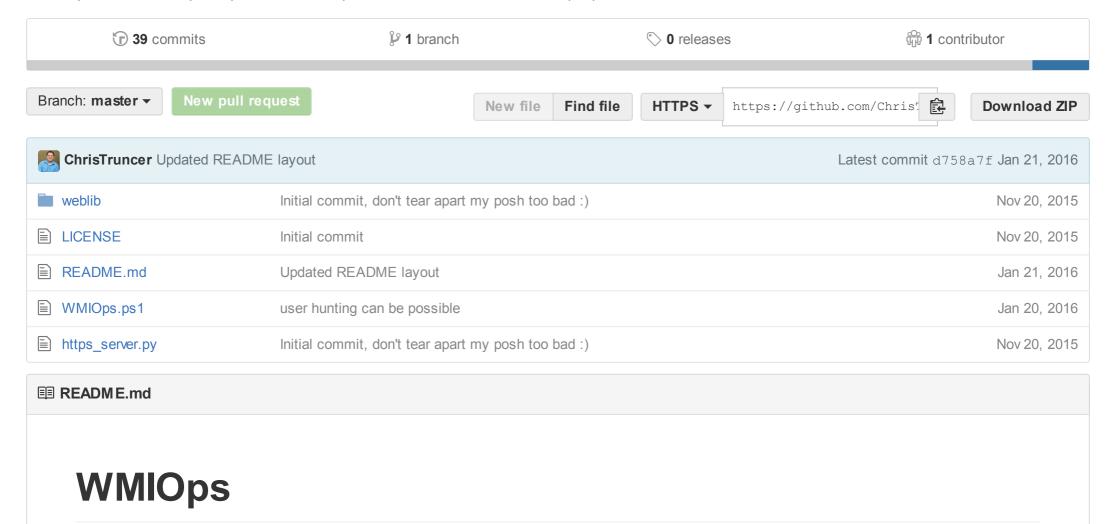


This repo is for WMIOps, a powershell script which uses WMI for various purposes across a network.



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
Invoke-KillProcessWMI
Get-RunningProcessesWMI

- Executes a user specified command on the target machine
- Kills a process (via process name or ID) on the target machine
- Returns all running processes from the target machine

# **User Operations**

Find-ActiveUsersWMT

- Checks if a user is active at the desktop on the target machine (or :

#### **Host Enumeration**

Get-SystemDrivesWMI Get-ActiveNICSWMI

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

## **System Manipulation Operations**

Invoke-CreateShareandExecute Invoke-RemoteScriptWithOutput Invoke-SchedJobManipulation Invole-ServiceManipulation Invoke-PowerOptionsWMI

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

### **File Operations**

Invoke-DirectoryListing Get-FileContentsWMT Find-UserSpecifiedFileWMI Invoke-FileTransferOverWMI

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

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

© 2016 GitHub, Inc. Terms Privacy Security Contact Help



Status API Training Shop Blog About Pricing