

 [pentestmonkey](#) / [pysecdump](#)

 Watch 7

 Star 27

 Fork 9

Python-based tool to dump security information from Windows systems










 13 commits


 1 branch

 0 releases

 3 contributors

 Branch: master [pysecdump](#) / + 

 Your Name	fixed issue 2: LSA Secrets do not start at offset 0xC on NT5 x64	Latest commit fbc4d6b on 31 Jul
 framework	fixed issue 2: LSA Secrets do not start at offset 0xC on NT5 x64	3 months ago
 wpc	Initial checkin	3 years ago
 CHANGELOG	Initial checkin	3 years ago
 COPYING	Initial checkin	3 years ago
 COPYING.PYSECDUMP	Initial checkin	3 years ago
 README.md	README: fix installer typo	2 years ago
 pysecdump.exe	fixed issue 2: LSA Secrets do not start at offset 0xC on NT5 x64	3 months ago
 pysecdump.py	Initial checkin	3 years ago

 README.md

# pysecdump

Python-based tool to dump security information from Windows systems

## Overview

pysecdump is a python tool to extract various credentials and secrets from running Windows systems. It currently extracts:

- LM and NT hashes (SYSKEY protected)
- Cached domain passwords
- LSA secrets
- Secrets from Credential Manager (only some)

pysecdump can also:

- Impersonate other processes - if you want a shell as another user
- Enable currently held windows privileges - see "whoami /priv"


It does exactly the same sort of things already implemented by gsecdump, Cain & Abel, metasploit and many other tools.


This implementation is in python and that's probably the only notable thing about this implementation.


If you think python is cool, this project might be of interest. If you don't, you should probably stop reading now.


## Credits


[Code](#)

 Issues 0


 Pull requests 0

 Wiki

 Pulse

 Graphs

HTTPS clone URL

<https://github.com> 

You can clone with [HTTPS](#), [SSH](#), or [Subversion](#).

 Clone in Desktop

 Download ZIP

This is a derivative work of:

creddump - <http://code.google.com/p/creddump/>

In fact very little of the code is different in pysecdump, which just pulls data from the registry instead of from on-disk hives

windows-privesc-check - <http://code.google.com/p/windows-privesc-check/>

This is used mostly for the registry API

I found the metasploit source code very handy for identifying the appropriate registry keys, so credit to those guys too for a great tool.

## Requirements

Nothing if you just want to run pysecdump.exe on a windows system.

If you want to modify pysecdump.py then run recreate the .exe you need:

- pywin32 - <http://sourceforge.net/projects/pywin32/>
- pycrypto - <https://www.dlitz.net/software/pycrypto/>
- pyinstaller - <http://www.pyinstaller.org/>

## Usage

Dump cached domain hashes (run as SYSTEM):

```
pysecdump -c
```

Dump LSA secrets (run as SYSTEM):

```
pysecdump -l
```

Dump local password hashes from SAM (run as SYSTEM):

```
pysecdump -s
```

Dump (some secrets) from Credential Manager (run as SYSTEM):

```
pysecdump -C
```

Impersonate process ID 1234:

```
pysecdump -i 1234  
whoami /all
```

Enable all currently held windows privileges (can also use with -i):

```
pysecdump -e  
whoami /priv
```

## Converting to .exe

```
cd C:\pyinstaller-2.0
pyinstaller.py -F "c:\somepath\pysecdump.py"
```

## Features

---

- Is written in python
- Supports XP family and Vista+ registry locations
- Uses impersonation of all available processes when dumping Credential Manager.

## Author

---

pysecdump was adapted from creddump by pentestmonkey.

creddump is written by Brendan Dolan-Gavitt ([bdolangavitt@wesleyan.edu](mailto:bdolangavitt@wesleyan.edu)). For more information on Syskey, LSA secrets, cached domain credentials, and lots of information on volatile memory forensics and reverse engineering, check out:

<http://moyix.blogspot.com/>

## License

---

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

