Activité : Audit sur la sécurité des identifiants avec Kali (avec une VM Windows 10)

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 :

- d'une **machine virtuelle Windows 10**,
- du **fichier ISO** de la distribution **Kali Linux** (Live Boot Kali 2021)

Etape 1 : Préparation des tests

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 **4 caractères alphabétiques**,
    3. **créez le compte local msa** qui ne soit **pas un compte Microsoft** avec un mot de passe de **plus de 4 caractères alphabétiques**.

Récupération des informations sur les comptes Windows

Les comptes Windows 10 sont enregistrés dans la base SAM de la base de registre. POur les récupérer vous allez utiliser l'utilitaire **PwDump8**.

- Téléchargez l'utilitaire pwdump8.2. Cet utilitaire supporte les hash des mots passe avec l'algorithme AES-128 utilisé 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 > c:\mdp.txt
```

Lien de téléchargement :

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

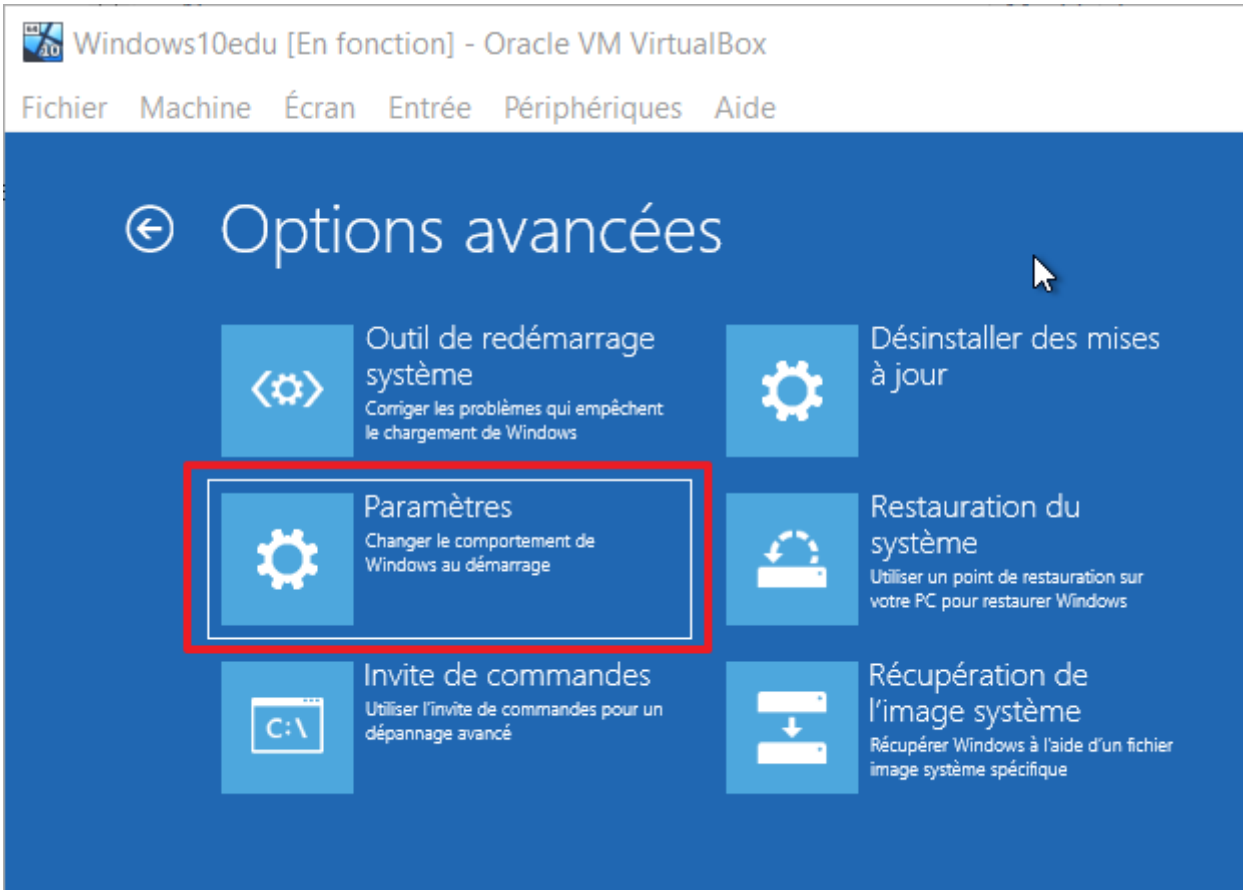
La **base SAM** du registre de Windows contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de hach :

- Les mots de passe locaux des utilisateurs sont hachés et stockés dans un fichier appelé Security Account Manager (SAM).
- Les hachages sont cryptés avec une clé qui se trouve dans un fichier nommé SYSTEM.

Lien : https://technicalconfessions.com/blogs/2021/using-samdump-for-windows-password-extraction/

Lancement du Live Kali

1. 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**

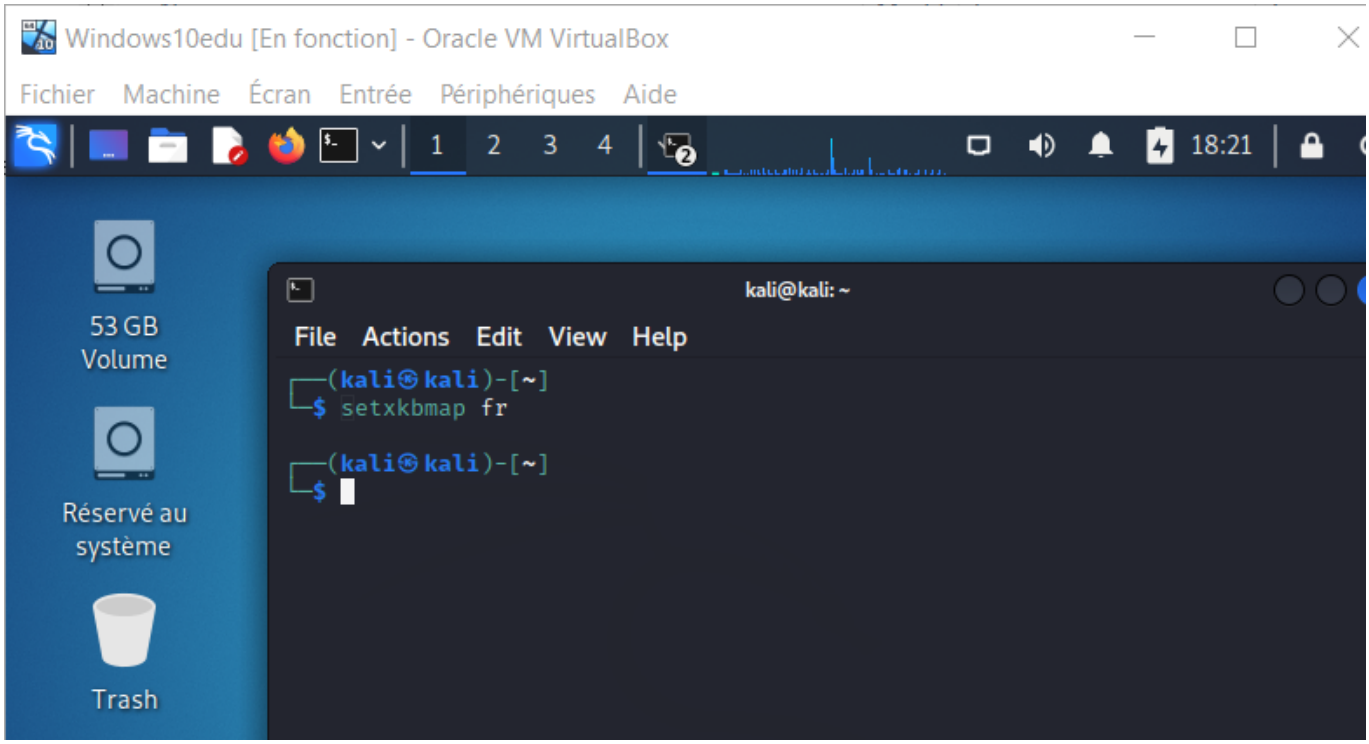


- Cliquez ensuite sur **Redémarrer**
- Choisissez l'option Live (amd64)

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
```

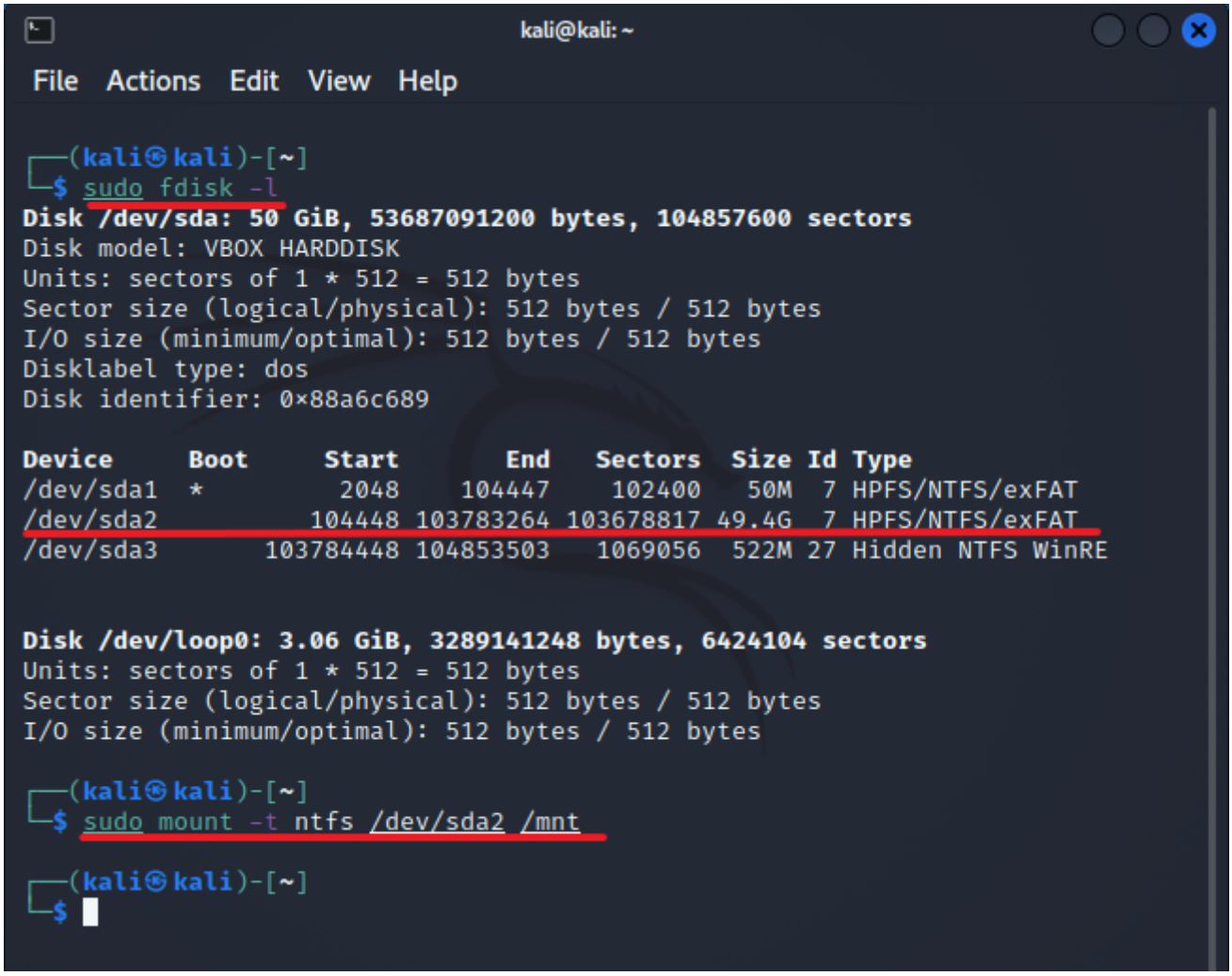
Généralement, les différentes partitions sont représentées par le mot **/dev/sda** suivi d'un numéro. Il est probable que la **partition la plus volumineuse** soit celle qui est recherchée.

Notez le numéro de la partition, qui sera utile par la suite.

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

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

- **x** représente le numéro de la partition
- **mnt** représente le dossier de destination



- avec l'outil chntpw lister les comptes utilisateurs présents dans la base SAM. Cet utilitaire vous

permet d'effacer les mots de passe du compte choisi :

```
$ cd /mnt/
$ chntpw -l SAM
```

```
┌──(kali㉿kali)-[/mnt/Windows/System32/config]
└─$ chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0×001020 * Subkey indexing type is: 686c <lh>
File size 65536 [10000] bytes, containing 8 pages (+ 1 headerpage)
Used for data: 352/40176 blocks/bytes, unused: 31/16912 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrateur                 | ADMIN  | dis/lock |
| 01f7 | DefaultAccount                 |        | dis/lock |
| 03ea | ENEDIS                         |        |          |
| 01f5 | Invit                          |        | dis/lock |
| 03eb | MSA                            |        |          |
| 03e9 | Sio                            | ADMIN  |          |
| 01f8 | WDAGUtilityAccount             |        | dis/lock |
```

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

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

- l'utilitaire **PwDump8** vous a permis de sauvegarder dans un fichier la liste des comptes avec les mots de passe hachés.

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** ; vous pouvez rajouter dans le fichier dictionnaire d'autre exemple de mot de passe,
- et le test par **dictionnaire**.

Remarques :

- Le dictionnaire **Rockyou.txt** se trouve dans le dossier wordlists : **/usr/share/wordlists**. Il doit être dézippé (gunzip) pour être utilisé.
- Le dictionnaire **password.lst** se trouve dans le dossier john : **/usr/share/john**. Ce dictionnaire peut être modifié par l'ajout de vos propres mots de passe. Dans le cas où les mots de passe ne sont pas connus, on peut deviner qu'un utilisateur aura pu utiliser par exemple l'organisation + son nom + un chiffre pour constituer son mot

de passe. Vous pouvez alors rajouter ces mots de passe possibles dans le fichier **password.lst**.

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