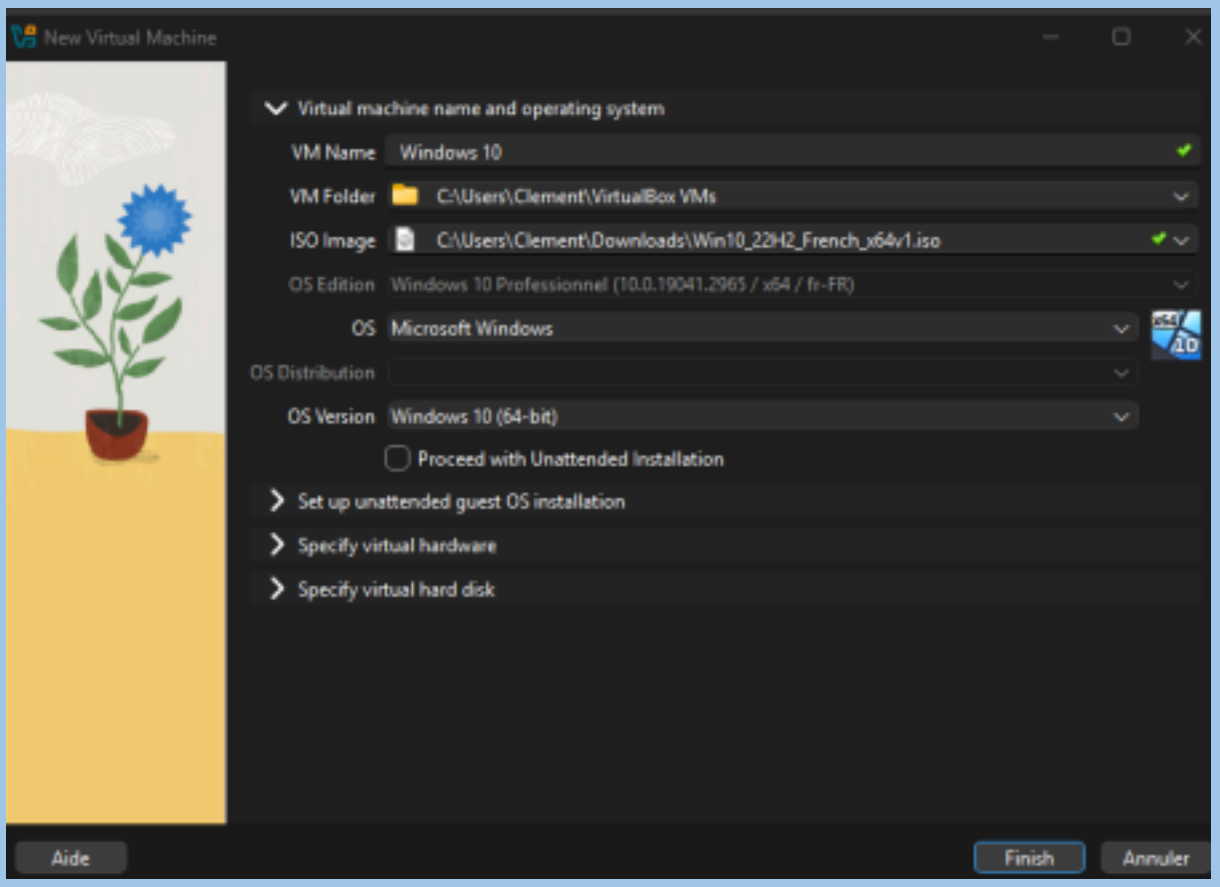
TH3 : CH4 : TD1

Sommaire:

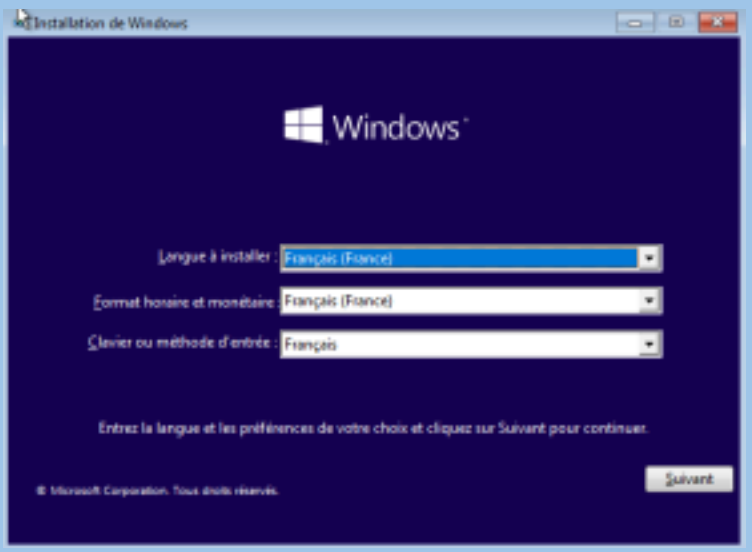
ETAPE 1

1. Préparez la machine virtuelle Windows 10 en reprenant les éléments mentionnés dans le guide de configuration

Dans un premier temps, nous allons créer une machine virtuelle Windows 10 à l'aide du logiciel de virtualisation VirtualBox.

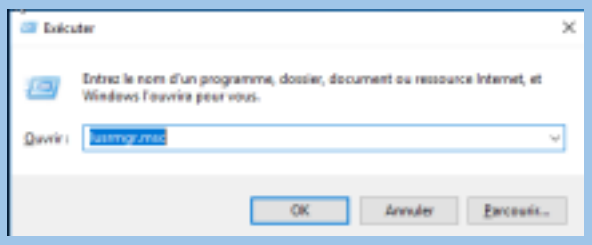


Nous procédons à l'installation de Windows 10.



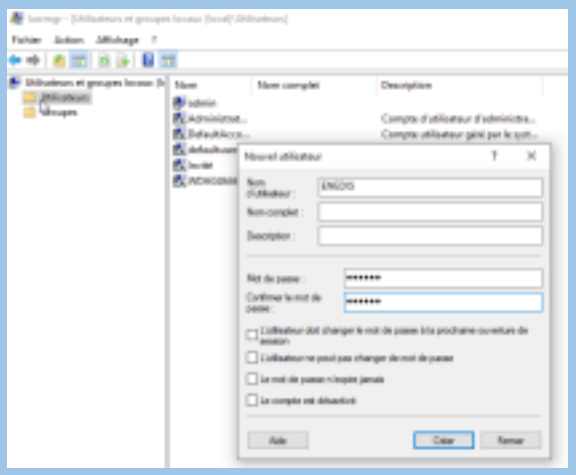
1. Création des comptes.

Nous allons créer trois comptes, ENEDIS, MSA et CLIC. Ces comptes vont être ajoutés au groupe Administrateurs afin de disposer des droits nécessaires à la réalisation des tests de sécurité. Cette étape nous sert à créer les mots de passes que l'on va tenter de cracker plus tard dans le TP.



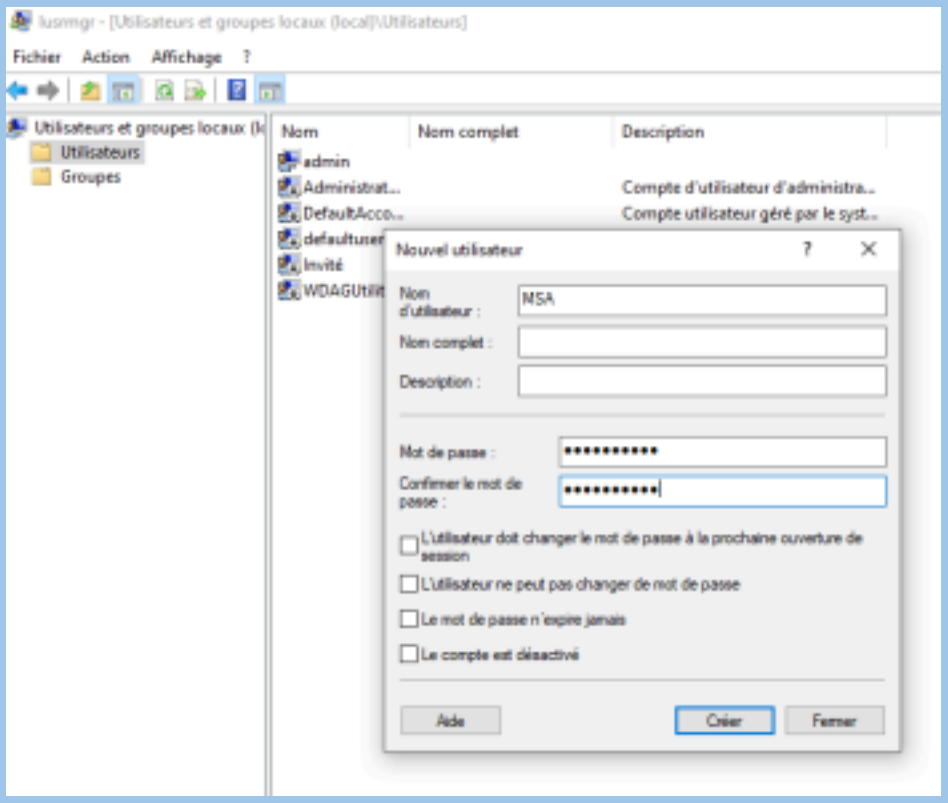
Création du compte ENEDIS

Afin de voir comment les outils de crack se comportent, nous allons faire plusieurs niveaux de robustesse, ici ENEDIS aura un mot de passe relativement simple.



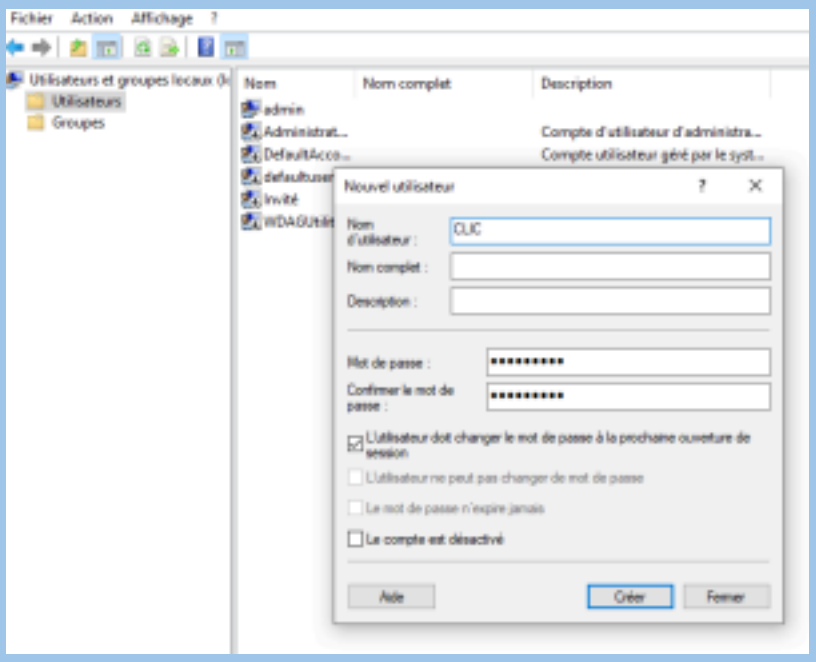
Création du compte MSA

L'utilisateur MSA quant à lui, aura un mot de passe un peu plus complexe que celui d'ENEDIS.



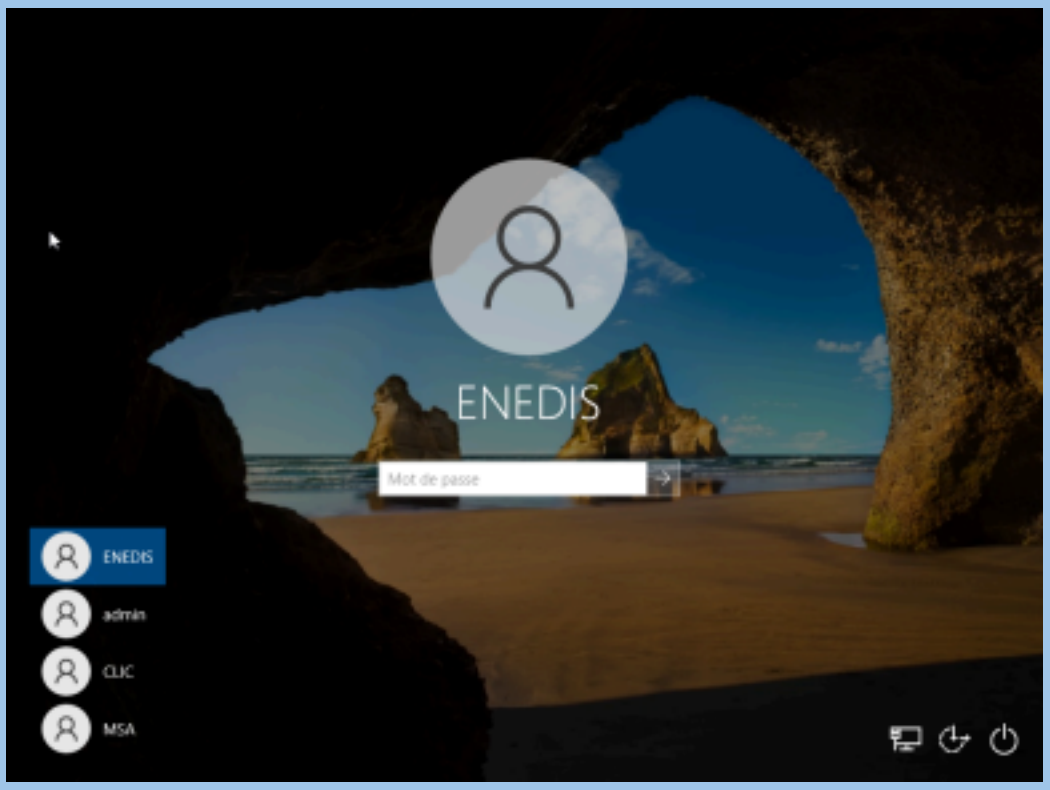
Création du compte CLIC

Pour CLIC nous choisissons d'augmenter encore le niveau de robustesse. Une fois les utilisateurs créés nous verrons plus tard comment les outils se débrouillent et quels mots de passe seront trouvés.



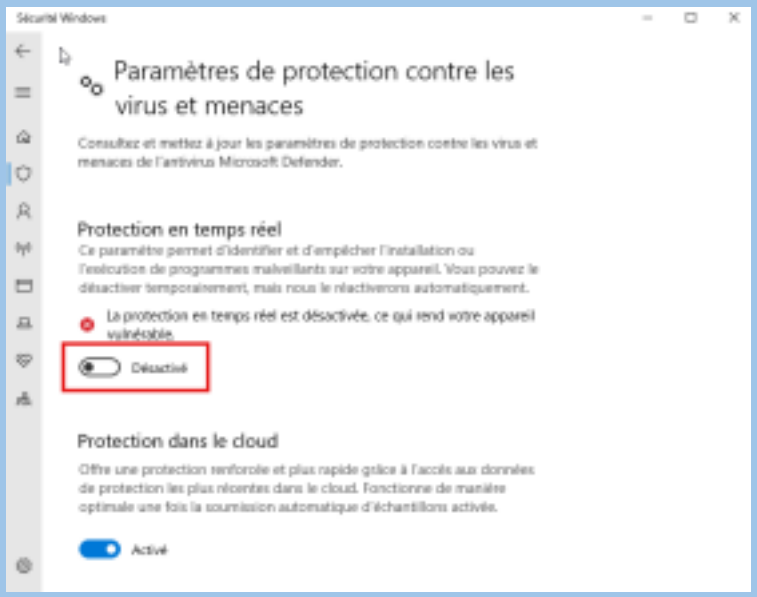
Nous nous assurons que tous les comptes ont bien été

créés, ici aucun problème ENEDIS, CLIC, MSA sont bien présents.



2. Désactivation de la protection en temps réel

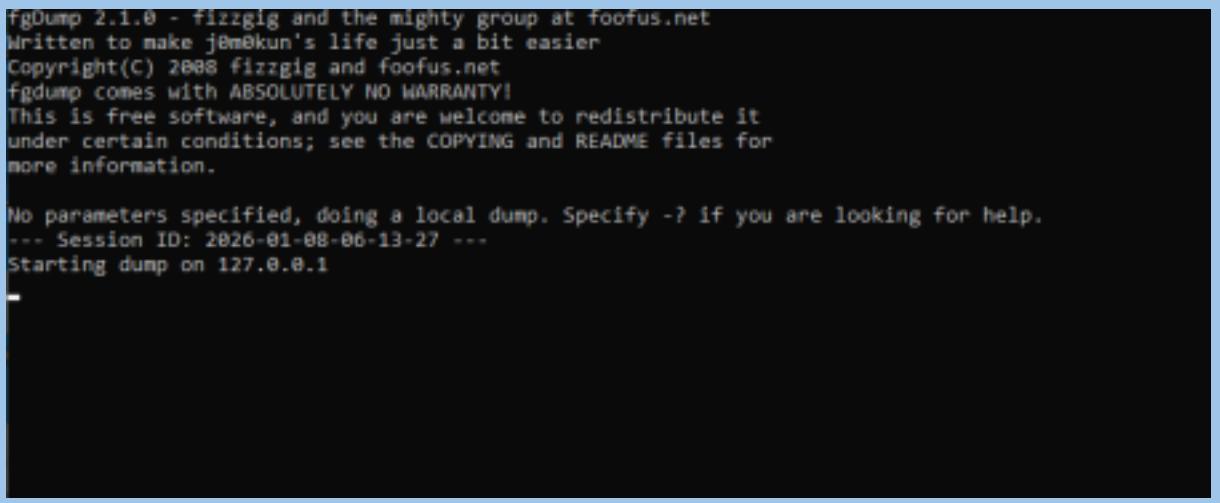
Afin d'exécuter l'outil FGDUMP, il faudra désactiver la protection en temps réel. Sans ça, Windows refusera d'exécuter l'outil.



3. Télécharger, décompresser, exécuter FGDUMP

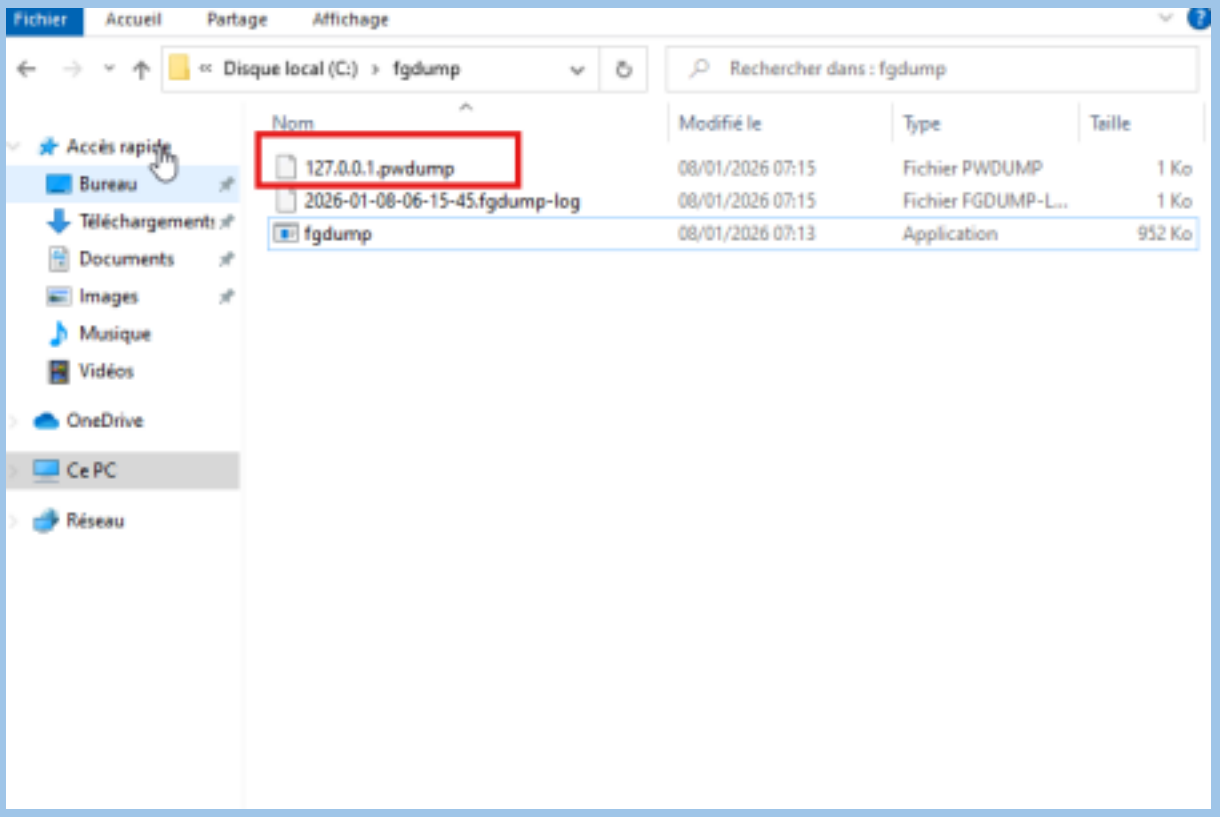
Pour commencer nous allons télécharger et exécuter l'outil FGDump. FGDump permet d'extraire les informations de sécurité de Windows, notamment les hashs des mots de passe des comptes utilisateurs. Ces mots de passe ne sont pas récupérés en clair, mais sous forme de hashs

Nous lançons l'outil FGDUMP en l'exécutant en mode administrateur. Ici on observe l'exécution de l'outil et le début du dump des informations du système local.



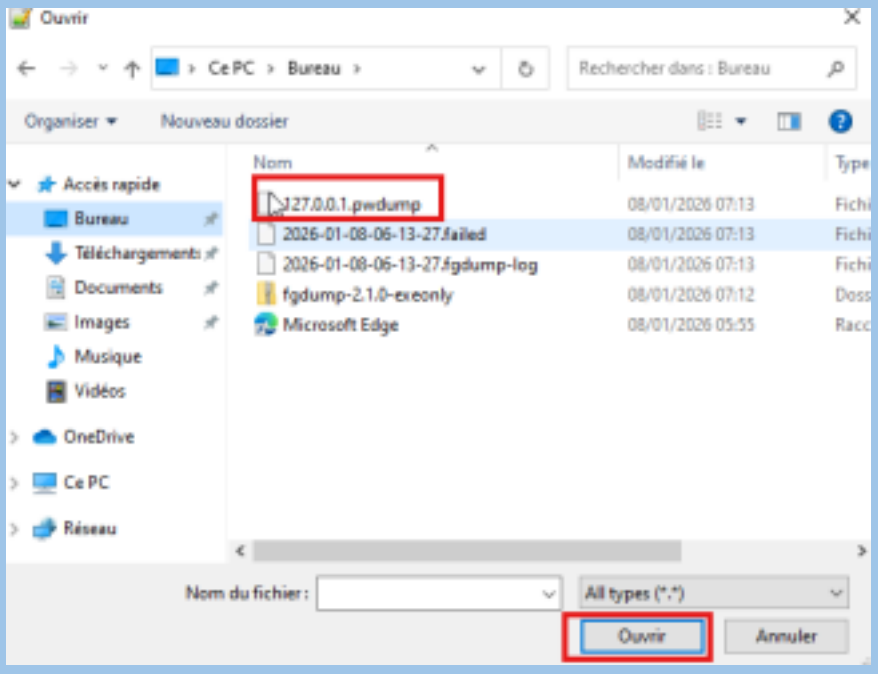
L'outil a effectué un dump local du système afin d'extraire les informations contenues dans les fichiers SAM et SYSTEM,

générant un fichier PWDUMP.



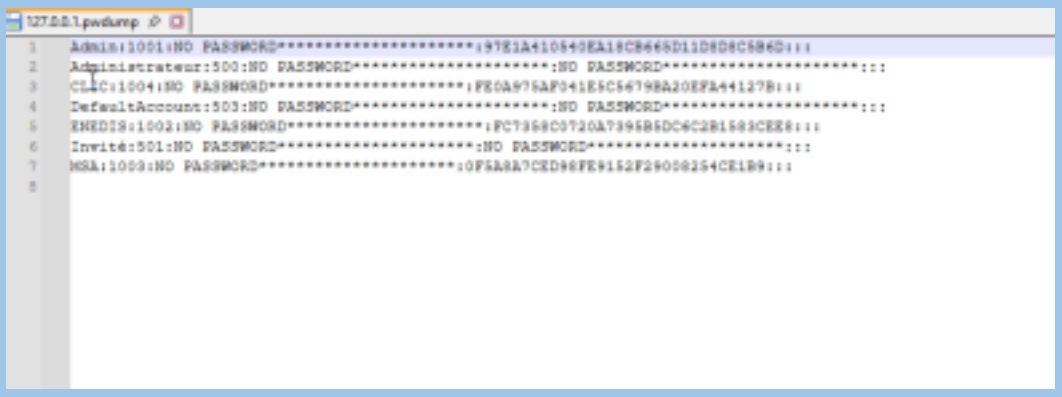
4. Télécharger et installer Notepad++

Nous avons téléchargé et installé l'éditeur de texte Notepad++. Cet outil va nous permettre d'ouvrir le fichier 127.0.0.1.pwdump généré par FGDump.



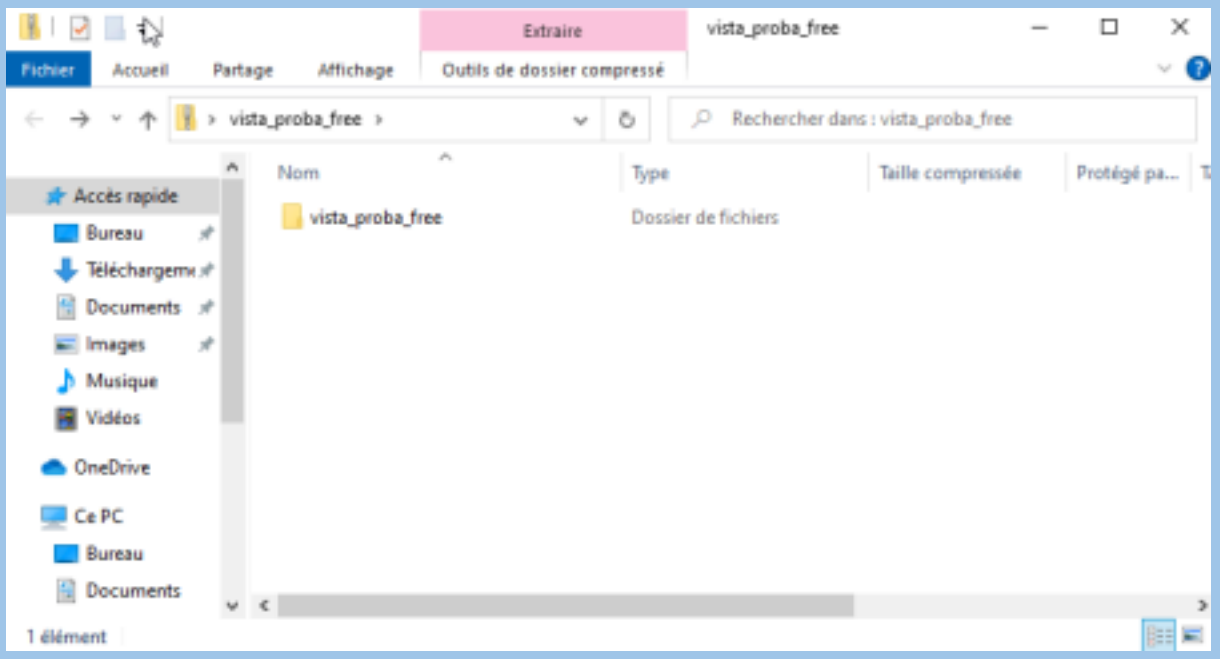
Nous ouvrons le fichier **127.0.0.1.pwdump** à l'aide de l'éditeur

de texte Notepad++ afin de visualiser les informations extraites par l'outil FGDump et de vérifier la présence des identifiants utilisateurs ainsi que des hashs de mots de passe. Cette étape est très importante, car en l'absence d'informations il ne sera pas possible de poursuivre la suite du TP.



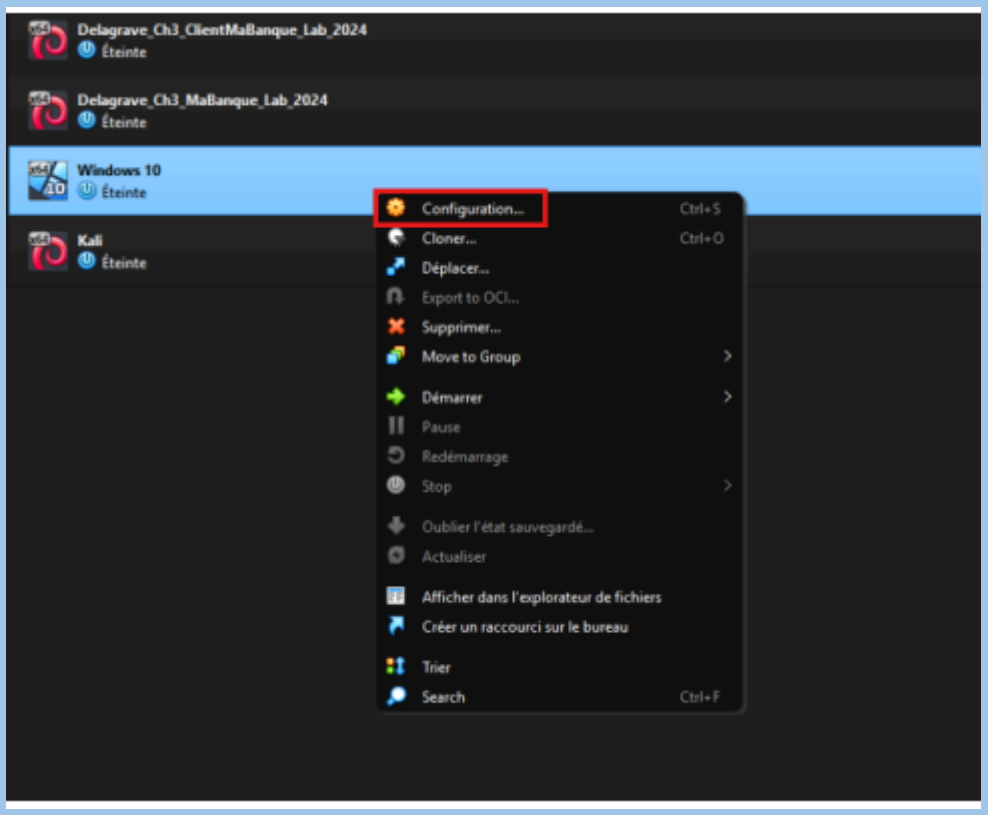
5. Télécharger et décompresser vista_proba_free.zip

Nous avons téléchargé puis décompressé l'archive vista_proba_free.zip. Ceci va nous être très utile puisqu'il va nous permettre d'obtenir le dossier contenant le fichier de hash et les tables nécessaires à la réalisation des tests avec l'outil John the Ripper que l'on verra plus tard dans le TP.



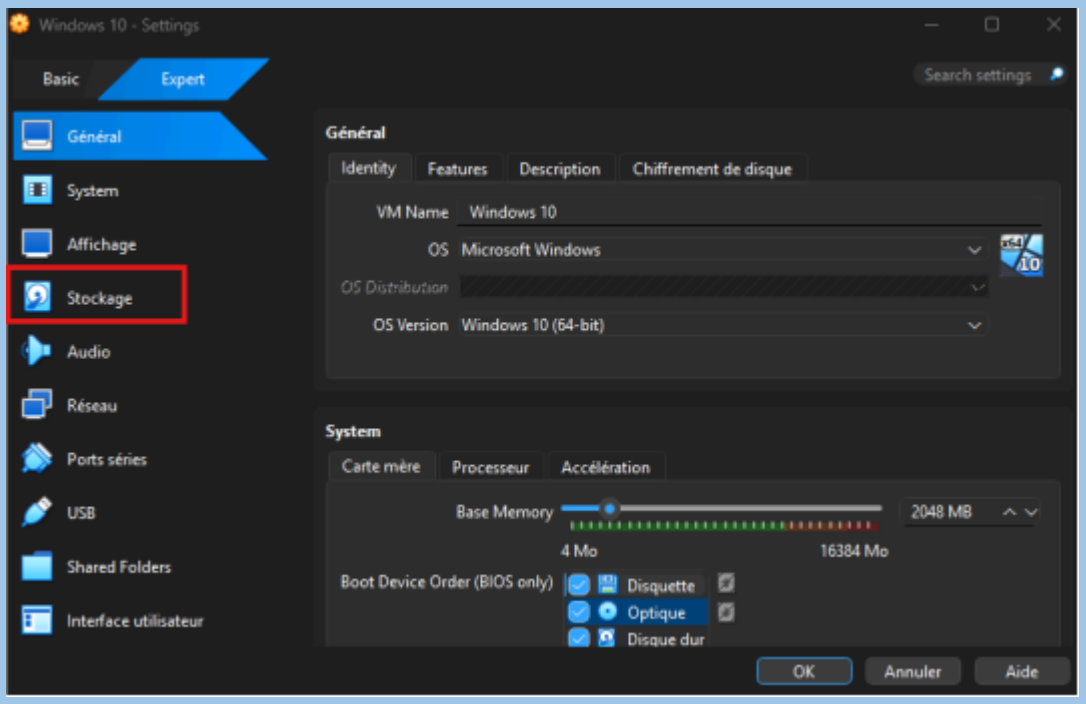
2. Configurez l’environnement de travail Kali selon les commandes fournies dans le document.

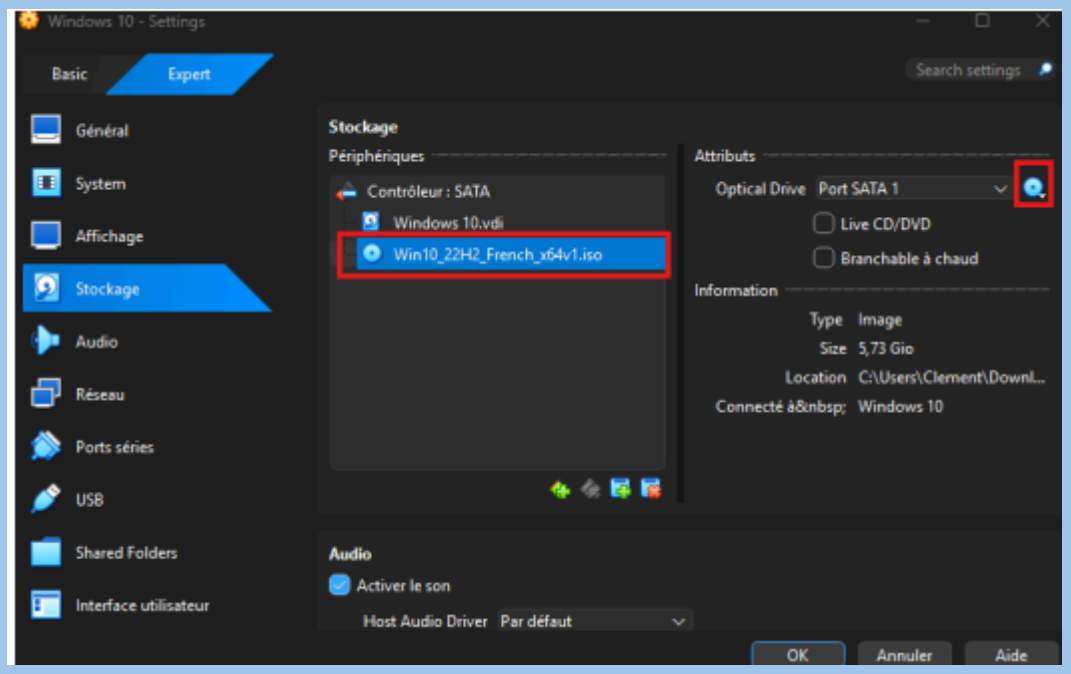
Nous allons télécharger l’image Kali afin de disposer d’un environnement de travail dédié aux tests d’audit de mots de passe. Cet environnement nous permettra d’utiliser des outils spécialisés tels que John the Ripper et Ophcrack. L’objectif est de démarrer Kali par dessus Windows.



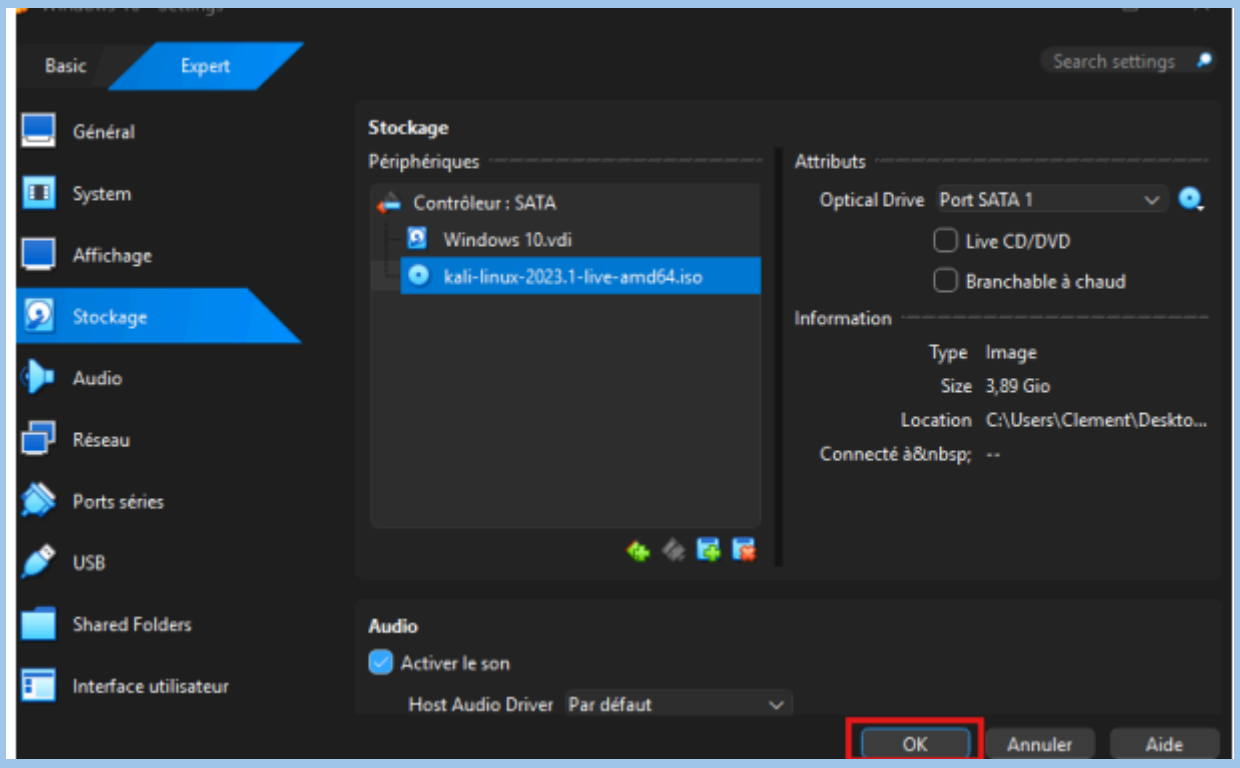
1. Lancement de la machine virtuelle Windows avec Kali

Nous allons configurer le lecteur optique de la machine virtuelle avec l'image ISO de Kali Linux. L'objectif est de monter Kali Linux par dessus Windows et d'utiliser les outils de crack.

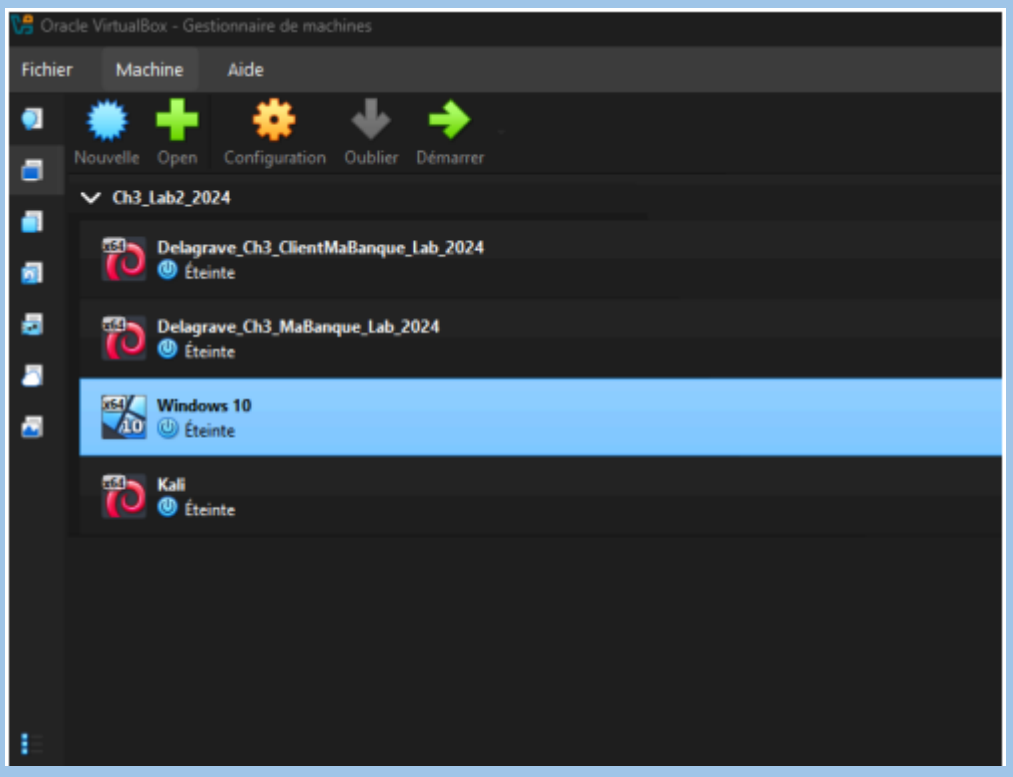




Une fois l'iso Kali Linux sur le lecteur optique de la machine virtuelle, nous appuyons sur OK.



Nous allons donc lancer la machine virtuelle windows 10 afin de démarrer sur l'environnement Kali Linux et débuter nos tests.



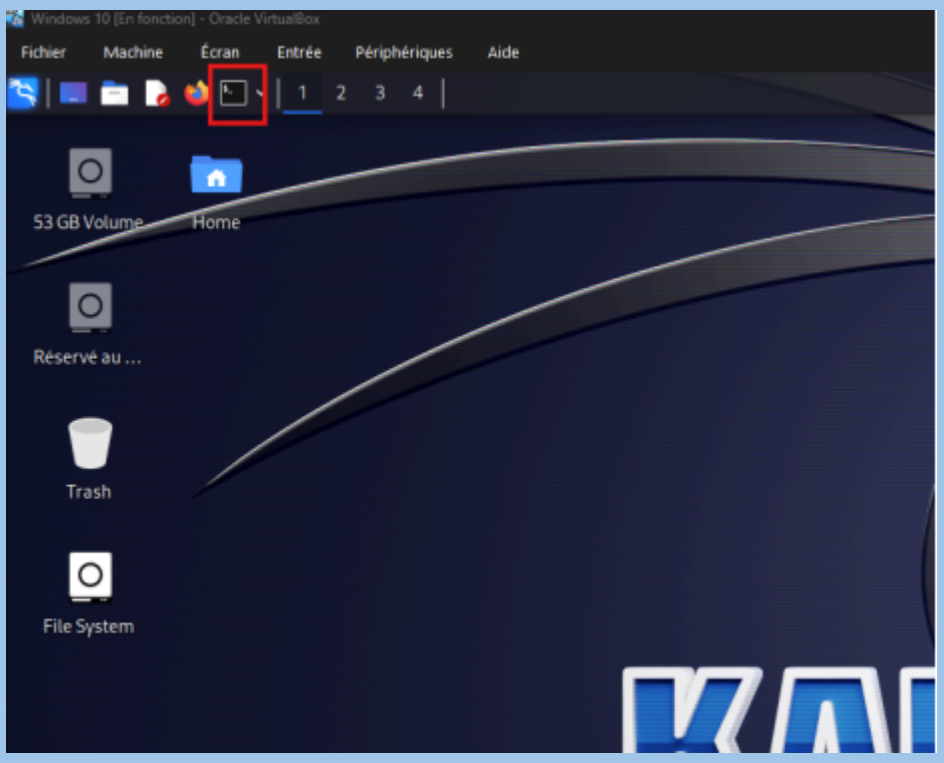
Lors du lancement de la machine virtuelle, le menu de démarrage de Kali Linux s'affiche. À cette étape, il faut choisir le mode Live system afin de démarrer Kali Linux sans installation sur le disque dur de la machine. Ce mode

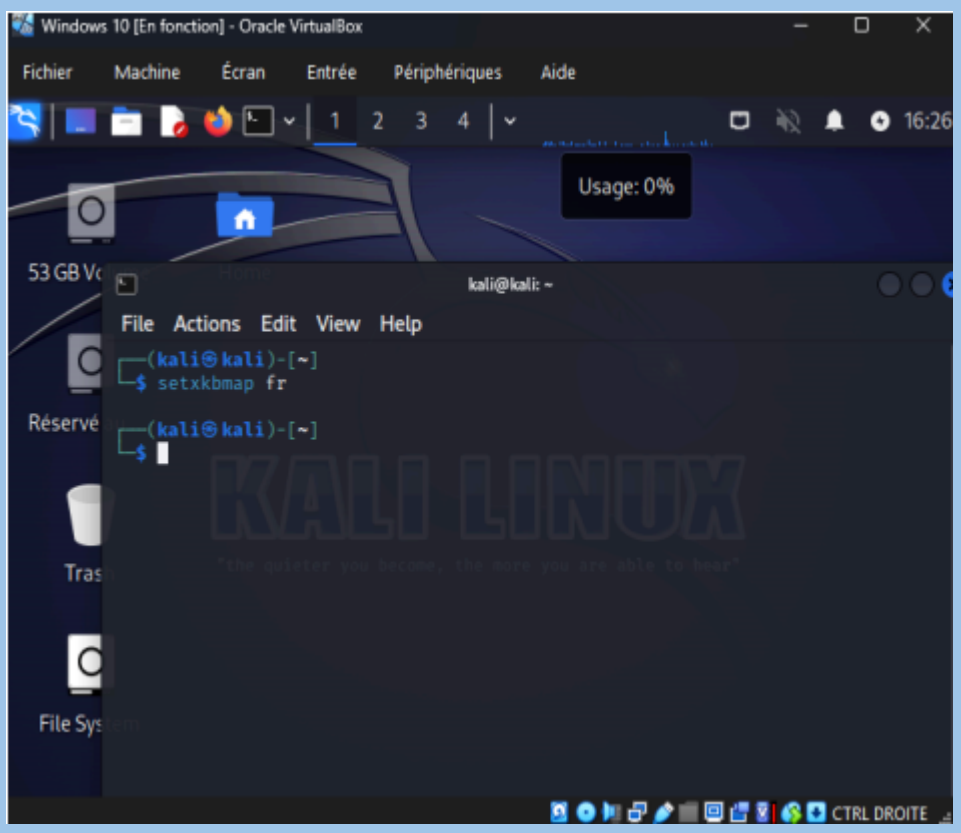
permet d'utiliser l'ensemble des outils de Kali Linux directement depuis l'image ISO, sans modifier le système Windows

Une fois les paramétrages et l'installation terminée, nous voila donc sur le bureau de Kali Linux.

2. Passage du QWERTY en AZERTY

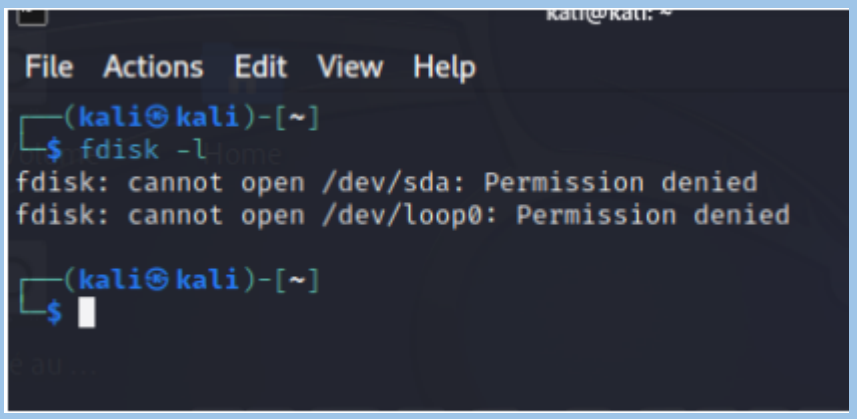
Le clavier est en QWERTY nous allons donc entrer dans le terminal et insérer une commande afin de **mettre le clavier en AZERTY**.



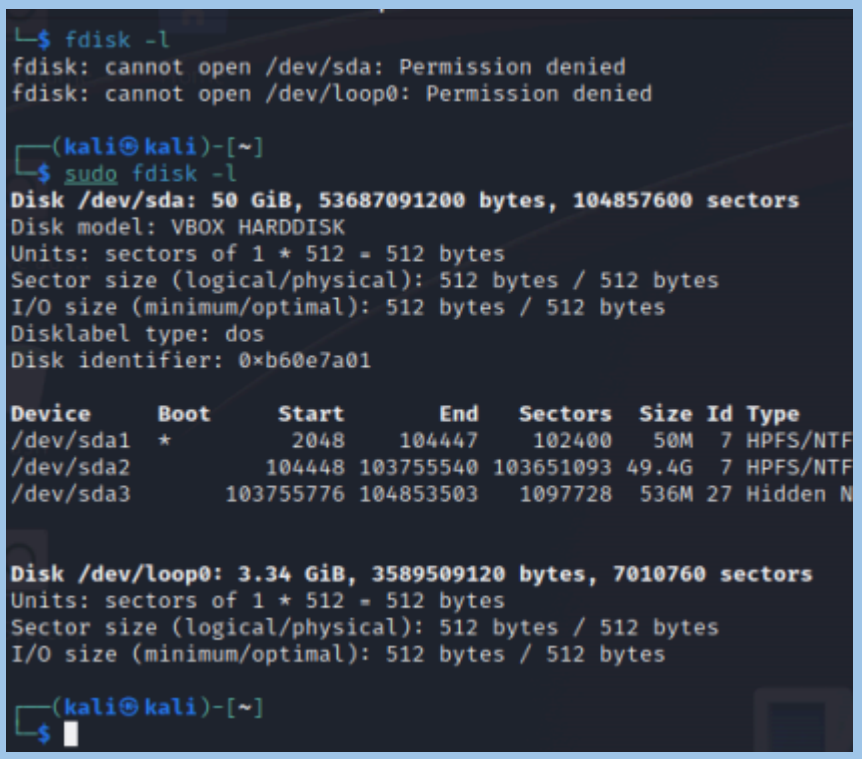


3. Repérer la partition Windows

A présent nous allons repérer la partition Windows présente sur le disque afin de pouvoir accéder aux fichiers du système depuis Kali Linux.



Cela nous affiche “permission refusée”, nous allons donc exécuter la commande avec les privilèges administrateur afin de pouvoir accéder aux informations des disques et des partitions du système.

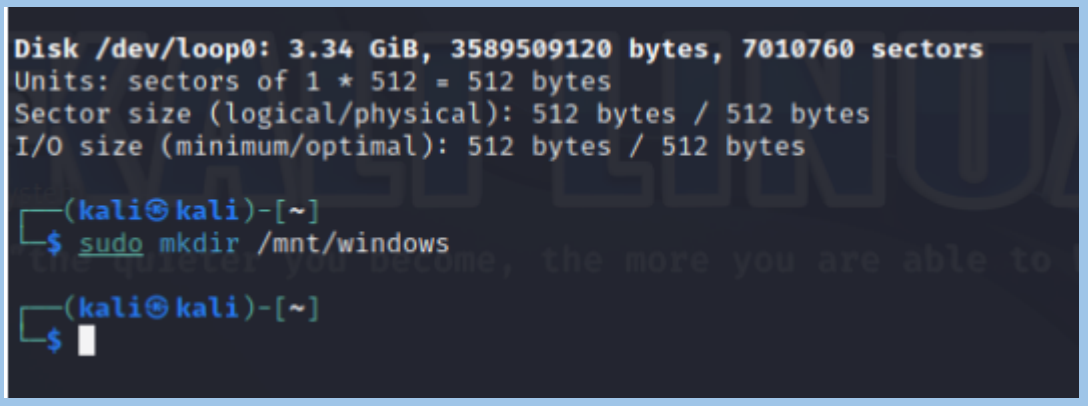


4. Accès aux fichiers Windows

Nous allons accéder aux dossiers et fichiers de la partition Windows depuis l'environnement Kali Linux afin de récupérer le fichier 127.0.0.1.pwdump présent sur le bureau de l'utilisateur administrateur. Ce fichier contient les identifiants chiffrés.

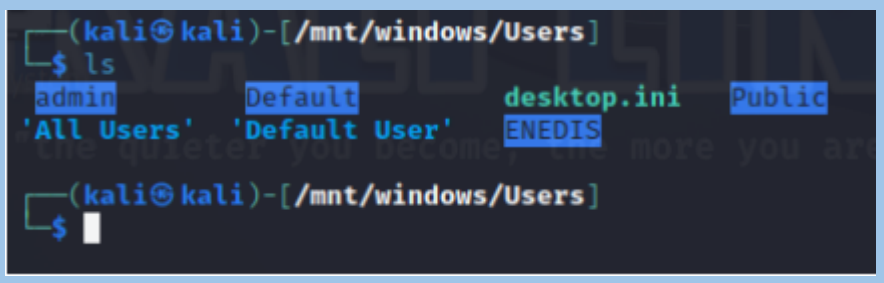
Pour ce faire, il faudra monter la partition Windows afin de rendre accessibles les dossiers et fichiers du système.

Nous allons créer un point de montage nommé /mnt/windows afin de pouvoir y attacher la partition Windows et rendre ses fichiers accessibles depuis l'environnement Kali Linux.

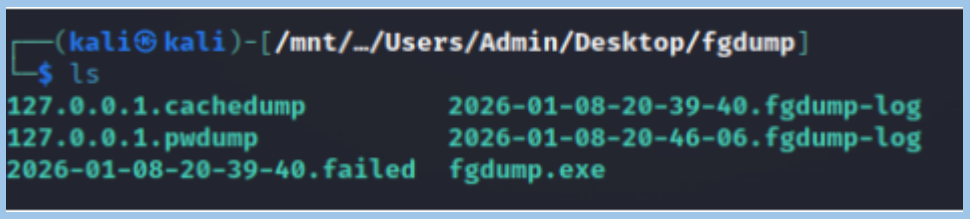


Afin d'accéder aux fichiers du système Windows, nous allons monter la partition Windows.

Nous allons accéder au dossier Users de la partition Windows afin d'identifier l'utilisateur administrateur et accéder à son bureau.



Nous allons accéder au bureau de l'utilisateur administrateur de Windows afin de localiser le fichier 127.0.0.1.pwdump, qui contient les hash des mots de passe nécessaires aux tests de robustesse.



ETAPE 2

3- Exécuter les différents tests avec l'outil John The Ripper

Nous commençons par lancer une attaque simple afin de tester des mots de passe construits à partir des identifiants des utilisateurs.
Cette méthode consiste à générer automatiquement des variantes du nom de compte comme l'ajout de chiffres ou de symboles afin de vérifier si le mot de passe est basé sur l'identifiant.

1 - Attaque simple

Cette méthode consiste à générer automatiquement des variantes du nom de compte afin de vérifier si le mot de passe est basé sur l'identifiant.

```
└─$ john --single --format=NT 127.0.0.1.pwdump
arning: invalid UTF-8 seen reading 127.0.0.1.pwdump
sing default input encoding: UTF-8
oaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
emaining 3 password hashes with no different salts
ress 'q' or Ctrl-C to abort, almost any other key for status
arning: Only 8 candidates buffered for the current salt, minimum 24 needed f
r performance.
lmost done: Processing the remaining buffered candidate passwords, if any.
g 0:00:00:00 DONE (2026-01-08 21:28) 0g/s 261800p/s 261800c/s 785400C/s admi
1902..admin1900
ession completed.
```

```
└─$ john --show --format=NT 127.0.0.1.pwdump
ENEDIS:gete55:1002:NO PASSWORD**********************:FC7358C0720A7395B5DC6C2B1
583CEE8:::
Warning: invalid UTF-8 seen reading 127.0.0.1.pwdump

1 password hash cracked, 3 left
```

Avec cette attaque, le mot de passe de l'utilisateur ENEDIS a été trouvé.

2 - Attaque par dictionnaire

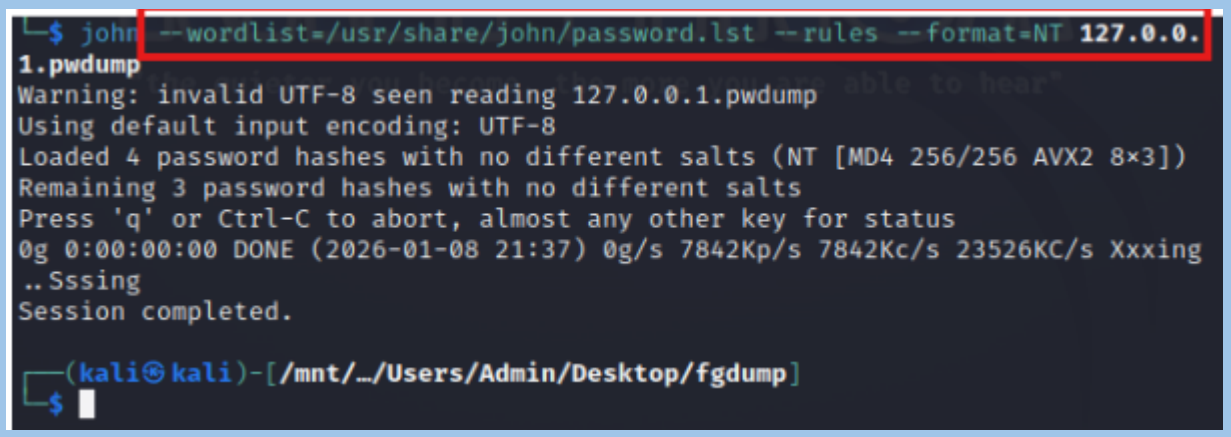
Une attaque par dictionnaire est réalisée à l'aide d'une liste de mots de passe courants.
Cette approche permet de tester rapidement des mots de passe fréquemment utilisés par les utilisateurs.

```
└─$ john --wordlist=/usr/share/john/password.lst --format=NT 127.0.0.1.pwdump
Warning: invalid UTF-8 seen reading 127.0.0.1.pwdump
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8×3])
Remaining 3 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2026-01-08 21:34) 0g/s 354600p/s 354600c/s 1063KC/s !@#$%
..sss
Session completed.
```

3 - Attaque par dictionnaire avec règles

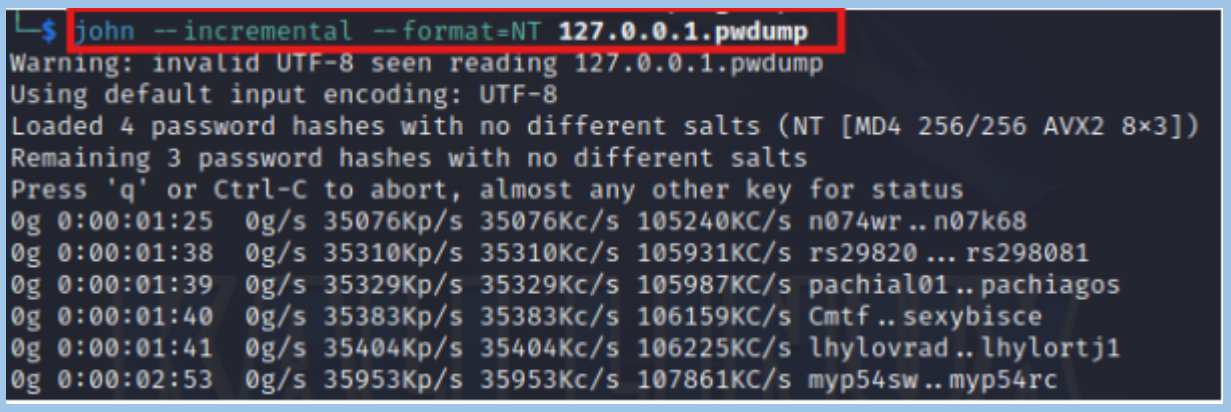
Des règles de transformation sont appliquées au dictionnaire afin de générer des combinaisons plus complexes.
Cette méthode simule les habitudes des utilisateurs

consistant à modifier légèrement un mot de passe simple pour le rendre plus fort.



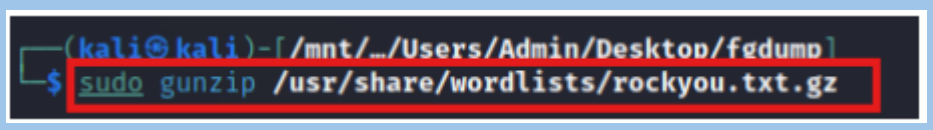
4 - Attaque par force brute

Une attaque par force brute est lancée afin de tester l'ensemble des combinaisons possibles.
Cette méthode est plus longue mais permet d'évaluer la résistance maximale des mots de passe..



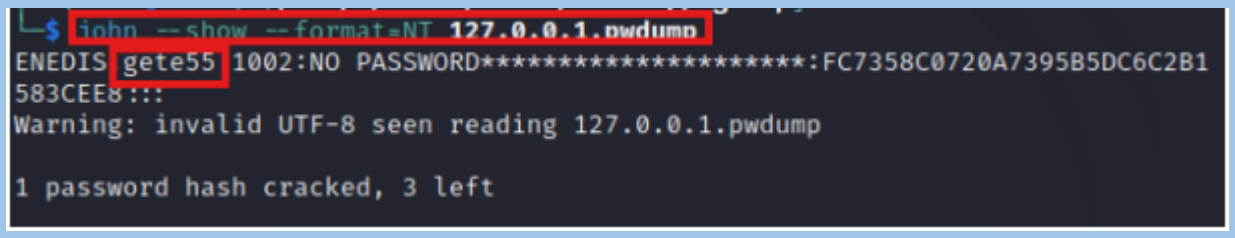
5 - Rockyou

L'utilisation du dictionnaire RockYou permet de réaliser une attaque par dictionnaire basée sur des mots de passe réellement utilisés.



6 - Affichage des mots de passe trouvés

La commande suivante permet d'afficher les mots de passe trouvés par John the Ripper.



4. Notez les identifiants trouvés et tirez les conclusions qui en découlent

À l'issue des différentes attaques réalisées à l'aide de l'outil John the Ripper, un seul mot de passe a été retrouvé.

- Compte ENEDIS : mot de passe retrouvé

- Compte CLIC : mot de passe non retrouvé
  (Trouvable si attaque plus longue)

- Compte MSA : mot de passe non retrouvé
  (Trouvable si attaque plus longue)

Les attaques simples, par dictionnaire avec règles et par force brute n'ont permis de compromettre qu'un seul

compte utilisateur. Seulement une attaque par force brute plus longue aurait surement pu permettre de retrouver leurs mots de passe

Les résultats montrent que le mot de passe du compte ENEDIS était faible, car il a pu être retrouvé à l'aide d'attaques basées sur des méthodes courantes. Cela indique l'utilisation d'un mot de passe insuffisamment robuste.

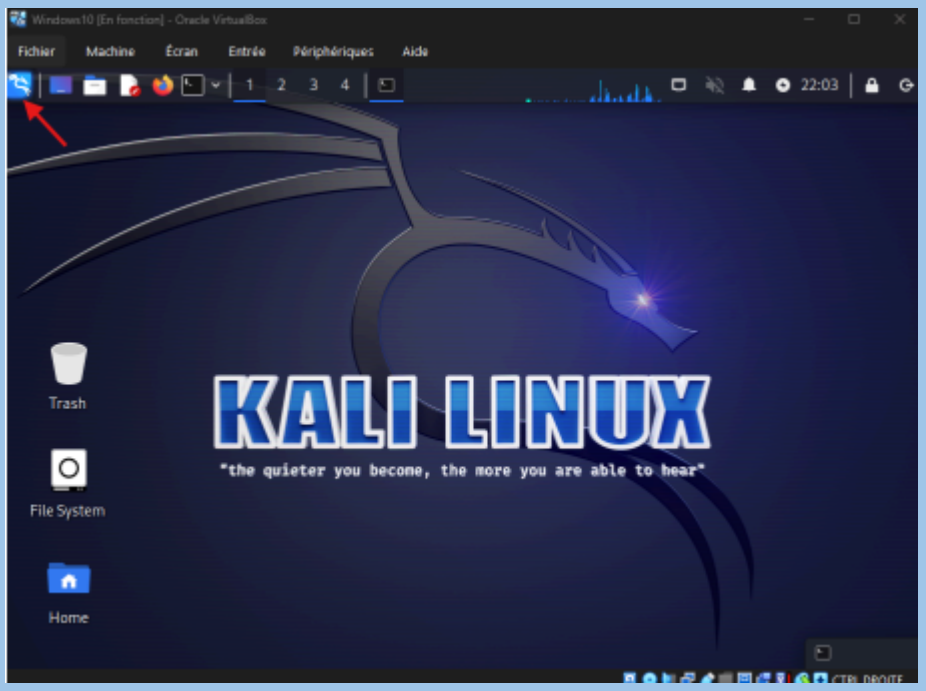
En revanche, les comptes CLIC et MSA ont résisté aux différentes attaques menées. Leurs mots de passe ne reposent pas sur des mots du dictionnaire, ni sur des variantes simples de l'identifiant, ce qui témoigne d'un meilleur niveau de sécurité.

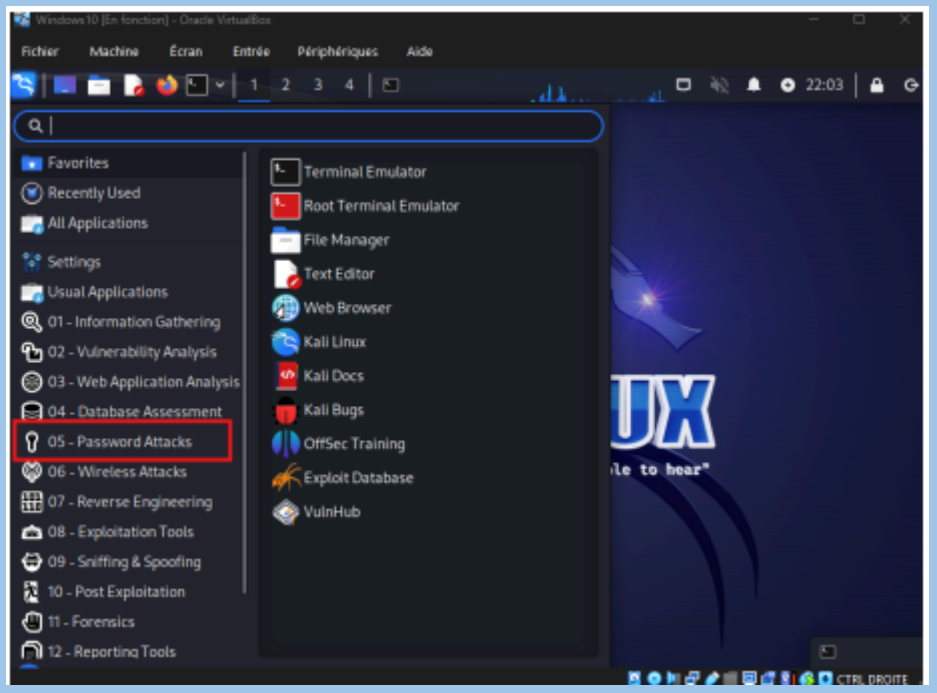
Ces tests mettent en évidence l'importance de choisir des mots de passe complexes, non liés à des informations personnelles, et suffisamment longs afin de limiter les risques de compromission.

ETAPE 3

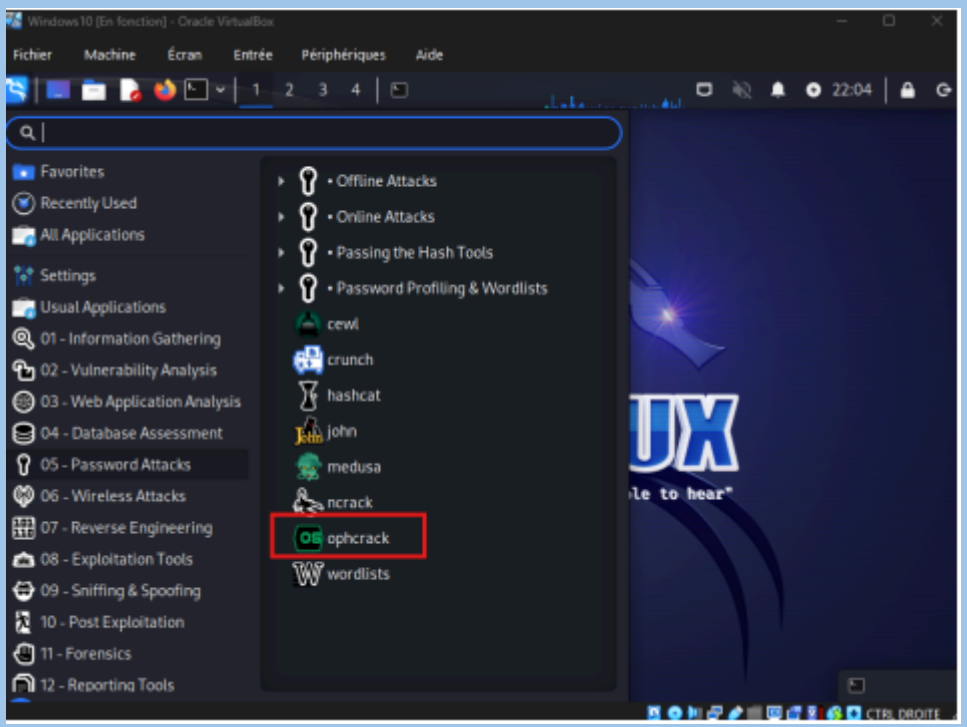
5. Exécutez le test à partir d'Ophcrack

Il faut maintenant exécuter l'outil Ophcrack depuis Kali Linux afin de réaliser le test de récupération des mots de passe à l'aide de tables arc-en-ciel, en utilisant la table vista_proba_free précédemment installée.

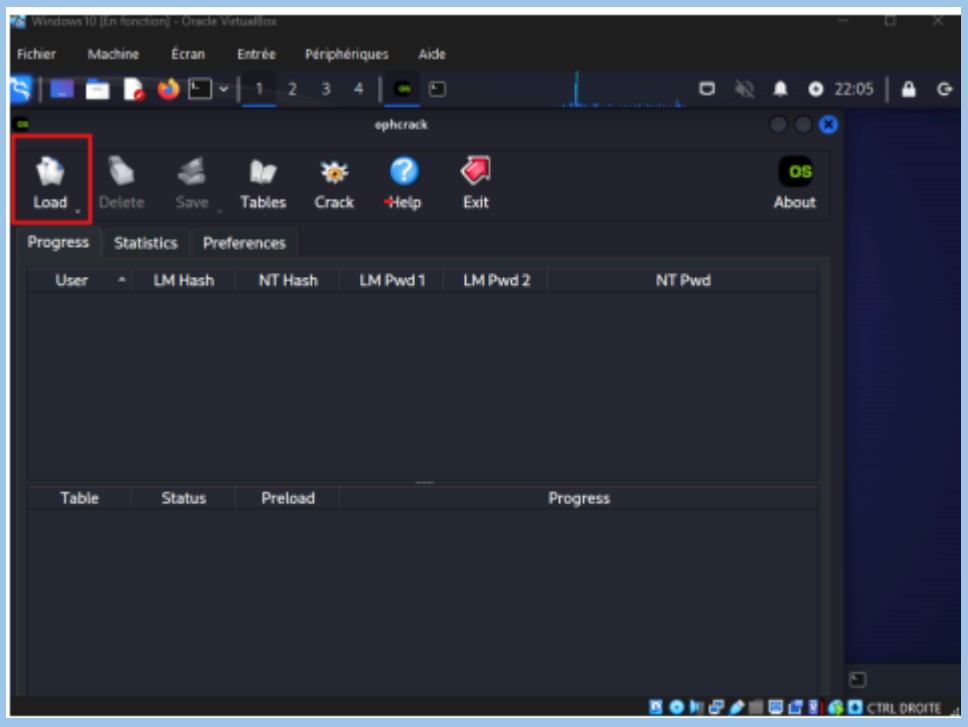




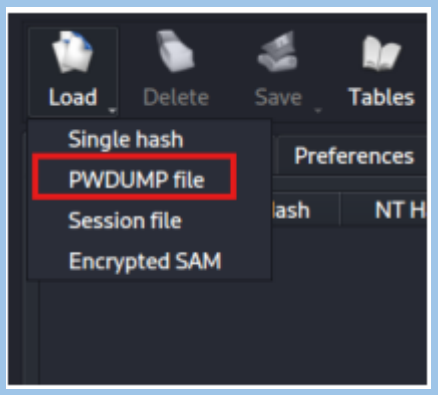
Nous sélectionnons ophcrack.

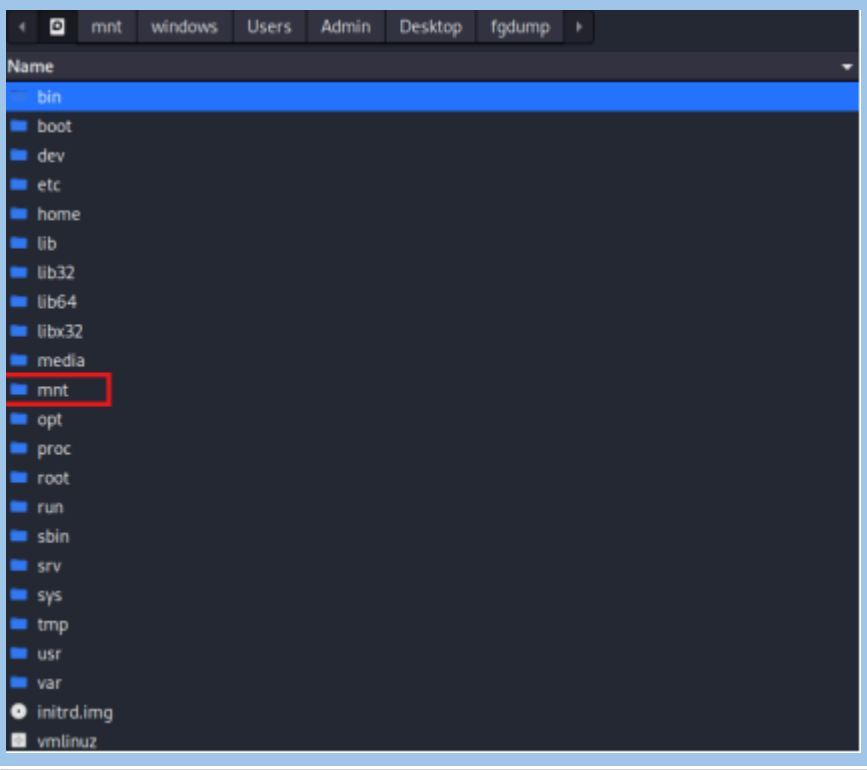


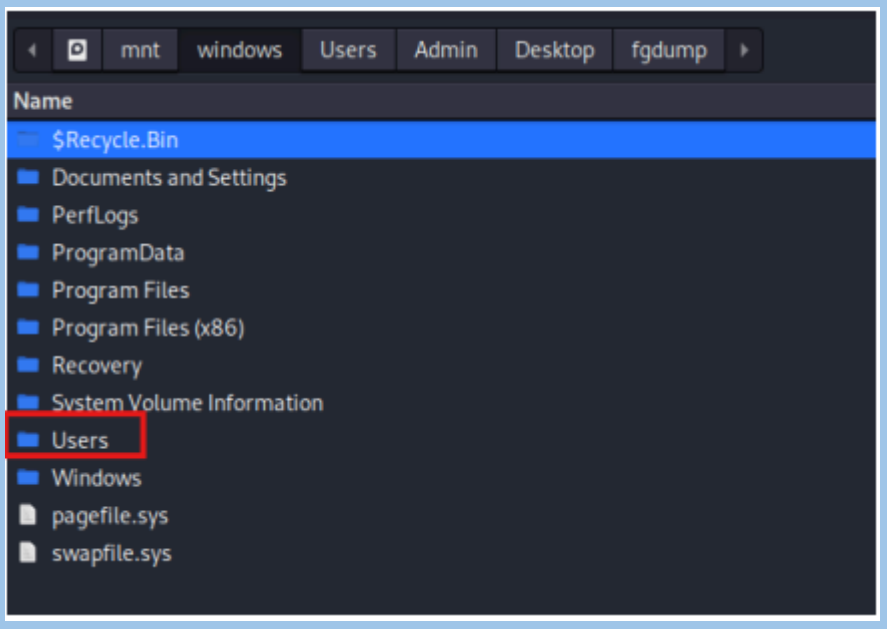
Ensuite nous allons charger dans Ophcrack le fichier 127.0.0.1.pwdump, qui a été généré au début du TP et qui contient les identifiants des utilisateurs ainsi que les hashs des mots de passe associés.


Fichier
Machine
Écran
Entrée
Périphériques
Aide
22:05
ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Table
Status
Preload
Progress
CTRL DROITE

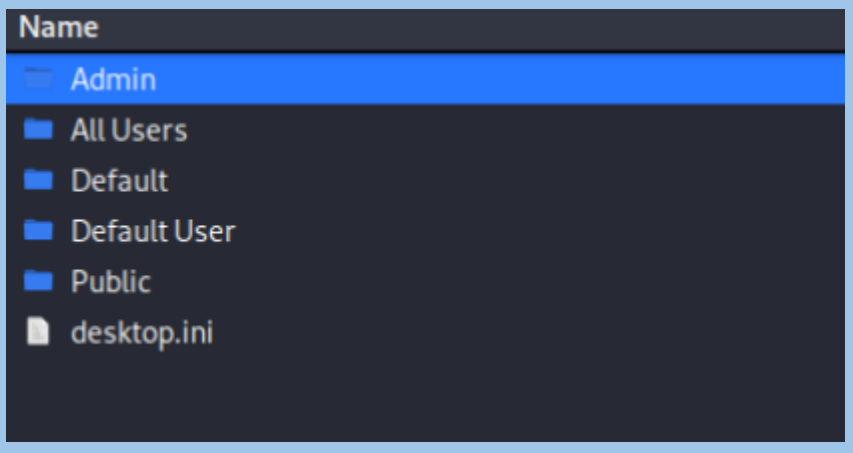
PWDUMP file


Load
Delete
Save
Tables
Single hash
PWDUMP file
Session file
Encrypted SAM
Preferences
NT H

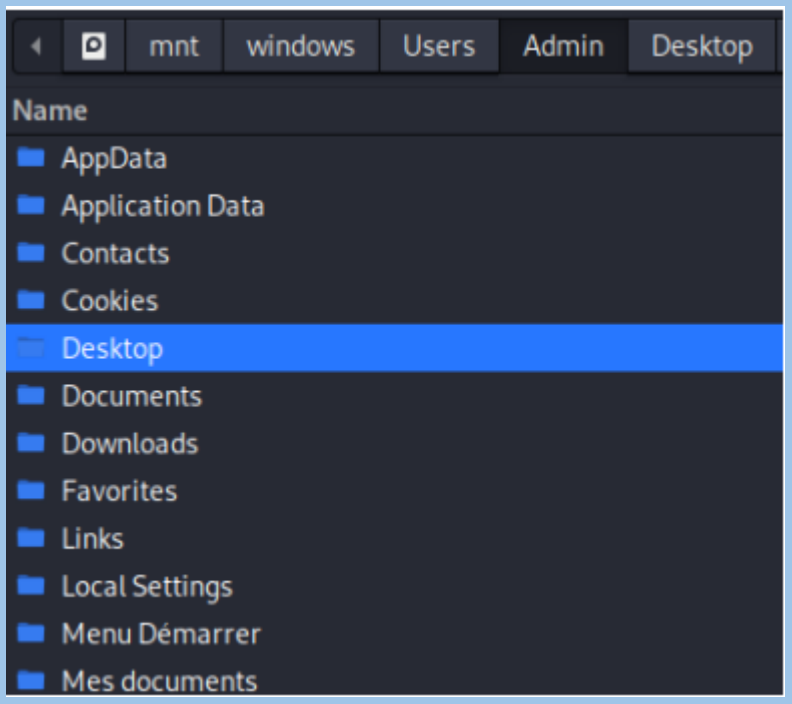




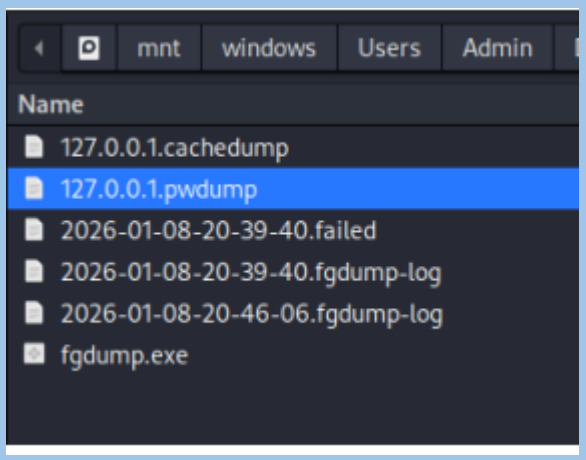
Admin

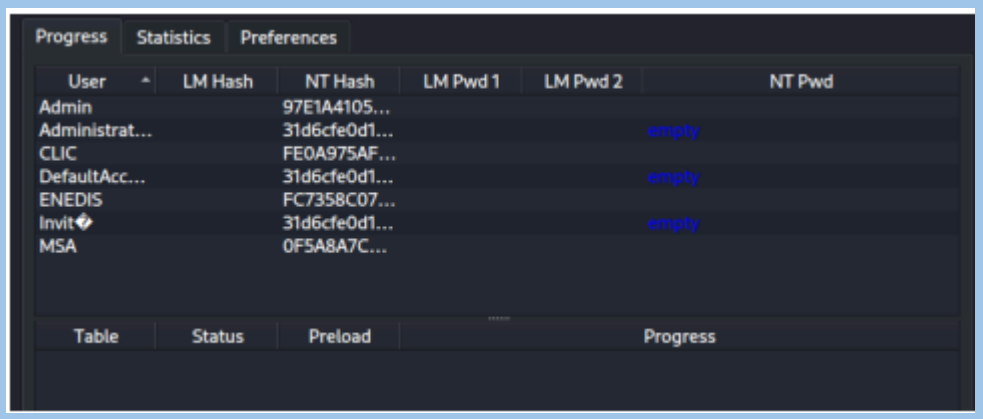


Desktop



Nous avons trouvé le fichier 127.0.0.1.pwdump.





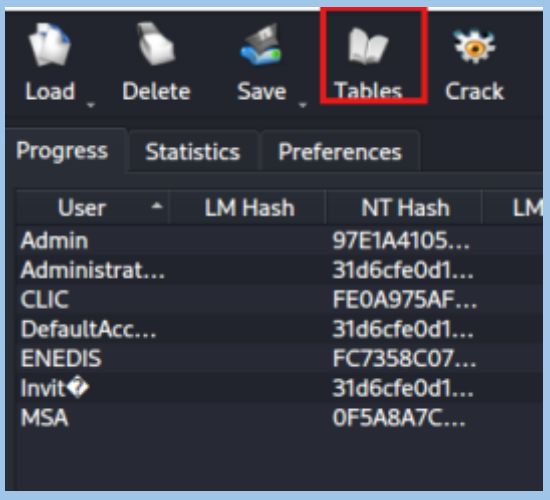
Récupération de la table vista_proba_free

Dans cette étape, nous allons récupérer la table arc-en-ciel vista_proba_free depuis la partition Windows et l'intégrer dans Kali. Pour rappel une table arc-en-ciel est un fichier qui contient des mots de passe déjà calculés à

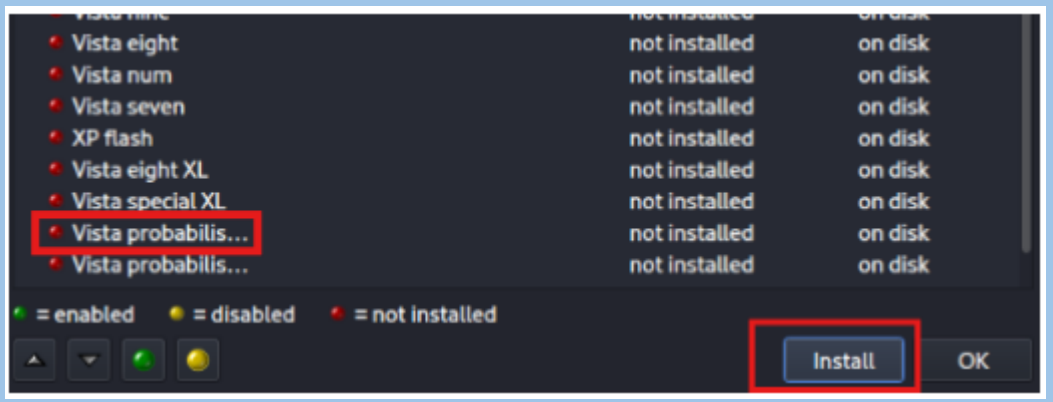
l'avance. Lorsqu'un hash est récupéré sur un système, l'outil peut le comparer directement avec ceux présents dans la table.

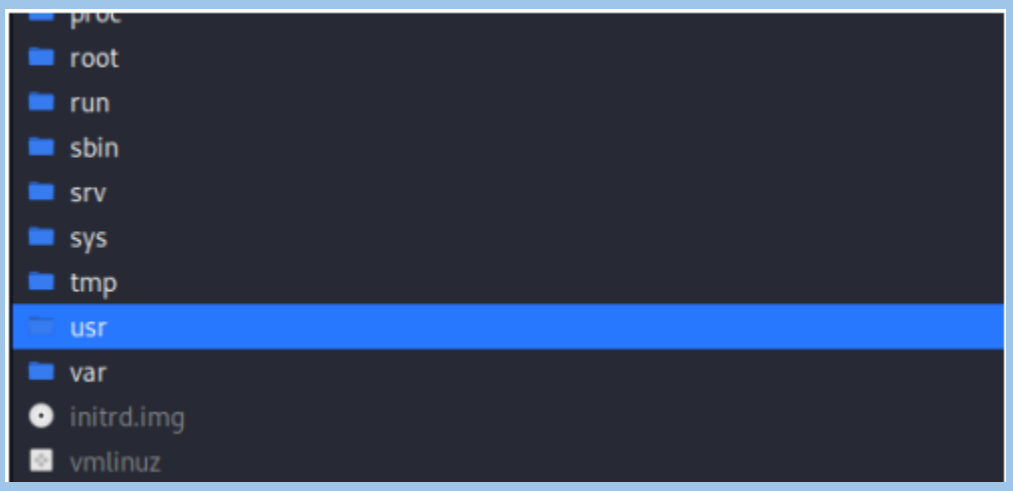
```
┌──(kali㉿kali)-[/mnt/…/Users/Admin/Desktop/fgdump]
└─$ sudo mkdir -p /usr/share/ophcrack/tables

┌──(kali㉿kali)-[/mnt/…/Users/Admin/Desktop/fgdump]
└─$ sudo cp -r /mnt/windows/Users/Admin/Desktop/vista_proba_free /usr/share/o
hcrack/tables/

┌──(kali㉿kali)-[/mnt/…/Users/Admin/Desktop/fgdump]
└─$ ls /usr/share/ophcrack/tables
ista_proba_free
```

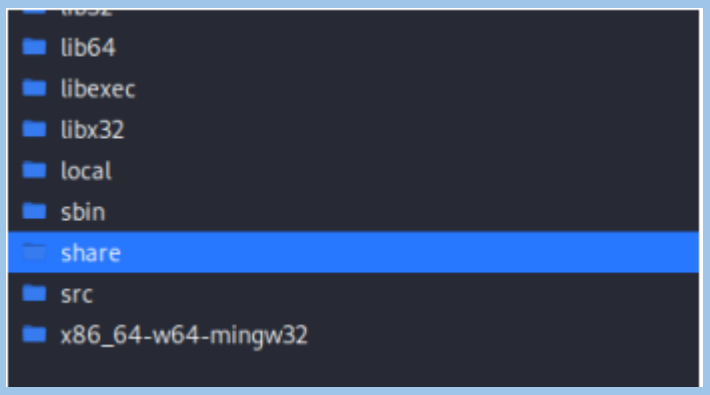
Revenons sur OPHCrack, maintenant que la table a été intégrée.



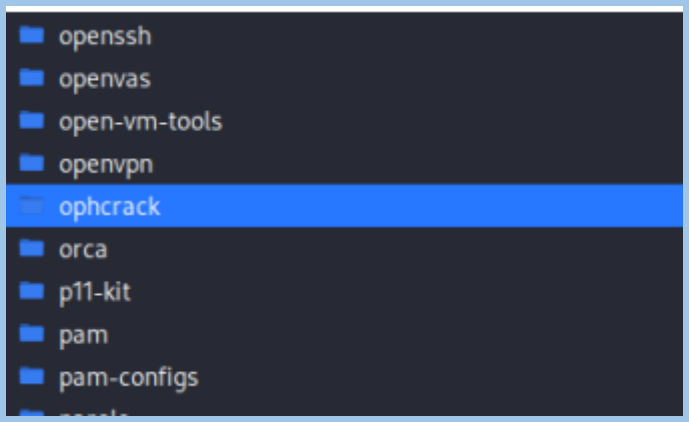
Nous allons à présent installer la table vista.



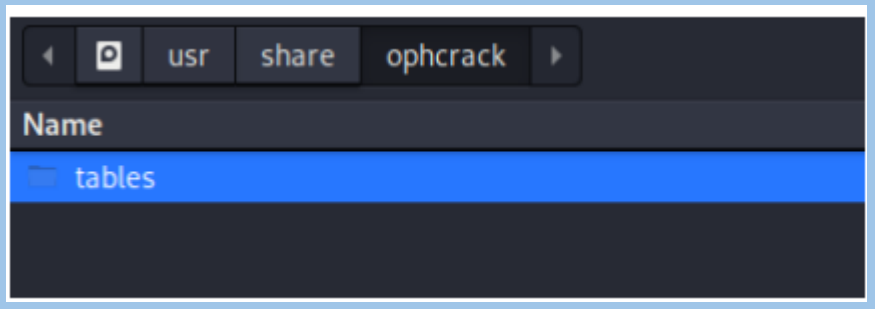




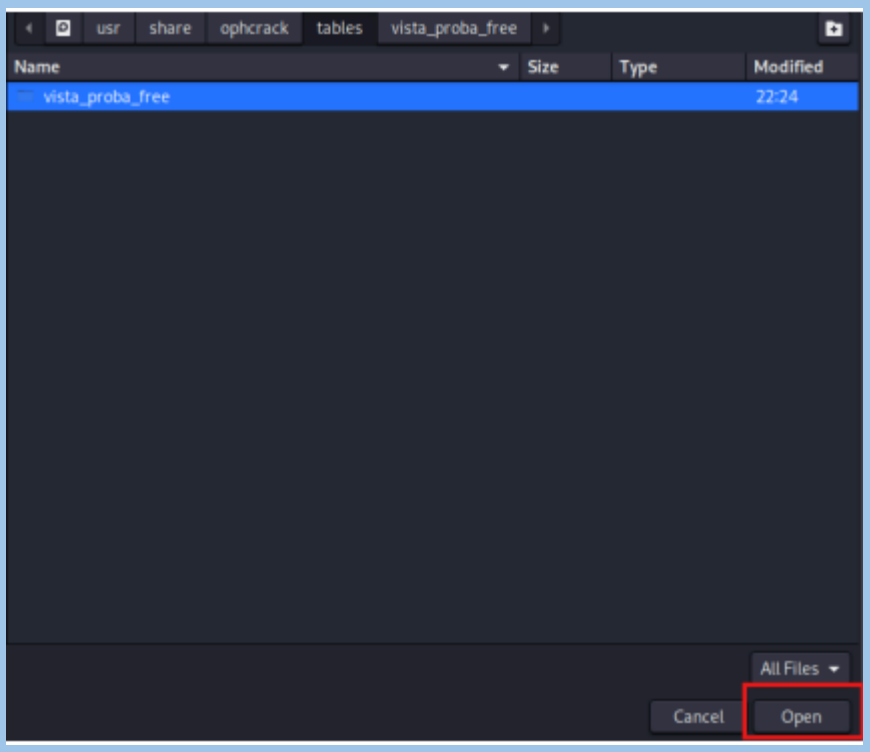
Sélectionnons ici ophcrack.



Puis tables.

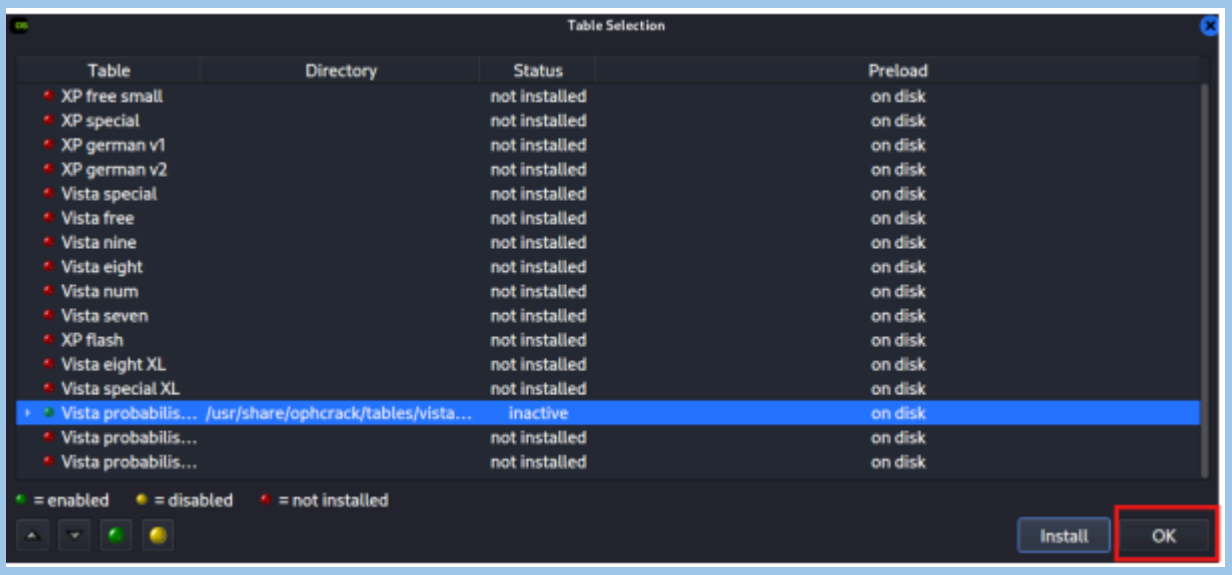


Nous avons trouvé la table.

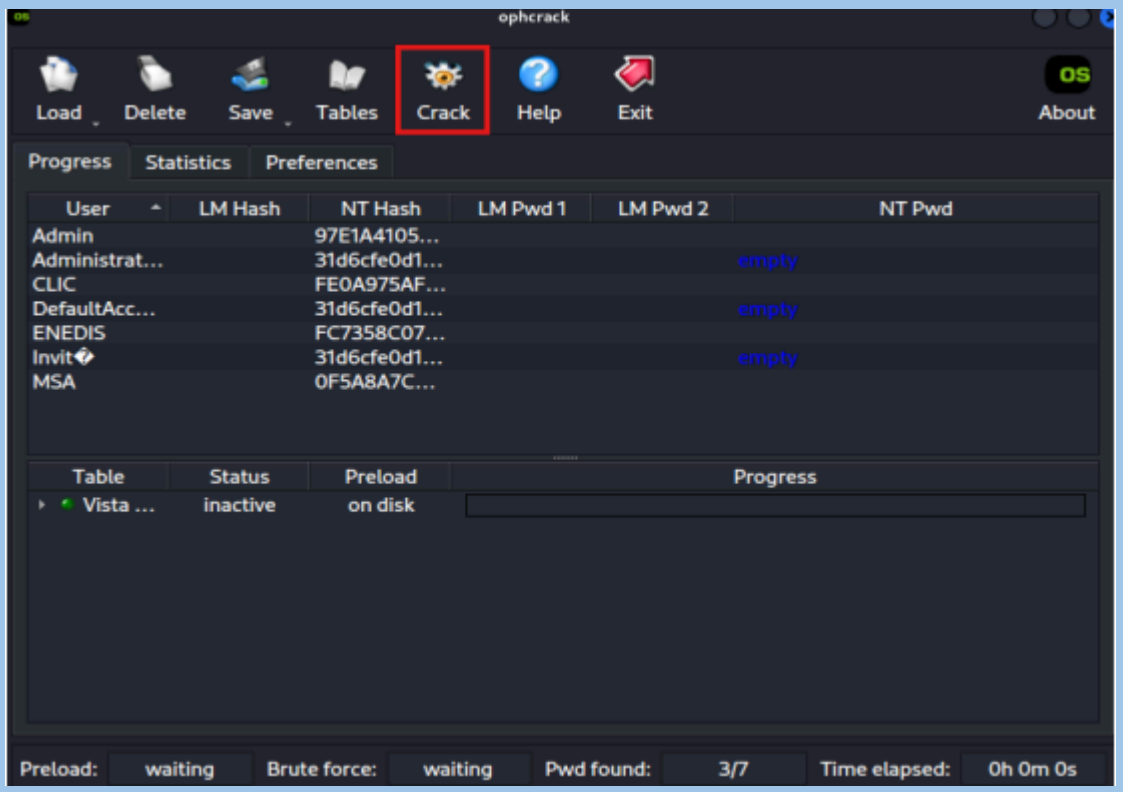


À ce stade, la table arc-en-ciel vista_proba_free est correctement installée et reconnue par Ophcrack. L'outil est

désormais prêt à exploiter cette table.



Il est alors possible de lancer le processus de récupération des mots de passe en démarrant l'attaque à l'aide du bouton Crack.

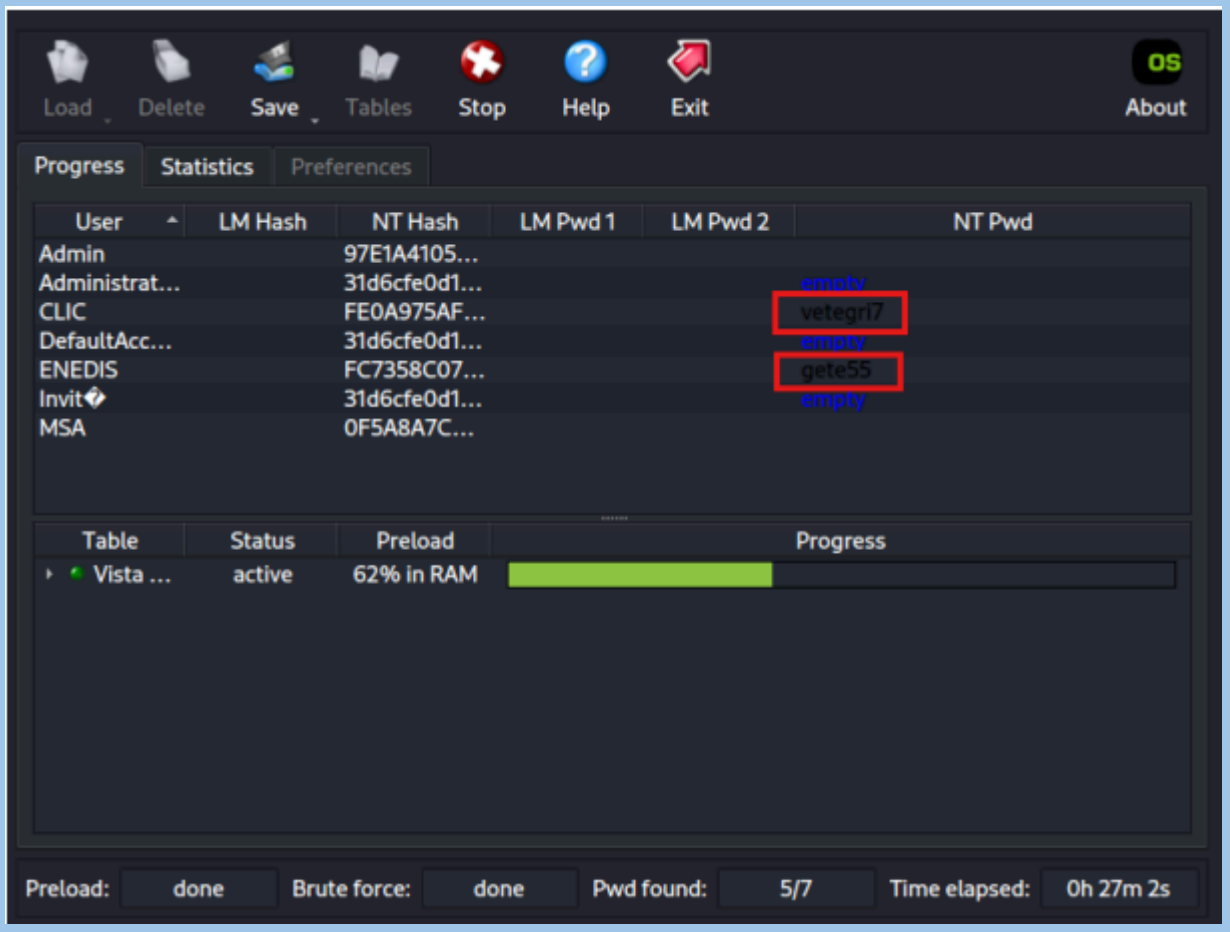


Résultat du crack :

Lors de l'exécution du crack avec Ophcrack et la table

arc-en-ciel vista_proba_free, les mots de passe des comptes CLIC et ENEDIS ont pu être récupérés.

Le crack n'ayant pas été mené jusqu'à son terme, il est possible que le mot de passe du compte MSA aurait pu être retrouvé si l'attaque avait été poursuivie plus longtemps. Ce résultat met en évidence que l'efficacité d'Ophcrack dépend à la fois de la table utilisée et du temps laissé à l'outil pour parcourir l'ensemble des correspondances possibles.



6. Proposez, d’après vos observations, plusieurs critères qui permettent d’améliorer la sécurité des mots de passe.

D’après nos observations issues des tests réalisés avec les outils John the Ripper et Ophcrack, plusieurs critères permettent d’améliorer significativement la sécurité des mots de passe. Tout d’abord, il est essentiel d’utiliser des mots de passe suffisamment longs, idéalement au moins 12 caractères, afin de limiter l’efficacité des attaques par force brute qui deviennent exponentiellement plus coûteuses en temps et en ressources. Ensuite il faut absolument éviter les mots de passe basés sur l’identifiant, le nom de l’utilisateur ou toute information personnelle facilement devinable, car ces éléments sont les premières cibles des attaques par dictionnaire.

Il est également recommandé de combiner différents types de caractères : lettres majuscules et minuscules, chiffres, ainsi que caractères spéciaux comme !, @, ou #, ce qui augmente considérablement la robustesse et rend les attaques plus complexes. Par ailleurs, il faut éviter l’utilisation de mots de passe courants ou présents dans des dictionnaires, ainsi que leurs variantes simples car John the Ripper excelle dans ce type d’attaques.

Mieux vaut privilégier des mots de passe non présents dans les tables arc-en-ciel, comme ceux ne reposant pas sur des mots usuels mais plutôt sur des phrases

aléatoires ou des combinaisons imprévisibles, rendant inefficaces les outils comme Ophcrack qui s'appuient sur ces tables. Un changement régulier de mots de passe est nécessaire, par exemple tous les 6 mois.

Enfin, les utilisateurs doivent être sensibilisés aux bonnes pratiques de sécurité afin de réduire les risques liés aux mots de passe faibles.

Ces mesures renforcent globalement la résistance face aux attaques par dictionnaire, par tables arc-en-ciel et par force brute.