Stealing User Passwords with Mimikatz DCSync

blog.netwrix.com/2022/09/30/extracting-user-password-data-with-mimikatz-dcsync

Mimikatz provides a variety of ways to extract and manipulate credentials, but one of the most alarming is the DCSync command. Using this command, an adversary can simulate the behavior of a domain controller and ask other domain controllers to replicate information — including user password data. In fact, attackers can get any account's NTLM password hash or even its plaintext password, including the password of the KRBTGT account, which enables them to create Golden Tickets.

Handpicked related content:
   [Free Guide] Privileged Access Management Best Practices

If that's not bad enough, this attack can be performed without running any code on a domain controller, unlike the other options Mimikatz offers to extract password data. Moreover, it takes advantage of the Microsoft Directory Replication Service Remote Protocol (MS-DRSR), which is a valid and necessary function of Active Directory and therefore cannot be turned off or disabled.

Who can perform a DCSync attack?

Running the Mimikatz DCSync requires an account with the rights to perform domain replication. This is controlled by the Replicating Changes permissions set on the domain. Having the Replicating Changes All or Replicating Directory Changes permission will allow you to perform this attack.

Mimikatz DCSync

By default, these permissions are limited to the Domain Admins, Enterprise Admins, Administrators and Domain Controllers groups. To find any additional accounts that can perform the DCSync attack, use the following PowerShell script. It will enumerate all domain-level permissions for a domain and find all accounts that are granted these rights and that have a RID above 1000, which will exclude all default permissions.

```
#Get all permissions in the domain, filtered to the two critical replication
permissions represented by their GUIDs
Import-Module ActiveDirectory
cd 'AD:DC=JEFFLAB,DC=local' # Replace with distinguished name of your domain
$AllReplACLs = (Get-AcL).Access | Where-Object {$_.ObjectType -eq '1131f6ad-9c07-
11d1-f79f-00c04fc2dcd2' -or $_.ObjectType -eq '1131f6aa-9c07-11d1-f79f-
00c04fc2dcd2'}

#Filter this list to RIDs above 1000 which will exclude well-known Administrator
groups
foreach ($ACL in $AllReplACLs)
{
    $user = New-Object System.Security.Principal.NTAccount($ACL.IdentityReference)
    $SID = $user.Translate([System.Security.Principal.SecurityIdentifier])
    $RID = $SID.ToString().Split("-")[7]
    if([int]$RID -gt 1000)
    {
        Write-Host "Permission to Sync AD granted to:" $ACL.IdentityReference
    }
}
```

Running this script will list each user and group who has that has the rights required to perform the DCSync attack but probably shouldn't:

Mimikatz DCSync 2

How is a DCSync attack launched?

If you have the necessary rights, the rest is quite simple. Simply execute the following command:

Lsadump::dcsync /domain:*<domain_name>* /user:*<user_name>*

To retrieve the KRBTGT account's password hash, an adversary can simply use the command shown below:

Mimikatz DCSync 3

If the password is stored with reversible encryption, the cleartext password will be shown:

Mimikatz DCSync 4

How can organizations defend against DCSync attacks?

The best way to prevent DCSync attacks is to strictly limit which accounts have permissions to replicate information in your domain. You can start by running the script provided above against all your domains to find any accounts that have improper

privileges to perform this attack. In addition, implement controls to protect the accounts that need these rights, especially to avoid their password details being stored where attackers could compromise them.

If you detect a DCSync attack, immediately disable the account involved to block the adversary from escalating their privileges or making any other changes to AD. Netwrix StealthINTERCEPT provides blocking policies that can prevent an account or workstation from executing additional replication, which can slow down an attack and give responders more time to eliminate the threat. Moreover, Netwrix StealthDEFEND supports these response steps by providing details about the DCSync attack perpetrator, sources, targets and queried objects.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.