

Writeup

- 1- Dézipper le fichier zip
- 2- Obtenir le fichier ch2.dmp
- 3- Utiliser volatility avec le plugin imageinfo pour trouver le profile

```
~/Documents/tools_hacking/volatility
/Users/roberto/.pyenv/versions/2.7.18/bin/python vol.py -f ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/Users/roberto/Documents/tools_hacking/volatility/ch2.dmp)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82929be8L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0x8292ac00L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2013-01-12 16:59:18 UTC+0000
      Image local date and time : 2013-01-12 17:59:18 +0100
```

- 4- Utiliser volatility avec le plugin envvars pour trouver le COMPUTERNAME

692	svchost.exe	0x002c07f0	USERNAME	WIN-ETSA91RKCFP\$
692	svchost.exe	0x002c07f0	USERPROFILE	C:\Windows\system32\config\systemprofile
692	svchost.exe	0x002c07f0	windir	C:\Windows
764	svchost.exe	0x002b07f0	ALLUSERSPROFILE	C:\ProgramData
764	svchost.exe	0x002b07f0	APPDATA	C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
764	svchost.exe	0x002b07f0	CommonProgramFiles	C:\Program Files\Common Files
764	svchost.exe	0x002b07f0	COMPUTERNAME	WIN-ETSA91RKCFP
764	svchost.exe	0x002b07f0	ComSpec	C:\Windows\system32\cmd.exe
764	svchost.exe	0x002b07f0	FP_NO_HOST_CHECK	NO
764	svchost.exe	0x002b07f0	LOCALAPPDATA	C:\Windows\ServiceProfiles\NetworkService\AppData\Local
764	svchost.exe	0x002b07f0	NUMBER_OF_PROCESSORS	1
764	svchost.exe	0x002b07f0	OS	Windows_NT