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. Création de la VM Live Kali

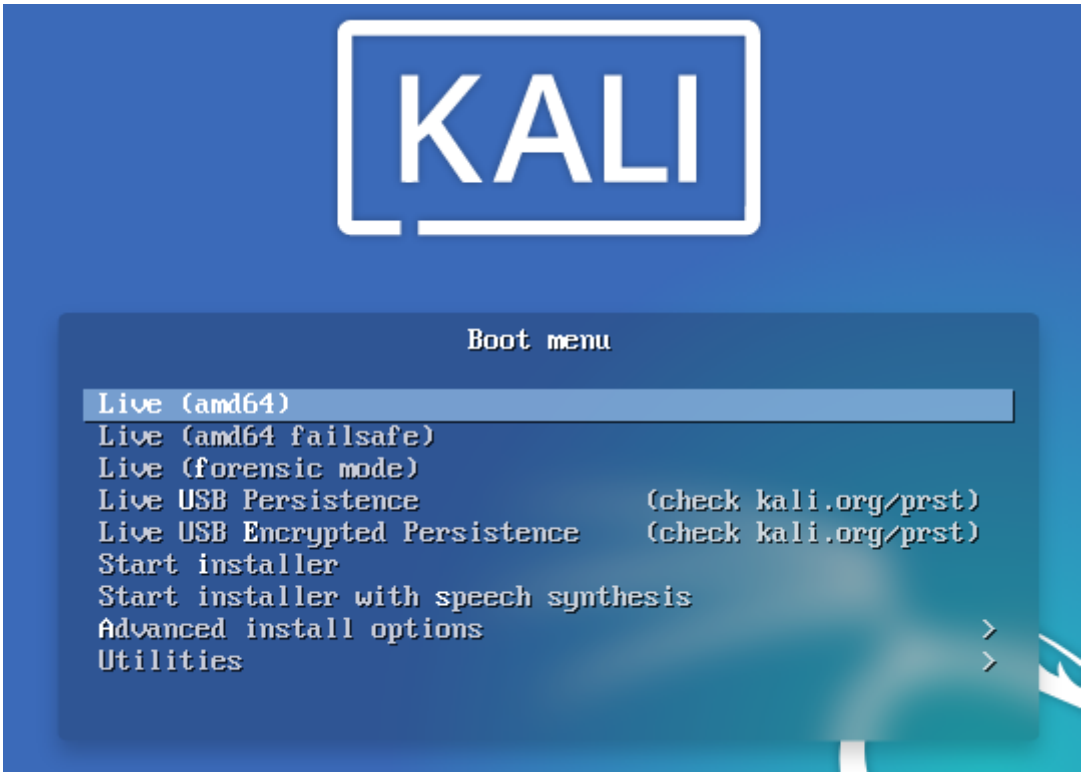
- Créer une VM :
  - **2 Gio** de Ram,
  - **sans** disque dur.

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)**

1.2.2. Lancement de la VM Live Kali

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



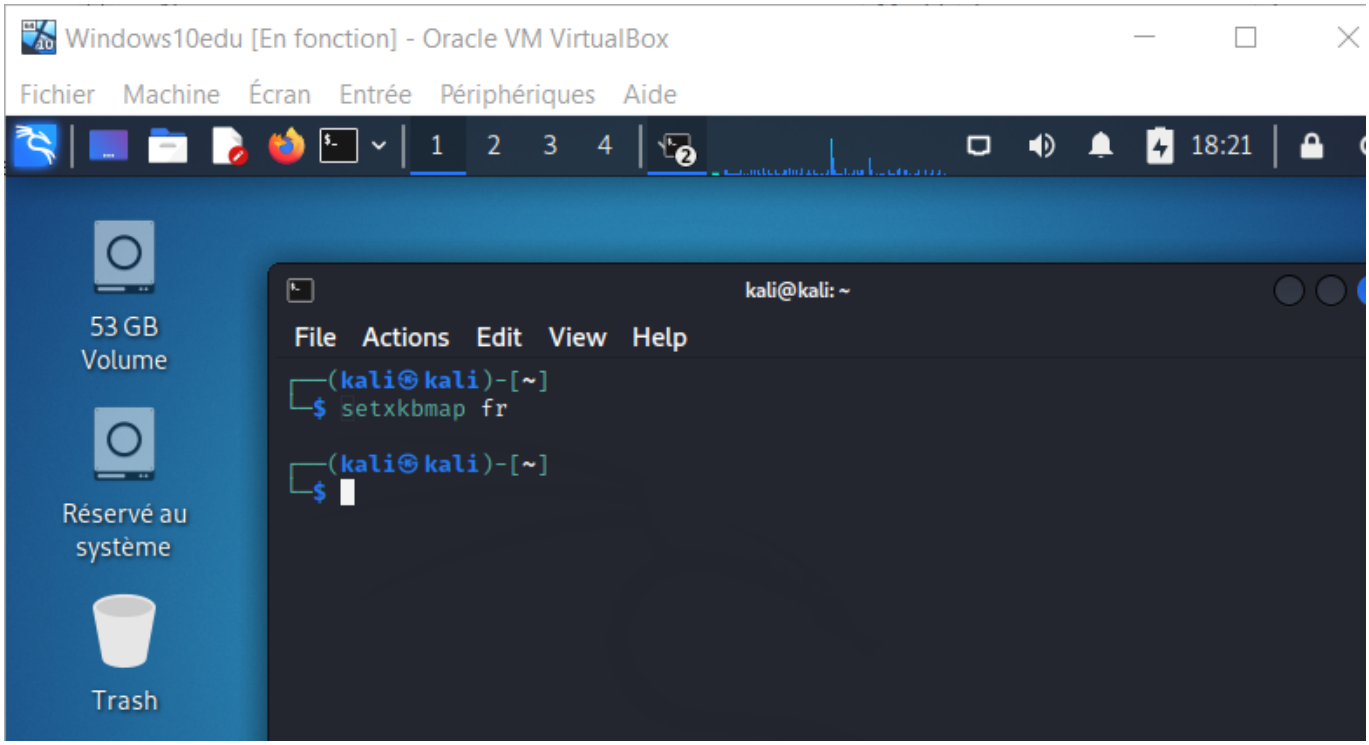
- Ouvrez une session avec les identifiants **kali** mot de passe **kali**.

Attention : la VM Kali utilise un clavier QWERTY.

1.2.3. 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
```

1.2.4. 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 utilisé par Kali est **yescrypt**.

Lors de l'utilisation de John The Ripper, le message *No password hashes loaded (see FAQ) **peut signifier que l'utilisateur n'a pas reconnu l'algorithme de hachage utilisé. Utilise alors le paramètre suivant : <code shell> $ john -format=crypt … </code> </WRAP> ===== 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**.**

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=1643578047

Last update: **2022/01/30 21:27**