Autor: Luis Fueris Martín
Fecha: 1-09-2016
Coms: Documentación sobre el backup [cfreds_2015_data_leakage_pc.dd].
URL: http://www.cfreds.nist.gov/data_leakage_case/data-leakage-case.html

Documentación
==========

kpartx - esta herramienta lee de la tabla de particiones del backup y
crea un mapeo en el dispositivo [/dev/loop[0-7]] en el cual están las
particiones creadas. Esto es llamado creación (o eliminación) en caliente.

Ejemplo man

To mount all the partitions in a raw disk image:

```
kpartx -av disk.img
```

This will output lines such as:

```
loop3p1 : 0 20964762 /dev/loop3 63
```

The loop3p1 is the name of a device file under /dev/mapper which you
can use to access the partition, for example to fsck it:

```
fsck /dev/mapper/loop3p1
```

When you're done, you need to remove the devices:

```
kpartx -d disk.img
```

Montamos los dispositivos [/dev/mapper/loop0p[12]]:

```
$> sudo mount -o ro,noexec,nodev,nosuid /dev/mapper/loop0p1 /mnt/windows/pc1/
$> sudo mount -o ro,noexec,nodev,nosuid /dev/mapper/loop0p2 /mnt/windows/pc2/
```

Herramienta de [Linux] para manipular los registros de [Windoze]:

```
>> Forensic Registry EDitor
$> wget -q http://deb.pinguin.lu/debsign_public.key -O- | sudo apt-key add -
```

Nos descargamos el [*.deb], en [https://pinguin.lu/pkgserver]

Sin embargo da muchos problemas en cuanto a su instalación... Es mejor
utilizar el comando [chntpw]. Con la opción [-e]

```
-e     Registry editor with limited capabilities (but it  does  include
       write support). For a slightly more powerful editor see reged
```

Nueva herramienta para visualizar los registros de [Windoze] en [Linux]
-> [RegRipper]

Instalación:

DEBIAN/UBUNTU

```
$> apt-get install cpanminus make unzip wget
FEDORA
$> dnf install perl-App-cpanminus.noarch make unzip wget perl-Archive-\
Extract-gz-gzip.noarch which

CENTOS/REDHAT
$> yum install  perl-App-cpanminus.noarch make unzip wget perl-Archive-\
Extract-gz-gzip.noarch which

$> mkdir /usr/local/lib/rip-lib
$> wget https://github.com/keydet89/RegRipper2.8
$> cpanm -l /usr/local/lib/rip-lib Parse::Win32Registry

$> perl -pi -e 's/\r\n/\n/g' rip.pl
$> chmod +x rip.pl

Exit the first line of rip.pl to use your systems perl interpreter to \
run rip.pl

$> which perl | sed 's/\//\\\//g' > /tmp/perlloc && sed -i \
"s/ c:\\\\perl\\\\bin\\\\perl.exe/`cat /tmp/perlloc`/" rip.pl

Add/Modify a few commands to allow the RegRipper plugins directory to be found:

$> echo $PWD | sed 's/\//\\\//g' > /tmp/pwd && sed -i \
"s/use Getopt::Long;/use Getopt::Long;\nuse lib \'`cat /tmp/pwd`\/\';\n/" rip.pl

$> sed -i "s/plugindir = \"plugins\\\\\\\\\/plugindir = \
\"`cat /tmp/pwd`\/plugins\//" rip.pl

$> sed -i 's/require "plugins\\\\".$plugins{$i}."\\.pl";/require \
"plugins\/".$plugins{$i}."\\.pl";/' rip.pl

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

[cpanm] es una herramienta para conseguir, descomprimir, construir e instalar
modulos de Perl.

Ejemplo [RegRipper]
-------------------------------------------------------------------------------
[leviathan3773@latitude:RegRipper2.8 ] $ ./rip.pl -r /mnt/windows/hdd/Windows/\
System32/config/SAM -f sam

Parsed Plugins file.
Launching samparse v.20160203
samparse v.20160203
(SAM) Parse SAM file for user & group mbrshp info


User Information
-------------------------
Username        : Administrator [500]
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Sun Nov 21 03:47:20 2010 Z
Pwd Reset Date  : Sun Nov 21 03:57:24 2010 Z
Pwd Fail Date   : Never
```

```
Login Count     : 6
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Wed Mar 25 10:33:22 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password not required
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : informant [1000]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 14:33:54 2015 Z
Name            :
Password Hint   : IAMAN
Last Login Date : Wed Mar 25 14:45:59 2015 Z
Pwd Reset Date  : Sun Mar 22 14:33:54 2015 Z
Pwd Fail Date   : Wed Mar 25 14:45:43 2015 Z
Login Count     : 10
  --> Password not required
  --> Password does not expire
  --> Normal user account

Username        : admin11 [1001]
Full Name       : admin11
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:51:54 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:57:02 2015 Z
Pwd Reset Date  : Sun Mar 22 15:52:10 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 2
  --> Password does not expire
  --> Normal user account

Username        : ITechTeam [1002]
Full Name       : ITechTeam
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Mar 22 15:52:30 2015 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Sun Mar 22 15:52:45 2015 Z
Pwd Fail Date   : Sun Mar 22 15:53:02 2015 Z
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

```
Username        : temporary [1003]
Full Name       : temporary
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Sun Mar 22 15:53:01 2015 Z
Name            :
Last Login Date : Sun Mar 22 15:55:57 2015 Z
Pwd Reset Date  : Sun Mar 22 15:53:11 2015 Z
Pwd Fail Date   : Sun Mar 22 15:56:37 2015 Z
Login Count     : 1
  --> Password does not expire
  --> Normal user account

-------------------------
Group Membership Information
-------------------------
Group Name    : Power Users [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Power Users are included for backwards compatibility and
possess limited administrative powers
Users         : None

Group Name    : Remote Desktop Users [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members in this group are granted the right to logon remotely
Users         : None

Group Name    : Backup Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Backup Operators can override security restrictions for
the sole purpose of backing up or restoring files
Users         : None

Group Name    : Guests [1]
LastWrite     : Wed Mar 25 10:15:19 2015 Z
Group Comment : Guests have the same access as members of the Users
group by default, except for the Guest account which is further restricted
Users :
  S-1-5-21-2425377081-3129163575-2985601102-501

Group Name    : Administrators [4]
LastWrite     : Sun Mar 22 15:52:30 2015 Z
Group Comment : Administrators have complete and unrestricted access
to the computer/domain
Users :
  S-1-5-21-2425377081-3129163575-2985601102-1000
  S-1-5-21-2425377081-3129163575-2985601102-500
  S-1-5-21-2425377081-3129163575-2985601102-1001
  S-1-5-21-2425377081-3129163575-2985601102-1002

Group Name    : Replicator [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Supports file replication in a domain
Users         : None

Group Name    : Cryptographic Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members are authorized to perform cryptographic operations.
Users         : None
```

```
Group Name    : Users [5]
LastWrite     : Sun Mar 22 15:53:01 2015 Z
Group Comment : Users are prevented from making accidental or
intentional system-wide changes and can run most applications
Users :
  S-1-5-21-2425377081-3129163575-2985601102-1002
  S-1-5-21-2425377081-3129163575-2985601102-1001
  S-1-5-21-2425377081-3129163575-2985601102-1003
  S-1-5-11
  S-1-5-4

Group Name    : Performance Monitor Users [0]
LastWrite     : Tue Jul 14 04:45:46 2009 Z
Group Comment : Members of this group can access performance counter data
locally and remotely
Users         : None

Group Name    : Distributed COM Users [0]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Members are allowed to launch, activate and use Distributed
COM objects on this machine.
Users         : None

Group Name    : Event Log Readers [0]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Members of this group can read event logs from local machine
Users         : None

Group Name    : Performance Log Users [0]
LastWrite     : Tue Jul 14 04:45:46 2009 Z
Group Comment : Members of this group may schedule logging of performance
counters, enable trace providers, and collect event traces both locally and
via remote access to this computer
Users         : None

Group Name    : IIS_IUSRS [1]
LastWrite     : Tue Jul 14 04:45:47 2009 Z
Group Comment : Built-in group used by Internet Information Services.
Users :
  S-1-5-17

Group Name    : Network Configuration Operators [0]
LastWrite     : Wed Mar 25 10:15:37 2015 Z
Group Comment : Members in this group can have some administrative privileges
to manage configuration of networking features
Users         : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
     - S-1-5-4  = Interactive
     - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin

samparse complete.
--------------------------------------------------------------------------------


Para extraer de los registros el [Hash] de los passwords.
--------------------------------------------------------------------------------
```

Normally, Windows store passwords on single computer systems in the registry in a hashed format using the NTLM algorithm. The registry file is located in

C:\windows\system32\config\SAM.

This area of the registry has restrictive permissions so that a normal user cannot see the contents of HKLM\SAM deep enough to access the hash. In order to view the hashes one must change the permissions on the registry keys, this requires an administrative account on the system in Windows XP. I am unsure if access is possible using an administrator account in Vista or 7.

Once one has access to the password hashes though, it is difficult to gain the passwords again. There are many places on the internet that you can find information about brute forcing a NTLM hash. However, if you are simply trying to reset a password, I would recommend using Offline NT Password and Registry Editor.

If you want to get your arms wet though, the hash is stored under the key

HKLM\SAM\SAM\Domains\Account\Users\00000XXX

with a value named V. The hash is stored at a variable offset that is stored at offset 0x9C and is a 4 byte little endian value.

Otra herramientas interesante para realizar un dump de los [hashes]:

Physical access

Given physical access to the system, typically during a laptop assessment or a successful social engineering engagement, the preferred way to safely dump the password hashes is to power off the machine, enter the BIOS menu at power-on time, review the boot order to allow boot from the optical drive and USB drive before local hard-disk, save the settings and reboot the system with your favourite GNU/Linux live distribution CD or USB stick. Two widely known tools to dump the local users' hashes from the SAM file, given the Windows file system block file, are bkhive and samdump2:

    bkhive - dumps the syskey bootkey from a Windows system hive.
    samdump2 - dumps Windows 2k/NT/XP/Vista password hashes.

These tools are generally included in many GNU/Linux live distributions. If they're not, make sure to bring a copy of them with you.
Usage:

```
    # bkhive
    bkhive 1.1.1 by Objectif Securite
    http://www.objectif-securite.ch
    original author: ncuomo@studenti.unina.it

    Usage:
    bkhive systemhive keyfile

    # samdump2
    samdump2 1.1.1 by Objectif Securite
    http://www.objectif-securite.ch
```

```
    original author: ncuomo@studenti.unina.it

    Usage:
    samdump2 samhive keyfile

Example of retrieving the SAM hashes from a Windows partition /dev/sda1:

    # mkdir -p /mnt/sda1
    # mount /dev/sda1 /mnt/sda1
    # bkhive /mnt/sda1/Windows/System32/config/SYSTEM /tmp/saved-syskey.txt
    # samdump2 /mnt/sda1/Windows/System32/config/SAM /tmp/saved-syskey.txt > /tm
p/hashes.txt
-------------------------------------------------------------------------------
-------------

[bkhive] se descarga pero no se instala... la solución es la siguiente:
-------------------------------------------------------------------------------
-------

The apt-get install bkhive command runs, but bkhive is not actually installed. I

found this workaround, however, downgrading to previous versions of bkhive and p
wdump2:

$> apt-get purge bkhive
$> apt-get purge pwdump2
$> apt-get purge samdump2
$> curl http://http.us.debian.org/debian/poo...1-1.1_i386.deb > samdump2_1.1.1-1
.1_i386.deb
$> dpkg -i samdump2_1.1.1-1.1_i386.deb
$> curl http://http.us.debian.org/debian/poo...1.1-1_i386.deb > bkhive_1.1.1-1_i
386.deb
$> dpkg -i bkhive_1.1.1-1_i386.deb

https://packages.debian.org/source/wheezy/bkhive

After that bkhive and pwdump2 work.
-------------------------------------------------------------------------------
```