1. Activité : Audit sur la sécurité des identifiants avec Kali (sans VM Windows 10)

1.1. Présentation

Le responsable de la Maison de services au public (MSAP) M. Brillat souhaite réaliser un **audit sur la sécurité des identifiants de connexion des utilisateurs**. Il s'agit de s'assurer que les utilisateurs respectent bien les recommandations sur l'utilisation de **mot de passe solide**.

Pour cela, il décide de faire réaliser des tests d'usurpation des éléments de connexion en utilisant les outils de la **distribution Kali**.

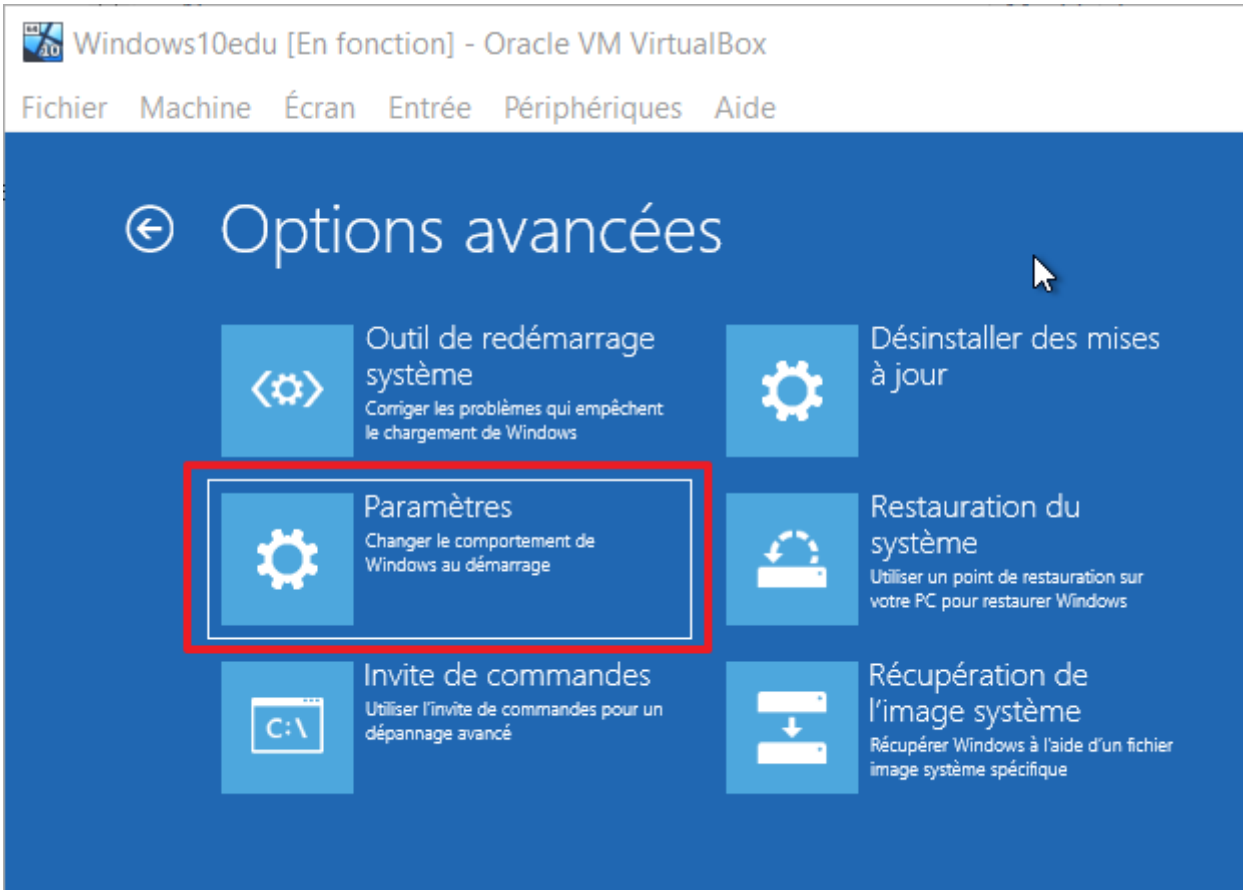
Vous devez disposer pour cette activité :

- du **fichier ISO** de la distribution **Kali Linux** (Live Boot Kali 2021)

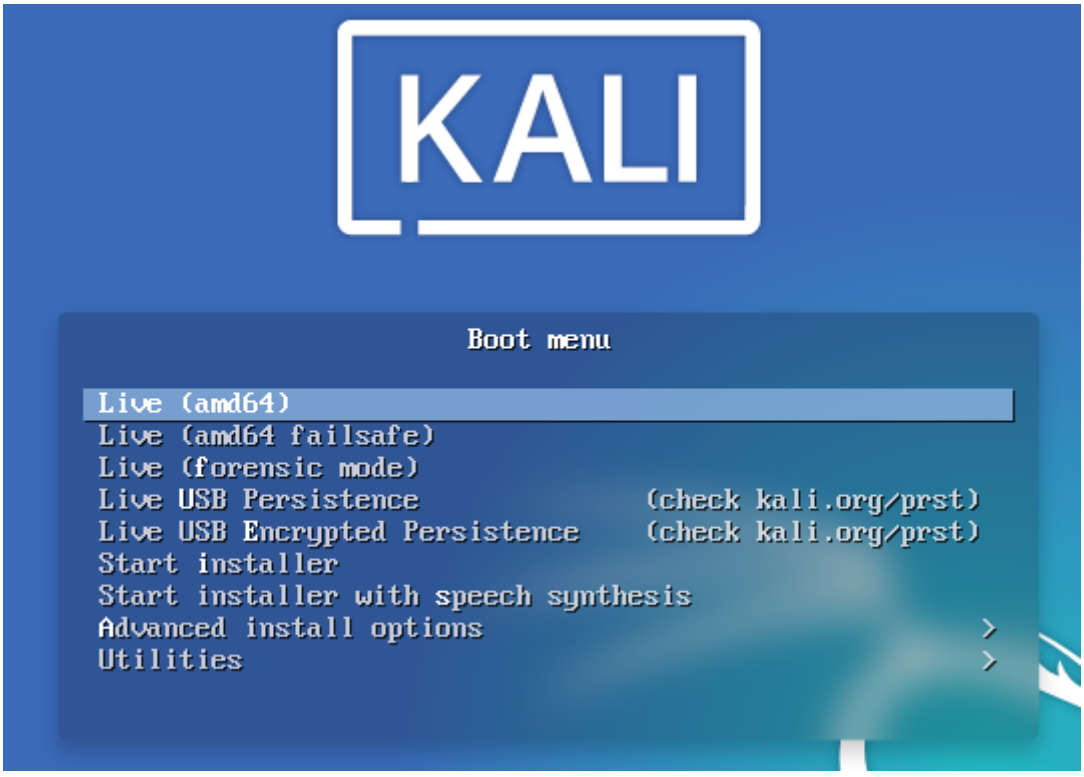
1.2. Etape 1 : Préparation des tests

1.2.1. Préparation de la VM Windows

1. **Préparez** la machine virtuelle Windows de test :
    1. ouvrez une session avec un **compte administrateur**,
    2. **créez le compte local ENEDIS** qui ne soit **pas un compte Microsoft** avec un mot de passe de **moins de huit caractères alphabétiques**,
    3. **créez le compte local MSA** qui ne soit **pas un compte Microsoft** avec un mot de passe de **plus de huit caractères alphabétiques**,
2. Dans le paramétrage de la VM Windows, indiquez que lors du lancement de la VM, le **boot sera réalisée à partir du lecteur de CD-ROM** :
    1. Associez le fichier **ISO de Kali** au **lecteur de CD-ROM**.
    2. dans la session Windows accédez à **Paramètres**,
    3. **Mise à jour et sécurité**,
    4. **Récupération**,
    5. Cliquez sur le bouton **Redémarrer maintenant**,
    6. Au redémarrage choisissez l'option **Dépannage → Options avancées → Paramètres**



- Cliquez ensuite sur **Redémarrer**
- Choisissez l'option Live (amd64)



1.2.2. Autre solution pour récupérer la base SAM avec Windows 10 sans utiliser de VM Windows 10

- Téléchargez et utiliser l'utilitaire pwdump8 8.2; Cet utilitaire supporte les hash en AES-128 utilisés par Windows 10.
- Récupérez les informations sur les comptes avec la commande en lançant une invite de commandes **cmd.exe** en tant qu'administrateur et enregistrez les dans un fichier mdp.txt:

```
pwdump8 > mdp.txt
```

Lien :

- https://www.openwall.com/passwords/windows-pwdump
- https://syskb.com/telecharger-pwdump/

Les mots de passe obtenus sont hashés et un utilitaire comme John The Ripper va permettre de les connaître

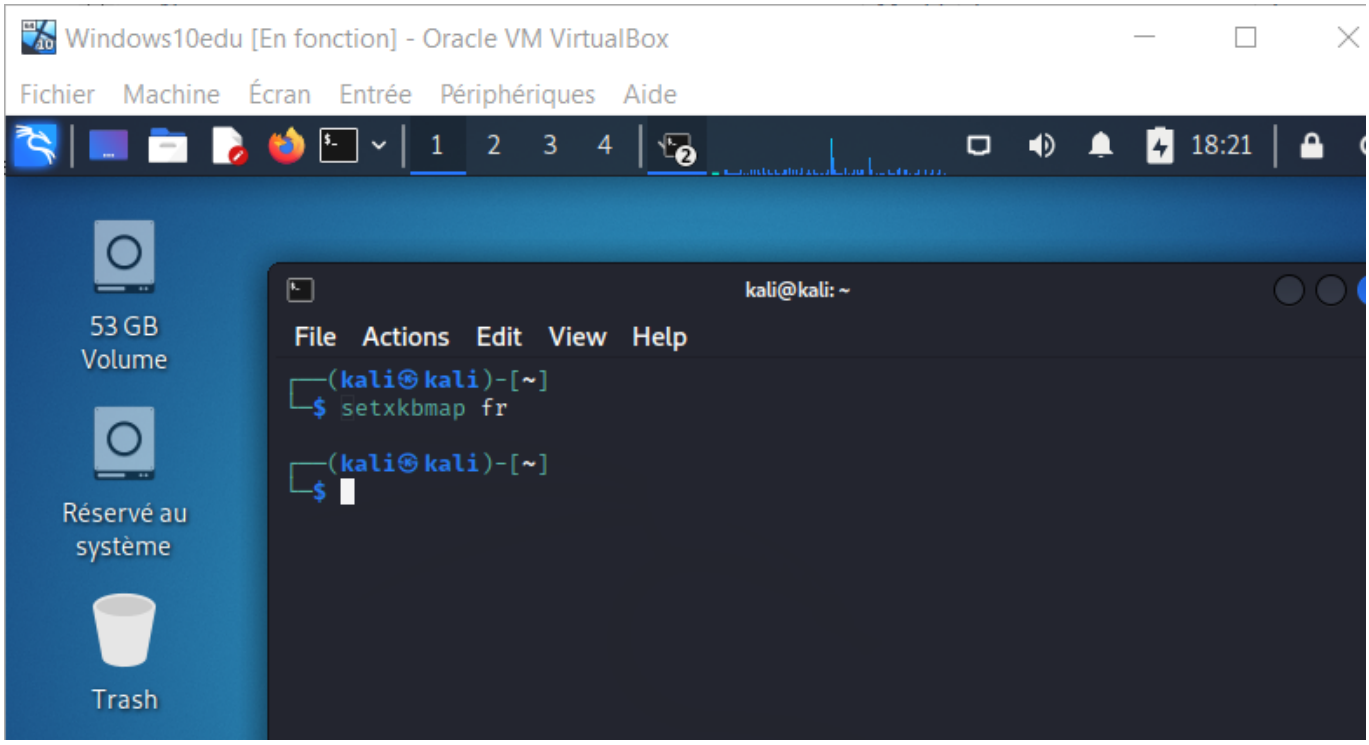
- Créer une VM Live Kali sans disque dur mais en associant le fichier ISO au lecteur de CD-ROM
- Lancez la VM Live Kali et ouvrez uns session avec les identifiants **kali** mot de passe **kali**.

Attention : la VM Kali utilise un clavier QWERTY.

1.2.3. Préparation de la VM Kali

1. lancer un terminal
2. Modifiez le clavier QWERTY en AZERTY avec la commande

```
$ setxkbmap fr
```

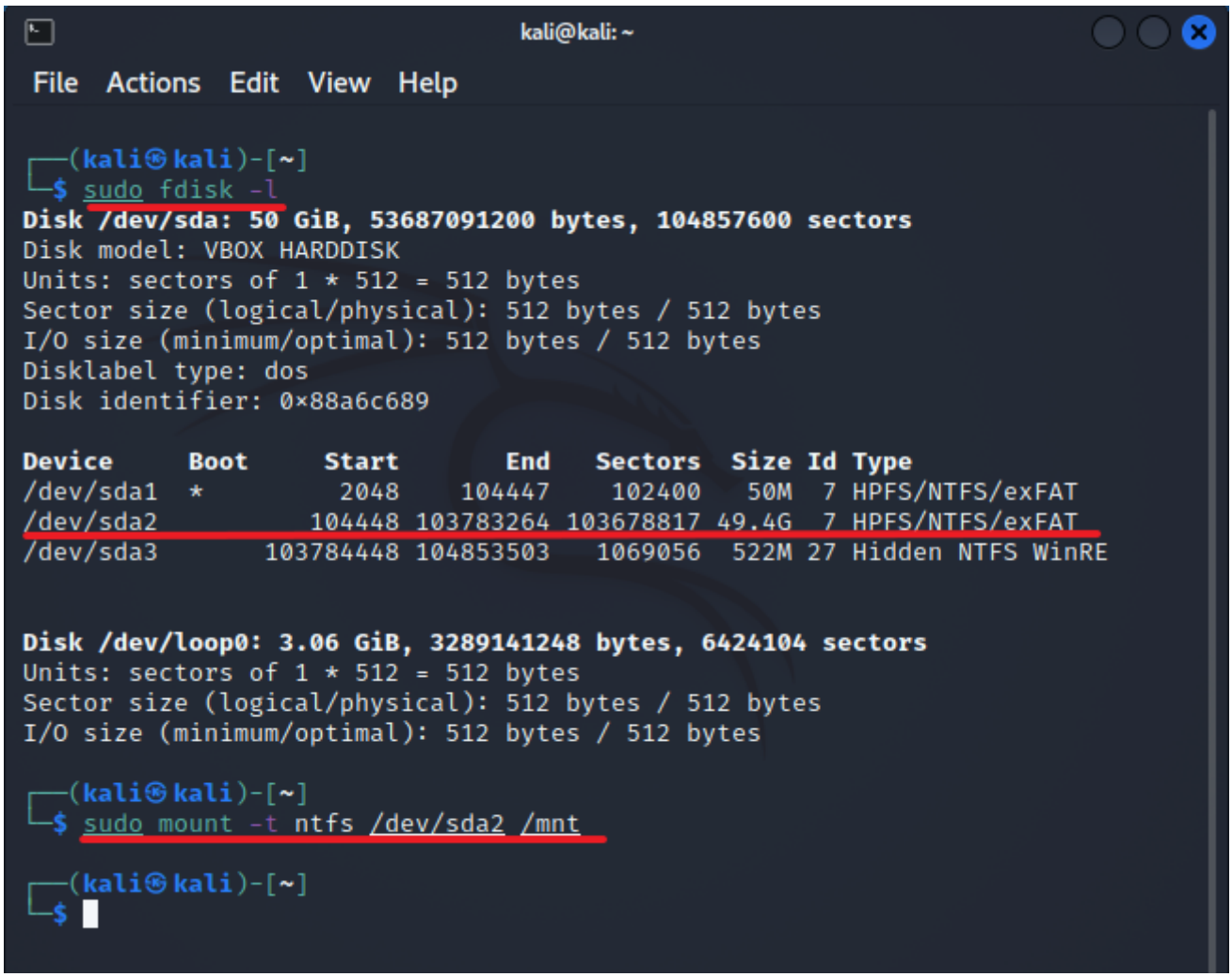


- Repérez la partition Windows avec la commande suivante :

```
$ sudo fdisk -l
```

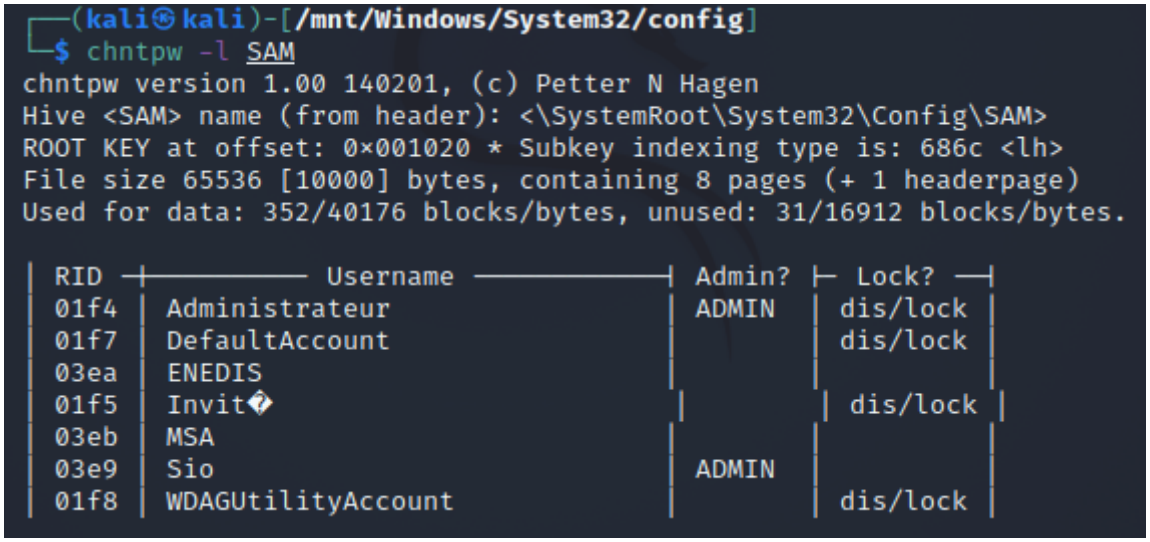
- **Montez** la partition Windows identifiée précédemment dans Kali :

```
$ sudo mount -t nfts /dev/sdax /mnt
```



- avec l'outil chntpw lister les comptes utilisateurs présents dans la base SAM et effacer leur mot de passe:

```
$ chntpw -l SAM
```



- pour effacer le mot de passe d'un compte en choisissant l'option correspondante :

```
$ chntpw -u compte SAM
```

- l'outil samdump2 permet d'obtenir les hash des mots de passe
  - se positionner dans le dossier de la base SAM
  - lancer l'outil et sauvegarder les informations dans un fichier

```
$ cd /mnt/windows/system32/config
```

```
$  samdump2 SYSTEM SAM > /mnt/mdp.txt
```

1.3. Etape 2 : Première réalisation des tests

Vous allez réaliser deux types de tests pour essayer de trouver ou non les identifiants et mots de passe de chaque compte.

Le compte administrateur sera également testé par défaut.

Exécutez les différents tests proposés par l'outil **John the ripper** pour trouver les identifiants et mots de passe en utilisant :

- le test par force **force brute**,
- et le test par **dictionnaire**.

Tests à l'aide de l'outil John The Ripper

From:
https://siocours.lycees.nouvelle-aquitaine.pro/ - **Les cours du BTS SIO**

Permanent link:
https://siocours.lycees.nouvelle-aquitaine.pro/doku.php/reseau/kali/password?rev=1643573953

Last update: **2022/01/30 20:19**