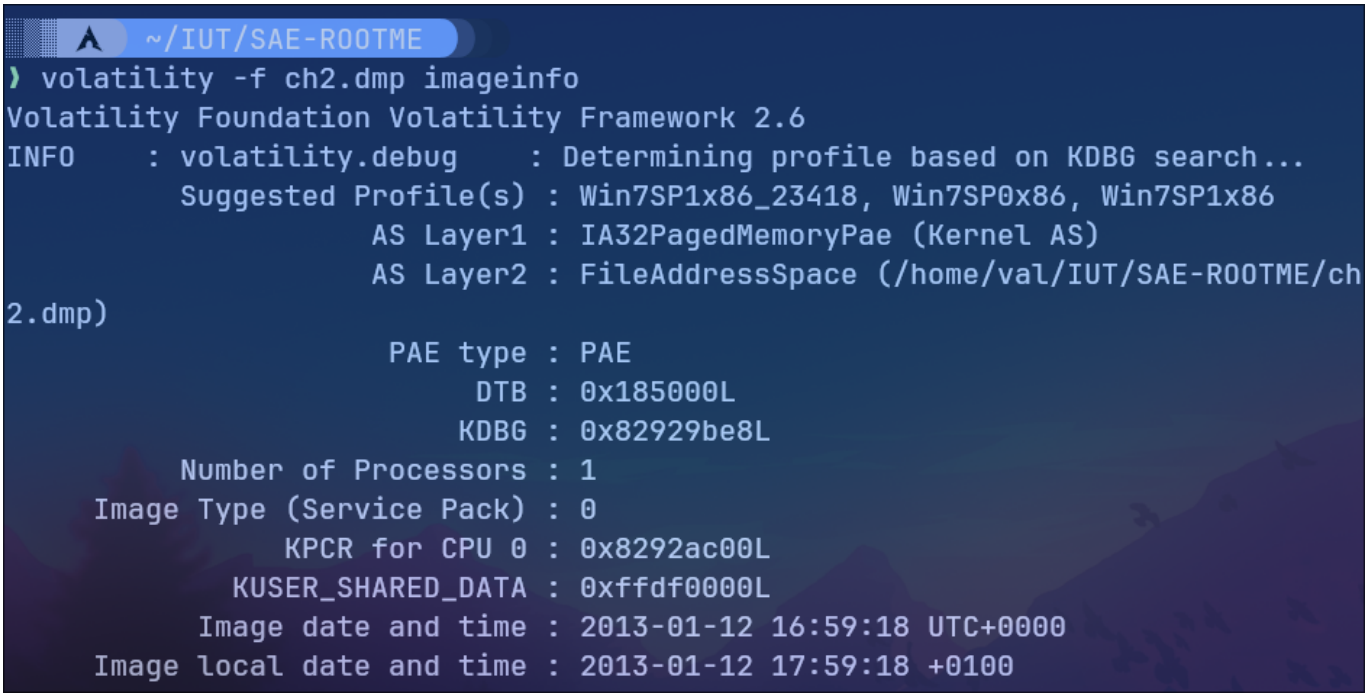
ROOT-ME - Command & Control niveau 2

Je dispose d'un dump mémoire a analysé, je vais utiliser Volatility afin de trouver le mot de passe, ici l'hostname de la machine.

Dans un premier temps, je regarde les infos sur le dump afin de savoir quel profile utilisé sur Volatility par la suite.



Le dump mémoire a été fait sur une machine Windows 7, j'utiliserai donc le profile **Win7SP1x86_23418** pour mes prochaines analyse.

Avec volatility, on peut afficher la hivelist, c'est un endroit principal du registre windows ou l'on retrouve des clés et des sous-clés du registre.

Computername registry key

on OCTOBER 21, 2018

If you want to look up registry key database to fetch computer name/domain name, then this post helps you find the key that has this information.

1. Open registry editor with the command `regedit`
2. Navigate to the node `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`
3. On the right side pane, look for the value `ComputerName`. This would show you the computer name.

This key shows computer name in all Windows versions – Windows 7, 8 and 10.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName` also has a key with the same name `Computername` which stores the active computer name.

En cherchant sur Internet, je peux trouver l'hostname de la machine dans la clé de registre suivante:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ComputerName\ComputerName`

Je vais donc chercher à retrouver la valeur de cette clé avec Volatility.

1. Afficher la hivelist

```
~/IUT/SAE-ROOTME
❯ volatility -f ch2.dmp --profile=Win7SP1x86_23418 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0x8ee66740 0x141c0740 \SystemRoot\System32\Config\SOFTWARE
0x90cab9d0 0x172ab9d0 \SystemRoot\System32\Config\DEFAULT
0x9670e9d0 0x1ae709d0 \??\C:\Users\John Doe\ntuser.dat
0x9670f9d0 0x04a719d0 \??\C:\Users\John Doe\AppData\Local\Microsoft\Windows\UsrClass.dat
0x9aad6148 0x131af148 \SystemRoot\System32\Config\SAM
0x9ab25008 0x14a61008 \SystemRoot\System32\Config\SECURITY
0x9aba79d0 0x11a259d0 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x9abb1720 0x0a7d4720 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

On souhaite récupérer la clé SYSTEM à l'adresse 0x8b21c008

2. Récupérer la clé

```
~/IUT/SAE-ROOTME
❯ volatility -f ch2.dmp --profile=Win7SP1x86_23418 printkey -o 0x8b21c008
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: CMI-CreateHive{F10156BE-0E87-4EFB-969E-5DA29D131144} (S)
Last updated: 2013-01-12 16:37:53 UTC+0000

Subkeys:
  (S) ControlSet001
  (S) ControlSet002
  (S) MountedDevices
  (S) RNG
  (S) Select
  (S) Setup
  (S) WPA
  (V) CurrentControlSet

Values:
```

Maintenant il faut récupérer la sous-clé qui contient la valeur de ComputerName. Cette sous clé se trouve dans ce chemin: `ControlSet001\Control\ComputerName\ComputerName` que l'on peut donner en argument de l'options -K.

3. Récupérer la valeur de l'hostname

```
~/IUT/SAE-ROOTME
❯ volatility -f ch2.dmp --profile=Win7SP1x86_23418 printkey -o 0x8b21c008 -K '
ControlSet001\Control\ComputerName\ComputerName'
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \REGISTRY\MACHINE\SYSTEM
Key name: ComputerName (S)
Last updated: 2013-01-12 00:58:30 UTC+0000

Subkeys:

Values:
REG_SZ                        : (S) mnmsrvc
REG_SZ        ComputerName    : (S) WIN-ETSA91RKCFP
```

On récupérer bien la valeur du ComputerName, qui est aussi le mot de passe du challenge donc `WIN-ETSA91RKCFP`