Aubrée Romain **Beauvallet**

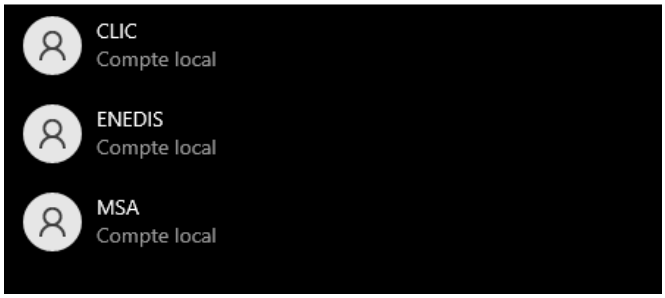
11/12/2025

Groupe 1

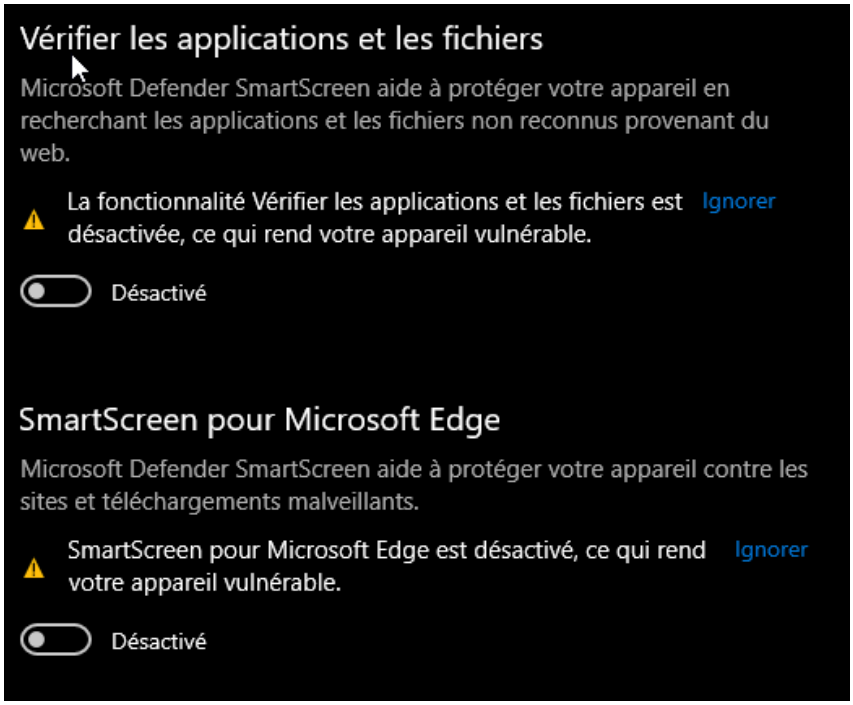
Bloc 3 CH 4 TH 3 TD 1

Exercice 1 2
Exercice 2 5
Exercice 3 5
Conclusion 6

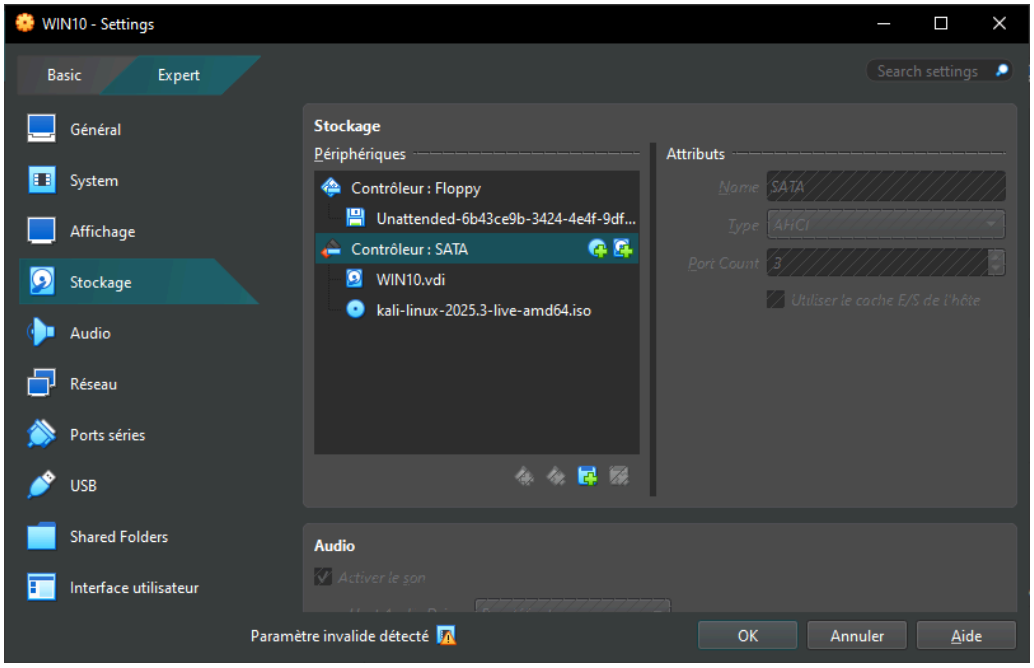
Exercice 1

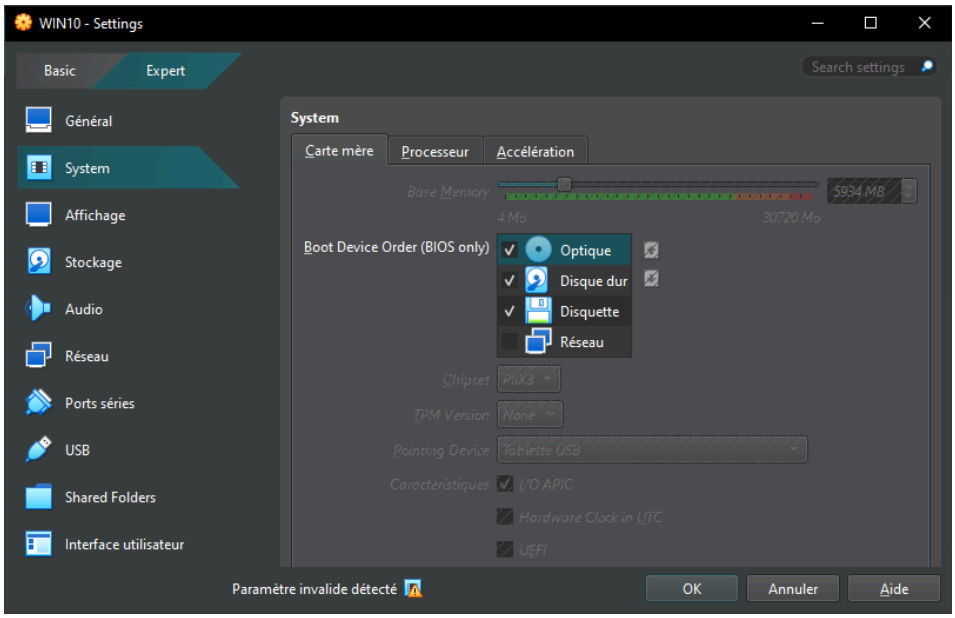

CLIC
Compte local
ENEDIS
Compte local
MSA
Compte local

Protection contre les virus et menaces
La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.
Activer

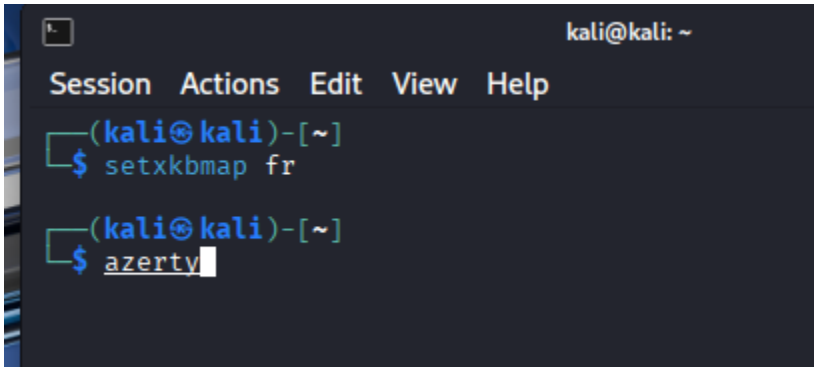

Vérifier les applications et les fichiers
Microsoft Defender SmartScreen aide à protéger votre appareil en recherchant les applications et les fichiers non reconnus provenant du web.
La fonctionnalité Vérifier les applications et les fichiers est désactivée, ce qui rend votre appareil vulnérable.
Ignorer
Désactivé
SmartScreen pour Microsoft Edge
Microsoft Defender SmartScreen aide à protéger votre appareil contre les sites et téléchargements malveillants.
SmartScreen pour Microsoft Edge est désactivé, ce qui rend votre appareil vulnérable.
Ignorer
Désactivé

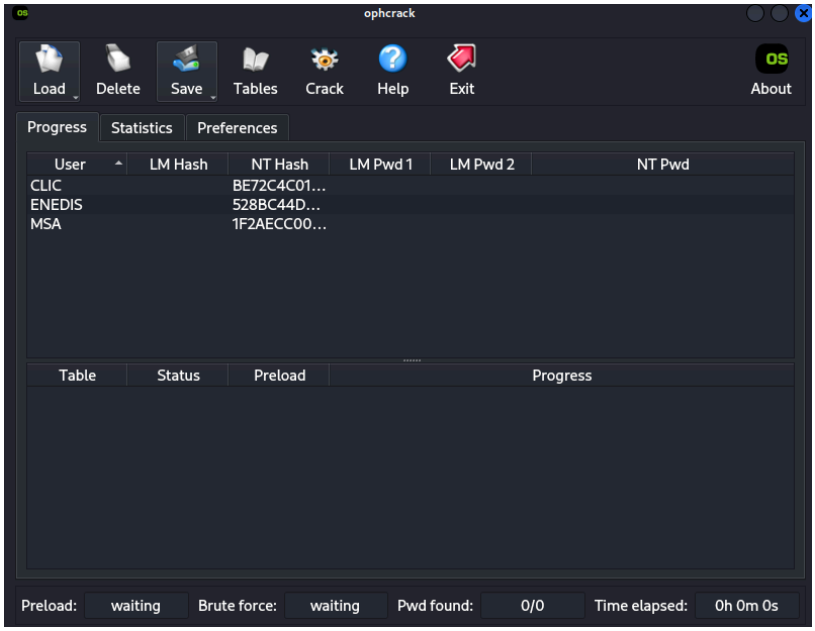
```
CLIC:1004:NO PASSWORD*********************:BE72C4C01C622CC10F7B0F70A9C2DFE8:::
ENEDIS:1002:NO PASSWORD*********************:528BC44DB20DF13A5B8DE27A8407DE9F:::
MSA:1003:NO PASSWORD*********************:1F2AECC00E935B615D54AE139CE161BA:::
```



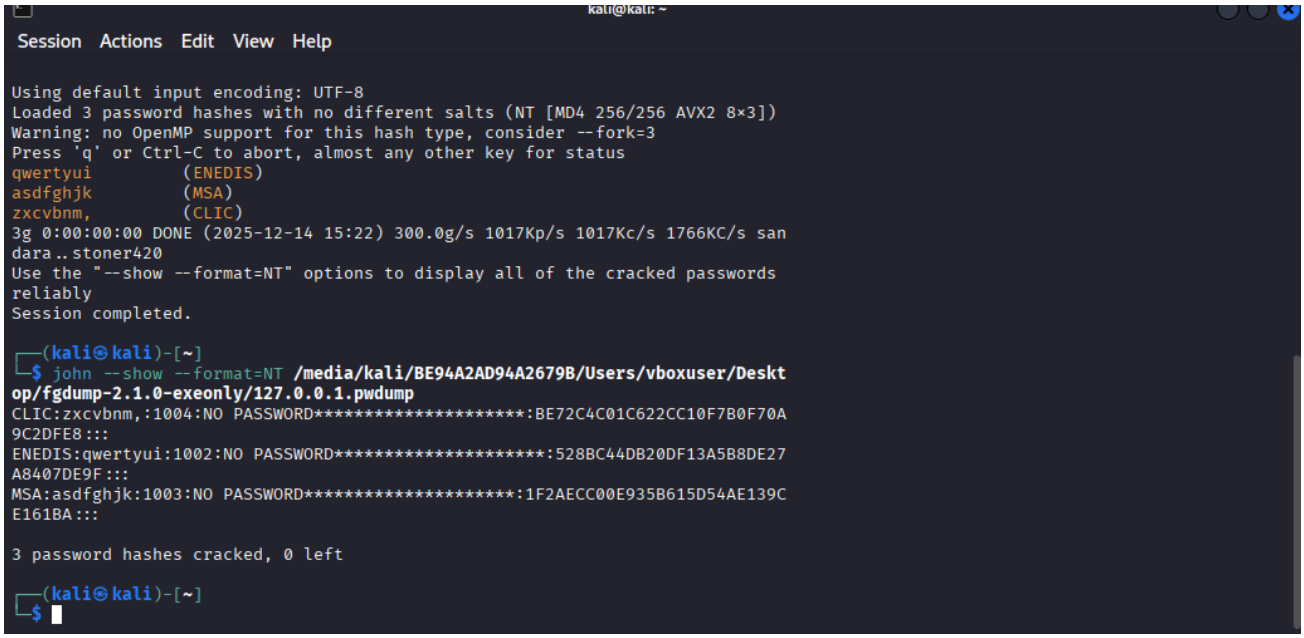


KALI
Kali Linux live menu (BIOS mode)
Live system (amd64)
Live system (amd64 fail-safe mode)
Live system (amd64 forensic mode)
Live system with USB persistence (check kali.org/prst)
Live system with USB Encrypted persistence
Start installer
Start installer with speech synthesis
Advanced install options
Utilities

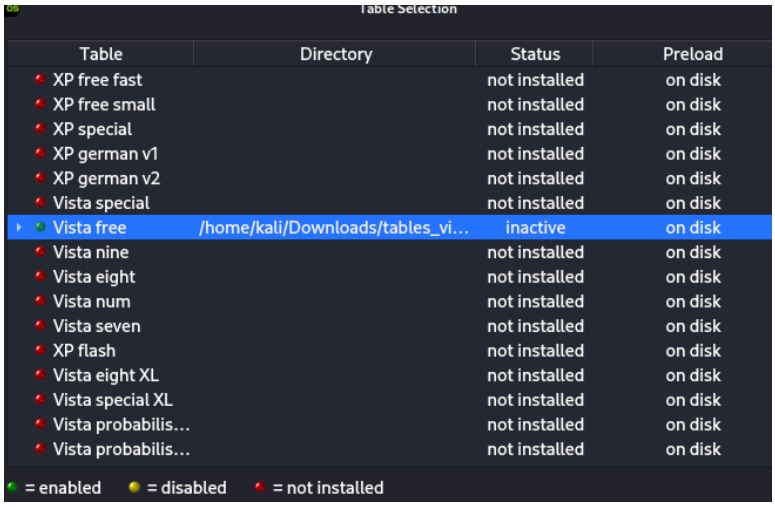

kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ setxkbmap fr
(kali㉿kali)-[~]
$ azerty

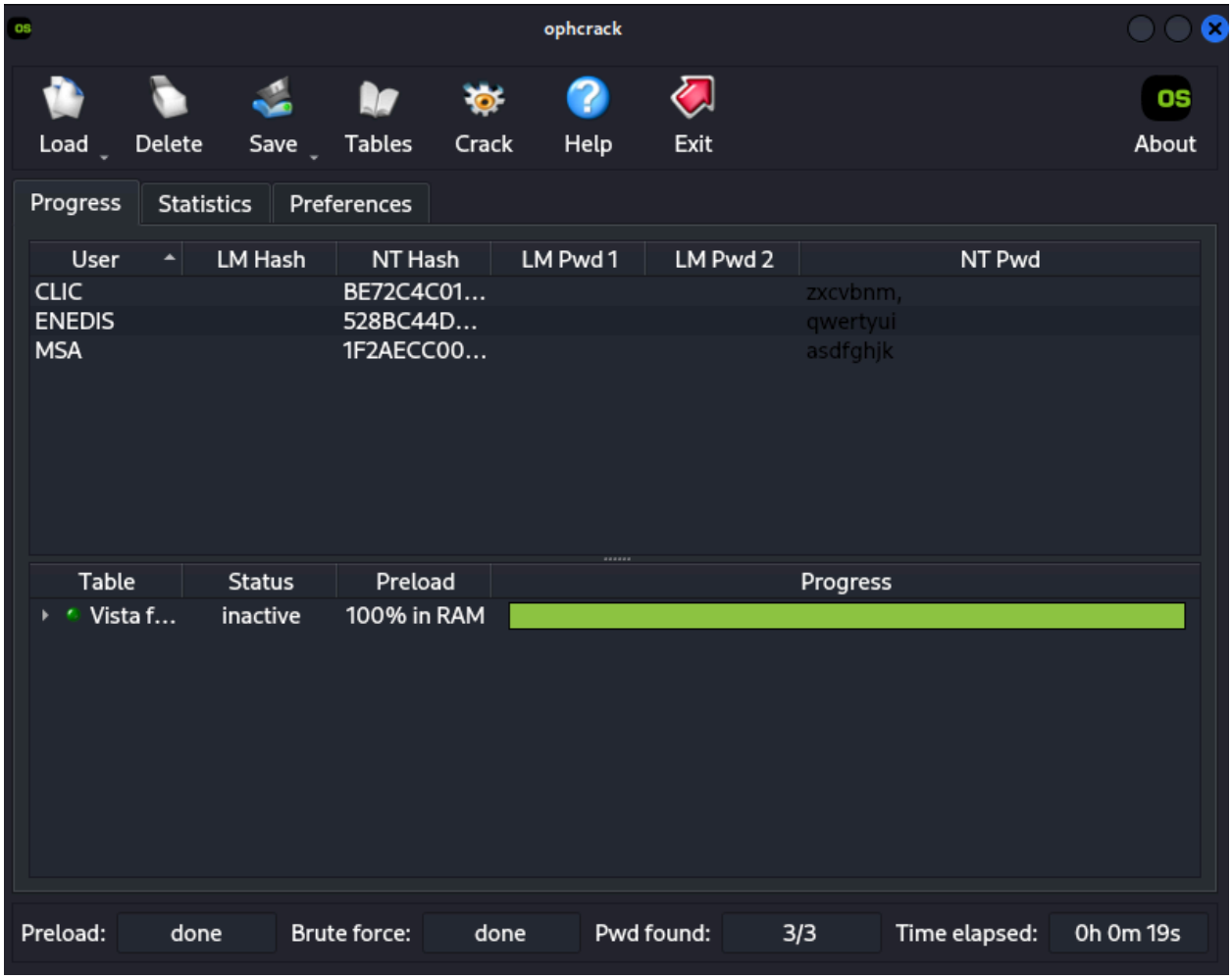

ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
CLIC
BE72C4C01...
ENEDIS
528BC44D...
MSA
1F2AECC00...
Table
Status
Preload
Progress
Preload: waiting
Brute force: waiting
Pwd found: 0/0
Time elapsed: 0h 0m 0s

Exercice 2



Exercice 3





Il faut mélanger Majuscules + Minuscules + Chiffres + Caractères Spéciaux (ex: @, #, !, %). Faire des mots de passe plus longs et ne jamais utiliser de suite de caractères (1234, azerty, etc).

Conclusion

Ce TP nous a introduit à la sécurité des mots de passe en simulant une attaque brute force.