ChrisTruncer / **WMIOps**

Watch 10 Star 50 Fork 4

Code Issues 0 Pull requests 0 Pulse Graphs

This repo is for WMIOps, a powershell script which uses WMI for various purposes across a network.

39 commits **1** branch **0** releases **1** contributor

Branch: **master** New pull request New file Find file HTTPS https://github.com/ChrisT Download ZIP

ChrisTruncer Updated README layout Latest commit d758a7f Jan 21, 2016

weblib	Initial commit, don't tear apart my posh too bad :)	Nov 20, 2015
LICENSE	Initial commit	Nov 20, 2015
README.md	Updated README layout	Jan 21, 2016
WMIOps.ps1	user hunting can be possible	Jan 20, 2016
https_server.py	Initial commit, don't tear apart my posh too bad :)	Nov 20, 2015

README.md

WMIOps

WMMIOps is a powershell script that uses WMI to perform a variety of actions on hosts, local or remote, within a Windows environment. It's designed primarily for use on penetration tests or red team engagements.

This is my first PowerShell script, so I am sure there's things that could have been done better. Please submit a request for anything that could be made more efficient and I'd be happy to look at it, and learn from it :).

Developed by @christruncer

Thanks to: @mattifestation for your major work in this area (Posh and WMI), @obscuresec, @enigma0x3, @424f424f, @xorrior, and @sixdub for having already solved a lot of PowerShell problems and publishing your code to let me, and others, learn from it @harmj0y - for helping to mentor me from the beginning @evan_Pena2003 - For your help with code reviews and teaching me what to look into and learn

WMIOps Functions:

Process Functions

```
 Invoke-ExecCommandWMI                -   Executes a user specified command on the target machine
Invoke-KillProcessWMI                -   Kills a process (via process name or ID) on the target machine
Get-RunningProcessesWMI              -   Returns all running processes from the target machine
```

User Operations

```
 Find-ActiveUsersWMI                  -   Checks if a user is active at the desktop on the target machine (or
Get-ProcessOwnersWMI                -   Returns all accounts which have active processes on the target system
```

Host Enumeration

```
 Get-SystemDrivesWMI                 -   Lists all local and network connected drives on target system
Get-ActiveNICSWMI                   -   Lists all NICs on target system with an IP address
```

System Manipulation Operations

```
 Invoke-CreateShareandExecute        -   Creates a share, copies file into it, uses WMI to invoke the script
Invoke-RemoteScriptWithOutput       -   Executes a powershell script in memory on the target host via WMI and
Invoke-SchedJobManipulation         -   Allows you to list, delete, or create jobs on a system over WMI
Invole-ServiceManipulation          -   Allows you to start, stop, create, or delete services on a targeted s
Invoke-PowerOptionsWMI              -   Force logs off all users, reboots, or shuts down targeted system
```

File Operations

```
 Invoke-DirectoryListing             -   Lists files/directories within a user specfied directory over WMI
Get-FileContentsWMI                 -   Reads the contents of a user specified file on a target system and di
Find-UserSpecifiedFileWMI           -   Search for a file (wildcard supported) on a target system
Invoke-FileTransferOverWMI          -   Uploads or Downloads files to/from the target machine over WMI
```

Original blog post documenting release - https://www.christophertruncer.com/introducing-wmi-ops/