**Neo-regeorg+proxifier**

正向代理：攻击机连接访问内网主机

反向代理：内网主机连接访问互联网攻击机

自搭建环境模拟Neo-regeorg+proxifier设置正向代理访问内网主机

环境搭建

攻击机：

主机名Win10(lizhikai001)

IP 192.168.100.129

Web服务器：

主机名 win10(lizhikai002)

互联网IP 192.168.100.130

内网IP 192.168.200.129

Phpstudy开启web服务

防火墙关闭

内网主机：

主机名 win10(lizhikai003)

内网IP 192.168.200.130

防火墙关闭

工具准备

需要准备的工具

攻击机

Python3环境

蚁剑

Neo-regeorg

Proxifier

内网

Phpstudy软件

蚁剑

下载地址：<https://github.com/AntSwordProject/AntSword-Loader>

用法见官网；

用一句话木马来访问

Neo-regeorg

下载地址：<https://codeload.github.com/L-codes/Neo-reGeorg/zip/refs/heads/master>

用法见官网

Proxifier

下载地址：<https://www.proxifier.com/download/ProxifierSetup.exe>

用法：

1 添加代理服务器为 127.0.0.1 端口号为Negeorg的默认端口1080

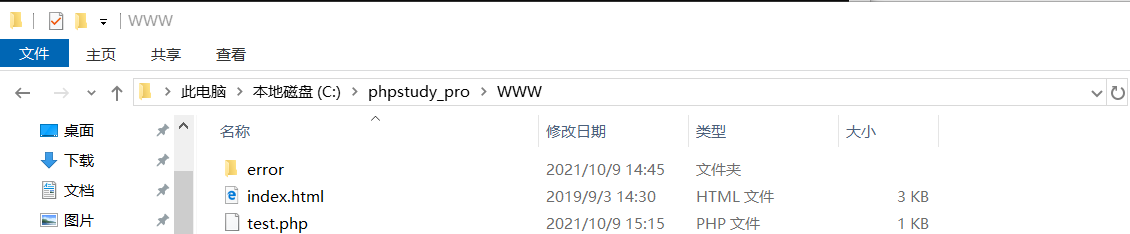
2 添加代理规则，其中自动添加的python.exe规则保持不变

3 在其他规则中添加需要设置代理的exe文件，并将该规则的代理模式改成socks5

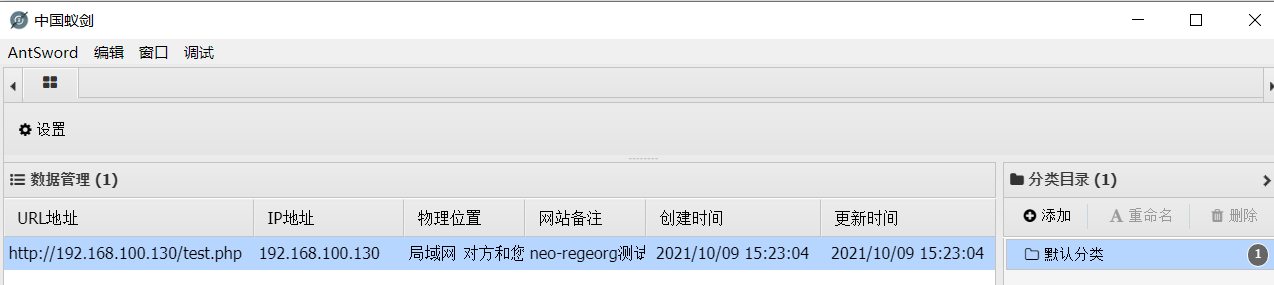
正向代理实验

一 获取服务器上传文件权限

这里直接在web服务器web站点目录上传一句话马



然后使用蚁剑连接



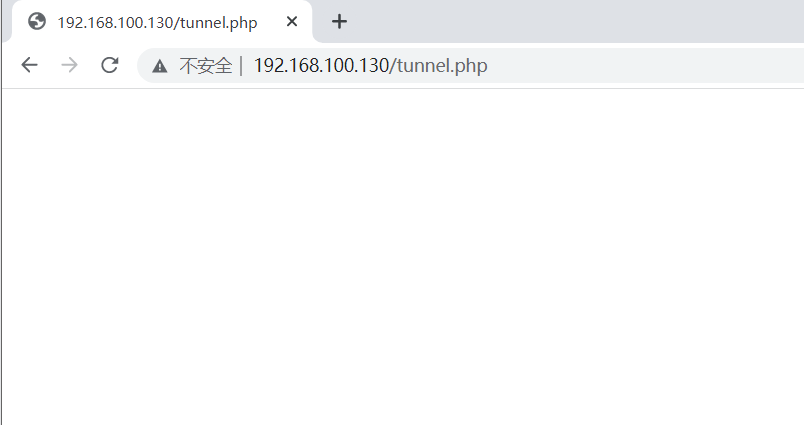
二 生成隧道搭建文件

命令

python neoreg.py generate -k admin

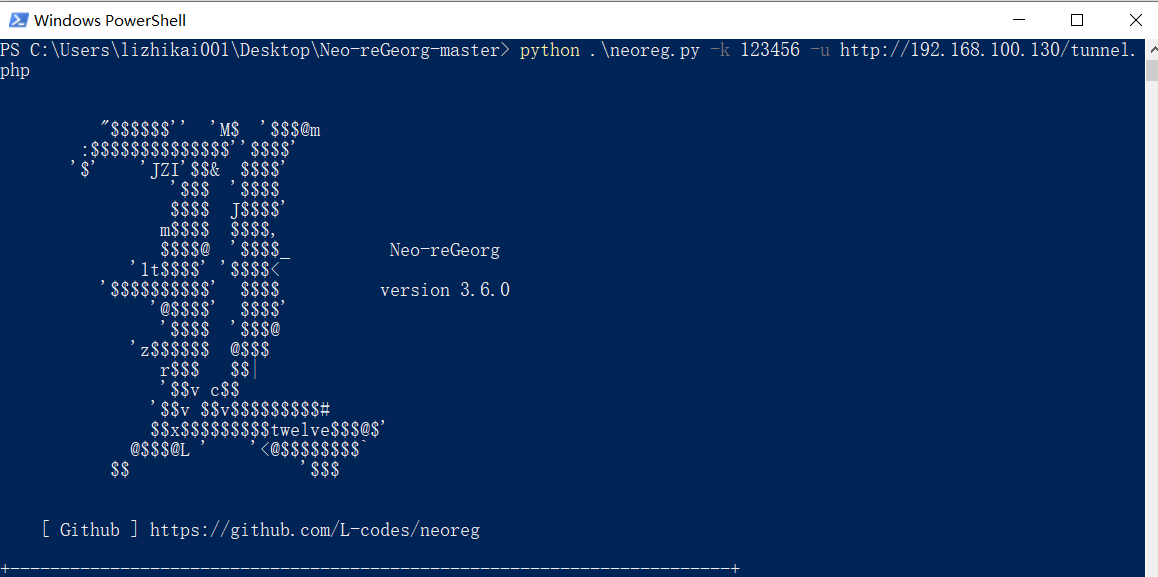
然后在neoreg-servers文件夹中找生成的php文件

最后将该php文件通过蚁剑或者其他上传文件接口上传到服务器，访问



并执行下面的命令：

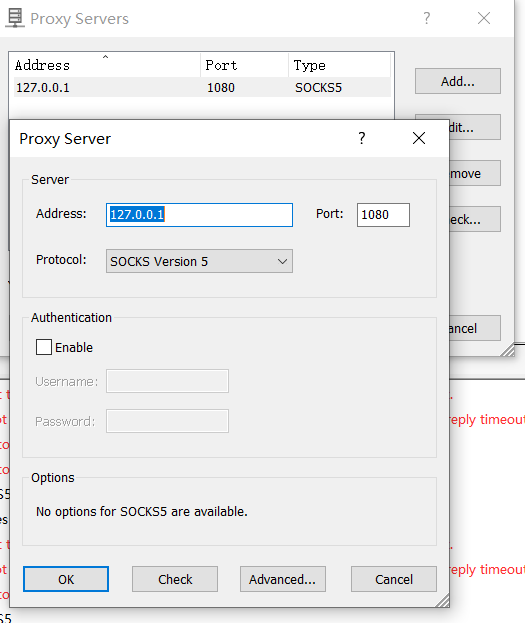
python neoreg.py -k admin -u <http://192.168.100.130/tunnel.php>



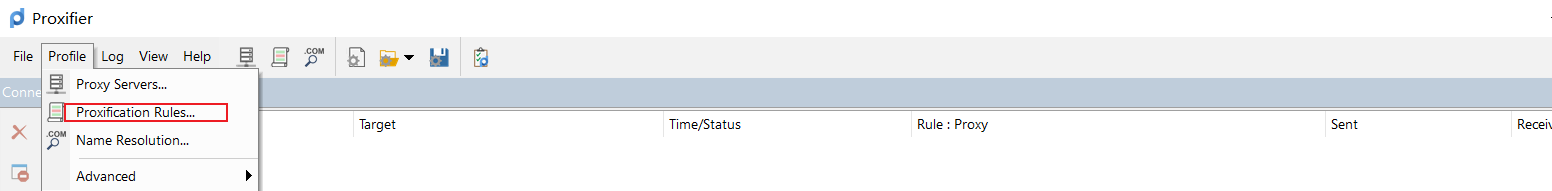
至此 隧道搭建完成，现在只需要通过proxifier对需要代理进内网的软件设置代理即可

三 proxifier设置代理

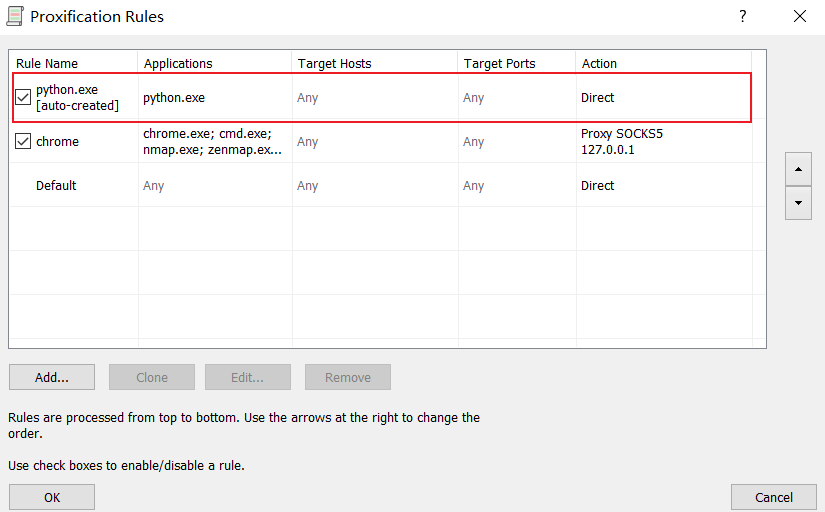
选择profile-proxy-server，添加服务器，设置如下：



确定之后，选择profile-proxification rules



设置如下

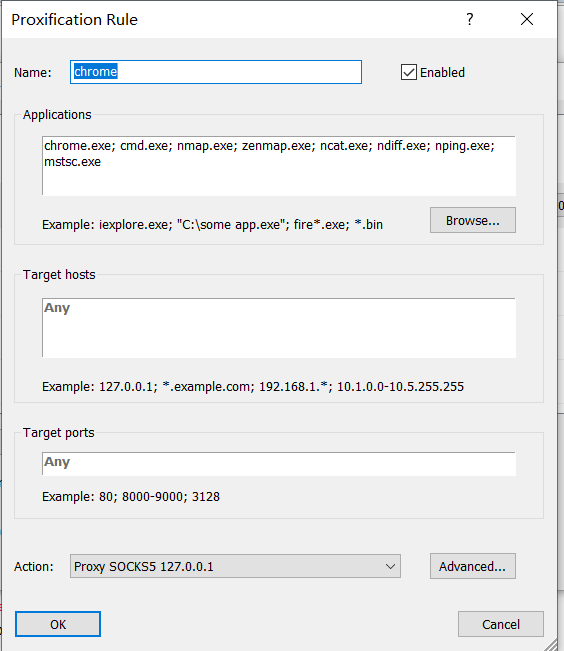


如图所示，第一条规则是自动创建的，只需要将action选项改成direct即可；

direct表示该规则中的exe文件不通过代理

proxy socks5 表示该规则中的exe文件会通过特定的代理运行

第二条规则的具体内容如下：



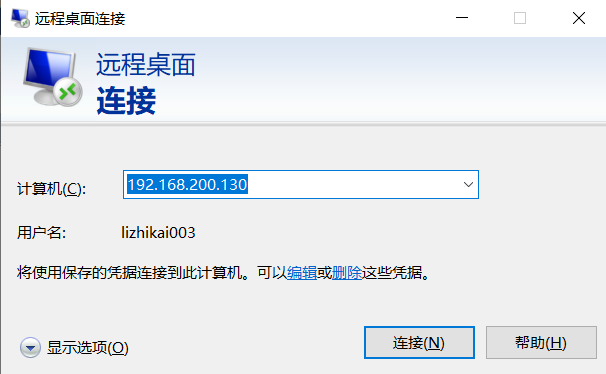
在application方框中选择需要设置代理的exe文件即可实现正向代理

四 远程连接至内网

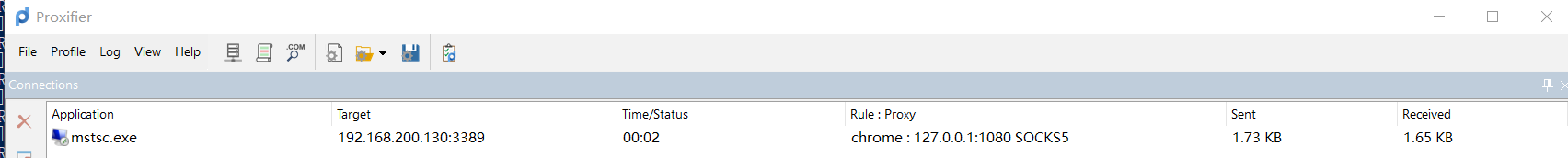
此处说明：没有设置过正向代理时，我检测过我这个实验环境中的互联网攻击机是不能够远程连接到内网ip主机的。

1 将mstsc.exe添加到application中，路径为C:\Windows\System32\mstsc.exe

2 远程连接



此时查看proxifier



发现有记录

3 连接成功

