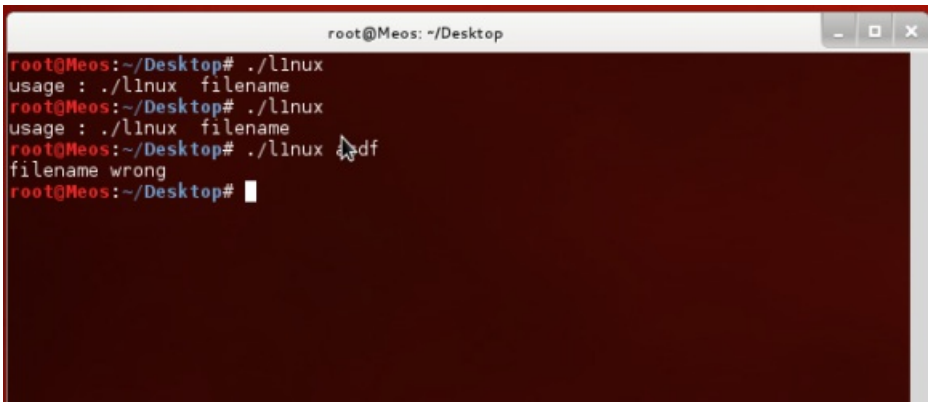
CUIT CTF WriteUp-鬼子进村

原创

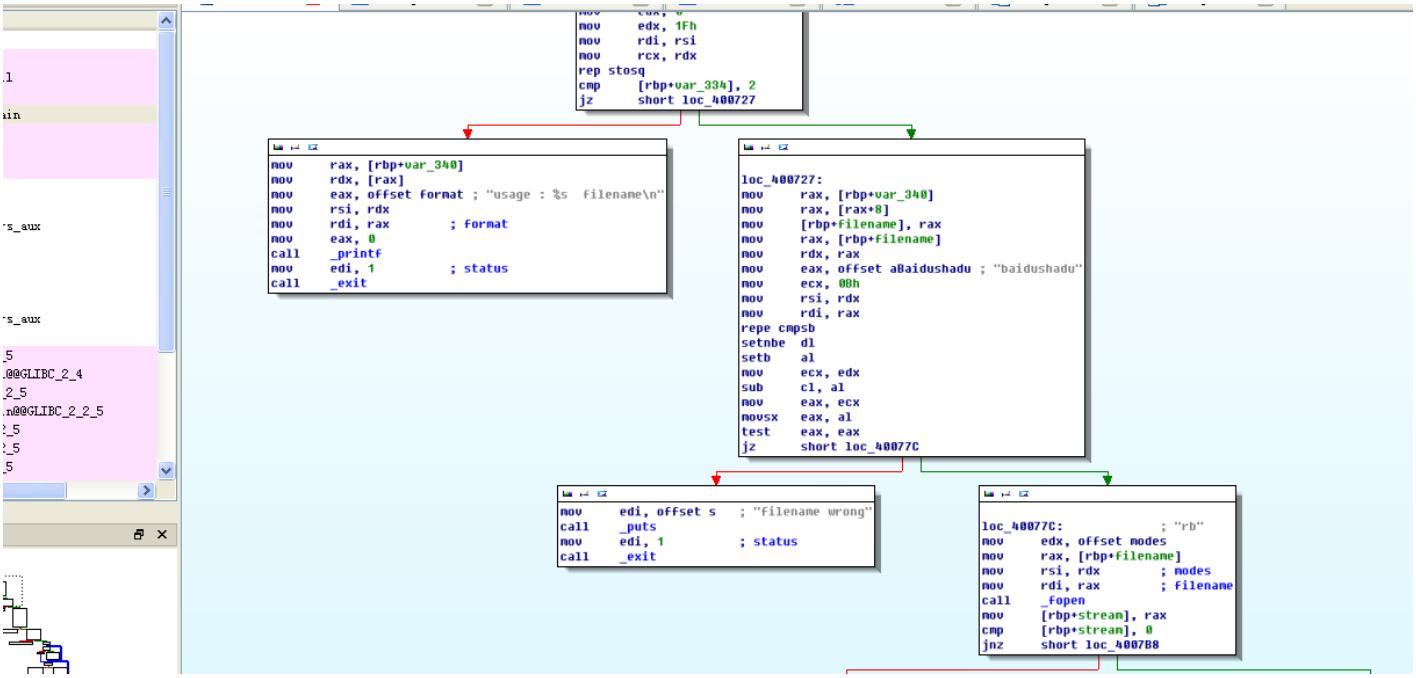
RickGray 于 2014-05-22 16:23:57 发布 1181 收藏
分类专栏： CTF纪实

该题也出的比较有意思，64位的linux下的逆向，对于我这种逆向菜鸟第一次利用IDA纯静态分析撸出题来，简直是一大突破，下面就简单分析下撸题过程。

首先运行看程序是个什么东西，运行后发现需要输入一个文件名作为参数



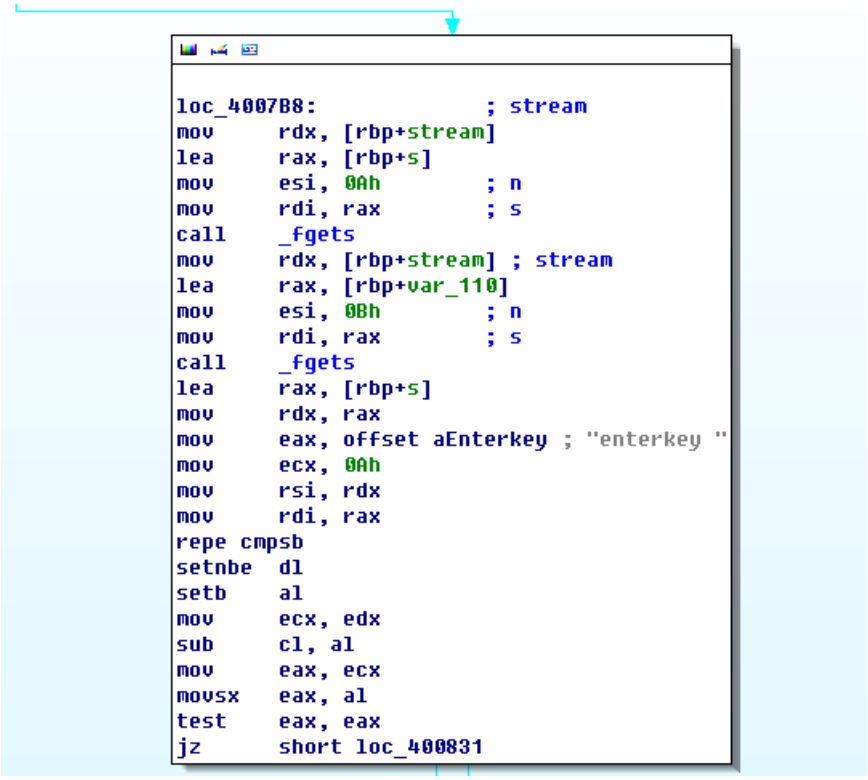
正确的文件名通过IDA定位后发现为“baidushadu”（这名字：好坑）



（IDA的Graph还真清晰呢）通过IDA的Graph显示就可以很清楚地看到整个程序的流程，后面的操作就好办多了

直接在Graph里面分析，当参数为“baidushadu”时，程序会分两次读取文件内的信息，两次读取的字节不一样

通过IDA分析可以知道，第一次读取10Bytes，第二次为12Bytes，并且通过IDA反汇编处的代码，可以判断出，程序会将第一次读取的字符串与“enterkey ”进行匹配



继续往下面看，发现程序会将第二次读入的12bytes进行处理然后与“pqllauzduh”进行比对，经过分析具体处理过程如下

设第二次读入的12bytes为字符串Str1，并令Str2 = “pqllauzduh”，那么处理过程如下

```
for i in range(0, 5):
    Str1[i] = chr(ord(Str[i]) - 4)

for i in range(5, 10):
    Str1[i] = chr(ord(Str[i]) + 3)
```

然后写个程序逆向处理可以得到Str1为：tupperware

```
s = ‘pqllauzduh’
flag = ‘’
for i in range(0, 5):
   flag += chr(ord(s[i]) + 4)
for i in range(5, 10):
   flag += chr(ord(s[i]) - 3)
```

So，flag： *tupperware*