




CTF Just-No-One

原创

艺博东  于 2020-10-10 00:00:50 发布  9753  收藏 4

分类专栏: [网络攻防](#) 文章标签: [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/108988603>

版权



[网络攻防](#) 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

难度系数: ★★★★★

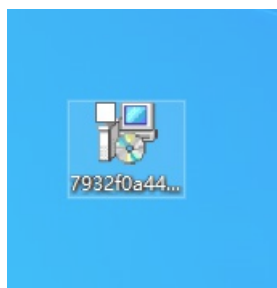
题目附件: 附件1

1、附件1

链接: <https://pan.baidu.com/s/1IB2R0XDKyYBnKX2kCIRFjQ>

提取码: 8zkt

2、文件 (一个应用程序)



3、解题

吐槽: 这题的flag很难找, 要很细心, 也感觉很奇怪; 不知道这题的重点是什么。

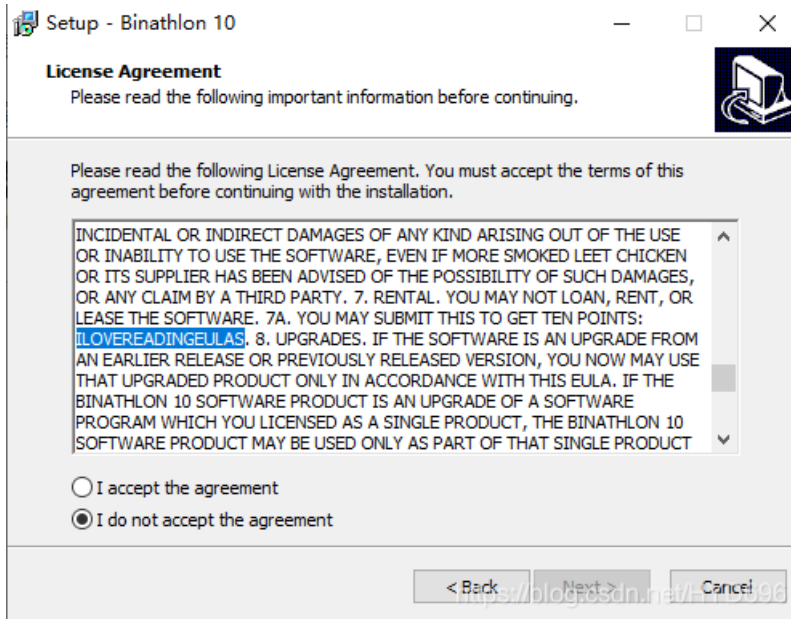
用逆向工具包打开程序查看源代码，找了很久也没有找到；

The screenshot shows a debugger window with assembly code on the left and registers on the right. The assembly code includes instructions like `call 7932F0A4.00403278`, `mov eax,edi`, `mov edx,[local.3]`, `call 7932F0A4.004032FC`, `mov esi,ebx`, `inc ebx`, `mov edx,7932F0A4.00408D7C`, `mov al,byte ptr ds:[ebx]`, `call 7932F0A4.004072D0`, `test al,al`, `jc X7932F0A4.00408D33`, `xor eax,eax`, `mov al,byte ptr ds:[ebx]`, `sub eax,0x31`, `cmp eax,[local.2]`, `jc X7932F0A4.00408D33`, `mov eax,edi`, `xor edx,edx`, and `mov dl,byte ptr ds:[ebx]`. The registers window shows values for EAX, ECX, EDX, EBX, ESP, EBP, ESI, EDI, EIP, C, P, A, Z, S, T, D, and EFL. The EFL register shows `ERROR_MOD_NOT_FOUND (0000007E)`. Below the registers is a table of memory addresses and data.

地址	HEX 数据	ASCII
0040BF30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BF90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFA0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFB0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFC0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFD0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFE0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----
0040BFF0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	-----

kail Linux 也整了很久，也不OK；

4、flag在安装软件的时候，在协议里



flag，很辣眼睛。

5、OK

ILOVEREADINGEULAS

温馨提示：ILOVEREADINGEULAS就是flag