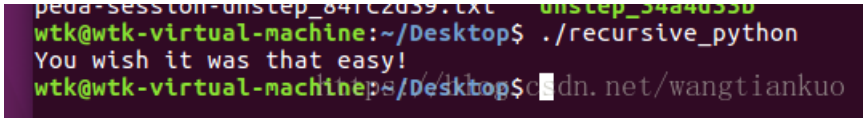
recursive_python writeup

原创

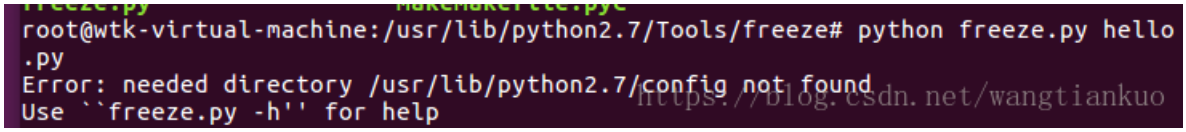
wangtiankuo 于 2018-07-17 16:28:29 发布 550 收藏
分类专栏： writeup 文章标签： recursive_pyhton

题目链接：http://ctf5.shiyanbar.com/reverse/recursive/recursive_python

运行recursive_python之后，输出了一句话“You wish it was that easy!”，然后生成了三个ELF文件，又立马删除了。



搜索资料后得到信息，该可执行文件应该是用freeze.py将python文件打包成可执行文件的。想自己写个程序然后用freeze.py打包成可执行文件，然后跟recursive_python对比着看一下，但是把freeze相关的文件都放到python2.7文件夹下，使用freeze.py报错如下：



解决办法：

1. 安装python2.7-dev、python2.7-example
2. 添加软链接 ln -s /usr/lib/python7/config /usr/lib/python2.7/config-x86_64-linux-gnu/

这两步操作完之后使用freeze就不会报错了。

生成的可执行的hello 之后，使用IDA查看，和recursive_python基本一致，查看字符串尝试找到“Hello world...”，并未找到。（用gdb调试程序，然后使用find Hello可以找到字符串。）

没有办法了，只能按照别人的writeup来做了。

使用命令“gdb recursive_python”调试程序

b chmod ；给chmod函数下断点

r ； 重新执行程序

```
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from recursive_python...done.
gdb-peda$ b chmod
Breakpoint 1 at 0x4179d0
gdb-peda$ r
Starting program: /home/wtk/Desktop/recursive_python
[Thread debugging using libthread_db enabled]
```

断下来之后，发现生成的一个文件unstep_84fc2d39，使用“shell”命令，回到非调试状态，查看该文件属性，不可执行。

```
root@wtk-virtual-machine:/home/wtk/Desktop# ll unstep_84fc2d39
-rw-r--r-- 1 root root 36470152 7月  17 15:25 unstep_84fc2d39
root@wtk-virtual-machine:/home/wtk/Desktop#
```

修改该文件权限，使其可执行，调试该文件，同样在chmod函数处下断点

```
root@wtk-virtual-machine:/home/wtk/Desktop# chmod +x unstep_84fc2d39
```

断下来之后，生成了unstep_34a4d33b，对unstep_34a4d33b进行和unstep_84fc2d39一样的操作，生成了unstep_579c82e9，对unstep_579c82e9进行同样操作，生成了unstep_f67baaeb，使用gdb调试unstep_f67baaeb，“start”启动程序，“find flag”找到了flag。

flag{python_taken_2_far}

```
root@wtk-virtual-machine:/home/wtk/Desktop# chmod +x unstep_f67baaeb
root@wtk-virtual-machine:/home/wtk/Desktop# gdb unstep_f67baaeb
```

```
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from unstep_f67baaeb...done.
gdb-peda$ start
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

[----------------------------------registers-----------------------------------
RAX: 0x485310 (<main>:  )
```

```
Temporary breakpoint 1, main (argc=0x1, argv=0x7fffff
268     frozen.c: No such file or directory.
gdb-peda$ find flag
Searching for 'flag' in: None ranges
Found 264 results, display max 256 items:
unstep_f67baaeb : 0x5aa2a3 --> 0x3a69007367616c66 ('f
unstep_f67baaeb : 0x5aa3b6 --> 0x642d007367616c66 ('f
unstep_f67baaeb : 0x5aa48f --> 0x6567007367616c66 ('f
```

```
unstep_f67baaeb : 0x8689e0 ("flags in Include/compile.h.\n\nNo fea
ver to be deleted from this file.\nt\r")
unstep_f67baaeb : 0x868ba6 --> 0x42867616c66
unstep_f67baaeb : 0x8693c3 ("flag{python_taken_2_far}s\032")
--More--(25/257)
```