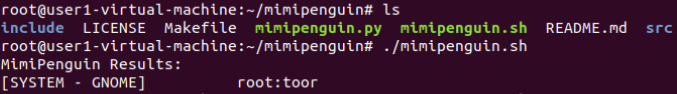
**mimipenguin(CVE-2018-20781):**

mimipenguin(CVE-2018-20781)转储特定进程，这些进程中很可能以明文形式包含用户的密码(只适用于有限版本的 Linux 系统)

https://github.com/huntergregal/mimipenguin(A tool to dump the login password from the current linux user)





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

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)