6.2、 AnyDesk内网使用[bug]

2023年9月22日 20:11

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/1XdVkAJU_Q9rD0PMiSDZFKQ?pwd=zdpm
提取码：zdpm
--来自百度网盘超级会员V4的分享

这个AnyDesk和RustDesk一样，在内网也可以使用现在，我开始模拟环境
Kai--->->->-------A(web)外网------->->->----------B(mysql)内网
192.168.86.174
192.168.132.128 192.168.132.130

1、通过漏洞拿到A机器权限，上传Neo-reGeorg 代理出网

```
└─$ python3 neoreg.py -k admin -u http://192.168.132.128/tunnel.php -l 192.168.86.142
```

```
      "$$$$$$''   'M$   '$$$@m
    :$$$$$$$$$$$$$''$$$$'
  '$'     'JZI'$$&  $$$$'
            '$$$  '$$$$
            $$$$  J$$$$'
           m$$$$  $$$$,
           $$$$@  '$$$$_          Neo-reGeorg
        '1t$$$$' '$$$$<
     '$$$$$$$$$'  $$$$          version 5.1.0
          '@$$$$'  $$$$'
            '$$$$  '$$$@
        'z$$$$$$  @$$$
```

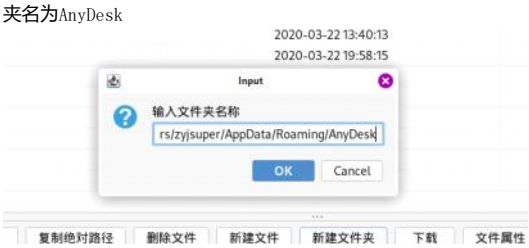
sudo vim /etc/proxychains4.conf

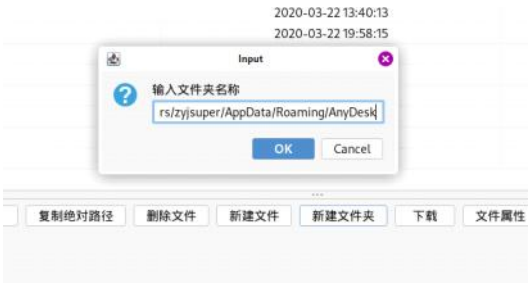
```
#       ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks5 192.168.86.142 1080

"/etc/proxychains4.conf" 162L, 5851B
```

2、设置哥斯拉代理连接内网机器

在哥斯拉中上传AnyDesk.exe到目标机器，同时创建目录**[上传完成之后不要运行，需要等四个配置文件上传到C:\Users\xxxxxx\AppData\Roaming\AnyDesk才能运行]**

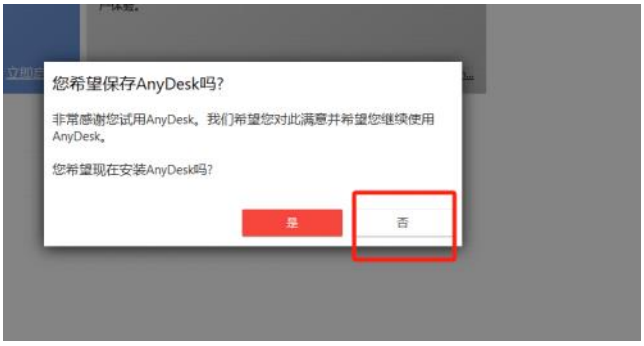
3、添加AnyDesk连接，创建目录在目标机器上的c盘 user/AppData/Roaming 处创建一个文件夹名为AnyDesk





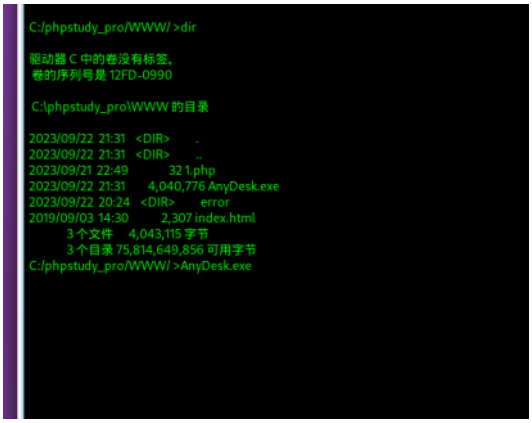
现在本地机器运行AnyDesk，这里不需要记住ID，因为是在内网，连接的时候，输入对方ip地址即可

同时设置密码和连接用户名



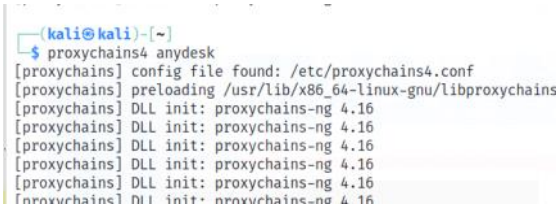
把这四个文件上传到目标机器的 C:\Users\xxxxx\AppData\Roaming\AnyDesk目录

4、运行AnyDesk

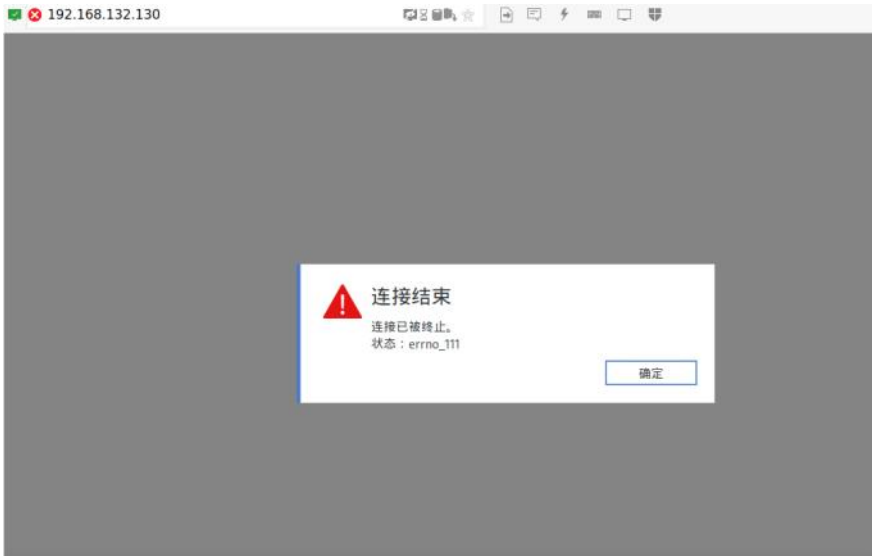


使用代码启动AnyDesk，连接内网机器

然后本地启动proxychains4 anydesk



如果出现



但是我不知道为什么老是连接失败

发现：

当多个网卡的时候

如：

A

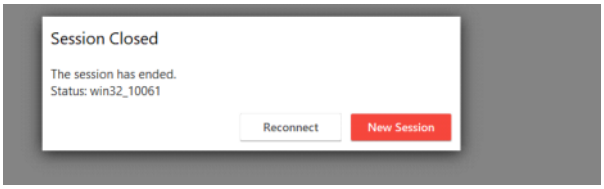
192.168.86.174

192.168.132.128

B

192.168.132.130

这个时候，A主机去连接B主机就会出现



一直失败，但是当A只有一张网卡可以成功[A--->B]

或者

B主机去访问连接了A主机成功[这个时候点击取消]，然后A再去连接B[B----(取消)-->A------->B]

也就是说：这个不适用于内网

发现错误的时候可以提醒我