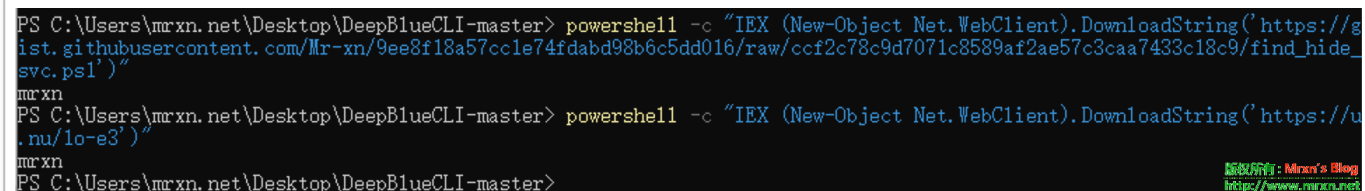


蓝队技巧：查找被隐藏的 Windows 服务项

“ 在上篇，我们说过红队技巧：隐藏 windows 服务，今天抽空来更新下，如何查找这类隐藏的 Windows 服务项。首先看下效果，使用 powershell 远程下载执行直接获得隐藏的 Wi...

在上篇，我们说过 红队技巧：隐藏 windows 服务，今天抽空来更新下，如何查找这类隐藏的 Windows 服务项。首先看下效果，使用 powershell 远程下载执行直接获得隐藏的 Windows 服务名称：



```
PS C:\Users\mrnx.net\Desktop\DeepBlueCLI-master> powershell -c "IEX (New-Object Net.WebClient).DownloadString('https://gist.githubusercontent.com/Mr-xn/9ee8f18a57cc1e74fdabd98b6c5dd016/raw/ccf2c78c9d7071c8589af2ae57c3caa7433c18c9/find_hidden_svc.ps1')"
```

mrnx

```
PS C:\Users\mrnx.net\Desktop\DeepBlueCLI-master> powershell -c "IEX (New-Object Net.WebClient).DownloadString('https://gist.githubusercontent.com/Mr-xn/9ee8f18a57cc1e74fdabd98b6c5dd016/raw/ccf2c78c9d7071c8589af2ae57c3caa7433c18c9/find_hidden_svc.ps1')"
```

mrnx

```
PS C:\Users\mrnx.net\Desktop\DeepBlueCLI-master>
```

版权所有：Mrnx's Blog
<http://www.mrxn.net>

通过远程下载执行无文件落地查看隐藏 Windows 服务：

```
powershell -c "IEX (New-Object Net.WebClient).DownloadString('https://gist.githubusercontent.com/Mr-xn/9ee8f18a57cc1e74fdabd98b6c5dd016/raw/ccf2c78c9d7071c8589af2ae57c3caa7433c18c9/find_hidden_svc.ps1')"
```

如果觉得链接太长影响你发挥，可以使用缩短网址：

```
powershell -c "IEX (New-Object Net.WebClient).DownloadString('https://u.nu/1o-e3')"
```

下面看下源码：

```
Windows PowerShell ISE
文件(F) 编辑(E) 视图(V) 工具(T) 调试(D) 附加工具(A) 帮助(H)

fuck_hide_service.ps1 X
1 Compare-Object -ReferenceObject `
2 (Get-Service | Select-Object -ExpandProperty Name)
3 { $_.Name -replace "[0-9a-f]{2,8}$" }
4 -DifferenceObject (gci -path hkim:\system\currentcontrolset\services |
5 { $_.Name -replace "HKEY_LOCAL_MACHINE\\", "HKLM:" } |
6 { Get-ItemProperty -Path $_.Path -name objectname -erroraction 'ignore' } |
7 { $_.Name -replace "[0-9a-f]{2,8}$" } -PassThru | ?{ $_.SideIndicator -eq "=" }
8 Write-Host "all done!"
9
```

查询视图里所有的服务（也即使用任务管理器这类看到的）

查询系统所有服务详细信息

前后筛选处服务名进行对比，即可筛选出隐藏服务

```
MRxDAV      SvcMemSoftLimitInMB : 12
              Type      : 32
              DependOnService : {rdbs}
              Description      : %%systemroot%\system32\webclnt.dll,-105
              DisplayName      : %%systemroot%\system32\webclnt.dll,-104
              ErrorControl      : 1
              ImagePath        : \SystemRoot\system32\drivers\mrxdav.sys
              Start            : 3
              Type             : 2
              mrxn             Type      : 16
                              Start      : 2
                              ErrorControl : 1
                              ImagePath   : C:/Users/mrxn.net/Desktop/mrxn.exe
                              ObjectName  : LocalSystem
              mrxsmb           DependOnService : {rdbs}
                              Description  : %%systemroot%\system32\mrxcsv.dll,-1002
```

```
Description : %systemroot%\system32\wkssvc.dll, 1003
DisplayName : %systemroot%\system32\wkssvc.dll, -1002
ErrorControl : 1
```

版权所有: Mrxrn's Blog
http://www.mrxrn.net

```
Compare-Object -ReferenceObject `
(Get-Service | Select-Object -ExpandProperty Name |
% { $_ -replace "[0-9a-f]{2,8}$" }) `
-DifferenceObject (gci -path hklm:\system\currentcontrolset\services |
% { $_.Name -Replace "HKEY_LOCAL_MACHINE\\", "HKLM:\" } |
? { Get-ItemProperty -Path "$_" -name objectname -erroraction 'ignore' } |
% { $_.substring(40) }) -PassThru | ?{$_sideIndicator -eq ">"} }
```

上图有分析 ps 语句，其实就是查找视图里的 Windows 服务和系统里的服务进行对比，筛选处不同的即为隐藏的 windows 服务。

查询出隐藏服务后，我们就可以查询隐藏服务的详细进程，近而去排查是否正常，是否需要立即停止或者删除等待操作：

```
sc qc mrxn
```

管理员: 命令提示符

```
sc query eventlog          - 显示 eventlog 服务的状态
sc queryex eventlog        - 显示 eventlog 服务的扩展状态
sc query type= driver      - 仅枚举活动驱动程序
sc query type= service    - 仅枚举 Win32 服务
sc query state= all        - 枚举所有服务和驱动程序
sc query bufsize= 50      - 枚举缓冲区为 50 字节
sc query ri= 14           - 枚举时恢复索引 = 14
sc queryex group= ""       - 枚举不在组内的活动服务
sc query type= interact   - 枚举所有不活动服务
sc query type= driver group= NDIS - 枚举所有 NDIS 驱动程序
```

```
C:\Windows\system32>sc qc mrxn
[SC] QueryServiceConfig 成功

SERVICE_NAME: mrxn
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2    AUTO_START
        ERROR_CONTROL       : 1    NORMAL
        BINARY_PATH_NAME    : C:/Users/mrxn.net/Desktop/mrxn.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : mrxn
        DEPENDENCIES         :
        SERVICE_START_NAME  : LocalSystem

C:\Windows\system32>
```

版权所有: Mrxn's Blog
<http://www.mrxn.net>

另外，根据原文中提到的 [DeepBlue.ps1](#) 我并没有复现成功，但是可以用来辅助分析 Windows 事件日志还是不错的。

参考：<https://www.sans.org/blog/defense-spotlight-finding-hidden-windows-services/>