Using PowerShell for Security Testing (4)

PowerShell contains a series of useful command that can be used to profile a target machine. These functions include the ability to profile the services running on a target system as well as identifying the IP address of the target machine. So, using the **Get-NetIPAddress** command we can identify network information associated with a target system.

```
PS C:\> Get-NetIPAddress
IPAddress         : 10.10.10.1
. . . . . .
```

We can also use PowerShell to identify various services and processes that are running on a target system. In the following we will use the **Get-Service** command to list all of the services running. It should be noted that this PowerShell command also supports listing the services running on a remote computer system via the following option **-ComputerName <STRING>**.

```
PS C:\> Get-Service
Status   Name               DisplayName
------   ----               -----------
. . . . . .
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  Browser            Computer Browser
. . . . . .
```

We can also use PowerShell to configure various services and processes that are running on a target system. In the following we will use the **Set-Service** command to list all of the services running. It should be noted that this PowerShell command also supports the configuration of services running on a remote computer system via the following option **-ComputerName <STRING>**. So in the following command, on the computer system ***WS2012-01*** we will configure the service ***MyService*** , so that it start upon reboot.

```
PS C:\> Set-Service -Name MyService -Computer WS2012-01 -StartupType "automatic"
```

As part of any Penetration Test, we will want to identify the number, and type of processes that are running on a target system. We can do this using the **Get-Process** command. . It should be noted that this PowerShell command also supports listing the processes running on a remote computer system via the **-ComputerName <STRING>** option.

```
PS C:\> Get-Process
Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
. . . . . .
    224      14     6716      19672       3.44   7420   1 conhost
    107       8     5464       1504       0.08   8692   1 conhost
    419      16     3668      15292       2.64   7672   1 ctfmon
    201      17     3452      10936              7568   0 dllhost
. . . . . .
```

Microsoft Windows make use for SMB shares for file sharing. Using the **Get-SMBShare** command we examine the SMB shares that the target system is exporting to the network.

```
PS C:> Get-SMBShare
Name   ScopeName Path       Description
----   --------- ----       -----------
ADMIN$ *         C:\Windows Remote Admin
C$     *         C:\        Default share
D$     *         D:\        Default share
E$     *         E:\        Default share
IPC$   *                    Remote IPC
PS C:\>
```