Product ⌄   Solutions ⌄   Resources ⌄   Open Source ⌄   Enterprise ⌄   Pricing   🔍   Sign in   Sign up

GhostPack / **SharpUp**   Public

🔔 Notifications   ⑂ Fork 245   ☆ Star 1.3k

<> Code   ⊙ Issues 3   � Pull requests 5   ▷ Actions   ▦ Projects   ⊘ Security   📈 Insights

master ⌄   ⑂   🏷

🔍 Go to file   <> Code ⌄

HarmJ0y Update SharpUp.csproj		8a75791 · last year	⏱ 39 Commits
📁 SharpUp	Update SharpUp.csproj		last year
🗎 .gitignore	Create .gitignore with common VS excl...		6 years ago
🗎 LICENSE	initial commit		6 years ago
🗎 README.md	Merge pull request #21 from IceMoon...		2 years ago
🗎 SharpUp.sln	initial commit		6 years ago

📖 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.

Usage

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

    audit   - Specifies whether or not to enable audit mode. If enabl
              regardless if the process is in high integrity or the
              If no checks are specified, audit will run all checks.
              be ran.

    check*  - The individual vulnerability check to be ran. Must be

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


    Examples:
```

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

● C# 100.0%

```
            SharpUp.exe audit
                -> Runs all vulnerability checks regardless of integrity

            SharpUp.exe HijackablePaths
                -> Check only if there are modifiable paths in the user':

            SharpUp.exe audit HijackablePaths
                -> Check only for modifiable paths in the user's %PATH%
```

Compile Instructions

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

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.