

ROOT-ME - Command & Control niveau 5

J'utilise Volatility pour récupérer le mot de passe du challenge, ici le mot de passe de l'utilisateur.

Récupération de l'information sur l'image du dump mémoire

```
.../IUT/SAE-ROOTME/ch5
> md5sum ch2.dmp
e3a902d4d44e0f7bd9cb29865e0a15de  ch2.dmp

.../IUT/SAE-ROOTME/ch5
> volatility -f ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                           AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                           AS Layer2 : FileAddressSpace (/home/va1/IUT/SAE-ROOTME/ch5/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
```

J'utiliserai le profile **Win7SP1x86_23418** pour la suite.

Avec Volatility on peut récupérer une liste des hashes contenant les informations de connexions des utilisateurs (l'équivalent du fichier /etc/shadow sous Linux) avec la commande suivante:

```
> volatility -f ch2.dmp --profile=Win7SP1x86_23418 hashdump
```

Récupération des hashes

```
.../IUT/SAE-ROOTME/ch5
> volatility -f ch2.dmp --profile=Win7SP1x86_23418 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
John Doe:1000:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930 :::
```

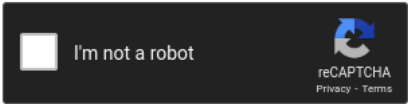
Chaque ligne de cette list est constitué de cette façon:

1er champ: Nom d'utilisateur 2ème champ: RID (Relative Identification) 3ème champ: Hash LM (Lan Manager) 4ème champ: Hash NTLM

On peut cracker ces hashes avec une attaque par dictionnaire utilisant une liste de hashes connues pour les mots de passe les plus fréquents. Le site crackstation permet de faire cela facilement.

Enter up to 20 non-salted hashes, one per line:

aad3b435b51404eeaad3b435b51404ee
b9f917853e3dbf6e6831ecce60725930



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
aad3b435b51404eeaad3b435b51404ee	LM	
b9f917853e3dbf6e6831ecce60725930	NTLM	passw0rd

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Le mot de passe est donc passw0rd.