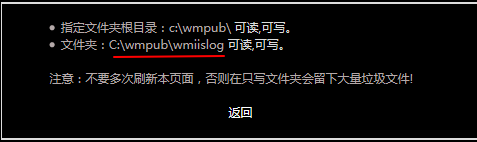
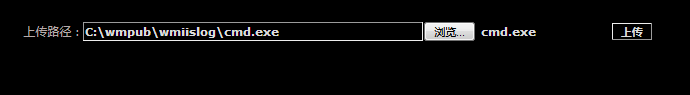
# servU提权

在提权之前需要拿到cmd.exe的shell来运行一些命令，查询磁盘可写目录

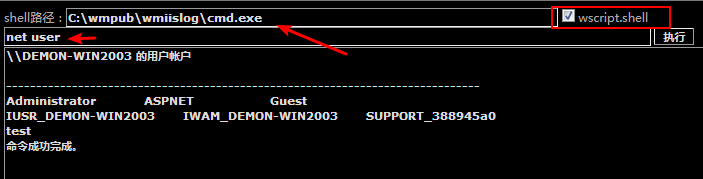




将cmd.exe上传到该目录下



勾选wscript.shell即可执行dos命令

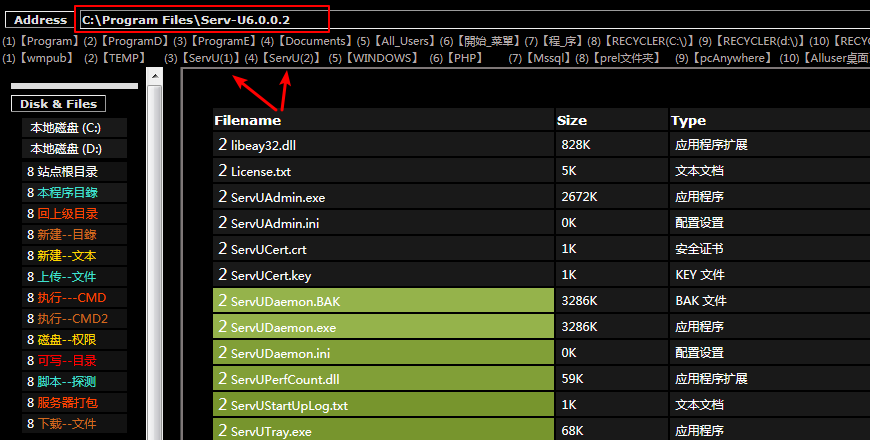


下面开始利用servU提权

方法一，修改配置文件添加用户

测试版本：ServU-V6

通过大马找到servU软件的安装位置，也可点快捷栏的按钮进入软件默认路径

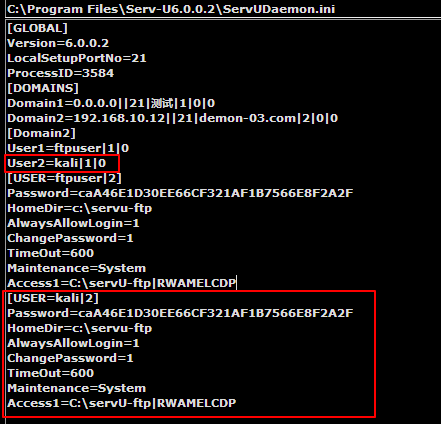


修改ServUDaemon.ini配置文件（前提是可写）

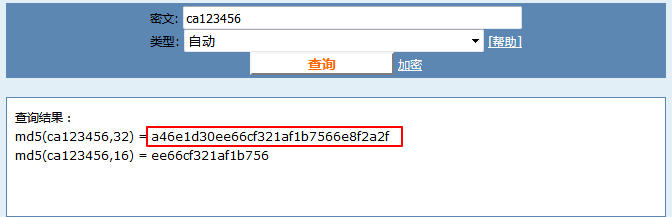


这里的Maintenance是指维护的意思，如果是system那么其则为system用户权限

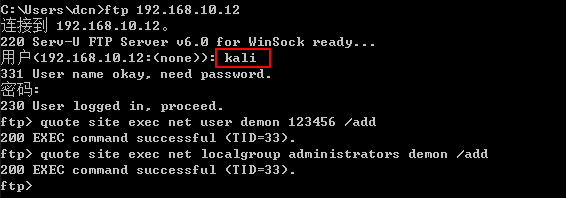
其权限比较高，复制ftpuser用户的配置，添加一个kali用户，如下操作



password 值中前两个字母ca是盐，后面是Md5加密值，如123456为

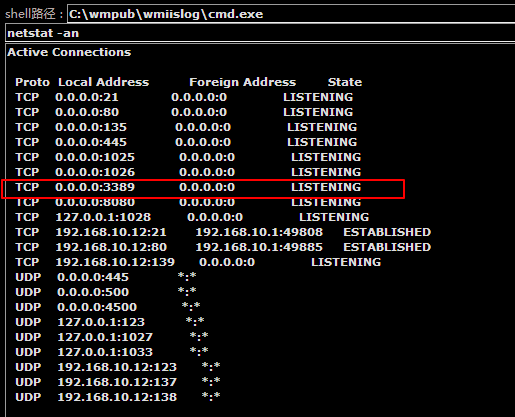


然后添加好后保存，然后用ftp连接登录kali账号，用quote命令创建demon超级用户



如上图所示，ftp中的命令 quote可以执行cmd.exe中的一些命令，但是查看不了信息

在大马中的cmd.exe查看是否开启3389端口

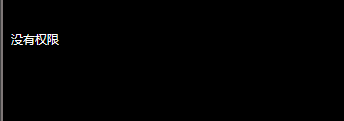




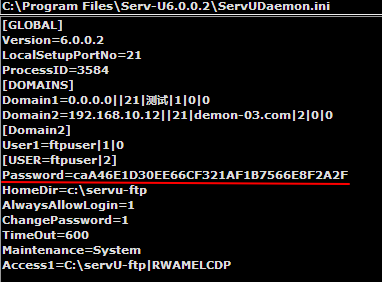


方法二，读取MD5破解密码

如果ServUDaemon.ini配置文件只能读不能改

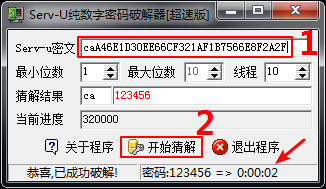


那么就爆破已有的账号的密码，前两个字母是盐，后面是MD5加密值



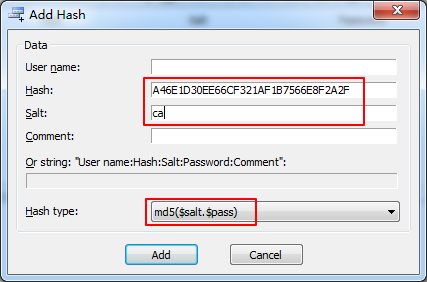
爆破工具推荐两款，一款纯数字爆破（速度快），另一款支持字母爆破（范围广）

Serv-U纯数字密码破解

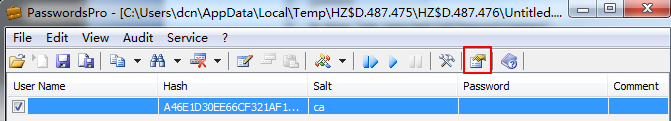


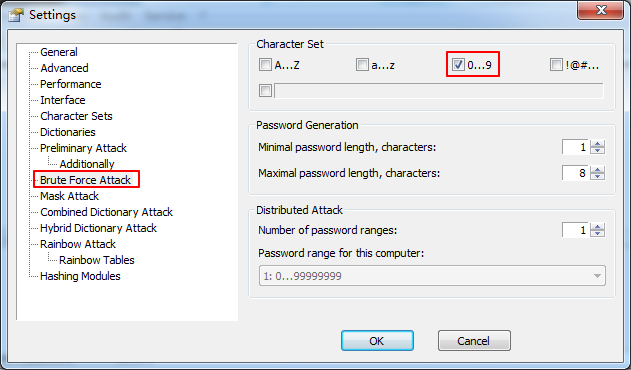
PasswordsPro密码破解工具

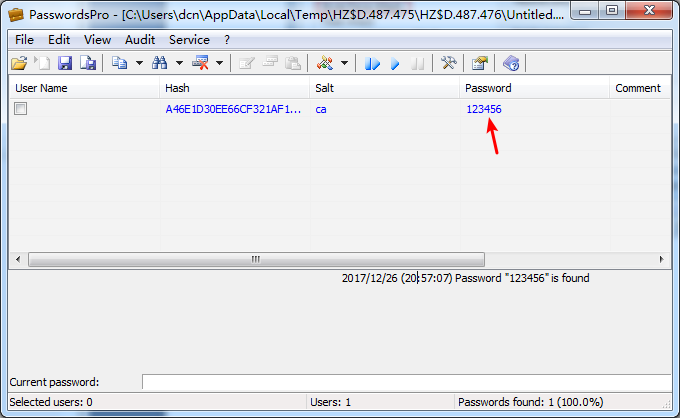
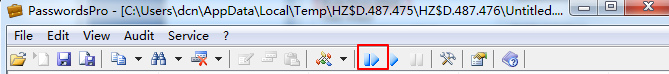




为了加快速度可以自定义密码字符范围







有了system权限的用户密码登录ftp后操作和上面一样。

方法三：默认管理员溢出提权

测试版本：servU7.3

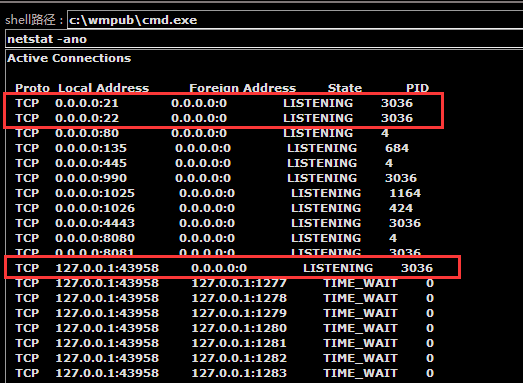


Diskill的大马中的ServU1 可以进入默认安装位置





使用Diskill自带的功能进行servU提权，前提是开了管理端口43958







如果运气不好可以试试下面一个功能



不过我试了很多次，可能是权限问题，总是无法创建成功