Using PowerShell for Security Testing (5)

One of the major advantages of power shell is that PowerShell is that you can use it to access remote machines and execute scripts on remote machines. To get a PowerShell session on a remote machine called **Server-03**, we can use the **Enter-PSSesion** command. You can exit a remote session via the **Exit-PSSesion** command.

```
PS C:\> Enter-PSSession Server-03
[Server-03] PS C:\Users\ABlyth\Documents>
```

We can also use PowerShell to execute a command, or a set of commands on a remote machine. To achieve this, we make use of the **Invoke-Command** command as follows. The following shows us how to execute the PowerShell command **Get-Services** on the server **Server-03**.

```
PS C:\> Invoke-Command -ComputerName Server-03 -ScriptBlock {Get-Services}
```

On the remote system we can also specify the location of the PowerShell that we would like to execute as follows:

```
PS C:\> Invoke-Command -ComputerName Server-03 -FilePath C:\Users\ABlyth\myps.ps1
```

Not only will PowerShell let us run a command on a remote system it will also let is run, and managed, multiple persistent sessions on a remote system. To achieve this, we assign the GGG cmdlet to a variable and then access the remote session via accessing that cmdlet.

```
PS C:\> $MySession01 = New-PSSession -ComputerName Server-03
```

Once we have a variable with the session information, we can then invoke functions on it. The reason why this is possible is because within PowerShell everything is an object.

```
PS C:\> Invoke-Command -Session $MySession01 {Get-Services}
```

We can use the **New-PSSession** command to allow for us to create a session with an SSH server. As follows

```
PS C:\> $session = New-PSSession -HostName UbuntuVM1 -UserName TestUser

The authenticity of host 'UbuntuVM1 (9.129.17.107)' can't be established.
ECDSA key fingerprint is SHA256:2kCbnhT2dUE6WCGgVJ8Hyfu1z2wE4lifaJXLO7QJy0Y.
Are you sure you want to continue connecting (yes/no)?
TestUser@UbuntuVM1s password:

PS C:\> session
Id  Name   ComputerName    ComputerType    State    ConfigurationName     Availability
--  ----   ------------    ------------    -----    -----------------     ------------
  1 SSH1    UbuntuVM1      RemoteMachine    Opened   DefaultShell       Available

PS C:\> Enter-PSSession $session

[UbuntuVM1]: PS /home/TestUser> uname -a
Linux TestUser-UbuntuVM1 4.2.0-42-generic 49~16.04.1-Ubuntu SMP Wed Jun 29 20:22:11
UTC 2016 x86_64 x86_64 x86_64 GNU/Linux

[UbuntuVM1]: PS /home/TestUser> Exit-PSSession
```