




Linux pwn入门教程,PWN入门的入门——工具安装

转载

十三金  于 2021-05-02 16:13:27 发布  127  收藏

文章标签: [Linux pwn入门教程](#)

安装pwntool:

命令行运行:

```
1 pip install pwntools
```

```
1 python2 importpwn3 pwn.asm("xor eax,eax")
```

出现'1\x0c' 说明安装成功

在pycharm中运行出错: `_curses.error: must call (at least) setupterm() first`

解决方案: <https://stackoverflow.com/questions/9485699/setupterm-could-not-find-terminal-in-python-program-using-curses/21571407#21571407>

```
1 sudo vi /usr/lib/pycharm-community/bin/pycharm.sh2 #set env for pwntools
```

```
3 export TERM=linux4 export TERMINFO=/etc/terminfo
```

如果是一台刚刚安装好的虚拟机[神码配置都没有], 如果安装中出现报错, 可能是漏装了依赖, 下面给出官方的安装教程:

```
apt-get update
```

```
apt-get install python3 python3-pip python3-dev git libssl-dev libffi-dev build-essential
```

```
python3 -m pip install --upgrade pip
```

```
python3 -m pip install --upgrade git+https://github.com/Gallopsled/pwntools.git@dev
```

对ubuntu16+默认python2 安装pwntools:

```
sudo apt install python-pip # 没有pip安装pip
```

```
mkdir GitHub
```

```
cd GitHub
```

```
sudo apt install git
```

```
git clone https://github.com/Gallopsled/pwntools
```

```
apt-get install libssl-dev libffi-dev build-essential
```

```
python setup.py install
```

安装checksec :

命令行运行:

```
1 apt-get install checksec
```

攻防世界的一道题试验一下：

get_shell

4 最佳Writeup由w0odpeck3r • 老王提供

难度系数：

题目来源： 暂无

题目描述： 运行就能拿到shell呢，真的

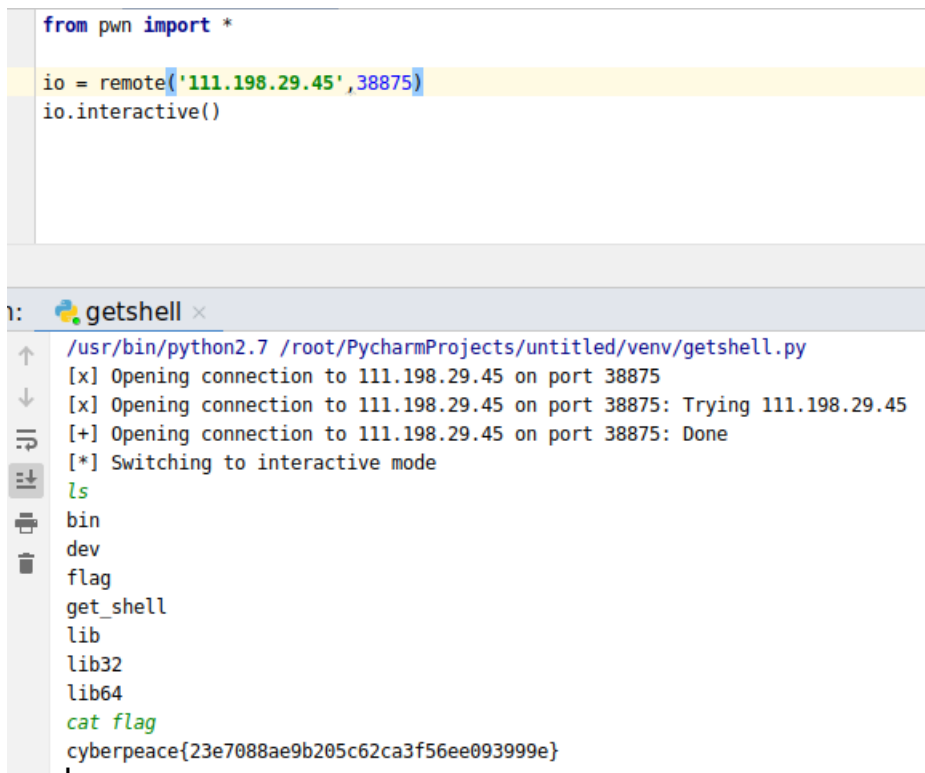
题目场景：

点击获取在线场景

题目附件：

```
from pwn import *

io = remote('111.198.29.45', 38875)
io.interactive()
```



```
getshell x
/usr/bin/python2.7 /root/PycharmProjects/untitled/venv/getshell.py
[x] Opening connection to 111.198.29.45 on port 38875
[x] Opening connection to 111.198.29.45 on port 38875: Trying 111.198.29.45
[+] Opening connection to 111.198.29.45 on port 38875: Done
[*] Switching to interactive mode
ls
bin
dev
flag
get_shell
lib
lib32
lib64
cat flag
cyberpeace{23e7088ae9b205c62ca3f56ee093999e}
|
```

安装LibcSearcher:

```
git clone https://github.com/lieanu/LibcSearcher.git
```

```
cd LibcSearcher
```

```
python setup.py develop
```

SSH指定端口下载文件:

```
scp -P 2222 -r random@pwnable.kr:random.c .
```