Sign in

GhostPack / SharpUp Public

Notifications | Fork 245 | Star 1.3k

Code | Issues 3 | Pull requests 5 | Actions | Projects | Security | Insights

master | Go to file | Code

SharpUp
.gitignore
LICENSE
README.md
SharpUp.sln

README | License

SharpUp

SharpUp is a C# port of various PowerUp functionality. Currently, only the most common checks have been ported; no weaponization functions have yet been implemented.

@harmj0y is the primary author.

SharpUp is licensed under the BSD 3-Clause license.

About

SharpUp is a C# port of various PowerUp functionality.

Readme
View license
Activity
Custom properties
1.3k stars
44 watching
245 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 8

Languages

Usage

```
SharpUp.exe [audit] [check1] [check2]...

    audit   - Specifies whether or not to enabl
              regardless if the process is in h
              If no checks are specified, audit
              be ran.

    check*  - The individual vulnerability chec

              - AlwaysInstallElevated
              - CachedGPPPassword
              - DomainGPPPassword
              - HijackablePaths
              - McAfeeSitelistFiles
              - ModifiableScheduledTask
              - ModifiableServiceBinaries
              - ModifiableServiceRegistryKeys
              - ModifiableServices
              - ProcessDLLHijack
              - RegistryAutoLogons
              - RegistryAutoruns
              - TokenPrivileges
              - UnattendedInstallFiles
              - UnquotedServicePath


    Examples:
        SharpUp.exe audit
            -> Runs all vulnerability checks re

        SharpUp.exe HijackablePaths
            -> Check only if there are modifiab

        SharpUp.exe audit HijackablePaths
            -> Check only for modifiable paths
```

Compile Instructions

We are not planning on releasing binaries for SharpUp, so you will have to compile yourself :)

C# 100.0%

SharpUp has been built against .NET 3.5 and is compatible with Visual Studio 2015 Community Edition. Simply open up the project .sln, choose "release", and build.

Acknowledgments

SharpUp incorporates various code C# snippets and bits of PoCs found throughout research for its capabilities. These snippets and authors are highlighted in the appropriate locations in the source code, and include:

- Igor Korkhov's code to retrieve current token group information
- JGU's snippet on file/folder ACL right comparison
- Rod Stephens' pattern for recursive file enumeration
- SwDevMan81's snippet for enumerating current token privileges
- Nikki Locke's code for querying service security descriptors
- Raika for providing example unquoted service path search code.
- RemiEscourrou for contributing additional ACE checking code and example modifiable service registry key code.
- Coder666 for adding ACE filtering code to filter only ACEs with access allowed.
- vysecurity for providing Registry Auto Logon and Domain GPP Password example code.
- djhohnstein for merging in several outdated PRs and refactoring the entire code base.

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.