

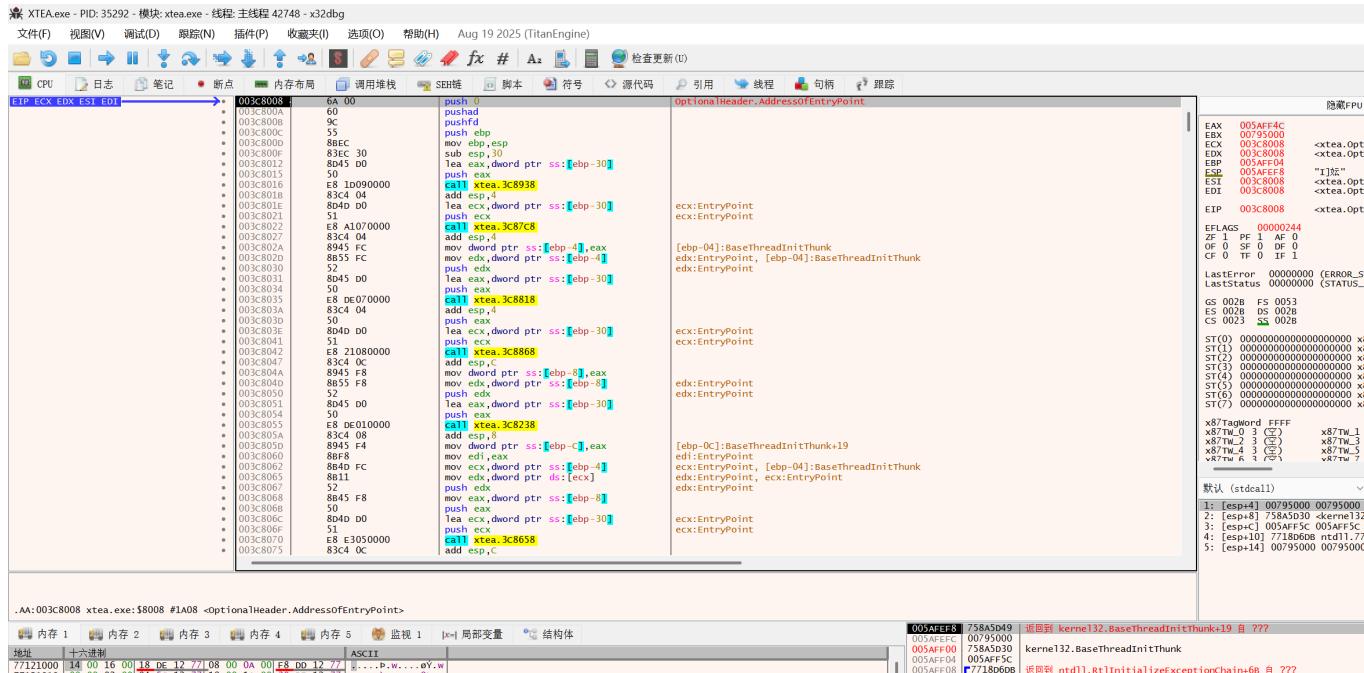
逆向wp-7

逆向题目wp

张程思

一,xtea(复现一下这次isctf没解出来的一个题)

1,这是一个程序带有一个别人的手搓壳,先x32dbg打开,用esp定律脱第一步,先f9跳到这里



2. 下个断点

XTEA.exe - PID: 34496 - 模块: xtea.exe - 线程: 主线程 11420 - x32dbg

文件(E) 视图(V) 调试(D) 跟踪(N) 插件(P) 收藏夹(I) 选项(O) 帮助(H) Aug 19 2025 (TitanEngine)

CPU 日志 笔记 断点 内存布局 调用堆栈 SEH链 脚本 符号 源代码 引用 线程 句柄 跟踪

OptionalHeader.AddressOfEntryPoint

EIP 00A2800A

```

00A2800A 6A 00 push 0
00A2800B 60 pushad
00A2800C 55 push ebp
00A2800D 8BEC mov ebp,esp
00A2800E 83E9 30 sub esp,30
00A28012 80E5 00 lea eax,dword ptr ss:[ebp-30]
00A28013 83C4 04 push eax
00A28014 E8 10900000 add esp,4
00A28015 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28016 80AD 00 push ecx
00A28017 51 call xtea.A28938
00A28018 83C4 04 add esp,-4
00A28019 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28020 80AD 00 push ecx
00A28021 51 call xtea.A287C8
00A28022 83C4 04 add esp,-4
00A28023 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28024 80AD 00 push ecx
00A28025 51 call xtea.A28868
00A28026 83C4 04 add esp,-4
00A28027 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28028 80AD 00 push ecx
00A28029 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28030 80AD 00 push ecx
00A28031 80AD 00 lea eax,dword ptr ss:[ebp-30]
00A28032 80AD 00 push ecx
00A28033 83C4 04 add esp,-4
00A28034 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28035 80AD 00 push ecx
00A28036 83C4 04 add esp,-4
00A28037 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28038 80AD 00 push ecx
00A28039 83C4 04 add esp,-4
00A28040 80AD 00 lea eax,dword ptr ss:[ebp-30]
00A28041 51 call xtea.A28868
00A28042 83C4 04 add esp,-4
00A28043 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28044 80AD 00 push ecx
00A28045 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28046 80AD 00 push ecx
00A28047 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28048 80AD 00 push ecx
00A28049 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28050 80AD 00 push ecx
00A28051 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28052 80AD 00 push ecx
00A28053 83C4 04 add esp,-4
00A28054 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28055 80AD 00 push ecx
00A28056 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28057 80AD 00 push ecx
00A28058 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28059 80AD 00 push ecx
00A28060 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28061 80AD 00 push ecx
00A28062 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28063 80AD 00 push ecx
00A28064 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28065 80AD 00 push ecx
00A28066 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28067 80AD 00 push ecx
00A28068 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28069 80AD 00 push ecx
00A28070 83C4 04 lea eax,dword ptr ss:[ebp-30]
00A28071 80AD 00 push ecx
00A28072 83C4 04 add esp,-4

```

隐藏CPU

EAX 0137F8C' 01322000 <xtea.OptionalHeader.AddressOfEntryPoint>
EBC 00A28008 <xtea.OptionalHeader.AddressOfEntryPoint>
EDC 00A28008 <xtea.OptionalHeader.AddressOfEntryPoint>
EDH 0137F834 <xtea.OptionalHeader.AddressOfEntryPoint>
EDL 0137F824 <xtea.OptionalHeader.AddressOfEntryPoint>
EDR 00A28008 <xtea.OptionalHeader.AddressOfEntryPoint>

EIP 00A2800A xtea.exe:00A2800A

EFLAGS 000000246 ZF 1 PF 1 AF 0 OF 0 SF 0 TF 0 CF 0 IF 0

LastError 00000000 (ERROR_SUCCESS)

LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)

GS 0028 FS 0053 ES 0028 CS 0028

ST(0) 00000000000000000000000000000000 x87r_0 0x0 0x00000000
ST(2) 00000000000000000000000000000000 x87r_2 0x0 0x00000000
ST(3) 00000000000000000000000000000000 x87r_3 0x0 0x00000000
ST(5) 00000000000000000000000000000000 x87r_5 0x0 0x00000000
ST(7) 00000000000000000000000000000000 x87r_7 0x0 0x00000000

x87Tw_0 0x0 0x00000000 x87Tw_1 0x0 0x00000000
x87Tw_2 0x0 0x00000000 x87Tw_3 0x0 0x00000000
x87Tw_4 0x0 0x00000000 x87Tw_5 0x0 0x00000000
x87Tw_6 0x0 0x00000000 x87Tw_7 0x0 0x00000000

默认 (stdcall) v 5 解锁

1: [esp+4] 00A28000 kernel32!BaseThreadInitThunk+19 0x758A5049
0137F830 01322000 01322000 0137F830 kernel32!BaseThreadInitThunk
2: [esp+4] 00A28000 kernel32!BaseThreadInitThunk+19 0x758A5049
3: [esp+4] 0137F830 01322000 0137F830 kernel32!BaseThreadInitThunk
4: [esp+10] 0137F83C 0137F83C 0137F83C kernel32!BaseThreadInitThunk
5: [esp+14] 77180606 ntdll!InitializeExceptionChain+68 0x77180606

3,跳到这里dump

XTEA.exe - PID: 34924 - 模块: xtea.exe - 线程: 主线程 39596 - x32dbg

文件(E) 视图(V) 调试(D) 跟踪(N) 插件(P) 收藏夹(I) 选项(O) 帮助(H) Aug 19 2025 (TitanEngine)

CPU 日志 笔记 断点 内存布局 调用堆栈 SEH链 脚本 符号 源代码 引用 线程 句柄

EIP 00A21873

```

00A21873 E8 C8030000 call xtea.A21C40
00A21874 E9 71FFFF jmp xtea.A216EE
00A21875 55 push ebp
00A21876 8BEC mov ebp,esp
00A21877 6A 00 pushad
00A21878 FF15 04304000 call dword ptr ds:[403004]
00A21879 FF75 08 push dword ptr ss:[ebp+8]
00A21880 FF15 04304000 call dword ptr ds:[403020]
00A21881 68 090400C0 push c0000409
00A21882 FF15 08304000 call dword ptr ds:[403008]
00A21883 50 push eax
00A21884 FF15 0C304000 call dword ptr ds:[40300C]
00A21885 5D pop ebp
00A21886 55 pushad
00A21887 8BEC mov ebp,esp
00A21888 81EC 24303000 sub esp,324
00A21889 6A 17 push 17
00A21890 FF15 10304000 call dword ptr ds:[403010]
00A21891 85C0 test eax,eax
00A21892 74 05 je xtea.A218BF
00A21893 6A 02 push 2
00A21894 59 pop ecx
00A21895 CD 29 int 29
00A21896 A3 B0414000 mov dword ptr ds:[4041B0],eax
00A21897 890D AC414000 mov dword ptr ds:[4041AC],ecx
00A21898 8915 A8414000 mov dword ptr ds:[4041A8],edx
00A21899 891D A4414000 mov dword ptr ds:[4041A4],ebx
00A2189A 8935 A0414000 mov dword ptr ds:[4041A0],esi
00A2189B 893B 9C414000 mov dword ptr ds:[4041C1],edi

```

esi:EntryPoint

ecx:EntryPoint

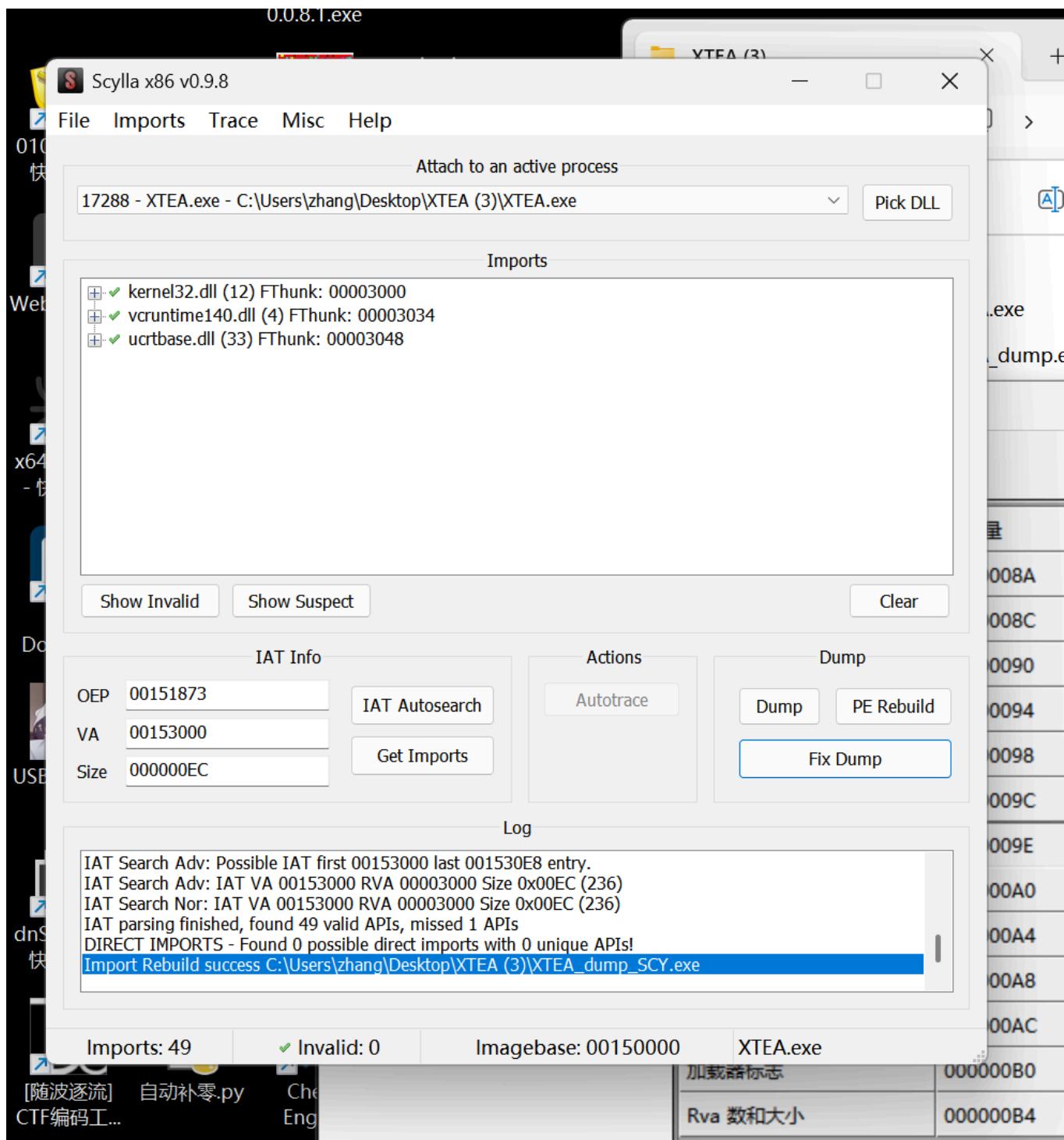
ecx:EntryPoint

ecx:EntryPoint

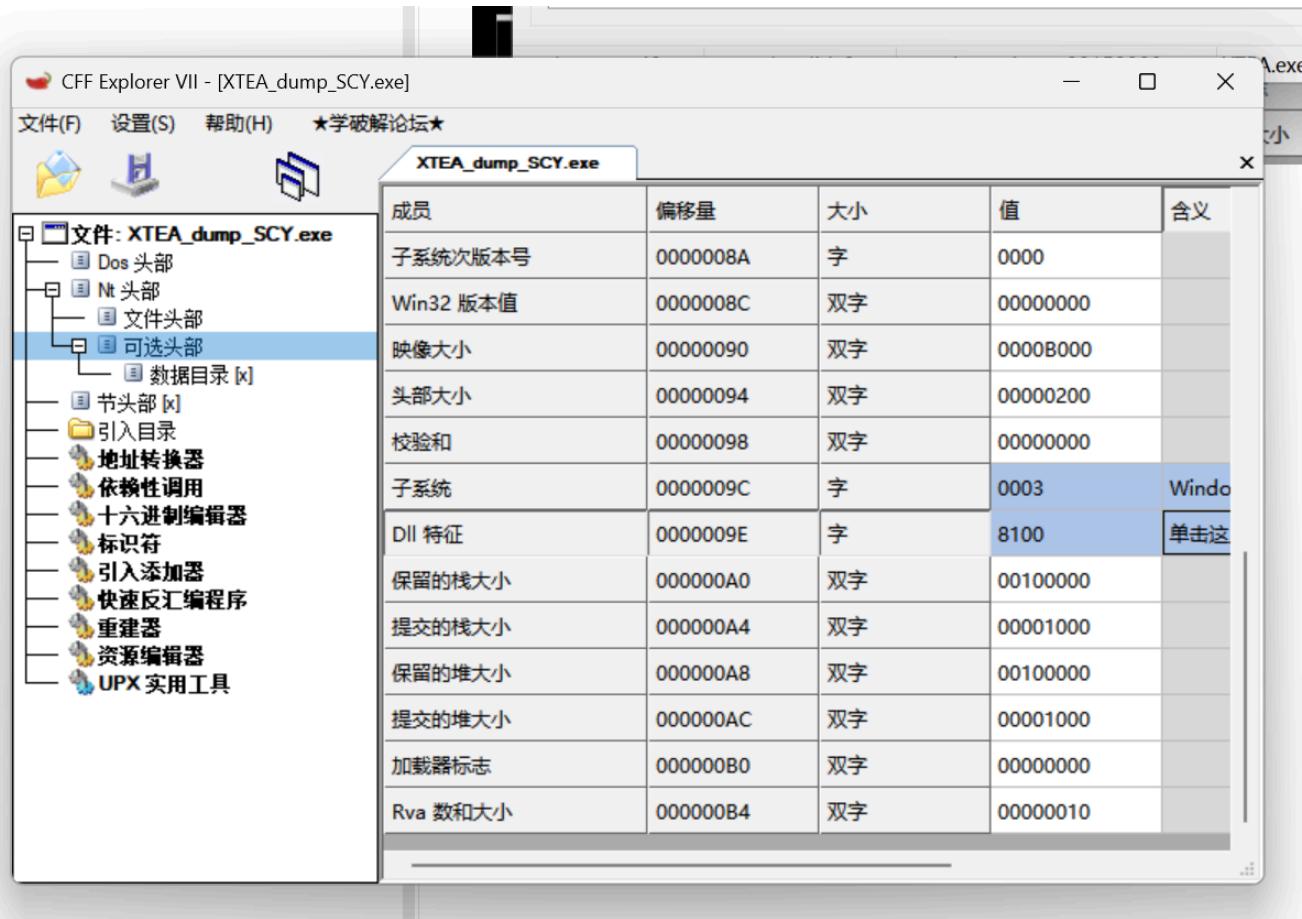
esi:EntryPoint

edi:EntryPoint

4,fixdump一下



5,再用cff去除重定位



6.终于能打开了!

剩下的很简单了,就是xtea算法加密解密