Sign in

□ bohops / **WSMan-WinRM** Public

🔔 Notifications ⑂ Fork 39 ☆ Star 221

<> Code | ⑂ Pull requests | ⊙ Actions | ⊘ Security | ⬚ Insights

⑂ master ⌄ | ⑂ | ⬙ | Go to file | <> Code ⌄

🕘

□ CppWSManWinRM.c...

□ LICENSE

□ README.md

□ SharpWSManWinRM....

□ WSManWinRM.js

□ WSManWinRM.ps1

□ WSManWinRM.vbs

📖 README | ⚖ BSD-3-Clause license | ☰

WSMan-WinRM

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

Background

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

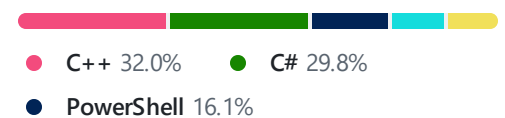☆ 221 stars

👁 10 watching

⑂ 39 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● C++ 32.0% ● C# 29.8%
● PowerShell 16.1%

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

WSManWinRM.vbs

```
Usage: cscript.exe SharpWSManWinRM.vbs <hostnai
Usage: cscript.exe SharpWSManWinRM.vbs <hostnai
```

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

WSManWinRM.js

```
Usage: cscript.exe SharpWSManWinRM.js <hostnam
Usage: cscript.exe SharpWSManWinRM.js <hostnam

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.