



**sensepost / impersonate** Public

Notifications Fork **32** Star **279**

**Code** Issues **1** Pull requests Actions Projects Security Insights

**main** Go to file **Code**

	CME_module	
	Impersonate	
	LICENSE	
	README.md	
	impersonate.py	
	list_tokens.c	

**README** GPL-3.0 license

# Impersonate

---

## Description

This repo contains the toolings that was developped while writing the following blog post <https://sensepost.com/blog/2022/abusing-windows-tokens-to-compromise-active-directory-without-touching-lsass/>. The blog post contains all necessary information to understand how

## About

A windows token impersonation tool

- Readme
- GPL-3.0 license
- Activity
- Custom properties
- 279 stars**
- 7 watching**
- 32 forks**

Report repository

## Releases

No releases published

## Packages

No packages published

## Contributors **2**

- Dfite Deft\_**
- leonjza** Leon Jacobs

the token manipulation internal mechanism works and how we can use it to our advantage.

## Content

This repo contains four tools:

- A standalone binary (Impersonate/) that you can use to manipulate tokens on a Windows computers remotely (PsExec/WmiExec) or interactively
- The CrackMapExec python module (impersonate.py) with the embedded Impersonate binary
- The embedded CrackMapExec binary (CME\_module/) which is the same as the Impersonate.exe binary without printf's
- The list\_tokens.c C++ code that is presented on the blog post

## Impersonate.exe usage

The Impersonate.exe tool contains three modules:

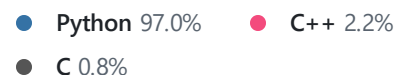
- Impersonate list: which will list available tokens

```
C:\Windows\system32\cmd.exe /c cd \ad\impersonate\Impersonate\x64\Release & Impersonate.exe list
[?] Enabling SeAssignPrimaryToken
[*] SeAssignPrimaryToken owned!
[*] SeAssignPrimaryToken enabled!
[?] Enabling SeDebugPrivilege
[*] SeDebugPrivilege owned!
[*] SeDebugPrivilege enabled!

[*] Listing available tokens
ID: 0] [SESSION: 1] [INTEGRITY: High ] [TokenPrimary ] [ ] User: NT AUTHORITY\SYSTEM
ID: 1] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: DESKTOP-IDGAQAS\windev
ID: 2] [SESSION: 1] [INTEGRITY: Medium] [TokenPrimary ] [ ] User: DESKTOP-IDGAQAS\windev
ID: 3] [SESSION: 1] [INTEGRITY: High ] [TokenPrimary ] [ ] User: DESKTOP-IDGAQAS\windev
ID: 4] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: NT AUTHORITY\SYSTEM
ID: 5] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: NT AUTHORITY\LOCAL SERVICE
ID: 6] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: Font Driver Host\UMFD-0
ID: 7] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: Font Driver Host\UMFD-1
ID: 8] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: NT AUTHORITY\NETWORK SERVICE
ID: 9] [SESSION: 1] [INTEGRITY: High ] [TokenPrimary ] [ ] User: Window Manager\DM-1
ID: 10] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityImpersonation] User: Window Manager\DM-1
ID: 11] [SESSION: 0] [INTEGRITY: High ] [TokenPrimary ] [ ] User: NT AUTHORITY\NETWORK SERVICE
ID: 12] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityIdentification] User: NT AUTHORITY\SYSTEM
ID: 13] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityIdentification] User: NT AUTHORITY\LOCAL SERVICE
ID: 14] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityIdentification] User: Window Manager\DM-1
ID: 15] [SESSION: 0] [INTEGRITY: ] [TokenImpersonation] [SecurityIdentification] User: NT AUTHORITY\NETWORK SERVICE
ID: 16] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityIdentification] User: DESKTOP-IDGAQAS\windev
ID: 17] [SESSION: 0] [INTEGRITY: High ] [TokenPrimary ] [ ] User: NT AUTHORITY\LOCAL SERVICE
ID: 18] [SESSION: 1] [INTEGRITY: ] [TokenImpersonation] [SecurityDelegation] User: DESKTOP-IDGAQAS\windev
ID: 19] [SESSION: 1] [INTEGRITY: Low ] [TokenPrimary ] [ ] User: DESKTOP-IDGAQAS\windev
ID: 20] [SESSION: 0] [INTEGRITY: Low ] [TokenPrimary ] [ ] User: NT AUTHORITY\LOCAL SERVICE
```

- Impersonate exec: which will allow you running commands impersonating a user
- Impersonate adduser: which will allow you elevating your privileges to domain admin

## Languages



## Compilation instructions

In order to compile the projects you will have to switch the Runtime library options to Multi-threaded Debug (/MtD) in the project properties.

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



© 2024 GitHub, Inc.