



Sign in

bohops / WSMAN-WinRM Public

 Notifications

Fork 39

☆ Star 221

[Code](#)
[Pull requests](#)
[Actions](#)
[Security](#)
[Insights](#)

 master ▼



Go to file

Code ▼

About

A collection of proof-of-concept source code and scripts for executing remote commands over WinRM using the WSMAN.Automation COM object

 [Readme](#)

 BSD-3-Clause license

 Activity

☆ 221 stars

 10 watching

 39 forks

Report repository

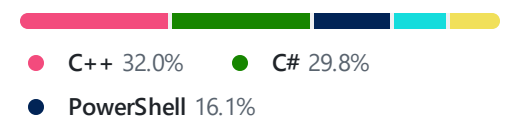
Releases

No releases published

Packages

No packages published

Languages



Page 1 of 3

For background information, please refer to the following blog post: [WS-Management COM: Another Approach for WinRM Lateral Movement](#)

VBScript 11.5%
JavaScript 10.6%

Notes

- SharpWSManWinRM.cs and CppWsManWinRM.cpp compile in Visual Studio 2019. Refer to the code comments for required imports/references/etc.
- All examples leverage the WMI Win32_Process class and WMI Create method for invocation.

Usage

SharpWSManWinRM.cs

```
Usage: SharpWSManWinRM.exe <hostname> <command>
Usage: SharpWSManWinRM.exe <hostname> <command>

Example: SharpWSManWinRM.exe host.domain.local
Example: SharpWSManWinRM.exe host.domain.local
```

WSManWinRM.ps1

```
Usage: Invoke-WSManWinRM -hostname <hostname>
Usage: Invoke-WSManWinRM -hostname <hostname>


Example: import-module .\WSManWinRM.ps1
         Invoke-WSManWinRM -hostname MyServer.local
Example: import-module .\WSManWinRM.ps1
         Invoke-WSManWinRM -hostname MyServer.local
```

WSManWinRM.vbs


```
Usage: cscript.exe SharpWSManWinRM.vbs <hostname>
Usage: cscript.exe SharpWSManWinRM.vbs <hostname>
```

```
Example: cscript.exe SharpWSManWinRM.vbs host.d  
Example: cscript.exe SharpWSManWinRM.vbs host.d
```

WSManWinRM.js

```
Usage: cscript.exe SharpWSManWinRM.js <hostname>   
Usage: cscript.exe SharpWSManWinRM.js <hostname>  
  
Example: cscript.exe SharpWSManWinRM.js host.d  
Example: cscript.exe SharpWSManWinRM.js host.d
```

CppWSManWinRM.cpp

```
Usage: CppWSManWinRM.exe <hostname> <command>   
  
Example: CppWSManWinRM.exe host.domain.local n  
  
Note: Username/password option does not work y
```

Ethics

WSMan-WinRM is designed to help security professionals perform ethical and legal security assessments and penetration tests. Do not use for nefarious purposes.

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.