Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

bohops / WSMan-WinRM Public

Notifications Fork 39 Star 221

Code Pull requests Actions Security Insights

master Go to file Code

bohops Adding POC implementations 2e3afbf · 4 years ago 6 Commits

CppWSManWinRM.cpp	Adding POC implementations	4 years ago
LICENSE	Initial commit	4 years ago
README.md	Update README.md	4 years ago
SharpWSManWinRM.cs	Adding POC implementations	4 years ago
WSManWinRM.js	Adding POC implementations	4 years ago
WSManWinRM.ps1	Adding POC implementations	4 years ago
WSManWinRM.vbs	Adding POC implementations	4 years ago

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

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

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> <domain\user> <pass

Example: SharpWSManWinRM.exe host.domain.local notepad.exe
Example: SharpWSManWinRM.exe host.domain.local "cmd /c notepad.exe"
```

WSManWinRM.ps1

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

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% ● VBScript 11.5%
● JavaScript 10.6%

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

WSManWinRM.vbs

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

Example: cscript.exe SharpWSManWinRM.vbs host.domain.local notepad.
Example: cscript.exe SharpWSManWinRM.vbs host.domain.local "cmd /c
```

WSManWinRM.js

```
Usage: cscript.exe SharpWSManWinRM.js <hostname> <command>
Usage: cscript.exe SharpWSManWinRM.js <hostname> <command> <domain\

Example: cscript.exe SharpWSManWinRM.js host.domain.local notepad.e
Example: cscript.exe SharpWSManWinRM.js host.domain.local "cmd /c n
```

CppWSManWinRM.cpp

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

Example: CppWSManWinRM.exe host.domain.local notepad.exe

Note: Username/password option does not work yet
```

Ethics

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