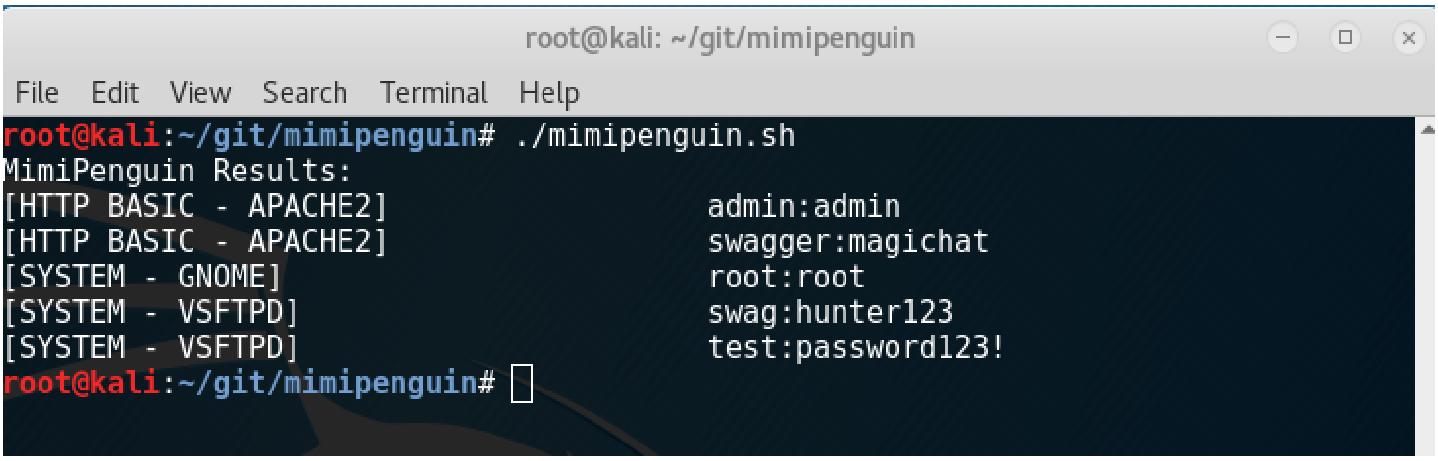
Mimipenguin：读取当前登录用户密码（Linux下的Mimikatz）

hades / 2017-04-05 05:50:31 / 浏览数 5257 安全工具 工具 顶(0) 踩(0)

来源地址：https://github.com/rasta-mouse/Sherlock

mimipenguin

A tool to dump the login password from the current linux desktop user. Adapted from the idea behind the popular Windows tool mimikatz.


root@kali: ~/git/mimipenguin
File Edit View Search Terminal Help

```
root@kali:~/git/mimipenguin# ./mimipenguin.sh
MimiPenguin Results:
[HTTP BASIC - APACHE2]                  admin:admin
[HTTP BASIC - APACHE2]                  swagger:magichat
[SYSTEM - GNOME]                        root:root
[SYSTEM - VSFTPD]                       swag:hunter123
[SYSTEM - VSFTPD]                       test:password123!
root@kali:~/git/mimipenguin# 
```

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.

Requires

- root permissions

Supported/Tested

- Kali 4.3.0 (rolling) x64 (gdm3)
- Ubuntu Desktop 12.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
- Ubuntu Desktop 16.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
- XUbuntu Desktop 16.04 x64 (Gnome Keyring 3.18.3-0ubuntu2)
- VSFTPd 3.0.3-8+b1 (Active FTP client connections)
- Apache2 2.4.25-3 (Active/Old HTTP BASIC AUTH Sessions)
- openssh-server 1:7.3p1-1 (Active SSH connections - sudo usage)

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

Contact

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

Licence

Special Thanks

- gentilkiki 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

点击收藏 | 0 关注 | 0

上一篇：CVE-2017-7269回显PoC解析 下一篇：从Pwnhub诞生聊Django安全编码

1. 1 条回复

hades 2017-04-05 05:58:54

PAM模块内存dump密码。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录