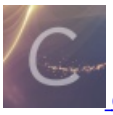
攻防世界Reverse进阶区-answer_to_everything-writeup

原创

y4ung 于 2020-10-01 10:27:06 发布 673 收藏

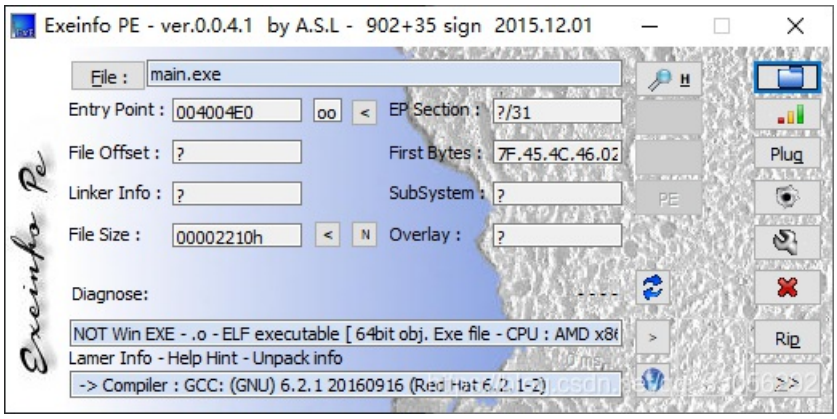
分类专栏： ctf 文章标签： ctf



本题是xctf攻防世界中Reverse的进阶区的题answer_to_everything
题目来源： 2019_ISCC
题目描述：sha1 得到了一个神秘的二进制文件。寻找文件中的flag，解锁宇宙的秘密。注意：将得到的flag变为flag{XXX}形式提交。

2. 分析

根据结果：`NOT Win EXE - .o - ELF executable [ 64bit obj. Exe file - CPU : AMD x86-64 - OS: unspecified ]`，该文件是一个linux下的64位可执行文件




```
$ chmod +x main.exe
$ ./main.exe
Gimme: 123
YOUSUCK
```

扔进IDA里看一下。`Gimme:` 在main函数中被引用。main函数中读取用户输入以后保存到v4，然后调用`not_the_flag(v4);`

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  unsigned int v4; // [rsp+Ch] [rbp-4h]

  printf("Gimme: ", argv, envp);
  __isoc99_scanf("%d", &v4);
  not_the_flag(v4);
  return 0;
}
```

跟进not_the_flag函数看一下。

```
__int64 __fastcall not_the_flag(int a1)
{
  if ( a1 == 42 )
    puts("Cipher from Bill \nSubmit without any tags\n#kdudpeh");
  else
    puts("YOUSUCK");
  return 0LL;
}
```

很明显输入必须是42。

```
$ ./main.exe 12
Gimme: 42
Cipher from Bill
Submit without any tags
#kdudpeh
```

`#kdudpeh`可能就是flag了，提交了发现不对。再看下输出，发现提示了`Submit without any tags`，再提交`kdudpeh`上去，发现还是不对。。。

再回头看看题目描述：`sha1 得到了一个神秘的二进制文件。寻找文件中的flag，解锁宇宙的秘密。注意：将得到的flag变为flag{XXX}形式提交。` 题目里提示了**sha1**!?
用sha1去加密试试得到`80ee2a3fe31da904c596d993f7f1de4827c1450a`。因此最后的flag为：`flag{80ee2a3fe31da904c596d993f7f1de4827c1450a}`，提交，正确

3. 总结

没头绪的时候可以看看**题目的描述**，有时候会有一些提示。。。