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

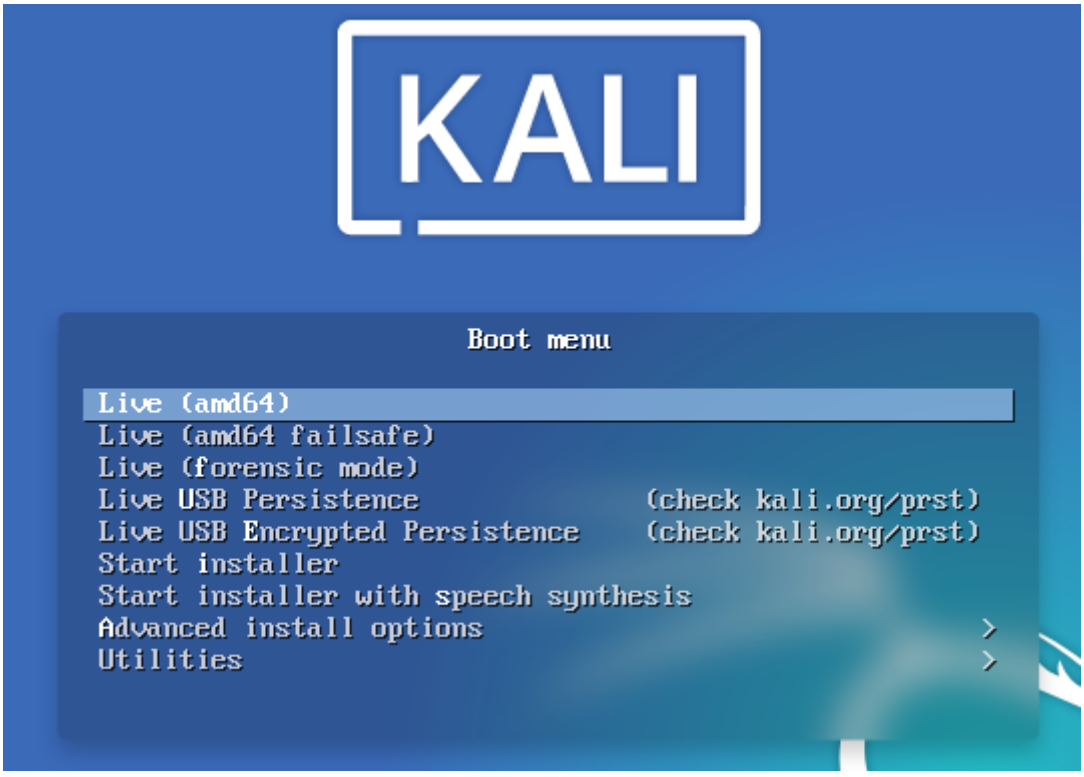
- Créer une VM :
  - **2 Gio** de Ram,
  - **sans** disque dur.

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

- Associez le fichier **ISO** au lecteur de CD ROM,
- Cochez la case **Live CD/DVD)**

Lancement de la VM Live Kali

- Lancez la VM Live Kali,
- Choisissez l'option **Live (amd64)**,



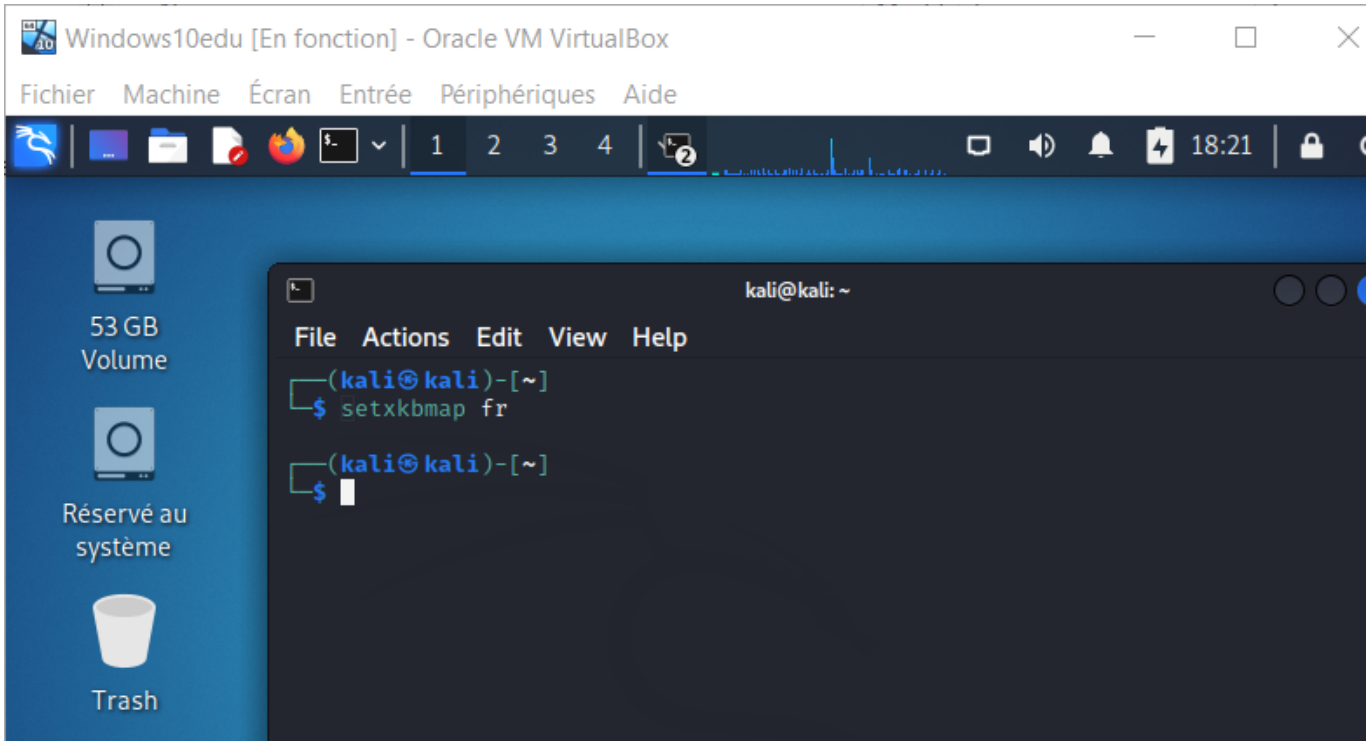
- Ouvrez une session avec les identifiants **kali** mot de passe **kali**.

Attention : la VM Kali utilise un clavier QWERTY.

Préparation de la VM Kali

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

```
$ setxkbmap fr
```



- créez le compte local **enedis** avec un mot de passe de 4 caractères alphabétiques,
- créez le compte local **msa** avec un mot de passe de plus de 4 caractères alphabétiques.

```
$ sudo adduser enedis
$ sudo adduser msa
```

Extraction de la liste des comptes linux et des mots de passe hachés

Sous linux :

- les comptes sont mémoriséss dans le fichier **/etc/passwd**
- les mots de passe sont mémorisés hachés dans le fichier **/etc/shadow**

Utilisez l'utilitaire **unshadow** pour regrouper ces informations dans un seul fichier que vous appellerez **mdp.txt** :

```
$ sudo unshadow /etc/passwd /etc/shadow > mdp.txt
```

Attention : l'algorithme de hachage des mots de passe utilisé par Kali est **yescrypt** (chaque hash commence par y.

Lors de l'utilisation de John The Ripper, le message **No password hashes loaded (see FAQ)** peut signifier que l'utilitaire n'a pas reconnu l'algorithme de hachage utilisé.

Utilisez alors le paramètre suivant pour le l'algorithme **yescrypt** :

```
$ john --format=crypt ...
```

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.

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