YÿÈ
0B	8E	D1	0F	3F	00	A4	05	24	13	55	88	8E	A1	23	B4	ò.ŽÑ.?.n.\$..Û*¿¡#?

使用kali 脱壳:

```
upx -d 847be14b3e724782b658f2dda2e8045b -o simple
```

查看:



ida64打开，f5伪代码，可以直接找到flag:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    int result; // eax@4
    __int64 v4; // rdx@4
    char v5; // [sp+0h] [bp-70h]@1
    __int64 v6; // [sp+68h] [bp-8h]@1

    v6 = *MK_FP(__FS__, 40LL);
    _isoc99_scanf((unsigned __int64)"%96s");
    if ( sub_400360(&v5, flag) )
        puts("Try again!");
    else
        puts("Congratulations!");
    result = 0;
    v4 = *MK_FP(__FS__, 40LL) ^ v6;
    return result;
}
```

https://blog.csdn.net/qq_42983283

双击flag:

```
~ .data:0000000000000000C000000000000000  dd  0
~ .data:00000000000000006CA09F          db  0
~ .data:00000000000000006CA0A0          public flag
~ .data:00000000000000006CA0A0 flag      db  'flag{UpX_1s_n0t_a_d3liv3r_c0mp4ny}',0
~ .data:00000000000000006CA0A0          ; DATA XREF: main+31f0
~ .data:00000000000000006CA0C3          align 8
~ .data:00000000000000006CA0C8          public _dl_tls_static_size
~ .data:00000000000000006CA0C8 _dl_tls_static_size dq 800h          ; DATA XREF: __libc_setup_tls+7E1r
~ .data:00000000000000006CA0C8          ; __libc_setup_tls+1B51r ...
~ .data:00000000000000006CA0D0          public _nl_current_default_domain
~ .data:00000000000000006CA0D0 nl current default domain dn offset nl default default domain
```