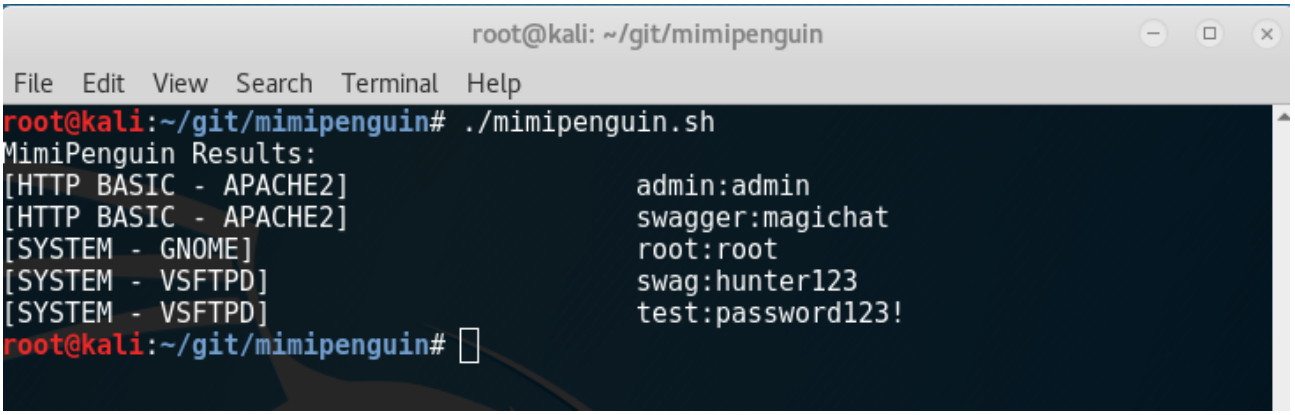
GitHub - huntergregal/mimipenguin: A tool to dump the login password from the current linux user

By huntergregal

Archived: 2026-04-06 00:45:19 UTC

A tool to dump the login password from the current linux desktop user. Adapted from the idea behind the popular Windows tool mimikatz. This was assigned *CVE-2018-20781* (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20781). Fun fact it's still not fixed after GNOME Keyring 3.27.2 and still works as of `3.28.0.2-1ubuntu1.18.04.1`.



Details

Takes advantage of cleartext credentials in memory by dumping the process and extracting lines that have a high probability of containing cleartext passwords. Will attempt to calculate each word's probability by checking hashes in /etc/shadow, hashes in memory, and regex searches. 2.0 introduces a clean C port that aims to increase the speed of execution and portability

Known Issues

- The 32bit variant of mimipenguin (C build) may fail in a 64bit userspace as it currently does not adequately handle searching a 64bit address space

Requires

- root permissions

Supported/Tested Systems

- Kali 4.3.0 (rolling) x64 (gdm3)
- Ubuntu Desktop 12.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)

- Ubuntu Desktop 14.04.1 LTS x64 (Gnome Keyring 3.10.1-1ubuntu4.3, LightDM 1.10.6-0ubuntu1)
- Ubuntu Desktop 16.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Ubuntu Desktop 16.04.4 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2, LightDM 1.18.3-0ubuntu1.1)
- Ubuntu 18
- XUbuntu Desktop 16.04 x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Archlinux x64 Gnome 3 (Gnome Keyring 3.20)
- OpenSUSE Leap 42.2 x64 (Gnome Keyring 3.20)
- VSFTPd 3.0.3-8+b1 (Active FTP client connections)
- Apache2 2.4.25-3 (Active/Old HTTP BASIC AUTH Sessions) [Gcore dependency]
- openssh-server 1:7.3p1-1 (Active SSH connections - sudo usage)

Building

- To Build the C variant release simply run `make` in the root directory of the project
- To build a debug binary with debug prints run `make debug`
- To build a static linked binaries run `make static`

Notes

- Password moves in memory - still honing in on 100% effectiveness
- Plan on expanding support and other credential locations
- Working on expanding to non-desktop environments
- Known bug - sometimes gcore hangs the script, this is a problem with gcore
- Open to pull requests and community research
- LDAP research (nscld winbind etc) planned for future

Development Roadmap

- Implement needles in C port (speed up)
- Add optional arg to target specific users only (speed up)

MimiPenguin is slowly being ported to multiple languages to support all possible post-exploit scenarios. The roadmap below was suggested by KINGSABRI to track the various versions and features. An "X" denotes full support while a "~" denotes a feature with known bugs.

Feature	**.sh**	**.py**
GDM password (Kali Desktop, Debian Desktop)	~	X
Gnome Keyring (Ubuntu Desktop, ArchLinux Desktop)	~	X
LightDM (Ubuntu Desktop)	X	X
VSFTPd (Active FTP Connections)	X	X
Apache2 (Active HTTP Basic Auth Sessions)	~	~

Feature	.sh	.py
OpenSSH (Active SSH Sessions - Sudo Usage)	~	~

Contact

- Twitter: @huntergregal
- Website: huntergregal.com
- Github: huntergregal

Licence

Special Thanks

- the-useless-one for remove Gcore as a dependency, cleaning up tabs, adding output option, and a full python3 port
- gentilkiwi for Mimikatz, the inspiration and the twitter shoutout
- pugilist for cleaning up PID extraction and testing
- ianmiell for cleaning up some of my messy code
- w0rm for identifying printf error when special chars are involved
- benichmt1 for identifying multiple authenticate users issue
- ChaitanyaHaritash for identifying special char edge case issues
- ImAWizardLizard for cleaning up the pattern matches with a for loop
- coreb1t for python3 checks, arch support, other fixes
- n1nj4sec for a python2 port and support
- KINGSABRI for the Roadmap proposal
- bourgouinadrien for linking https://github.com/koalaman/shellcheck
- bcoles for adding more needles
- space-r7 and bcoles for work on the Metasploit MimiPenguin module port

---