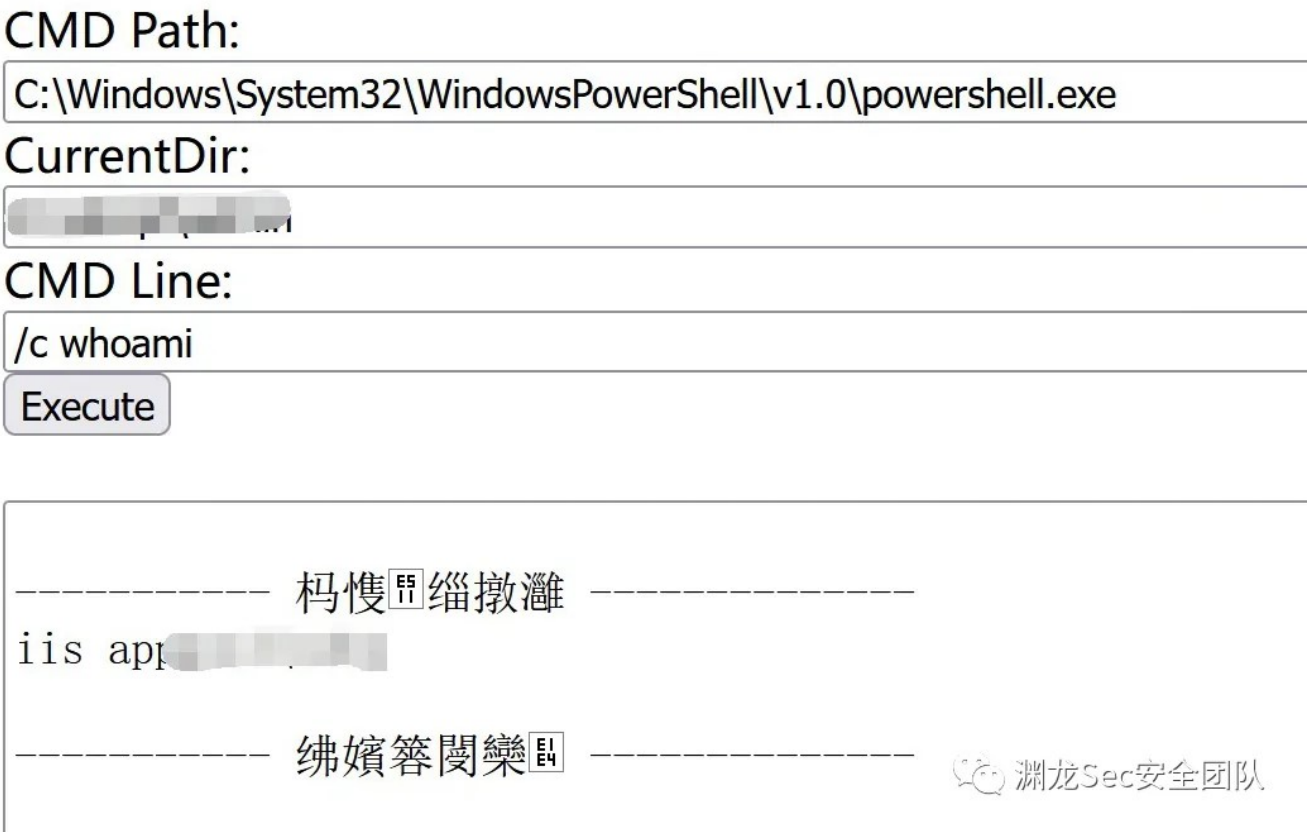
2# 入口点

通过某小公司系统拿到了该系统的Shell权限😸

当时相关权限如下图所示，非管理员权限：



然后就开始了艰难的内网上线之路🥹

3# 艰难的内网渗透

本来刚开始拿到Shell很开心的，终于可以扫内网了😆

结果现实给我重重来了一拳🤦

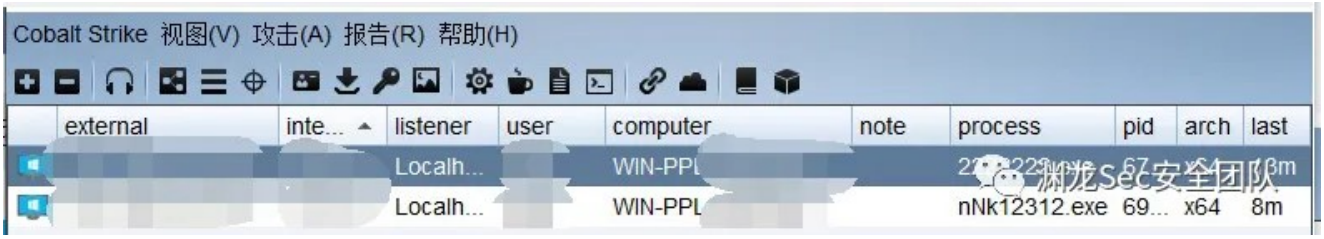
具体情况如下：

- 我的C2落地就被秒杀🎊
- Powershell无权限访问和执行😠

结果一执行 `tasklist` 才发现，服务器有条狗和卡巴斯基：

这可把我弄傻了，卡巴斯基咋个整？😡

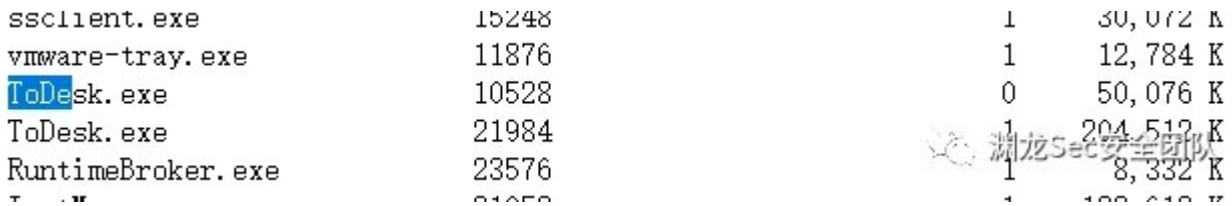
本来想着用过360的进程迁移大法试试，确实上线了，但是...还没到60s就被杀了
我进程还没迁移呢！！！就死了！



不知什么原因（可能是卡巴斯基策略），Powershell无权限不能执行命令
所以只能通过exe来上线，但是免杀我实在是菜菜，于是就开始坐牢😫

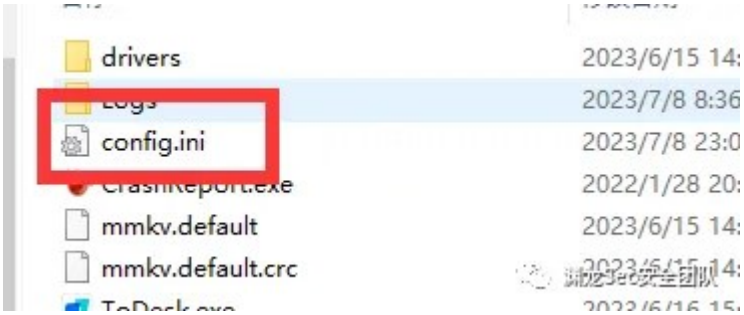
故找了一堆公开的免杀项目，从C找到Python，又从Python找到Go最后找到Rust
结果都是同样的结果：无法上线！🤫

又搞了快一天的时候，无聊又执行了一边 `tasklist` ，结果看到了一个神奇的进程：



ToDesk！！！！！！😜
突然想到能不能直接连上 `ToDesk` 进行远程控制来上线呢？

说干就干，我看了自己电脑上的 ToDesk ，想到远程控制的密钥可能就在本地某个配置文件



果然 ToDesk 的密钥就在安装目录的 config.ini 下，但密钥是加密过的，这又让我陷入难题了。。。遇事不决，百度一下！

然后发现早在去年，就已经有师傅通过 ToDesk 进行内网远程操作上线了！

并且 Todesk 每次启动，都会去安装路径下的 config.ini 下面读取一遍密钥并解密显示在程序上

那是不是可以通过系统自带的 type 命令，把被攻陷服务器上面的 Todesk 的 config.ini 读取出来，拿到本地来解密呢？说干就干！

```
[ConfigInfo]
passUpdate=3
PrivateScreenLockScreen=1
autoLockScreen=0
downloadtimes=202[redacted]0
clientId=961[redacted]
PrivateData=04928cf36e50897788[redacted]
PluginExpiresDays=0
Resolution=1920x1080
tempAuthPassEx=d15be2512fd52aeb28[redacted]
updatePassTime=202[redacted]
isOpenTempPass=0
language=936
isAdmissionControl=1
WeakPasswordTip=0
Version=4[redacted]
isUpdate=0
PresetDialogUpdateDat[redacted]
PresetDialogShowCount=0
UpdateFrequencyPromptBubble=0
LastPushTimeEx=202[redacted]
authPassEx=b64fa[redacted]
AuthMode=1
```

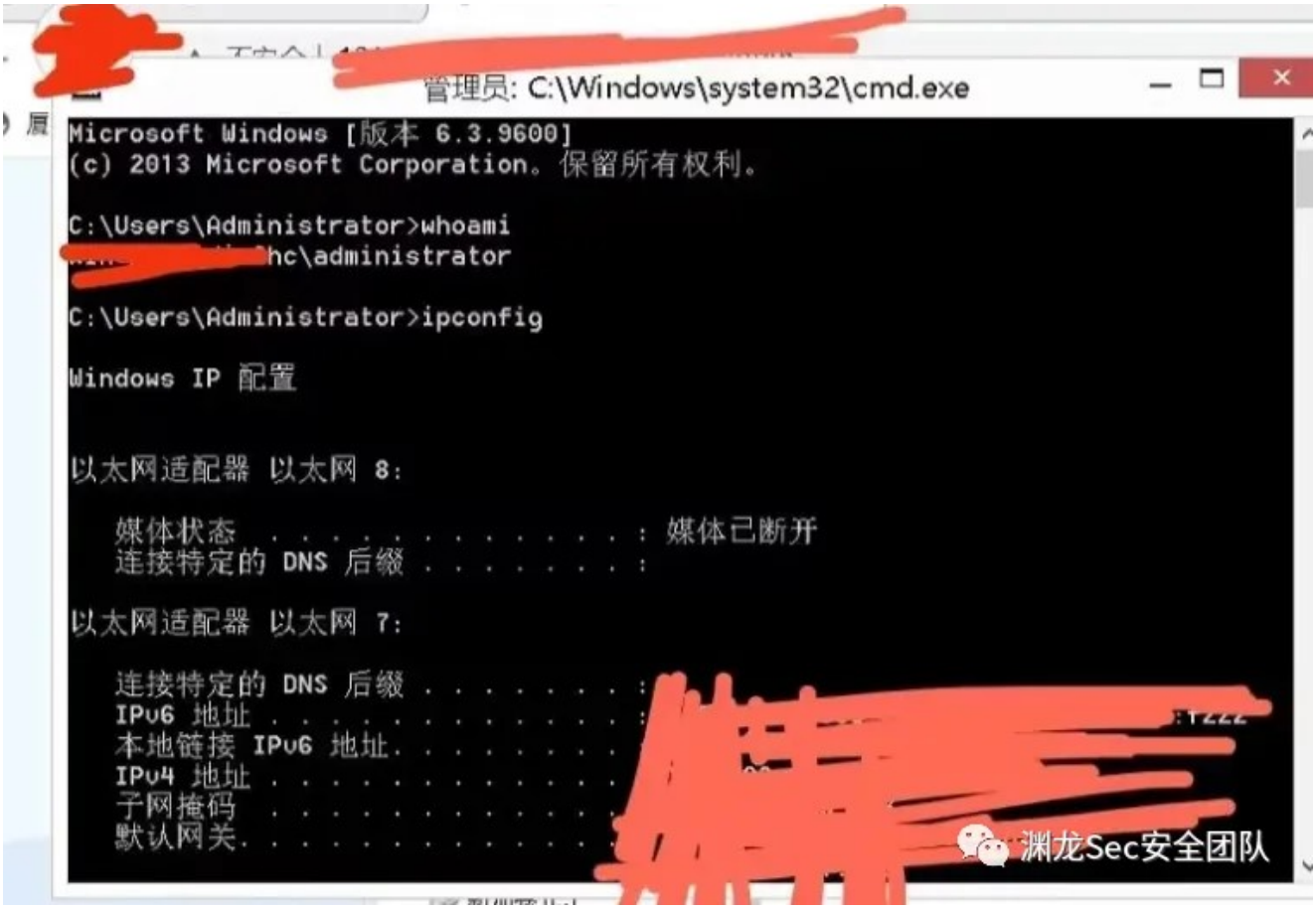

通过执行以下命令：

```
1   wmic process where name="ToDesk.exe" get processid,executablepath,name
```

获取到了 Todesk 的安装路径，再执行系统自带的 type 命令进行读取 Todesk 安装文件夹下的 config.ini 配置文件😁

在配置文件中 clientid 就是 ToDesk 的连接ID
下面的 tempAuthPassEx 、 authPassEx 、 passex 就是加密后的密钥
将这3个被加密后的密钥拉到本地的 config 的 tempAuthPassEx ，然后打开我本地的 ToDesk 客户端🤔

就可以看到我们的临时密码已经变成服务器上 ToDesk 的远程控制的密码了，然后拿这个密码去连接服务器🤪



连接成功，直接拿到运维权限！😎

接下来就是搭起隧道~开始愉快的内网扫描~

4# 信息收集后话

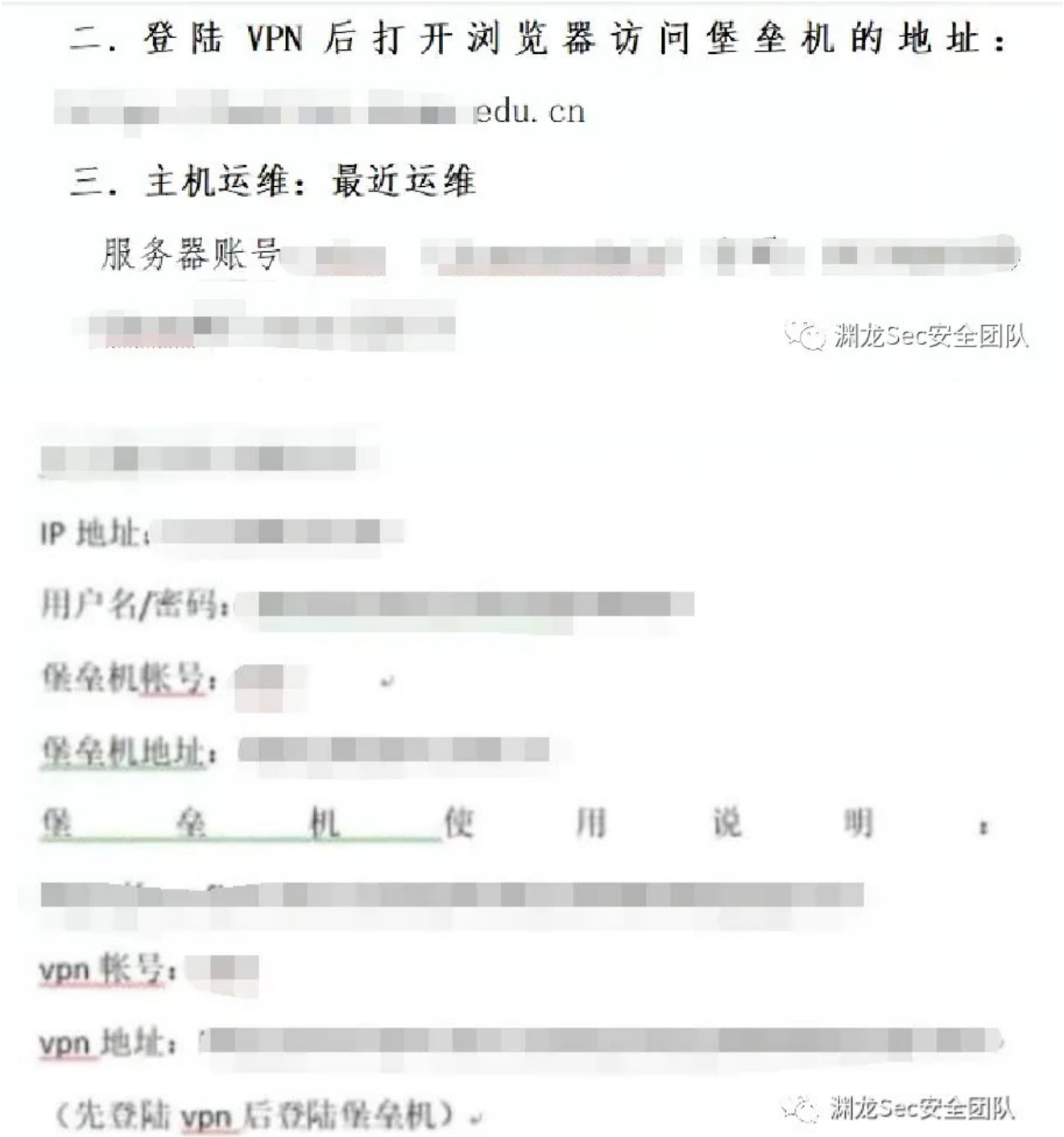
拿到权限后，第一步就是先收集了一波信息
结果令我大失所望：并没有收集到比较有价值的信息🥹

但是在桌面瞅到了QQ，于是我又开始联想：
首先，QQ会自动将图片和接受到文件都保存在QQ的默认路径下
其次，有没有可能，运维人员在和业主或者Leader沟通的时候，会传递什么敏感文件呢？😟

然后来到文档的路径直接开始直接搜索

```
1   *.jpg *.png *.txt *.doc *.docx *.xlx *.xlxs
```

搜了一波这些敏感后缀名的文件，意想不到就出了货😎



成功拿到其他多个高校的堡垒机地址和账号密码，轻松拿下多个严重！！！🤤

5# 总结

- 在渗透测试过程中，很多时候遇到解决不了的问题的时候，要多去敢想敢做，要利用好自己所收集到的信息和内容。很多时候，是有其他的突破口，要静下心来去思考问题。
- 同样，信息搜集也需要结合实际业务场景来做，通过搜集运维和其他管理人员沟通和整理的文件，拿到了敏感密码本成功搞定多个严重，这个思路非常赞！！！
- 最后再吐槽一下这次内网！真是太恶心了！全是罐子！！！简直是在罐子里面搭的内网！