SentinelOne blog

EN

Detecting DSRM Account Misconfigurations

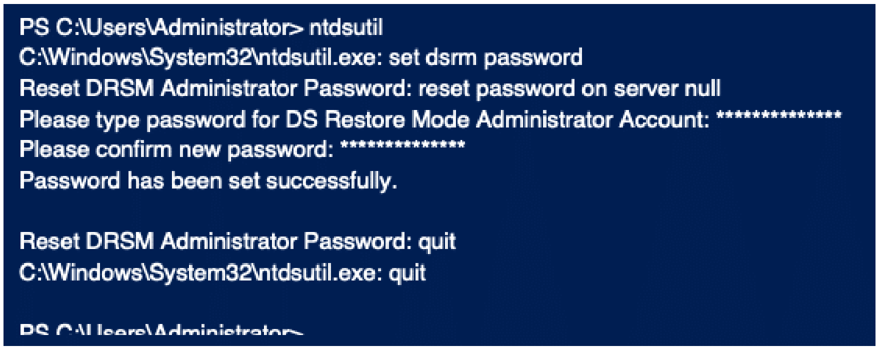
August 24, 2021
by Vikram Navali

PDF

Table of Contents

During a Domain Controller (DC) promotion, administrators create a Directory Services Restore Mode (DSRM) local administrator account with a restore AD backups or recover the server from a failure.

Attackers could abuse DSRM account to maintain their persistence and access to the organization's Active Directory. Administrators set the DSRM password while configuring Active Directory and typically do not follow the recommendation of changing its passwords regularly. Knowing this, attackers will attempt to create a permanent backdoor to establish a connection in the future. An attacker can change the DSRM account password by running the following command on every DC (or remotely against every DC by replacing "null" with DC name).



```
PS C:\Users\Administrator> ntdsutil
C:\Windows\System32\ntdsutil.exe: set dsrm password
Reset DRSM Administrator Password: reset password on server null
Please type password for DS Restore Mode Administrator Account: **************
Please confirm new password: **************
Password has been set successfully.

Reset DRSM Administrator Password: quit
C:\Windows\System32\ntdsutil.exe: quit

PS C:\Users\Administrator>
```

Once an attacker has the DSRM password, it is possible to use this account to log on to the DC over

Search ...

Recent Posts

Safely Expanding the Frontiers of AI & LLMs | S Ventures' Investment in Galileo
October 25, 2024

The Good, the Bad and the Ugly in Cybersecurity – Week 43
October 25, 2024

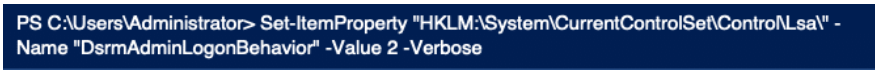
Climbing The Ladder | Kubernetes Privilege Escalation (Part 1)

source credential dumping tool, such as running Mimikatz with the commands "*lsadump::sam*" and "*lsadump::lsa /patch*", respectively.

With the local administrator password hash, the attacker can change the Windows registry to log into the DC using DSRM hashes without rebooting the server. The attacker can confirm the "DsrmAdminLogonBehavior" registry key value under HKLMSystemCurrentControlSetControlLsa and create possible REG_DWORD values as shown below:

- 0 – the default value. Can use the DSRM administrator account only if the DC starts in DSRM.
- 1 – Use the DSRM administrator account to log on if the local AD DS service is stopped.
- 2 – Always use the DSRM administrator account (This setting is not recommended because password policies do not apply to the DSRM administrator account).

Cloud
Company
Data Platform
Feature Spotlight
For CISO/CIO
From the Front Lines
Identity
Integrations & Partners
macOS
PinnacleOne
The Good, the Bad and the Ugly



```
PS C:\Users\Administrator> Set-ItemProperty "HKLM:\System\CurrentControlSet\Control\Lsa\" -
Name "DsrmAdminLogonBehavior" -Value 2 -Verbose
```

An attacker further uses additional techniques such as Pass the Ticket (PTT) to access the DC and laterally move on the network. The following Mimikatz commands help to achieve their goals.

- "*privilege::debug*"
- "*sekurlsa::pth /domain:attivo1.local /user:Administrator /ntlm: fc063a56bf43cb54e57a2522d4d48678*"

How to Mitigate DSRM Account Misconfigurations?

Security administrators must ensure the DSRM account passwords are unique for every Domain Controller and change them regularly (at least as often as other account passwords). Also, ensure the registry key DsrmAdminLogonBehavior is not set to 2, and the same registry key value does not exist by default.

Conclusion

network. Administrators should implement appropriate password and registry key settings for these accounts and continuously monitor for misconfigurations that expose Active Directory to an attack.

Singularity™ Ranger AD is a cloud-delivered solution designed to uncover vulnerabilities in Active Directory and Azure AD. Get additional AD attack detection and conditional access capabilities to protect enterprise identity infrastructure with Singularity Ranger AD Protect.

References

https://adsecurity.org/?p=1714

https://adsecurity.org/?p=1785

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

Directory

- Exit Sandman | How SentinelOne Deflects APT-Level Identity Security Risks

Read More

Defeat every attack, at every stage of the threat lifecycle with SentinelOne

Book a demo and see the world's most advanced cybersecurity platform in action.

SentinelLabs: Threat Intel & Malware Analysis

We are hunters, reversers, exploit developers, & tinkerers shedding light on the vast world of malware, exploits, APTs, & cybercrime across all platforms.

MITRE Engenuity ATT&CK Evaluation Results

SentinelOne leads in the latest Evaluation with 100% prevention. Leading analytic coverage. Leading visibility. Zero detection delays.

SentinelOne Secure Tomorrow™

Company

Our Customers

Why SentinelOne

Platform

About

Partners

Support

Resources

Blog

Labs

Product Tour

Press

News

FAQ

Master Subscription Agreement

Investor Relations

Sign Up For Our Newsletter

Business Email →

By clicking Subscribe, I agree to the use of my personal data in accordance with SentinelOne Privacy Notice. SentinelOne will not sell, trade, lease, or rent your personal data to third parties. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Language

English

Global Headquarters

444 Castro Street
Suite 400
Mountain View, CA 94041

+1-855-868-3733

sales@sentinelone.com