Sneaky Active Directory Persistence #13: DSRM Persistence v2

adsecurity.org

Sean Metcalf September 25, 2015

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
```

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:

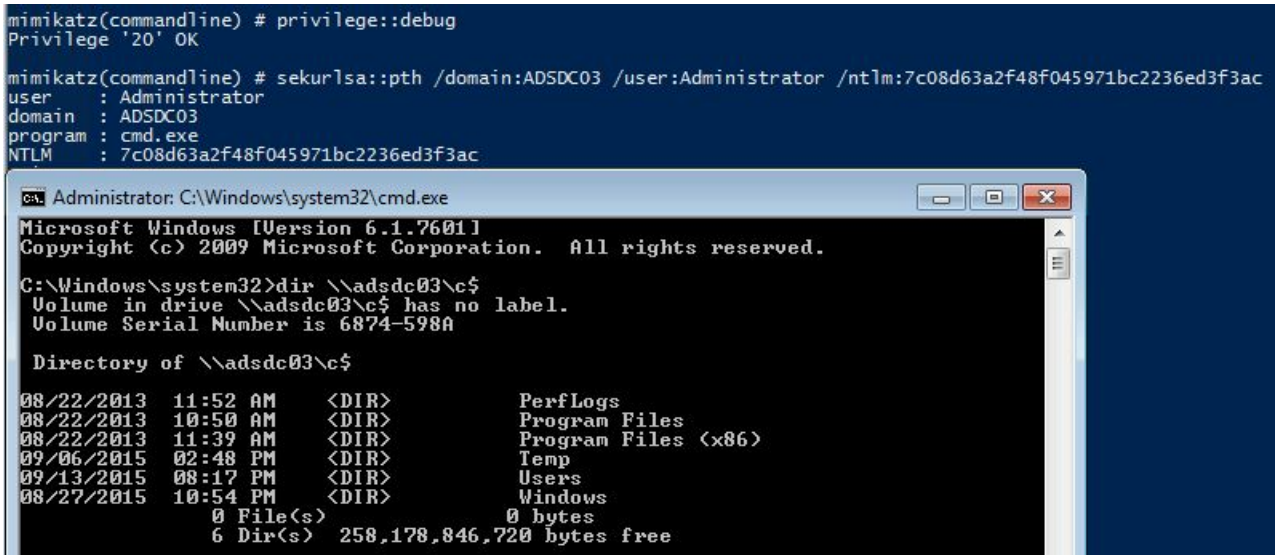
1. Restart in Directory Services Restore Mode (*bcdedit /set safeboot dsrepair*)
2. Access DSRM without rebooting (Windows Server 2008 and newer)
    1. Set the registry key DsrmAdminLogonBehavior to 1
    2. Stop the Active Directory service
    3. Logon using DSRM credentials on the console.
3. Access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

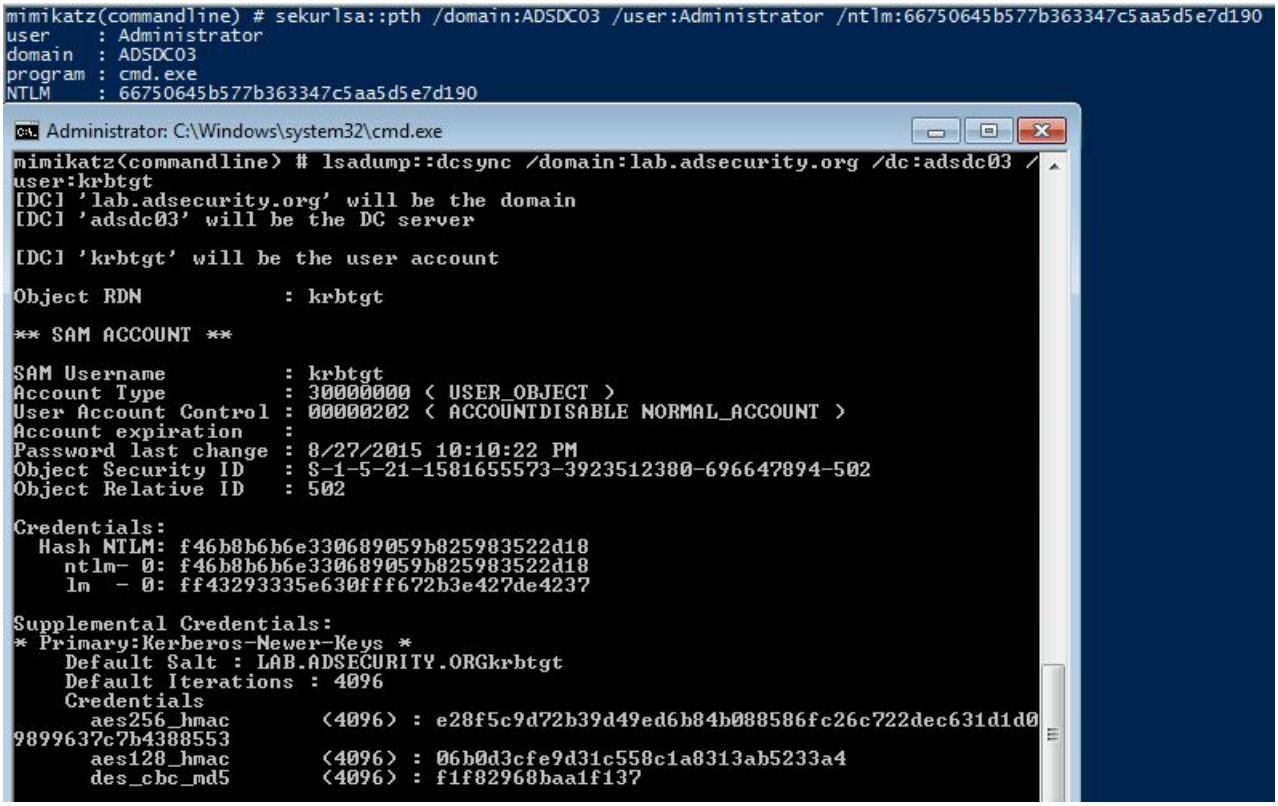
Mimikatz “privilege::debug” “sekurlsa::pth /domain:ADSDC03 /user:Administrator /ntlm:7c08d63a2f48f045971bc2236ed3f3ac” exit



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 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 DsrmAdminLogonBehavior 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 DsrmAdminLogonBehavior 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\DsrmAdminLogonBehavior* should not exist or be set to 1.

(Visited 15,918 times, 7 visits today)