攻防世界逆向高手题之APK-逆向2

原创

沐一 · 林 于 2021-12-11 19:24:50 发布 547 收藏

分类专栏： CTF 逆向 文章标签： ctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/121877597

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

逆向

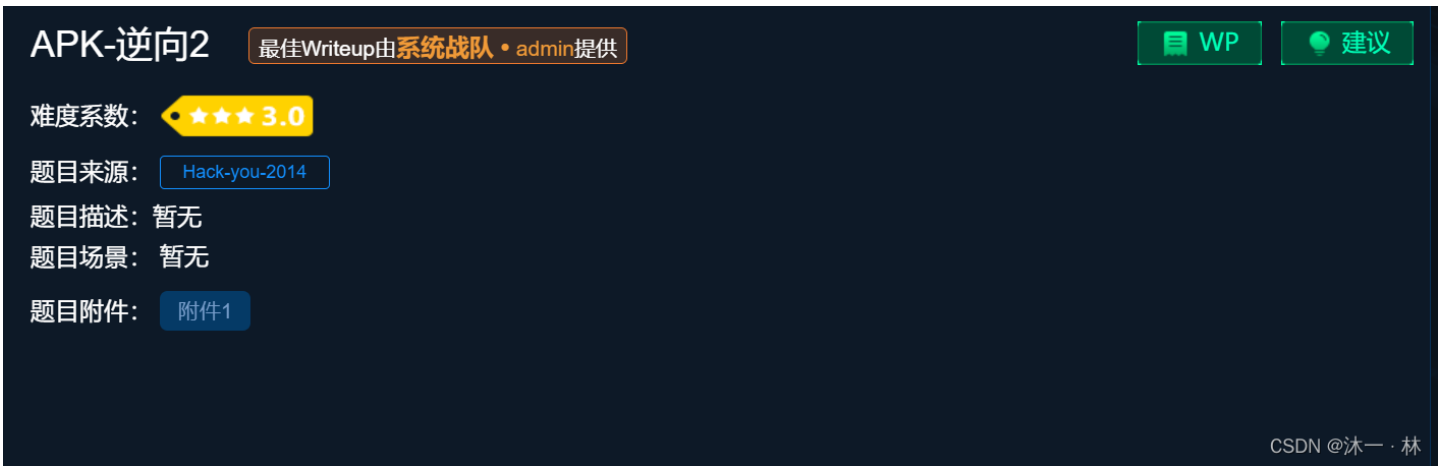
95 篇文章 6 订阅

订阅专栏

攻防世界逆向高手题之APK-逆向2

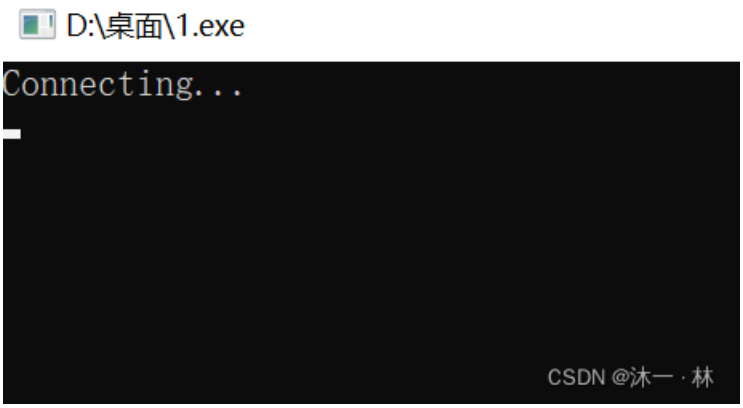
继续开启全栈梦想之逆向之旅~

这题是攻防世界逆向高手题的APK-逆向2

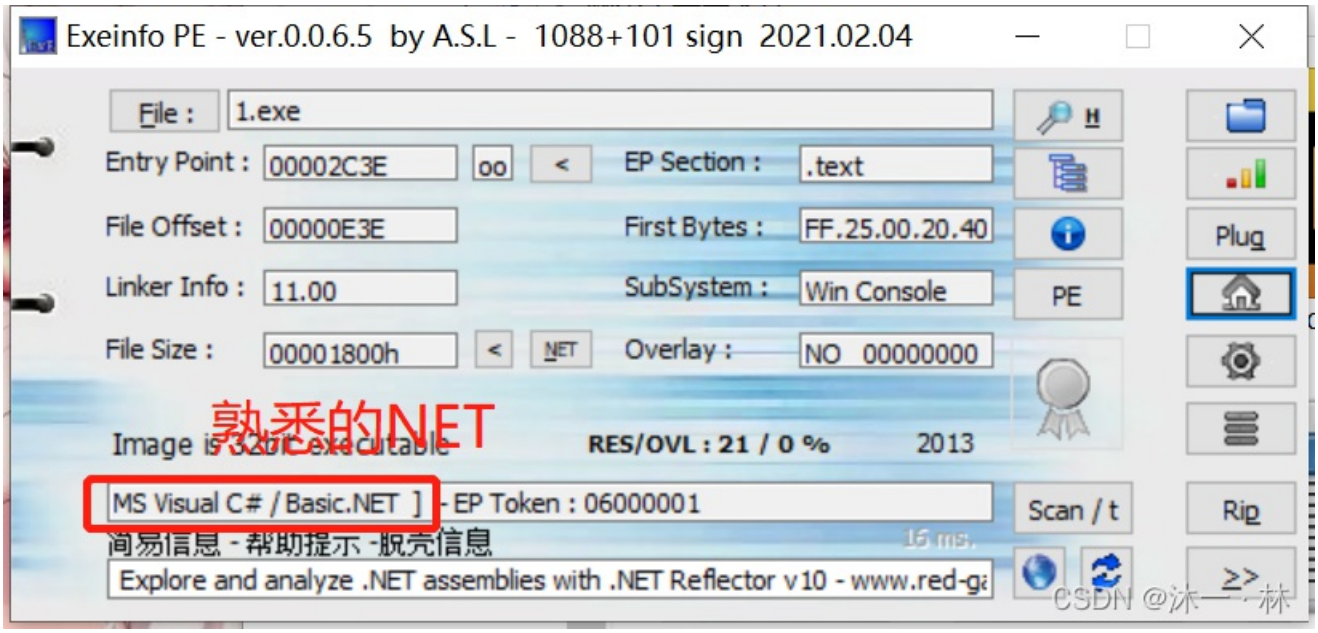


照例下载附件，这次竟然是个exe文件：

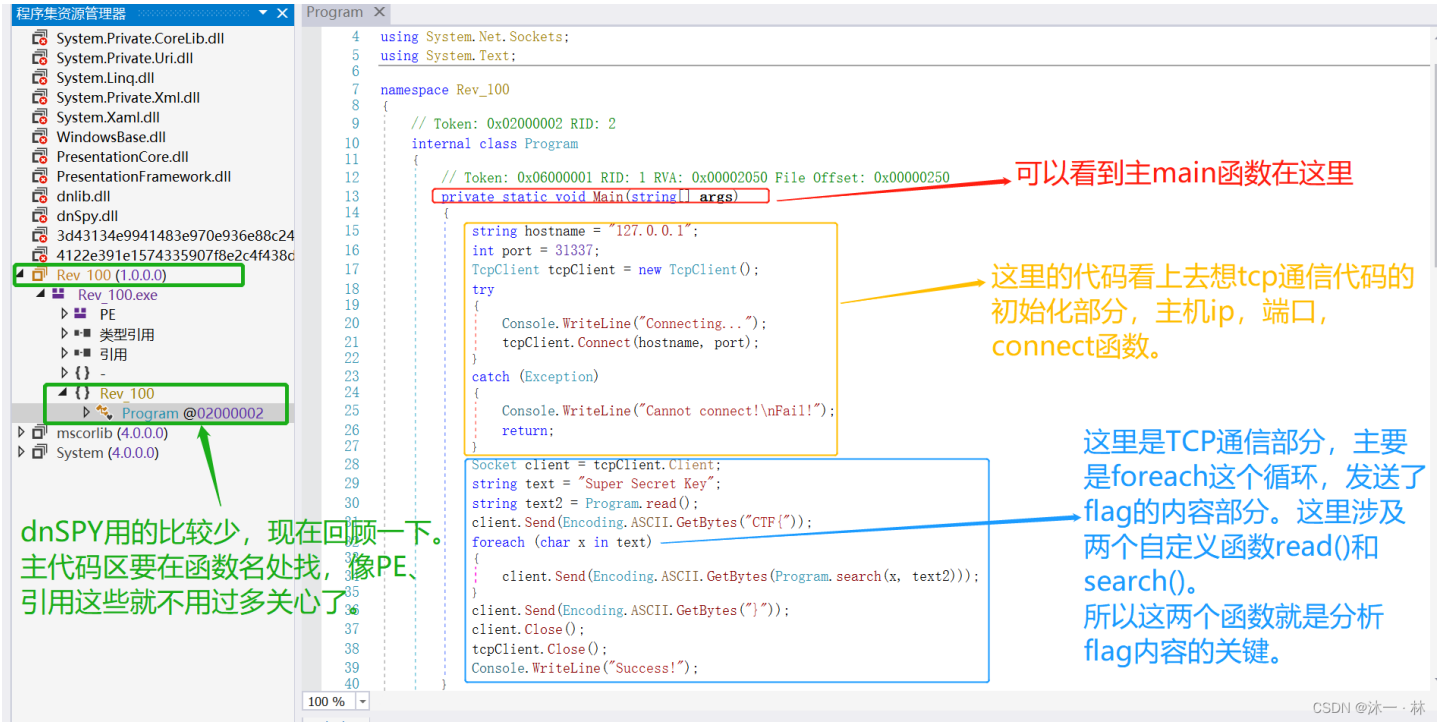
直接运行看一下主要回显信息，connecting了一会直接就退出了，根据经验可以判断是与本地环境相关：



照例放入exeinfope中查看文件类型：



NET 类型以前做过，要用 ILSPY 或 dnSPY 分析，ILSPY用来静态分析代码最好了，它的函数名虽然可能乱码不显示，但是单击函数名还是能跟踪的。而dnSPY用于动态调试的，它的函数名不仅乱码不显示，点击后还无法跟踪：(最好两个都下载，一个 动态 分析，一个 静态 分析)



所以总的流程梳理：

`程序连接本机31337端口-------->比较text和文件内容相同时的索引--------------->该索引i*1337%256并左边2位对齐补0后即可输出flag。`

.

.

所以flag只有程序`运行`起来就会显示，我们有`两个`做题方法，第一个直接开启并监听`31337`端口，第二个直接`读取`文件输出对应逻辑的i*1337%256。

.

.

第一种方法，使用python的http.server模块简单地实行HTTP servers服务：（为此我还简单学了一下http.server模块~）

```
import http.server

server_address = ('127.0.0.1', 31337)
handler_class = http.server.BaseHTTPRequestHandler
httpd = http.server.HTTPServer(server_address, handler_class)
httpd.serve_forever()
```

.

.

第二个更简单的直接nc -l -p 31337端口：

.

.

第三个直接读取文件后用同样逻辑正向输出即可，这里要注意exe文件中是unicode编码，所以读取出来时要用unicode-escape解码：

```
key1="Super Secret Key"
key2=open('1.exe','r',encoding = 'unicode-escape').read()    #新操作之文件字节码编码,exe文件中是unicode编码
num=len(key2)

flag="CTF{"

def search(x,key2,num):
 for i in range(num):
  if x==key2[i]:
   value=i * 1337 % 256;
   return '%02x' %value          #新操作之return直接返回print语句

for j in key1:
 flag+=search(j,key2,num)


flag+="}"
print(flag)
```

结果：

```
└─$ python 2.py
CTF{7eb67b0bb4427e0b43b40b6042670b55}
```

.

.

.

解毕！敬礼！