

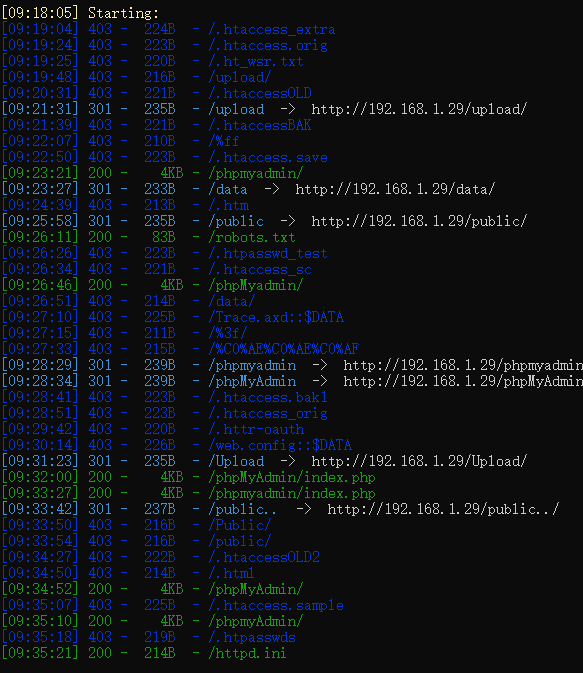
目标web：192.168.1.29

信息收集：

端口信息：



目录信息：

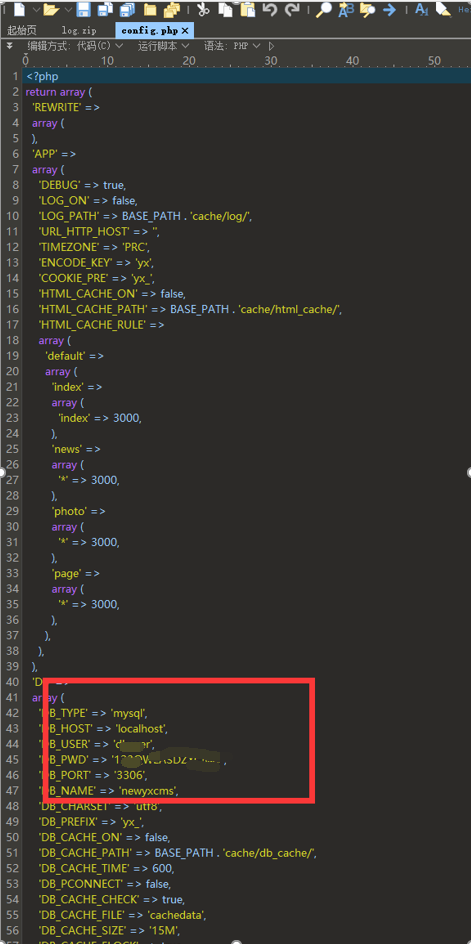


phpmyadmin



尝试弱密码登陆失败

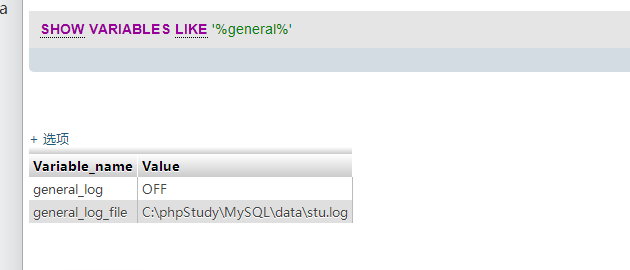
扫描出根目录有beifen.rar，里面是网站源码；



源码泄露找到数据库账号密码；

成功登录，信息收集

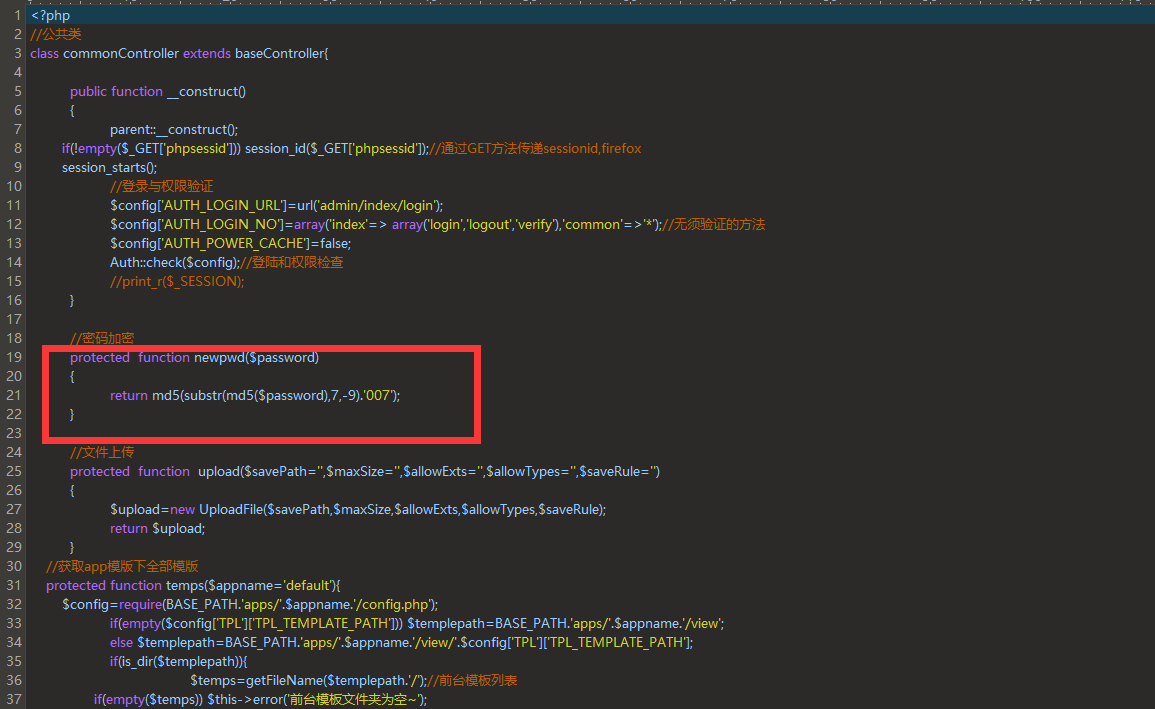




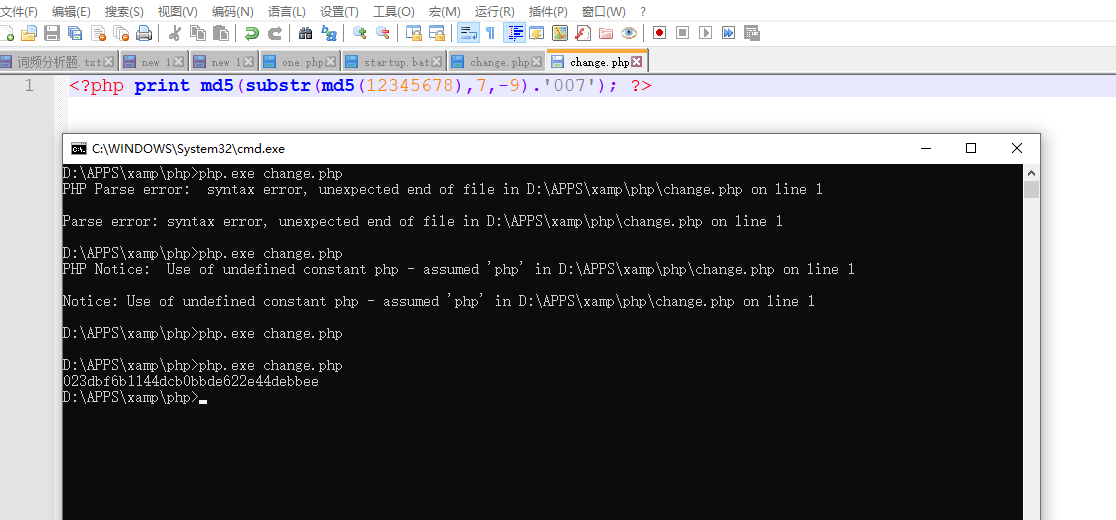


无法开启全局日志，权限不够，且没找到web路径；

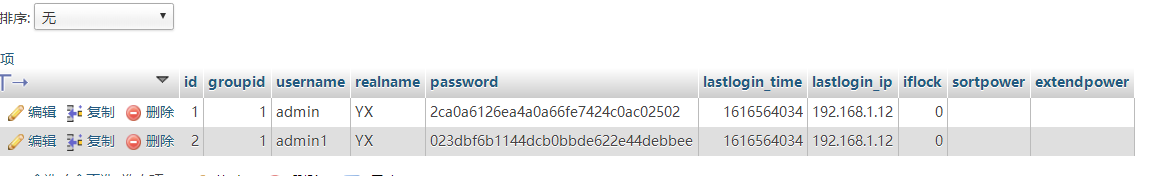
源码审计找到管理员密码生成方式



使用md5(substr(md5(12345678),7,-9).'007'); 得到一个12345678的hash，

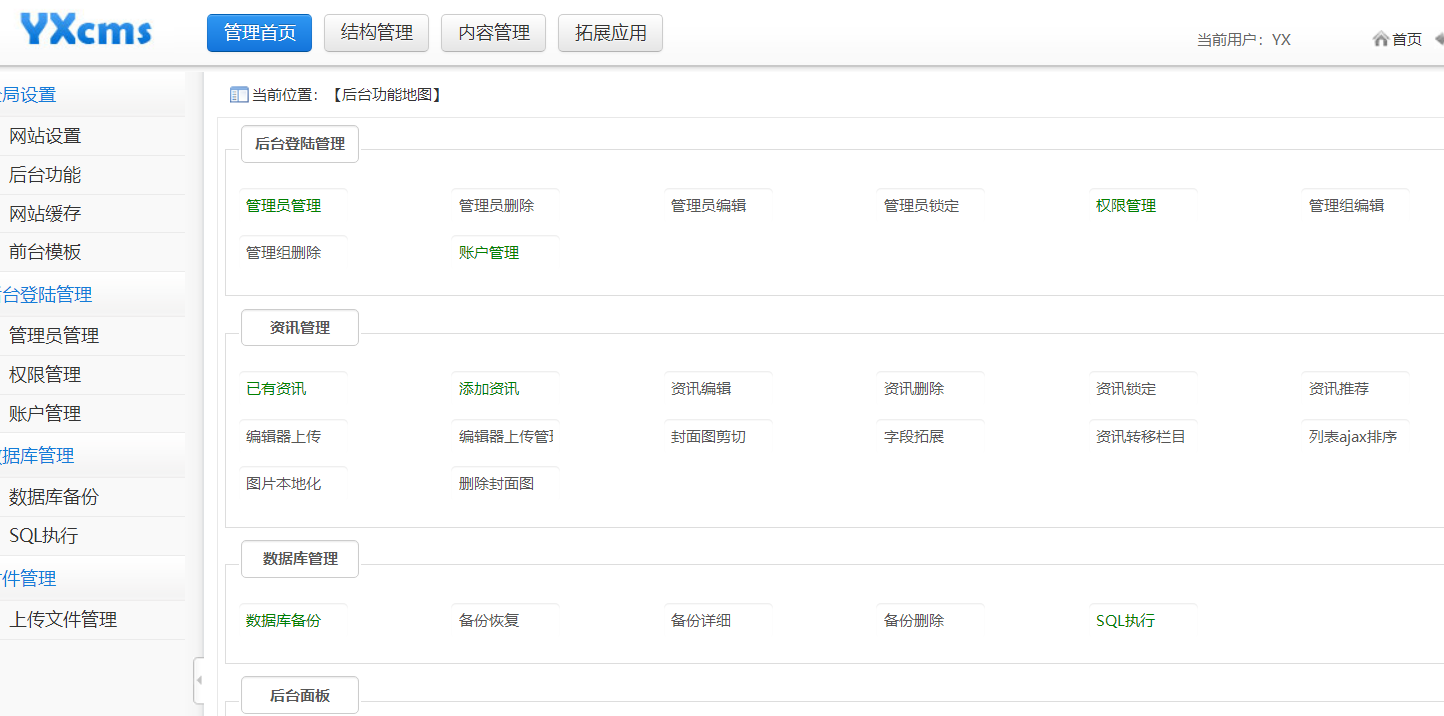
在数据库里改管理员密码或新建管理员赋值；得到一个可登录后台的管理员账号；

这里新建admin1



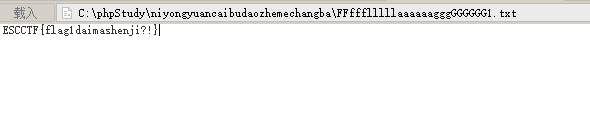


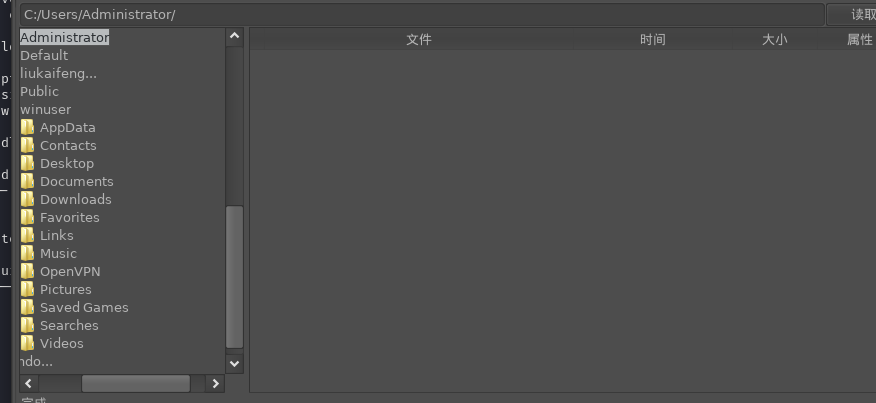
后台getshell；

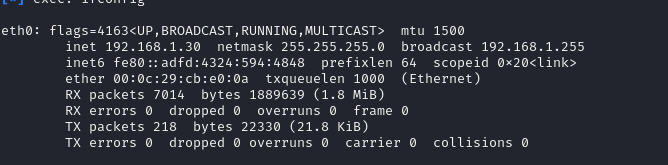


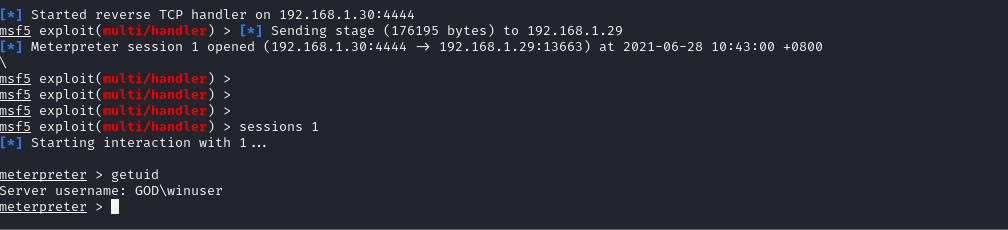
FLAG1



flag2提示在桌面，翻了user桌面没有，其他账户无权限；

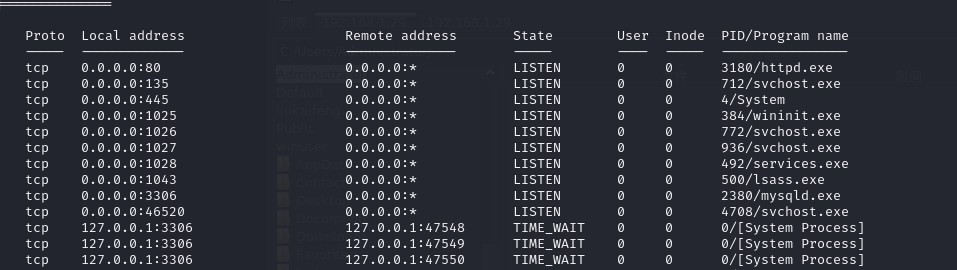


Kali1.30

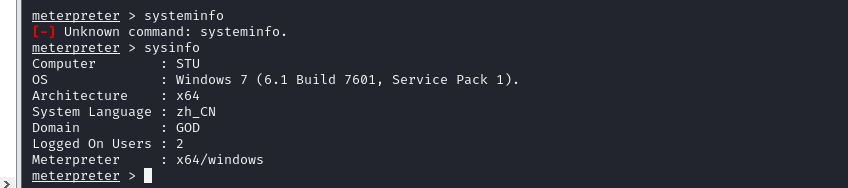


信息收集：

端口

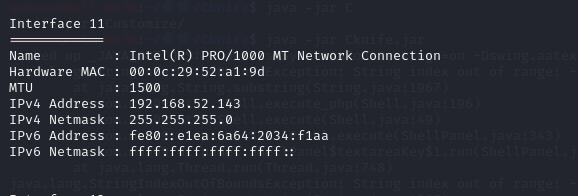


系统：

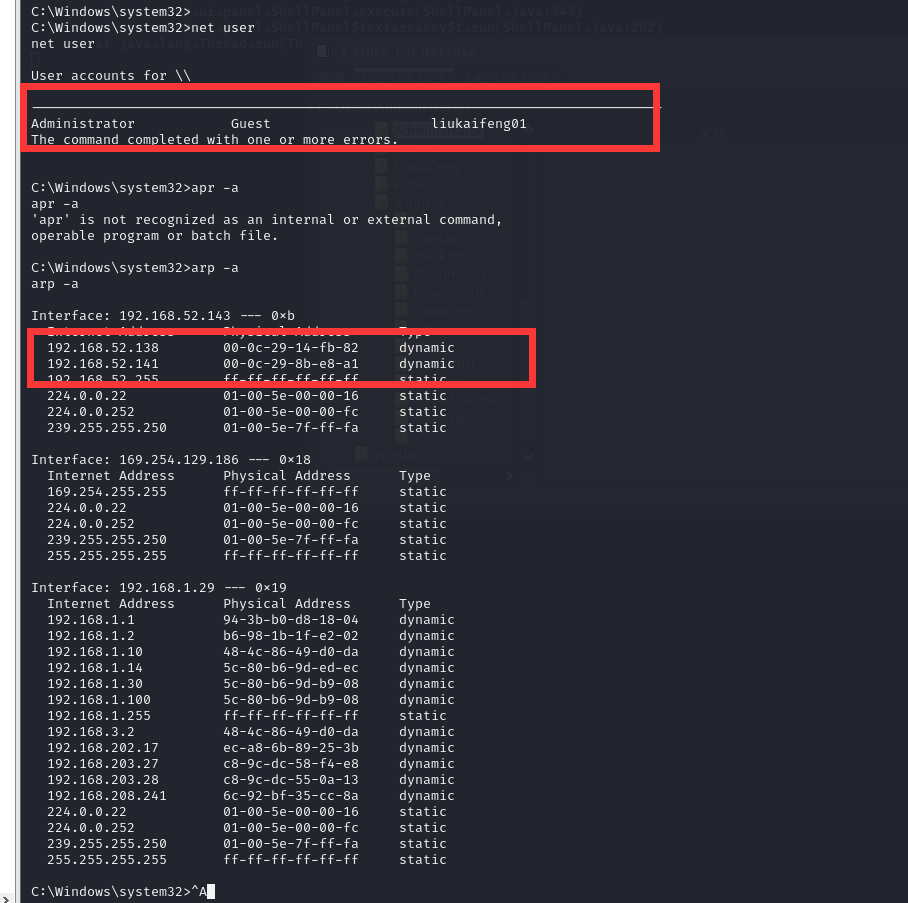


有域，域名god

网络：内网地址

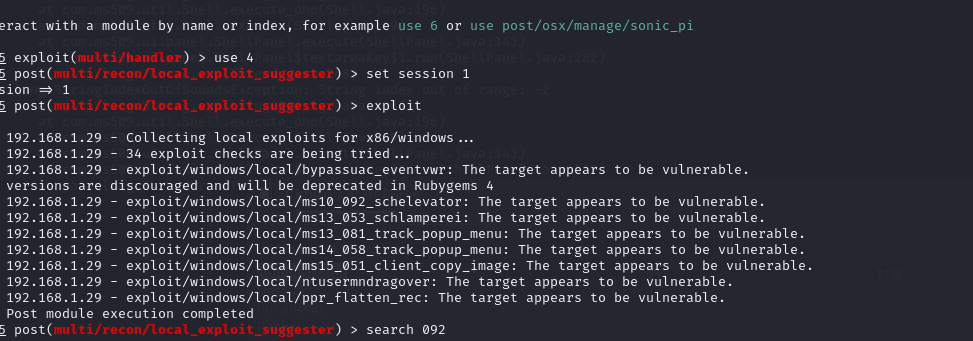


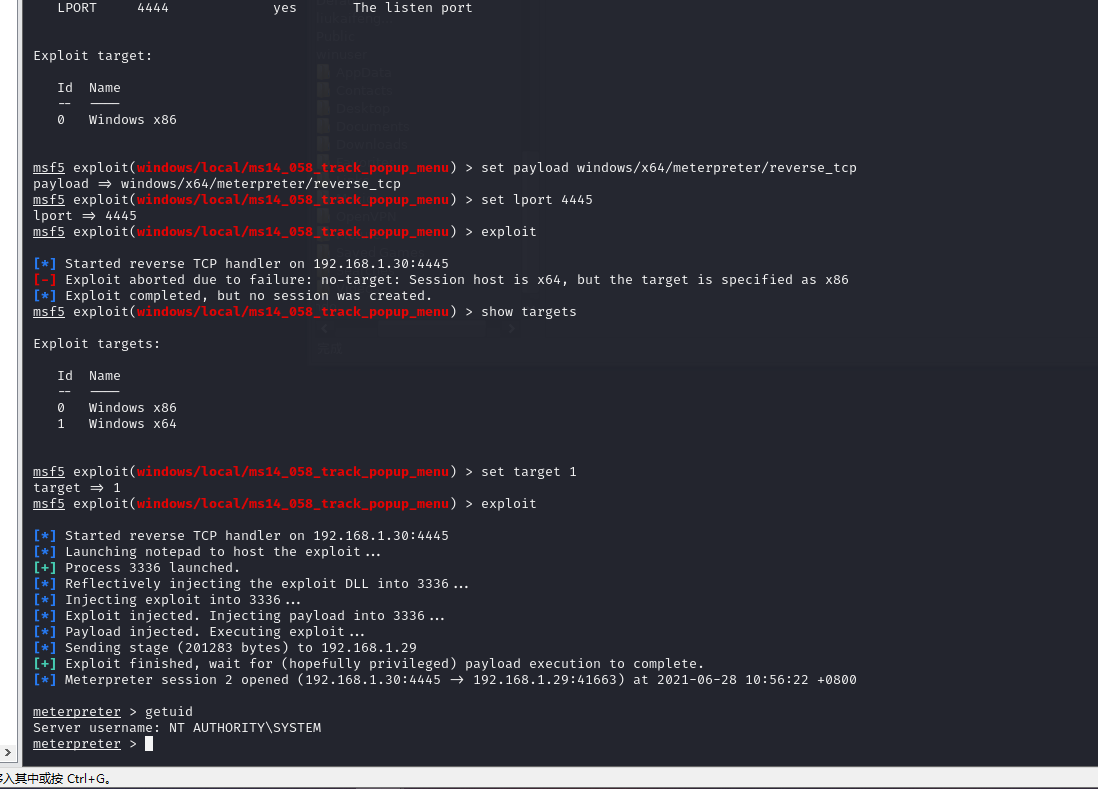
用户信息；内网信息



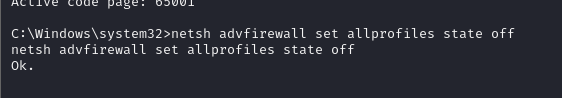
疑似两台内网服务器ip；

提权

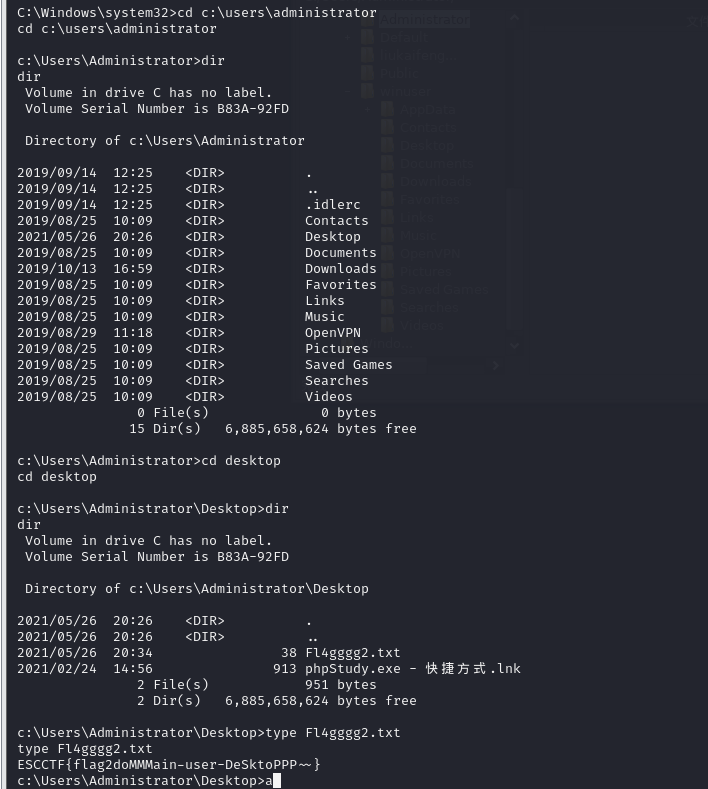




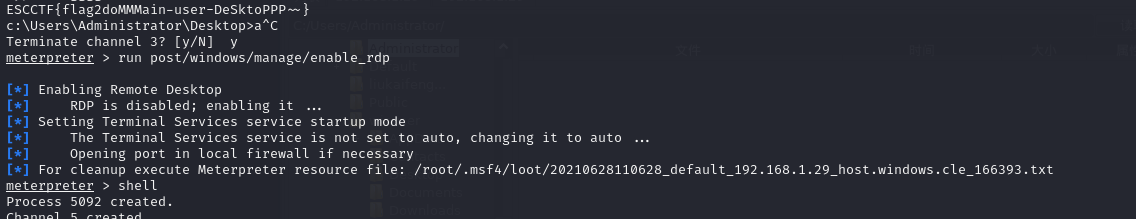
关防火墙



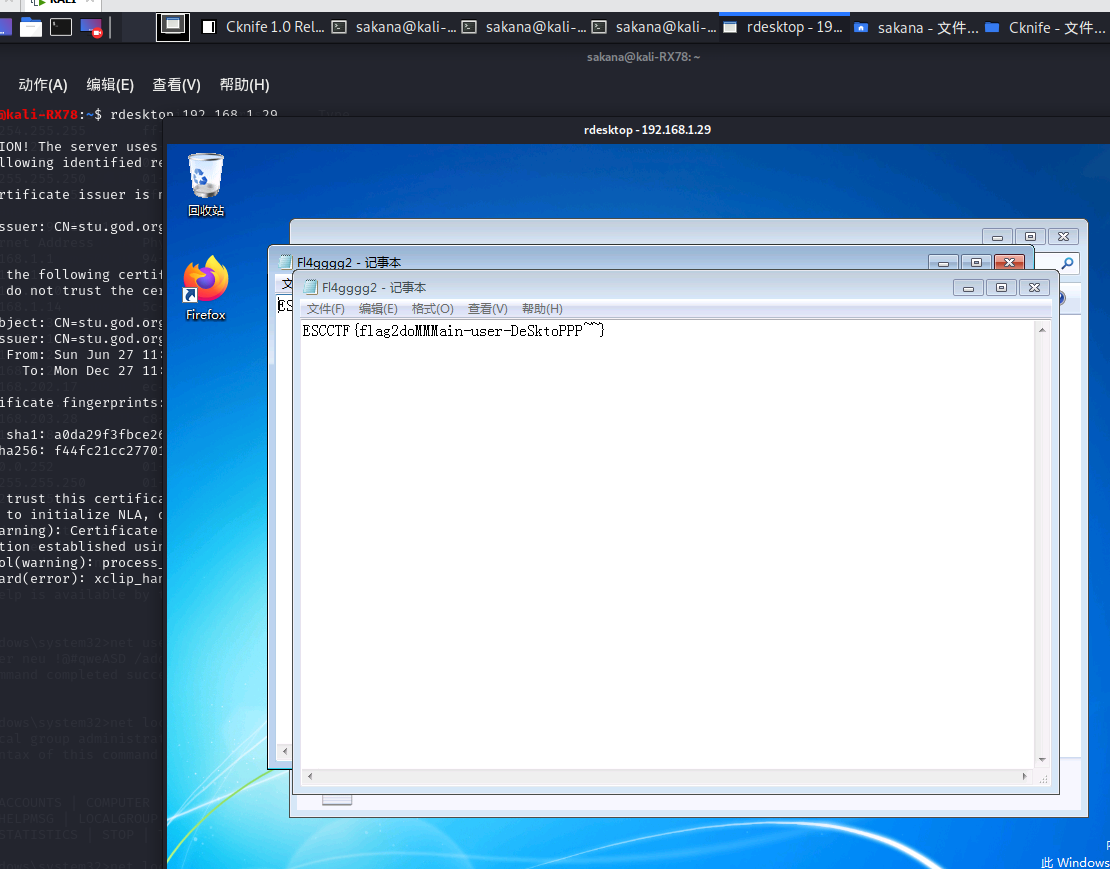
Systemshell直接查Administrator的桌面文件，发现flag2；（这里是文件形式，shell很容易找到）



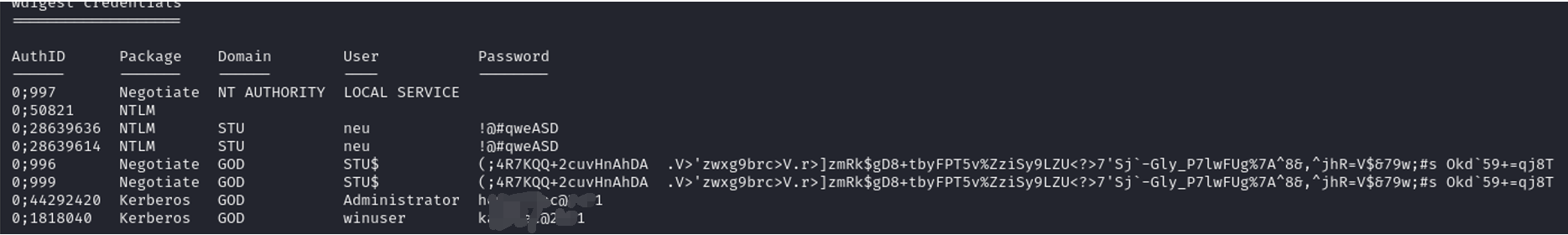
另：如果没翻到，可以开远程桌面，加个主机管理员，上去找



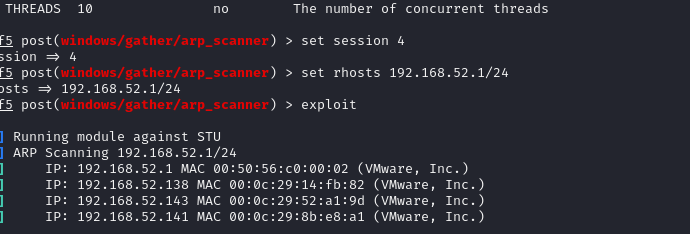
Neu，加入Administrator组，远程桌面



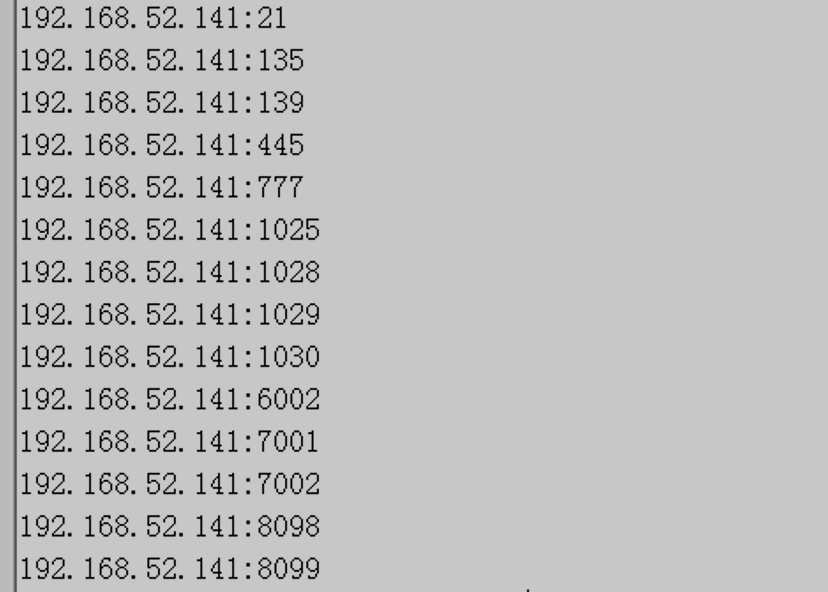
Mimikatz dump 出域管账号

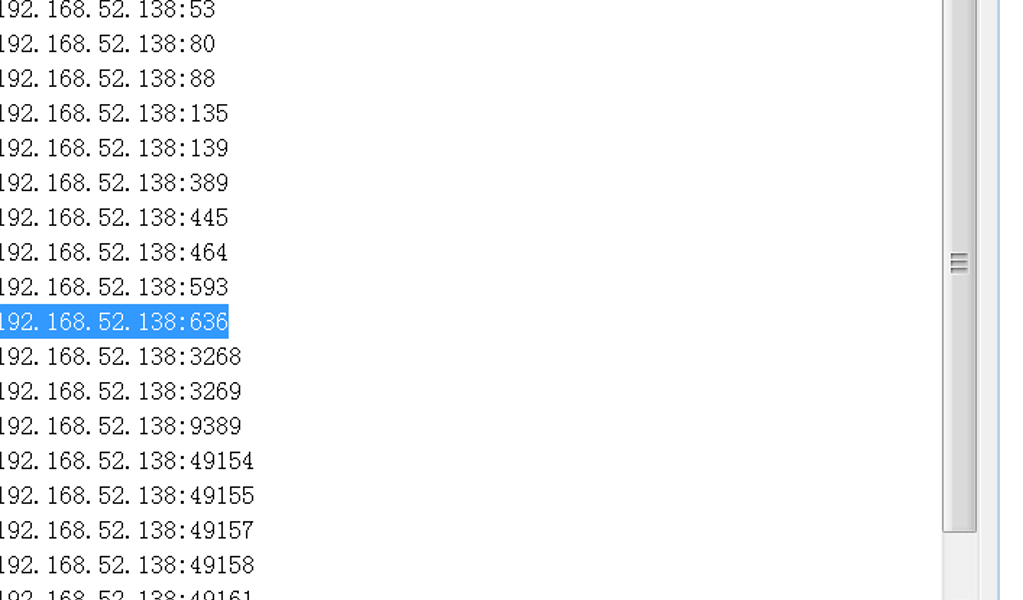


内网存活主机



端口：

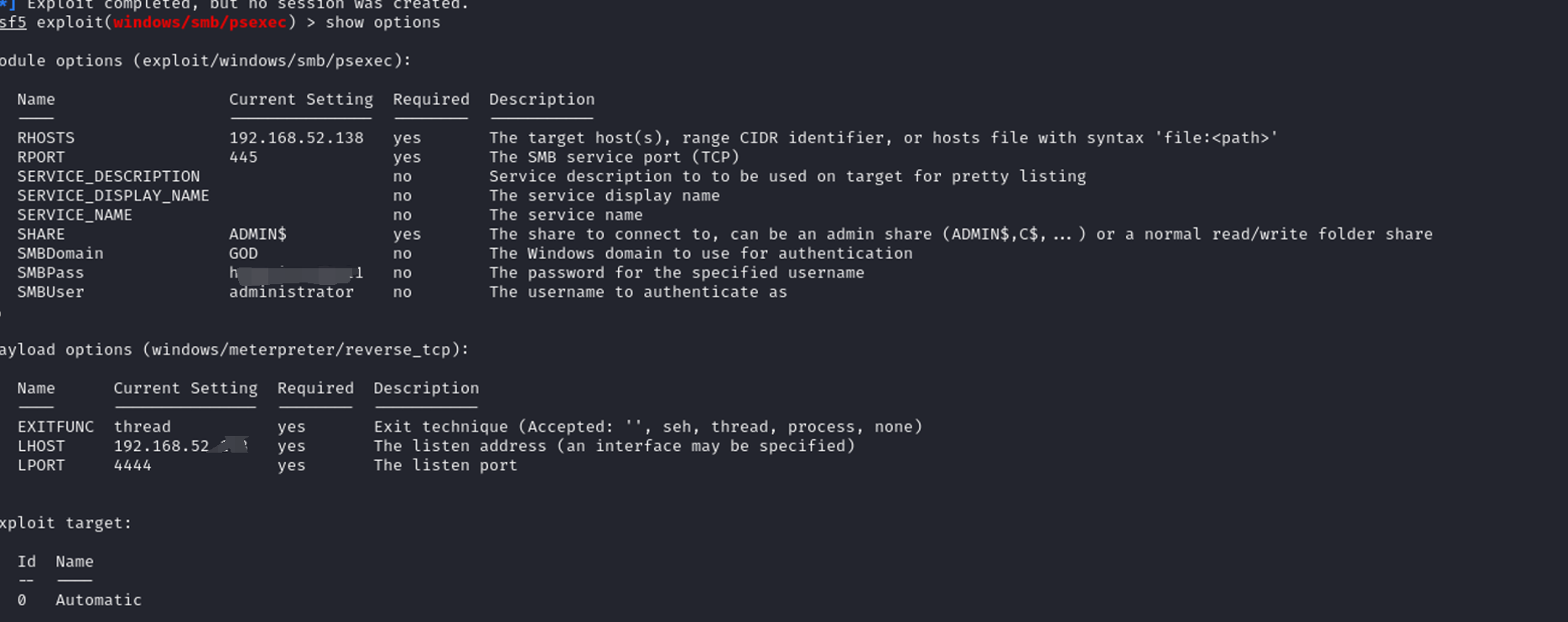




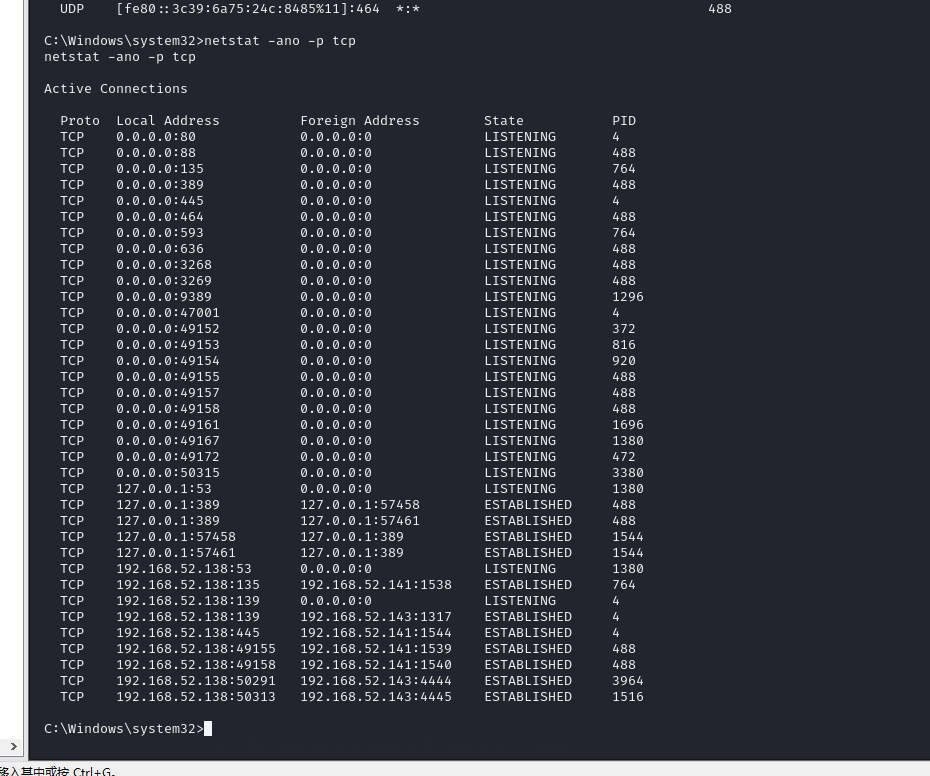
## 方法1：

域：smb psexe

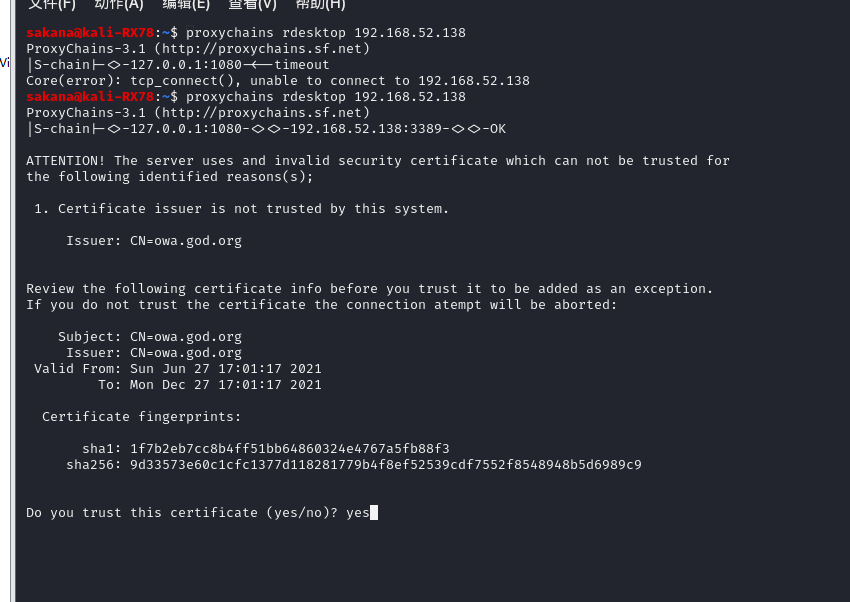
直接域控138 dump出域管明文

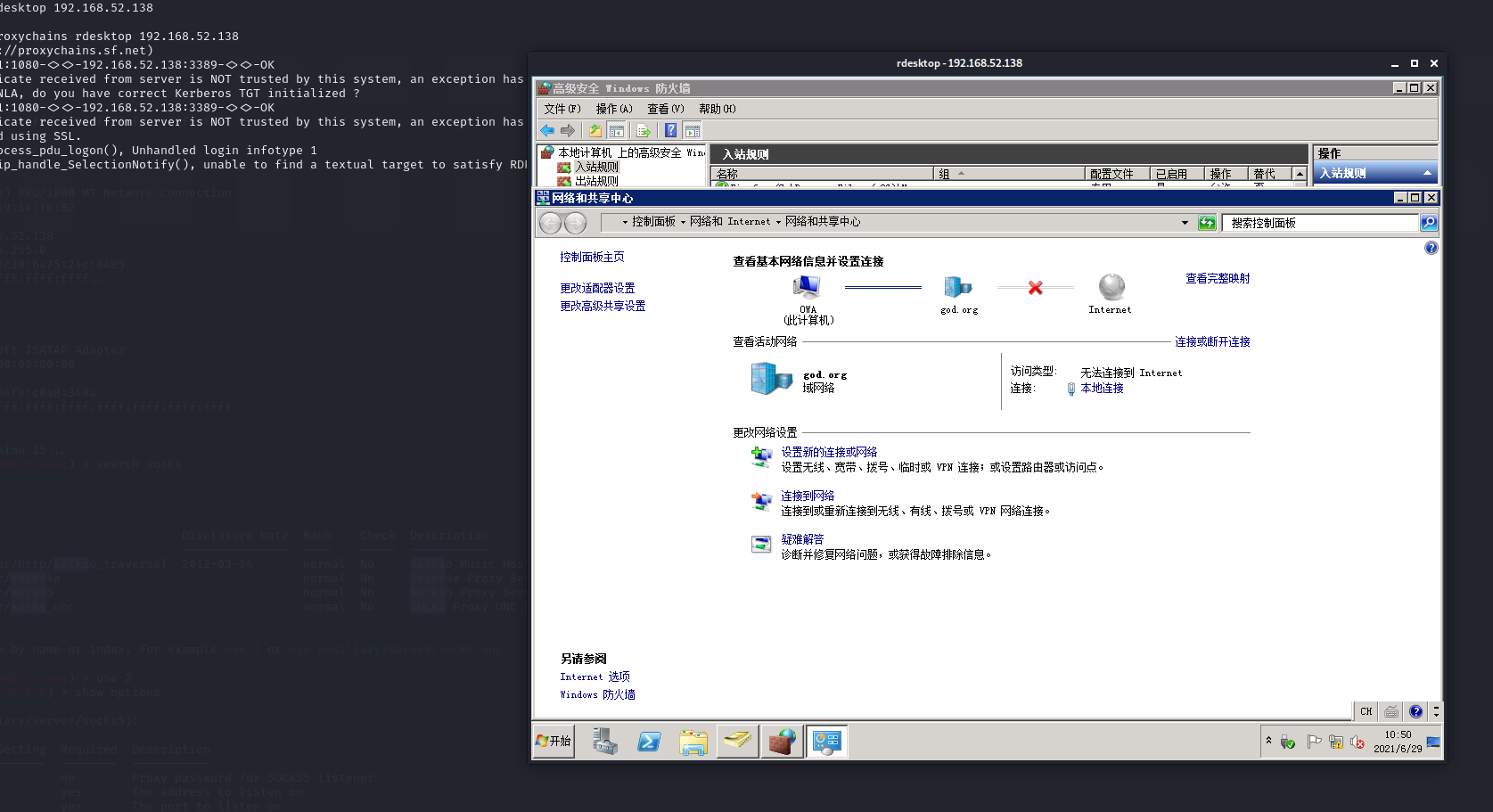


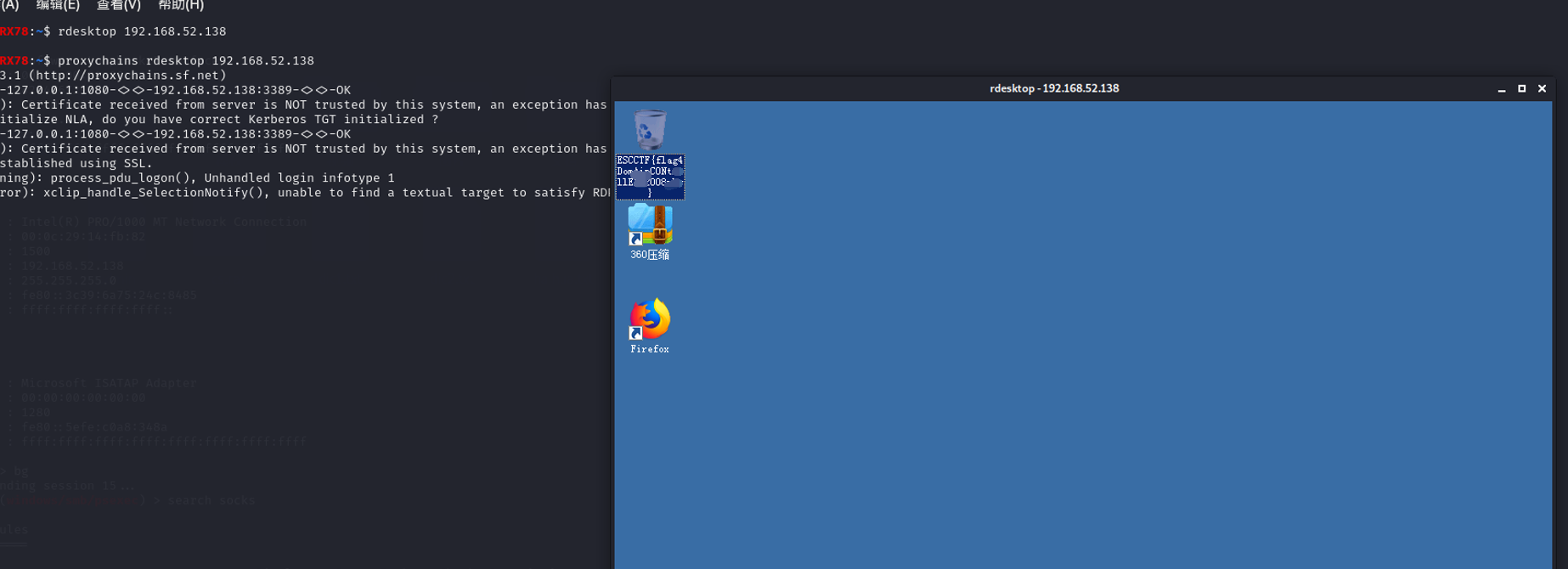




端口信息，关防火墙，开3389







Flag4在域控桌面的回收站图标命名

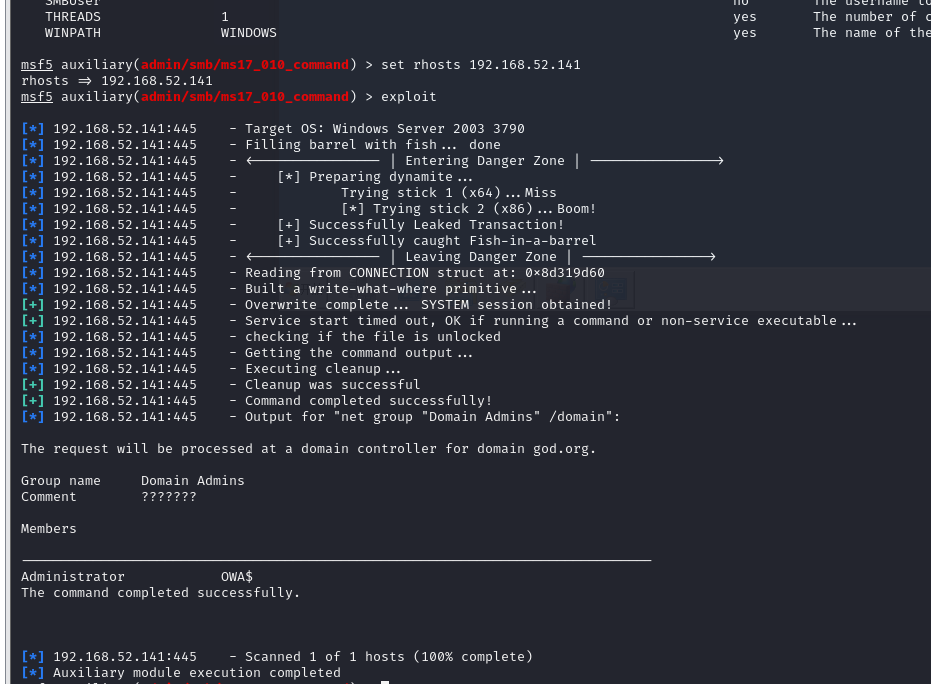
直接可以从域控连141域成员。

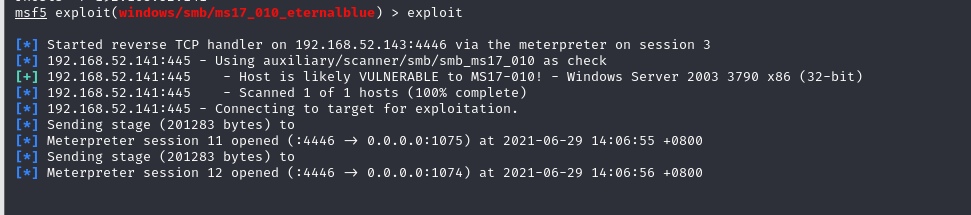
方法2：扩展一下思路，如果无域管，这个靶场也是有很多姿势可以拿到flag的。

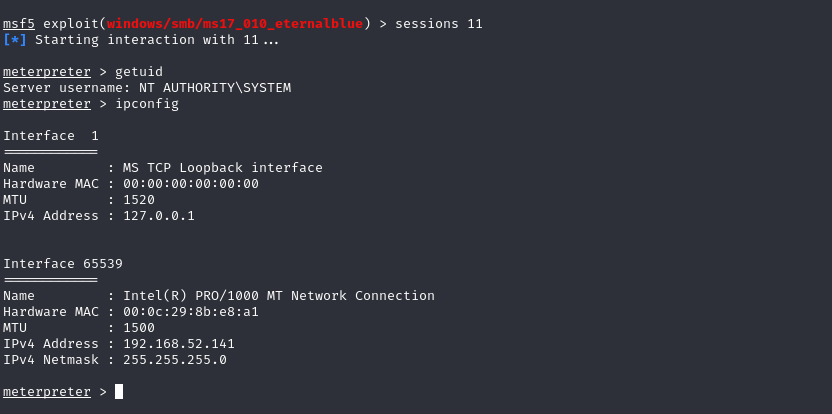
用138域成员举例：

同psexec，有域管账号可获得shell，提供几个其他思路，若无域管情况可尝试内网内核溢出。

Auxiliary 17010模块先进行扫描。

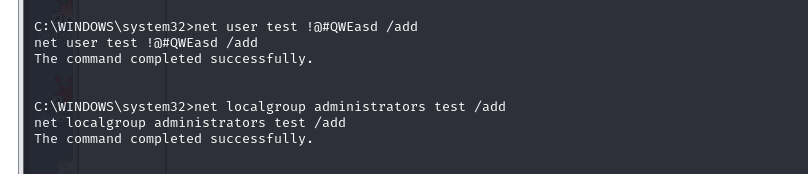


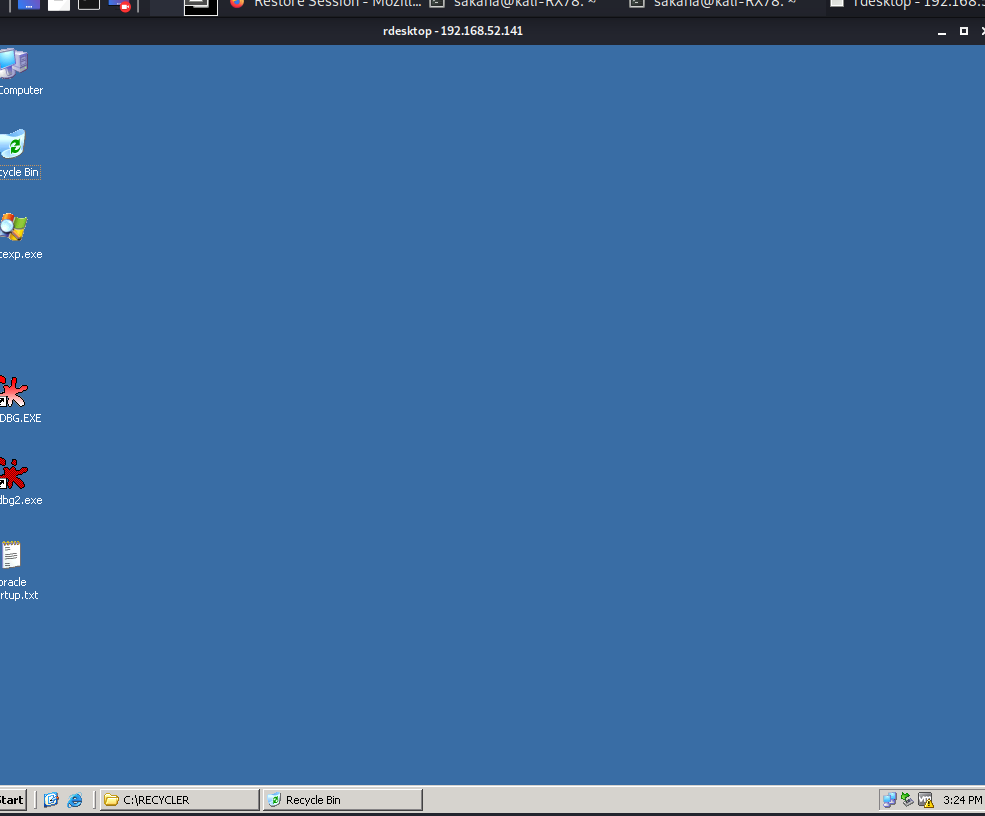




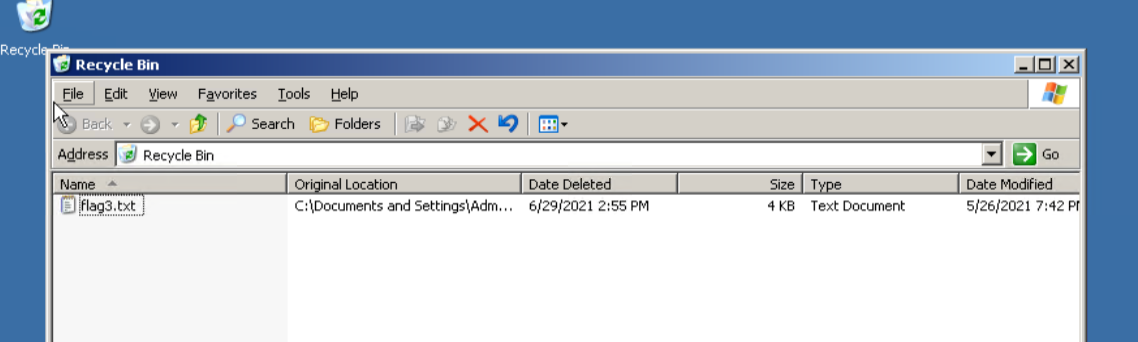
内网思路提权成system，可以查看god\administrator 桌面文件

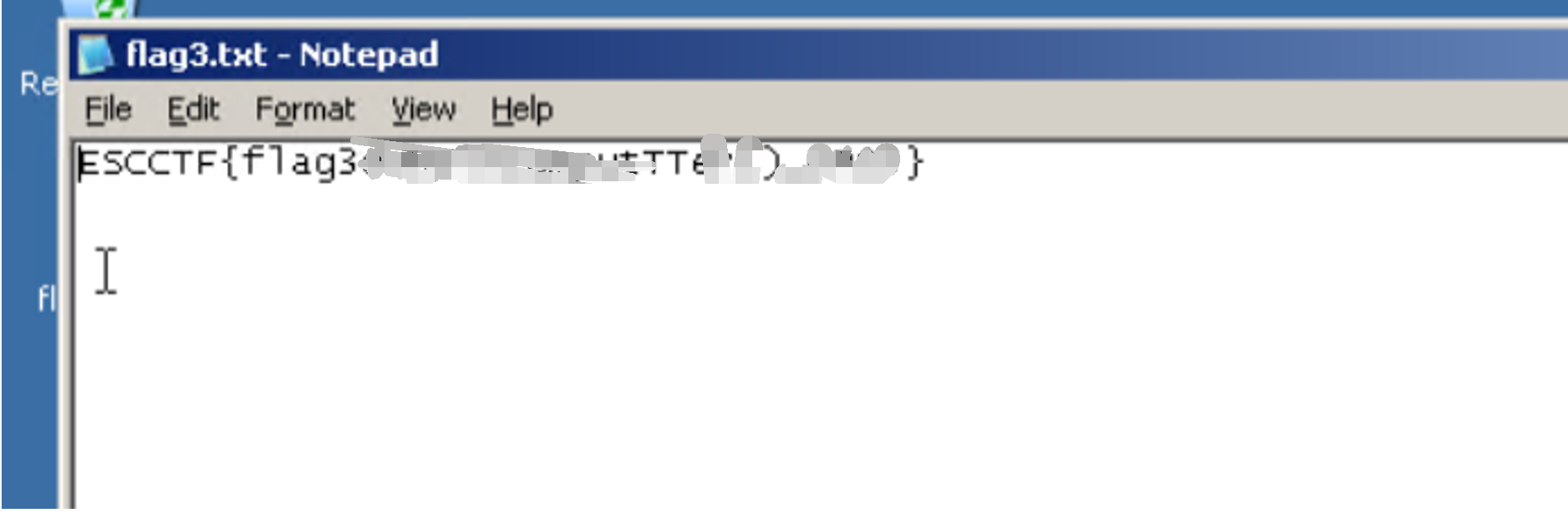
建立test用户。





Flag3在域管的桌面回收站的里面，留个思考没有域管账号的话你怎么能查到它。



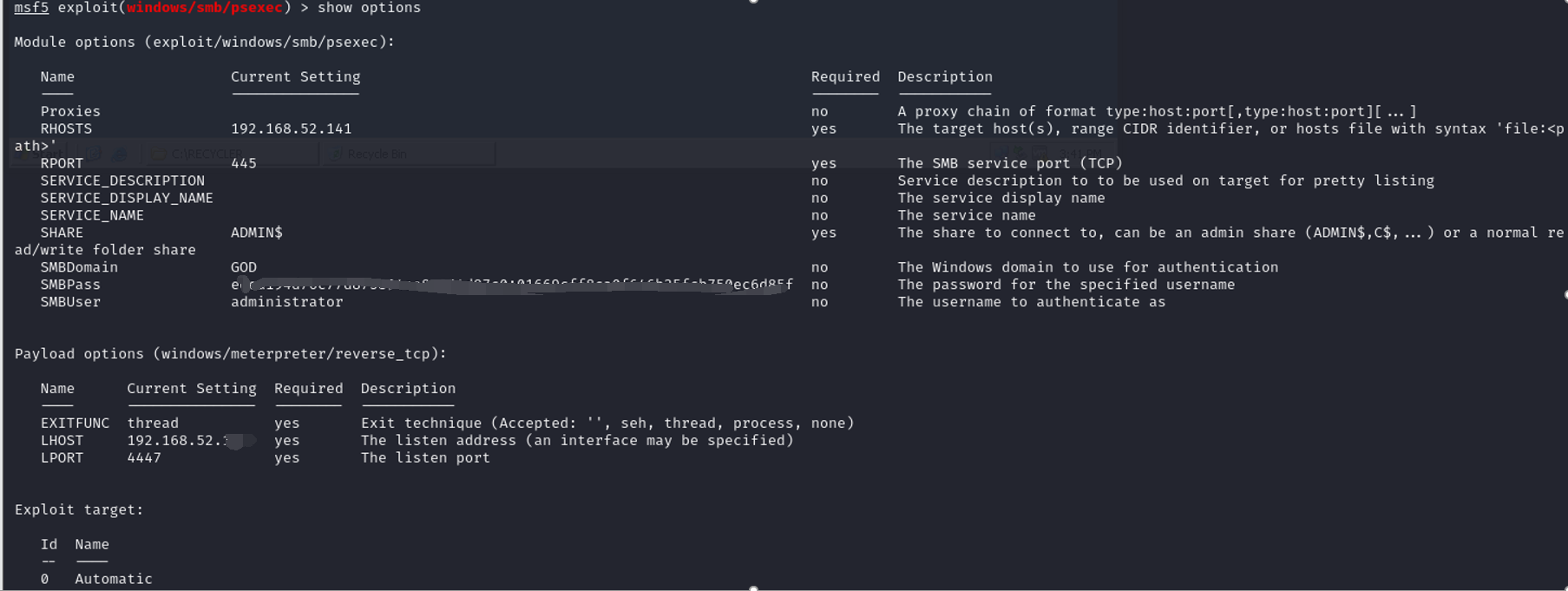


解法？自己思考吧



## 方法1.5：

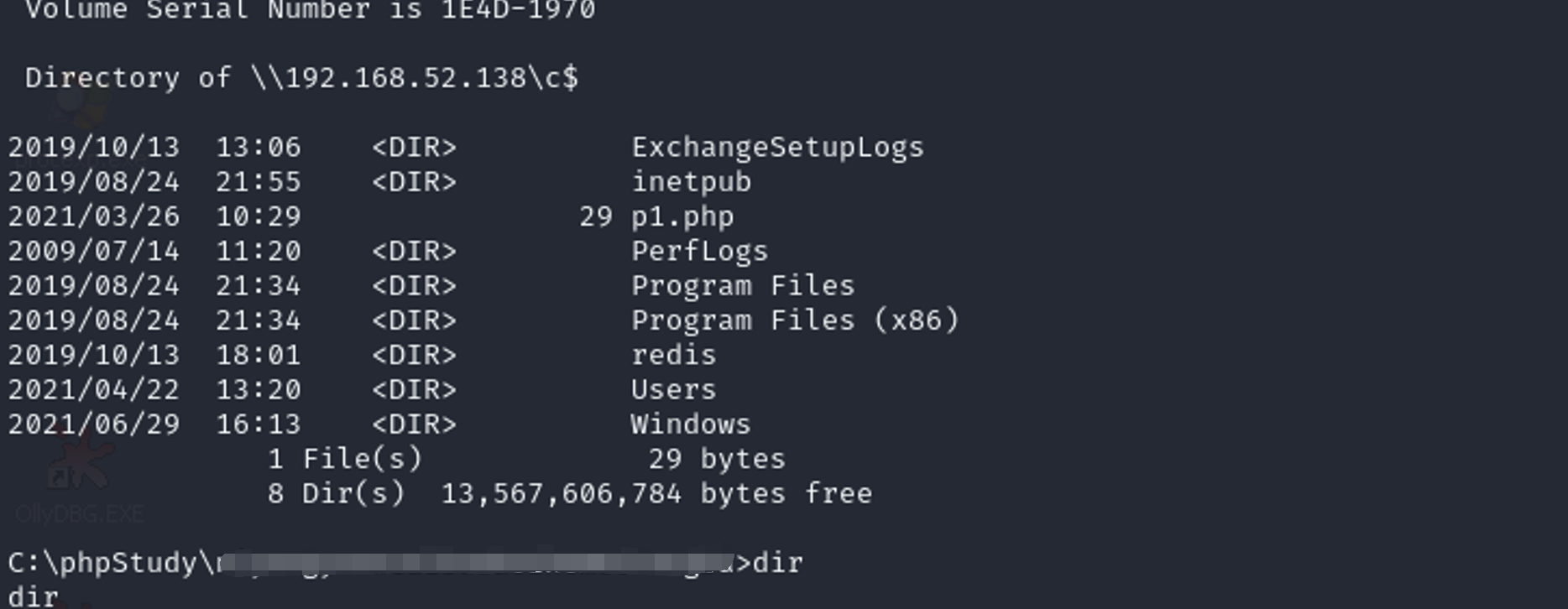
无明文密码，可以通过票据传递





方法3：139 net use；

Win7(web入口服务器)shell，执行netuse



因为有域管登陆过此服务器，所以直接可连141和138域控，拷贝木马文件，使用at命令执行，直接可获取另两台机器权限，同样bind是打不进的，因为配置了防火墙白名单，要使用反向shell即可；

后续操作同上