

TP INTRUSION SIMPLE WINDOWS

Dans ce TP on va tenter d'accéder un utilisateur administrateur local sous Windows, protégé par un mot de passe.

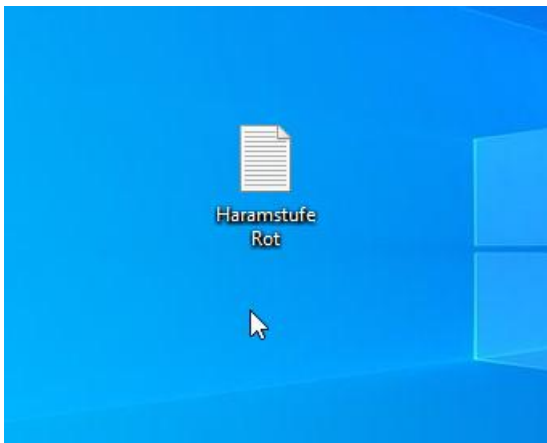
Sans réinitialiser le mot de passe :

Préparation :

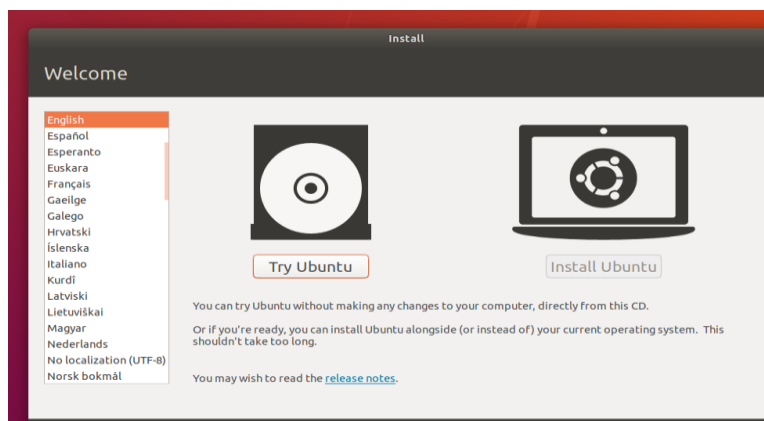
- Windows 10 (XP, Vista et 7 marchent aussi) avec un compte utilisateur administrateur locale (pas connecté avec Microsoft)
- Une DVD ou une clé USB avec une .iso d'Ubuntu (j'utilise la version 18)

Si le but est seulement d'accéder les fichiers de notre utilisateur, il ne faut même pas passer le mot de passe.

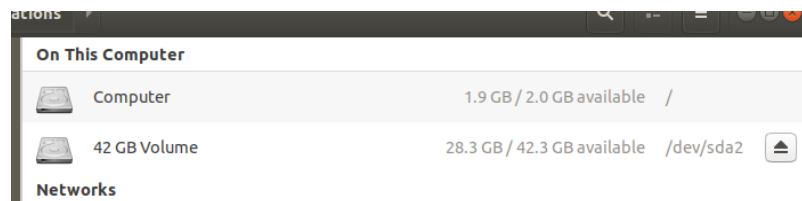
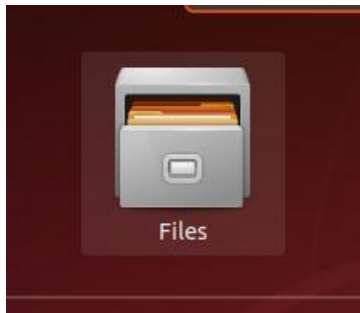
Pour vérifier cela on prépare par se connecter à notre utilisateur admin et créer un fichier .txt sur le bureau. Dans mon cas le fichier s'appelle « Haramstufé Rot » qui consiste du texte d'une chanson. Puis on éteint l'ordinateur.



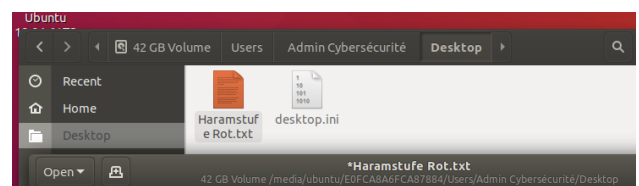
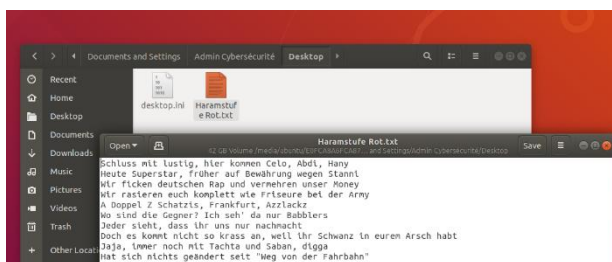
Maintenant on allume l'ordinateur mais on lance Ubuntu à la place de Windows. On choisit « Try Ubuntu » pour ne pas écrire sur le système de Windows.



Quand le système charge, on ouvre l'application « Files » et entre dans « + other locations » et puis dans le premier dossier sous « Computer ». Pour moi c'est « 42 GB Volume » ou « sda2 ».



Pour retrouver notre fichier « Haramstufe Rot » on fait le pas /Documents and Settings/**NOMUTILISATEUR**/Desktop/Haramstufe Rot.txt



Ici on voit qu'on ne peut pas seulement voir le fichier et son contenu mais aussi le modifier.

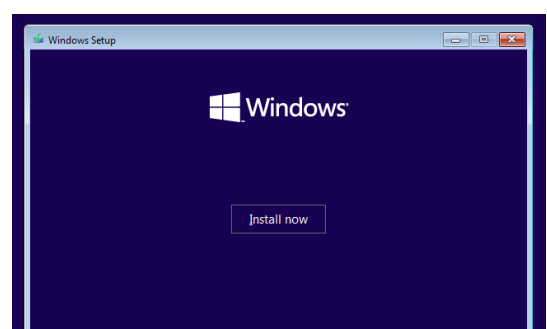
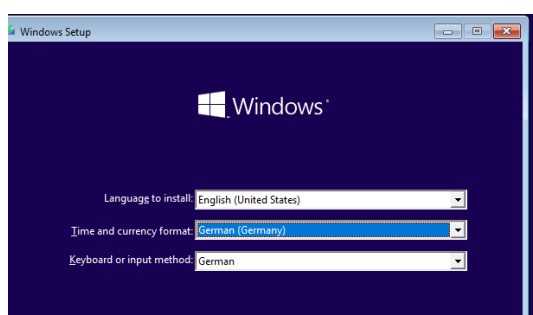
Réinitialiser le mot de passe :

Préparation :

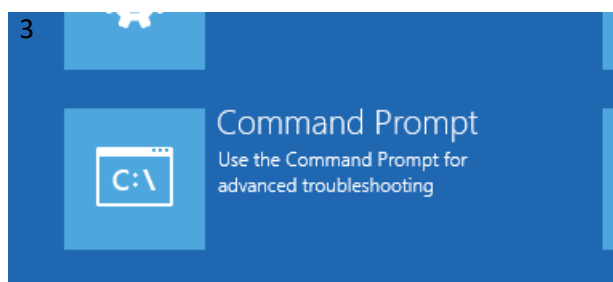
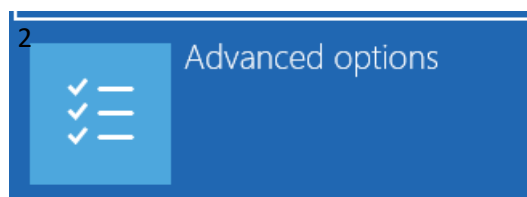
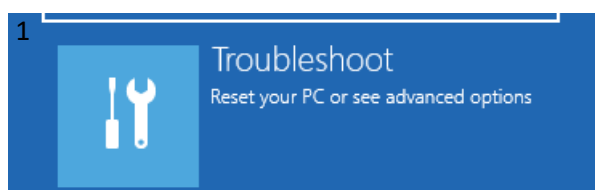
- Windows 10 (XP, Vista et 7 marchent aussi) avec un compte utilisateur administrateur locale (pas connecté avec Microsoft)
- Une DVD ou une clé USB avec une .iso de Windows

Maintenant on veut accéder l'utilisateur admin. Pour cela on va changer le mot de passe. Avec les « Options de démarrage avancées » on peut accéder la console pour la modifier mais pour faire cela il nous faut le mot de passe. Donc on a besoin un « Utilisateur » plus puissant que l'administrateur. Donc il nous faut une .iso de Windows pour l'écraser.

On lance alors l'ISO, on choisit nos préférences et on clique sur l'option « Repair your computer » qui est en fait les « Options de démarrage avancées » mais avec des droits supérieurs parce qu'on est sur l'ISO de réparation.



On choisit maintenant « Troubleshoot », « Advanced options » et puis « Command Prompt » pour accéder la console.



D'abord on cherche notre partition avec les fichiers de Windows donc on tape C : et puis *dir*. Avec ces commandes on entre un disque et laisse afficher les dossiers dedans. Si le dossier « Windows » n'est pas visible on continue avec D :, E :, ... jusqu'à ce qu'on voit le dossier. Pour moi c'était dans le disque D :.

```
X:\sources>d:
D:\>dir
Volume in drive D has no label.
Volume Serial Number is FCA8-7884

Directory of D:\

12/07/2019  01:14 AM    <DIR>          PerfLogs
10/17/2023  11:53 PM    <DIR>          Program Files
05/05/2023  04:27 AM    <DIR>          Program Files (x86)
11/26/2023  11:48 PM    <DIR>          Users
10/17/2023  11:59 PM    <DIR>          Windows
             0 File(s)                0 bytes
             5 Dir(s)  20,711,759,872 bytes free

D:\>_
```

Puis on tape et exécute en ordre :

```
cd Windows
```

```
cd System32
```

```
copy Utilman.exe Utilman.exe.bak
```

```
copy cmd.exe Utilman.exe
```

```
yes
```

Ce fait quoi ? Utilman.exe est un programme qui modifie l'ordinateur pour aider les gens avec des problèmes de vues, etc. Ce programme s'exécute déjà quand Windows démarre et pour modifier l'ordinateur il faut des droits administratifs. Donc on utilise ces commandes pour remplacer Utilman.exe par la console (cmd.exe) (d'abord on crée une sauvegarde d'Utilman.exe nommé Utilman.exe.bak pour inverser les changements plus tard) pour pouvoir accéder la console qui a des droits administratifs parce que ces droits étaient réservés pour Utilman.exe.

Maintenant on redémarre l'ordinateur. Dans l'écran de bienvenue on appuie le bouton de Windows et « U » pour ouvrir Utilman.exe qui est maintenant la console.

Ici on tape

Net user "NOMUTILISATEUR" nouveau mot de passe pour changer le mot de passe.

```
C:\Windows\system32>net user "Admin Cybersécurité" newpassword
```

Après quitter la console vous pouvez accéder l'utilisateur admin avec le nouveau mot de passe.



Pour inverser les changements d'Utilman.exe on tient « shift » et redémarre l'ordinateur pour ouvrir les « Options de démarrage avancées ». On entre encore « Troubleshoot », « Advanced options » et puis « Command Prompt ».

Ici on tape :

d : (votre disque)

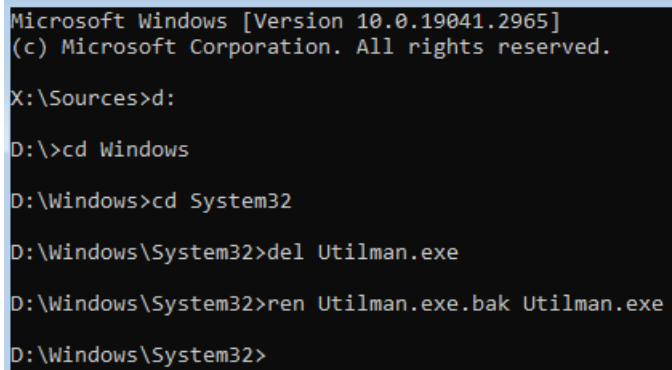
cd Windows

cd System32

del Utilman.exe

ren Utilman.exe.bak Utilman.exe

et on ferme la console.



```
Microsoft Windows [Version 10.0.19041.2965]
(c) Microsoft Corporation. All rights reserved.

X:\Sources>d:
D:\>cd Windows
D:\Windows>cd System32
D:\Windows\System32>del Utilman.exe
D:\Windows\System32>ren Utilman.exe.bak Utilman.exe
D:\Windows\System32>
```

Là on a supprimé Utilman.exe qui était la console et puis on a renommé la sauvegarde Utilman.exe.bak, alors le vrai Utilman.exe, en Utilman.exe.

Réinitialiser le mot de passe en Linux :

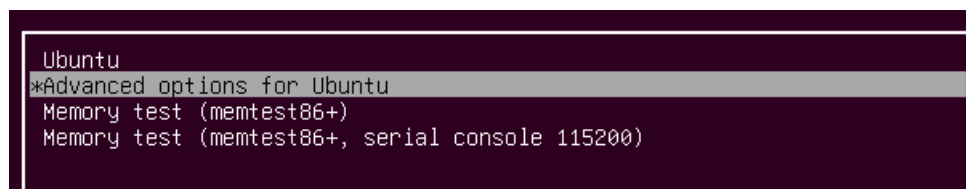
Préparation :

- Un utilisateur sur un système Ubuntu installé
- Une DVD ou une clé USB avec une .iso d'Ubuntu

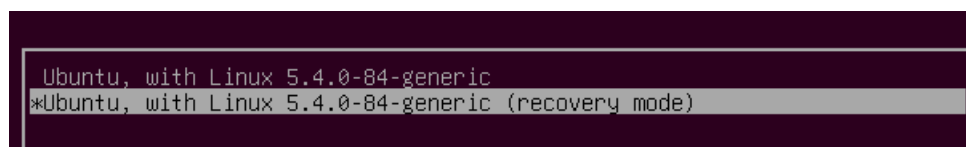
Cela marchait avec Windows, mais est-ce que cela marche aussi avec Linux ?

On lance Ubuntu mais avant taper le mot de passe on redémarre et puis on appuie sur le bouton « shift ».

Cela nous donne plusieurs options de démarrage. Ici on choisit « Advanced options for Ubuntu » et puis on lance le « Recovery Mode ».

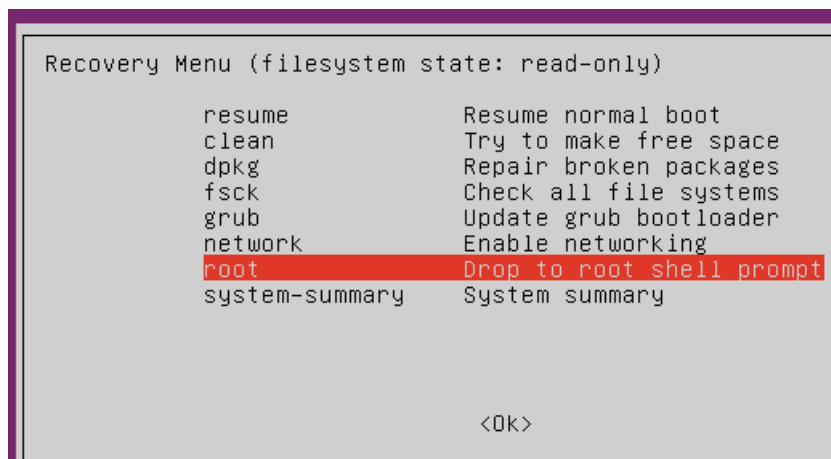


```
Ubuntu
*Advanced options for Ubuntu
Memory test (memtest86+)
Memory test (memtest86+, serial console 115200)
```



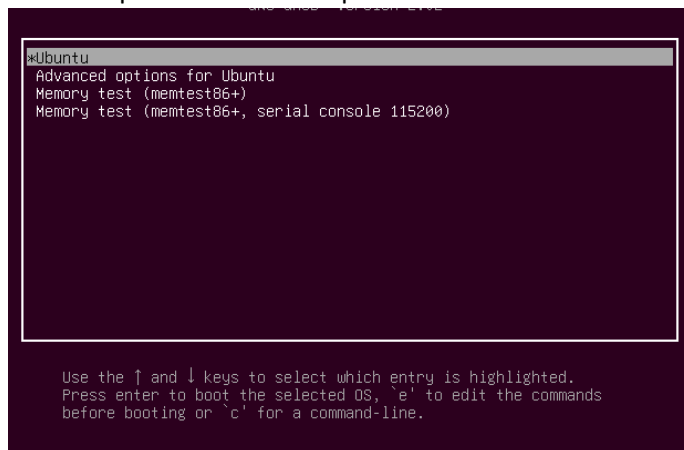
```
Ubuntu, with Linux 5.4.0-84-generic
*Ubuntu, with Linux 5.4.0-84-generic (recovery mode)
```

Ici on choisit root.



Attention : Normalement un mot de passe n'est pas demandé. S'il est demandé suivez l'étape suivante, sinon, passez l'étape.

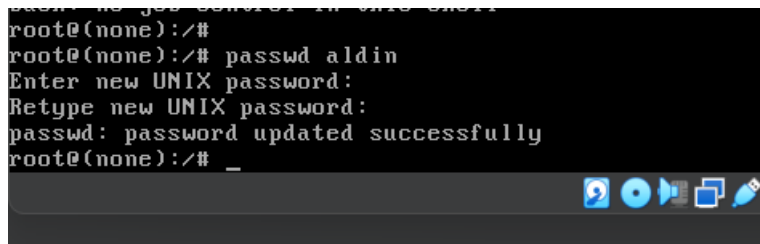
On choisit « resume » et on refait les étapes pour revenir dans les options de démarrage mais cette fois on tape le bouton « e » pour éditer les commandes de booting.



Ici on remplace *ro quiet splash \$vt_handoff* avec *rw init=/bin/bash*. Puis on tape F10 pour lancer la console.



Dans la console on écrit *passwd* **NOMUTILISATEUR** et puis on tape notre nouveau mot de passe. Après finir on redémarre l'ordinateur parce que je ne sais pas comment fermer la console ici.



```
root@(none):/#  
root@(none):/# passwd aldin  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@(none):/# _
```

Maintenant on peut se connecter à notre utilisateur avec le nouveau mot de passe.

L'extrait du Mr.Robot :

Dans le vidéo on voit un homme qui réinitialise le mot de passe d'un PC qui n'est pas à lui. Mais comment il a fait ça ?

Il fait la même chose qu'on a fait pour réinitialiser le mot de passe d'un utilisateur sous Windows.

Il lance l'ordinateur depuis la clé USB, contient d'une .iso du système, qu'il a inséré dans le PC. Depuis la clé il lance le « Startup repair » pour accéder les fichiers de Windows. Pour nous c'était le « Repair your computer ». Là il renomme la console (cmd.exe) en sethc.exe qui est probablement un programme qui s'exécute avant se connecter à un utilisateur. Après ce changement il démarre le PC et presse un bouton qui lui permet de lancer sethc.exe qui est maintenant la console. Dans la console il écrit *net user* pour voir les utilisateurs sur ce PC. Il choisit un utilisateur et change son mot de passe. Après il peut accéder au compte de cet utilisateur.

Conclusions :

On a appris qu'il existe des failles dans la sécurité de Windows, un système bien populaire, ce que veut dire que beaucoup des ordinateurs, surtout les ordinateurs personnels, sont potentiellement en danger. Même avec le meilleur mot de passe du monde on n'est pas protégé parce qu'il est possible d'effacer le mot de passe complètement. Ce qu'il faut faire est donc pas seulement protéger son compte de Windows mais l'ordinateur en lui-même. Le problème était qu'il est possible d'accéder des outils avec des droits administrateur quand on accède Windows. Mais si on protège l'ordinateur déjà avant lancer Windows ?

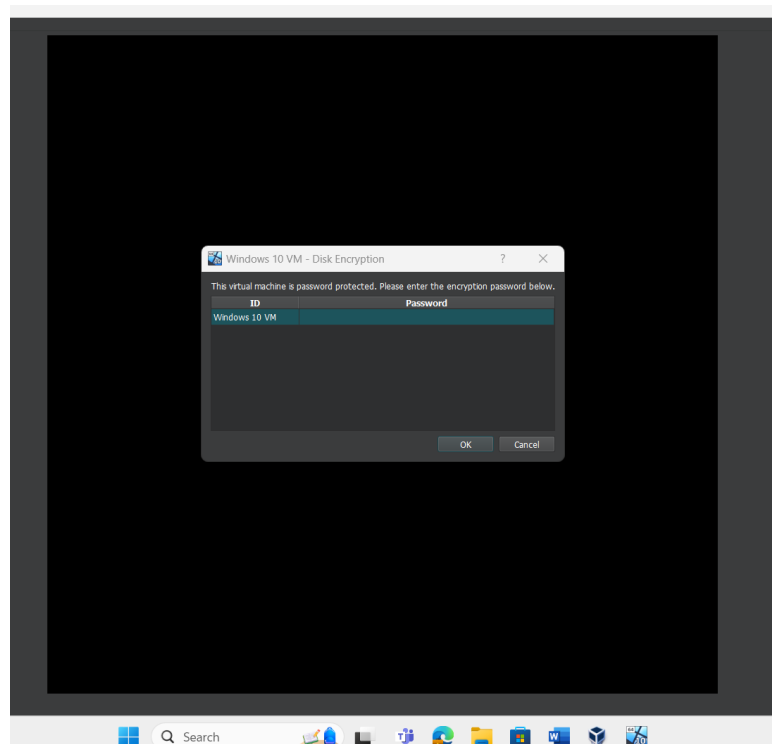
Comment se protéger :

Il existe plusieurs moyennes de se protéger.

A)

Une possibilité est de chiffrer le disque dur. On peut utiliser un programme de chiffrement comme BitLocker ou VeraCrypt pour chiffrer et protéger notre disque dur avec un mot de passe. Cela veut dire qu'il faut ce mot de passe pour accéder l'ordinateur même si on lance l'ordinateur depuis une CD ou une clé USB. En dessous on voit ce qu'il se passe quand on essaie d'accéder l'ordinateur.

Si vous utilisez une machine virtuelle vous pouvez également chiffrer et protéger la VM avec un mot de passe depuis votre hyperviseur.



VM chiffré dans VirtualBox

B)

Une autre solution serait de protéger son BIOS avec un mot de passe. Dans cette solution il faut ce mot de passe pour passer le BIOS et allumer l'ordinateur.



C)

Une autre solution serait de bloquer les clés USB et les CDs depuis une fonction de BIOS.

Malheureusement cette solution n'est pas optimale parce dans ce cas on ne peut pas utiliser des clé USB et CDs nous-même.