Activité : Audit sur la sécurité des identifiants avec Kali (sans 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 :

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

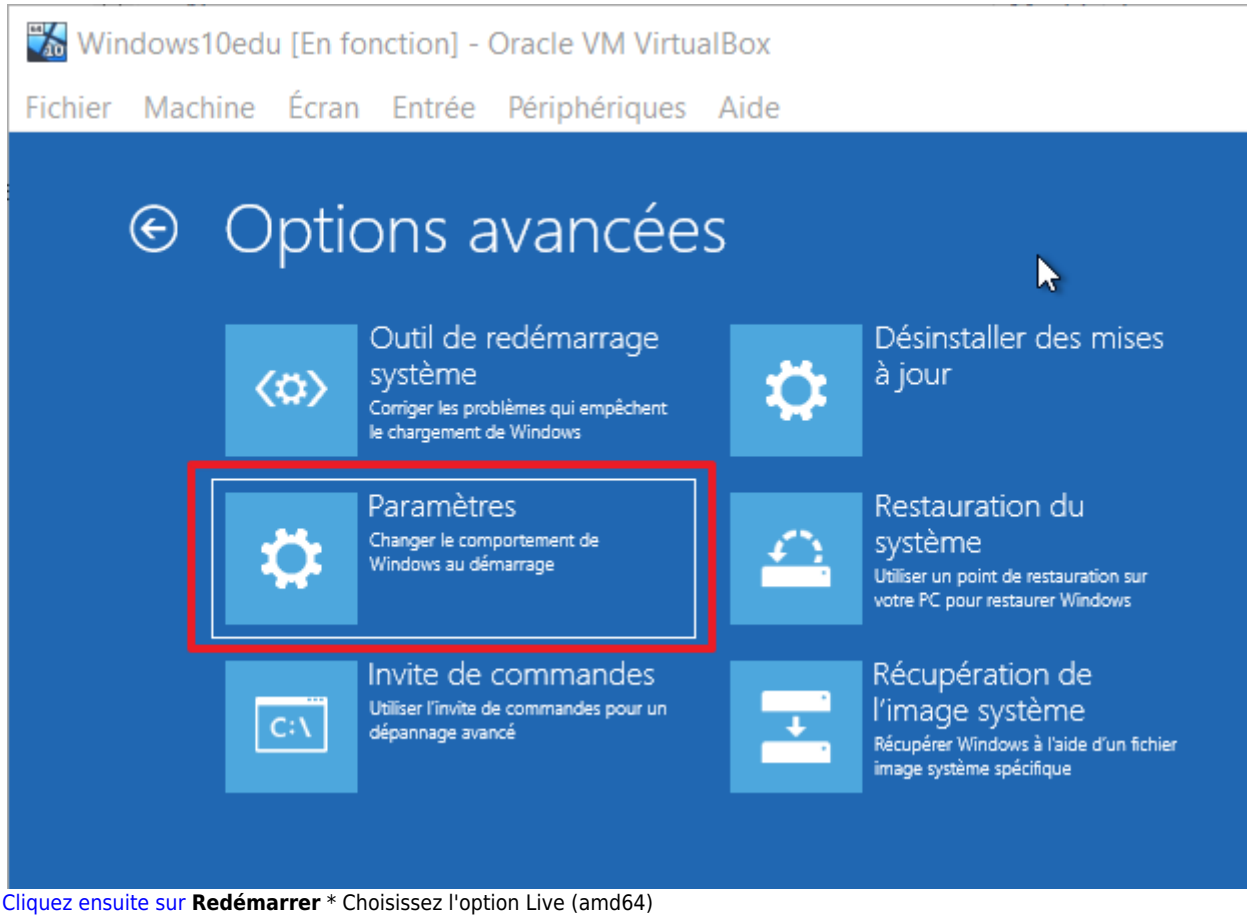
Etape 1 : Préparation des tests

Création de la VM Live Kali

- Créer une VM :
  - 2 Gio de Ram
  - san disque dur

Après la création de la VM, accédez à sa configuration et sa rubrique Stockage :

- Asdociez le fichier ISO au lecteur de CD ROM,
- Cochez la case ***Live CD/DVD) Lancez ensuite la VM***

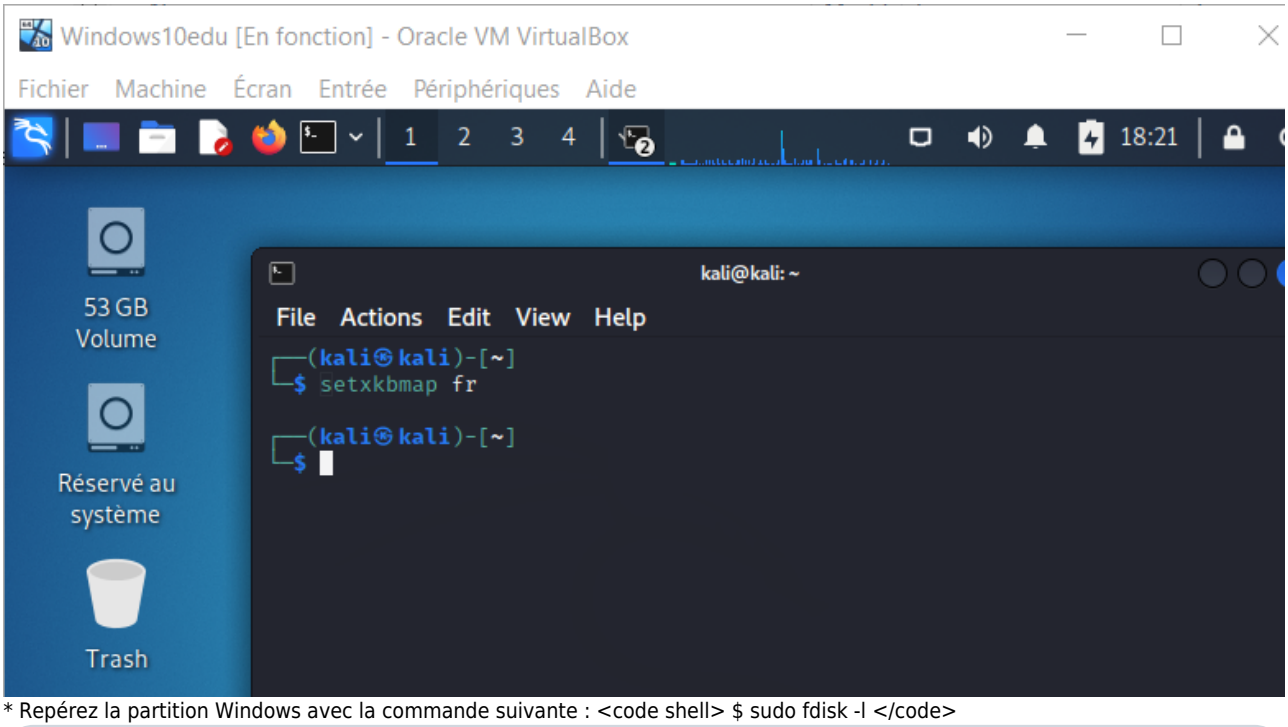


* Cliquez ensuite sur **Redémarrer** * Choisissez l'option Live (amd64)

==== 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: <code shell> pwdump8 > mdp.txt </code> 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.

==== Préparation de la VM Kali ==== - lancer un terminal - Modifiez le clavier QWERTY en AZERTY avec la commande <code shell> $ setxkbmap fr </code>



* Repérez la partition Windows avec la commande suivante : <code shell> $ sudo fdisk -l </code>

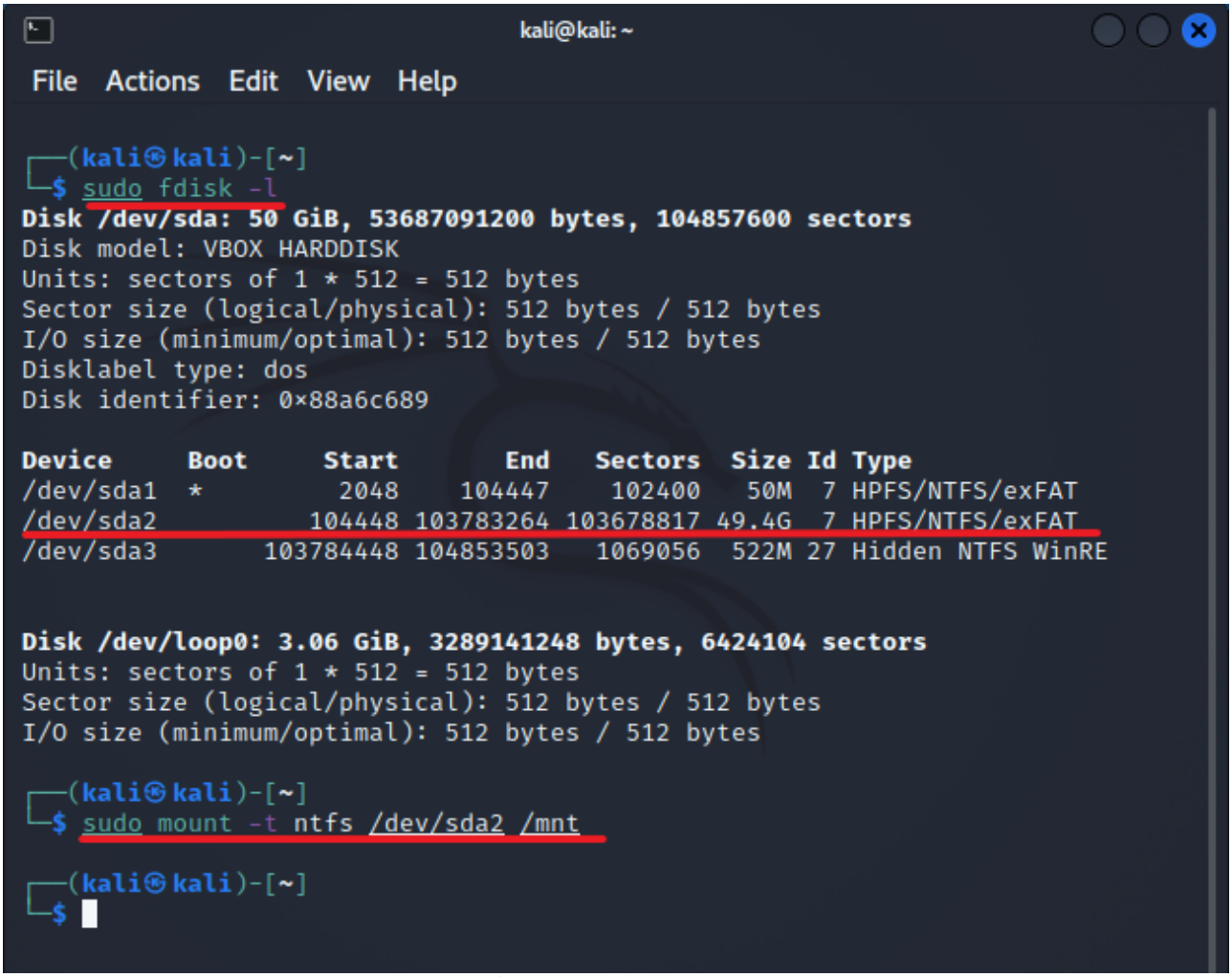
Généralement, les différentes partitions sont représentées par le mot **/dev/sda** suivi d'un numéro. Il est probable

que la **partition la plus volumineuse** soit celle qui est recherchée.

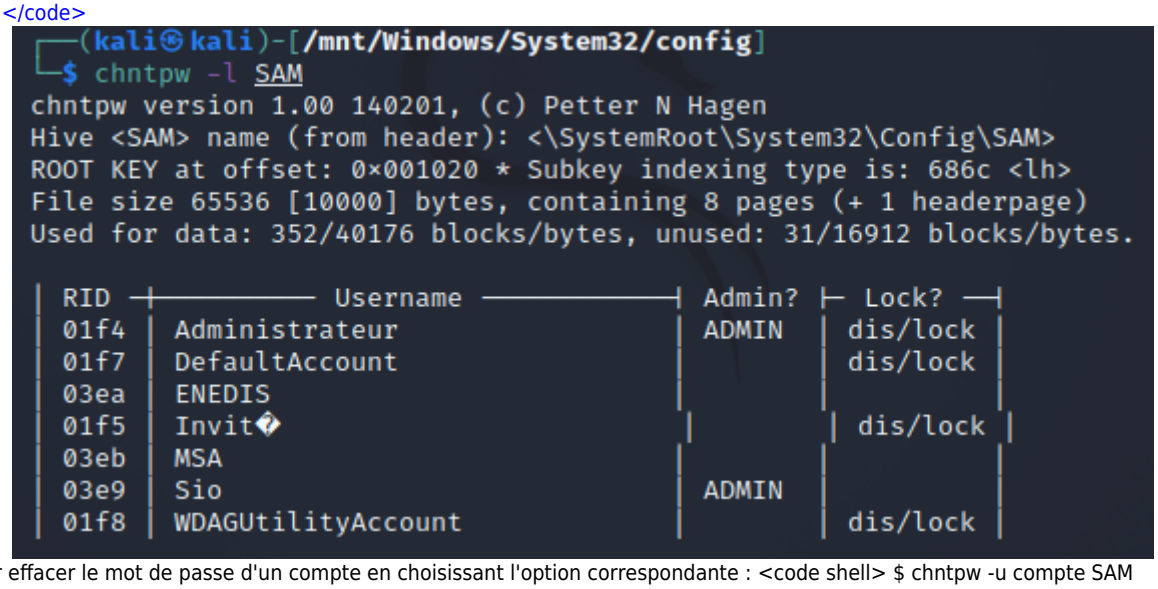
Notez le numéro de la partition, qui sera utile par la suite.

* **Montez** la partition Windows identifiée précédemment dans Kali : <code shell> $ sudo mount -t nfts /dev/sdax /mnt </code>

- **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 et effacer leur mot de passe: <code shell> $ chntpw -l SAM </code>



* pour effacer le mot de passe d'un compte en choisissant l'option correspondante : <code shell> $ chntpw -u compte SAM </code> * 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 <code shell> $ cd /mnt/windows/system32/config $ samdump2 SYSTEM SAM > /mnt/mdp.txt </code>

La **base SAM** du registre de Windows contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de hach calculé avec l'**algorithme MD5** :

- 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/

===== 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**.

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