AKALAN Selim
1BTS SIO

TP Intrusion simple Windows – Bloc 3 – AKALAN Selim

Sommaire

Intrusion simple Windows 10(pro) via utilman.exe.

- Pour commencer, nous installons Windows 10(pro) sur notre VM (machine virtuelle).
- Lors de l'installation, arriver sur la 2ème page de l'installation, nous voyons une icône « Réparer l'ordinateur ».
- Cliqué sur « Réparer l'ordinateur ».

Figure 1 : en bas de la page lors de l'installation de Windows, suivre les figures suivantes.

- Choisir l'option « Dépannage ».

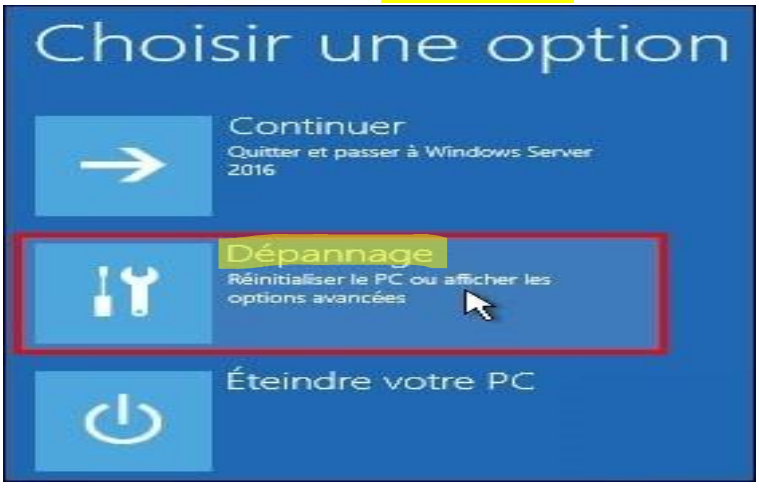

Figure 2

- Choisir l'option « Invite de commandes ».

Figure 3

- Aller dans le dossier « Windows\System32 » :

-c :

-cd Windows

-cd System32

- Créer une sauvegarde du fichier Utilman :

-copy Utilman.exe Utiman.exe bak

- On remplace maintenant Utilman par une simple Invite de Commandes « cmd ».

– copy cmd.exe Utilman.exe

- Confirmer l'écrasement par « O » ou « Oui ».

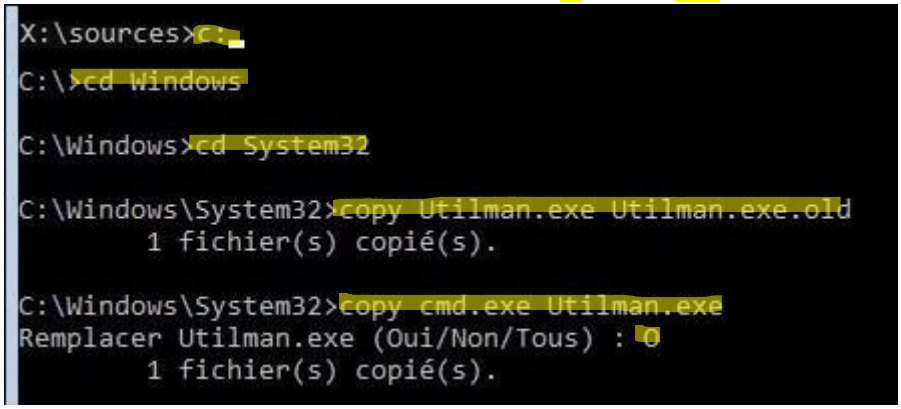

Figure 4

- Valider par « Entrée » et fermer cette commande.
- Cliquer sur « Redémarrage »
- Un redémarrage du PC sera effectué et Windows se charge normalement jusqu'à l'écran du mot de passe oublié.
- Ici, cliqué sur « Option d'ergonomie » pour ouvrir une « Invite de commandes ».

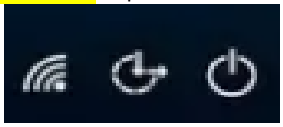

Figure 5 : en bas à droite lors du démarrage du PC.

- Une fois l'invite de commande est lancer, écrire la commande suivante pour modifier le mot de passe d'un compte utilisateur / administrateur local :

– net user « Utilisateur » « Nouveau MDP »

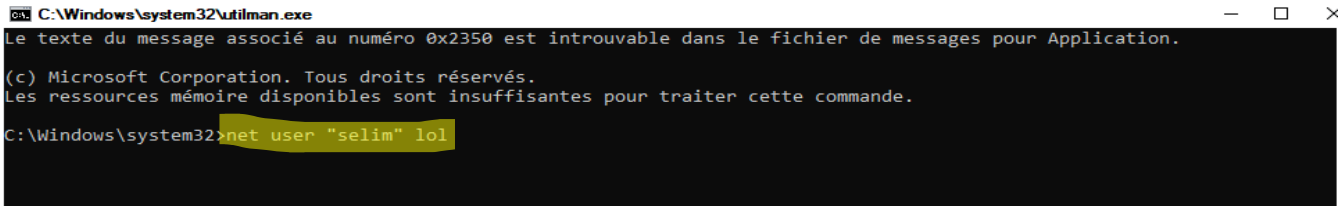

Figure 6 : l'invite de commande pour modifier le mdp.

- *Félicitation vous avez « cracker » le mot de passe, ou modifier le mot de passe car suite à cette étape lorsque vous vous reconnectez à votre PC vous tapez le mot de passe que vous avez choisi, pour moi ça sera « lol » l'essentiel c'est d'avoir réussi.*

Récupérer les données avec Ubuntu.

- Pour commencer, crée votre dossier et l'enregistrer sur le bureau de votre PC. Eteindre ensuite votre VM.

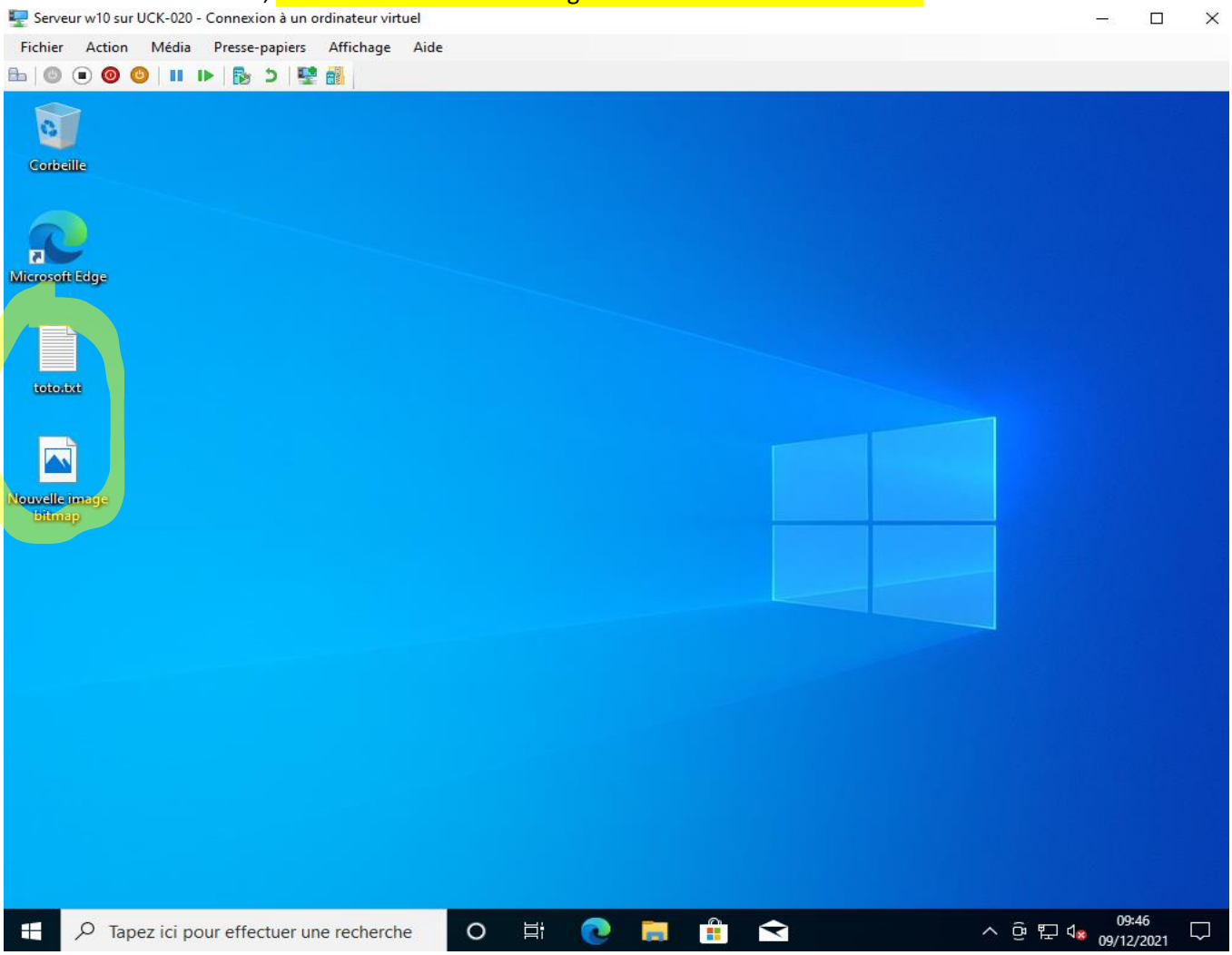

Figure 7 : les deux fichiers a enregistré dans le bureau et suivre les étapes suivantes

- Installer sur notre VM le fichier d'installation de Ubuntu (.ISO).
- Aller sur les paramètres de la VM → Lecteur de DVD → Support : Fichier image, cliqué sur « Parcourir » et choisir le fichier « iso » de Ubuntu 20.04.1, « Appliquer » et clic sur « OK » et fermer les paramètres.
- On va ensuite dans l'onglet BIOS → vérifier que le Bios est sur « CD ».

- (⚠ Si un problème apparaît lorsque vous essayer de lancer votre VM, penser fermer hyper-V et relancer votre VM. ⚠)

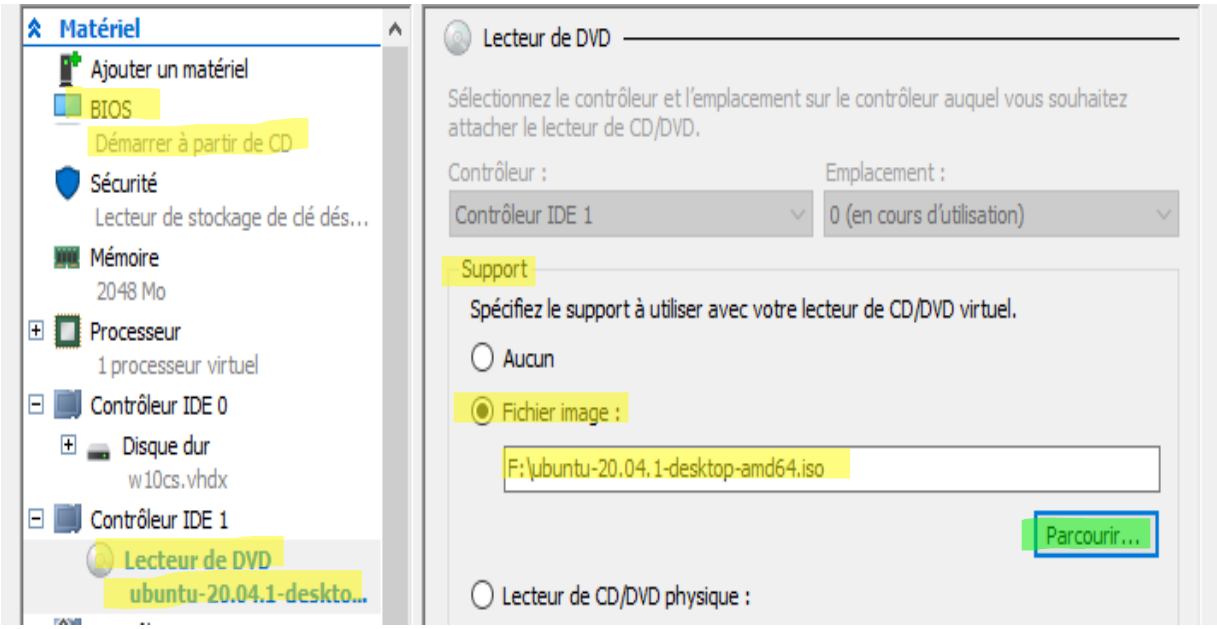

Figure 8 : paramètre de la VM.

- Donc Ubuntu est installée et lancée, on arrive sur la page d'accueil pour l'installation Ubuntu → choisir la langue → cliquer sur « Try Ubuntu », vous arrivez sur cette page, aller sur le dossier « Ubuntu ».

Figure 9 : bureau de Ubuntu

- Cliqué en bas à gauche sur « + Autres emplacements » → choisir le disque dur « Volume de 34 GB ».

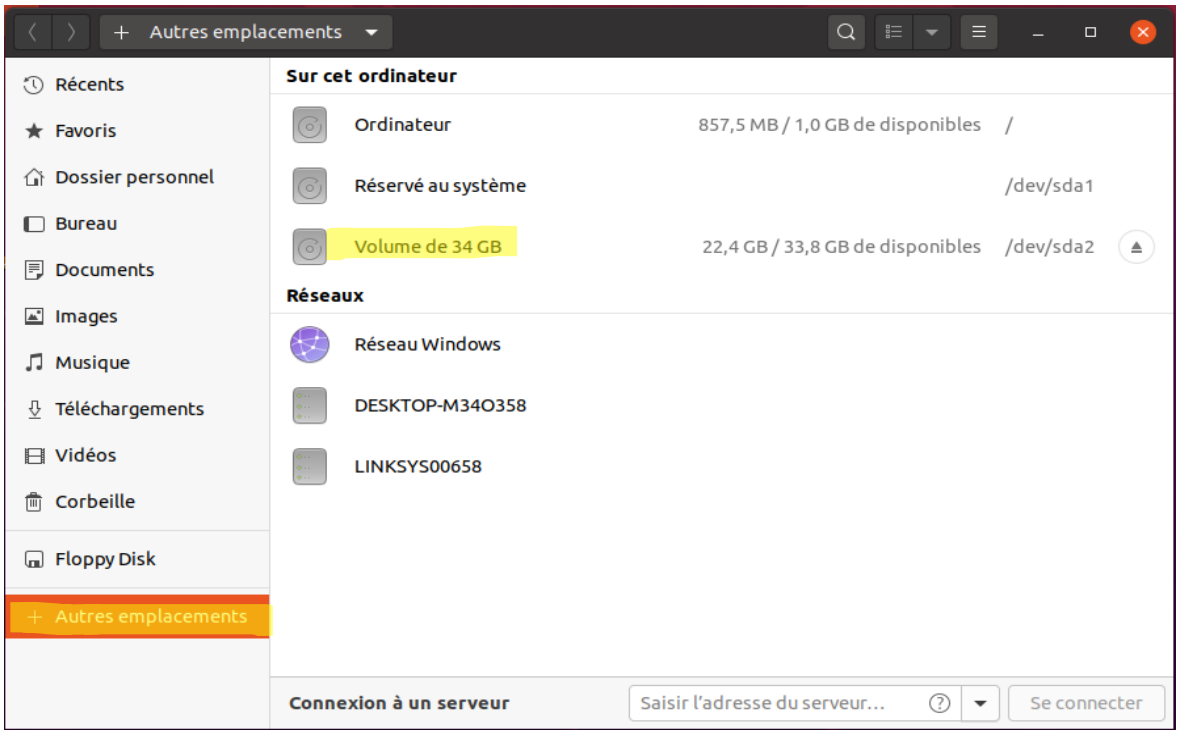

Figure 10 : le dossier Ubuntu.

- Une fois sur cette page, on clique sur « Users ».

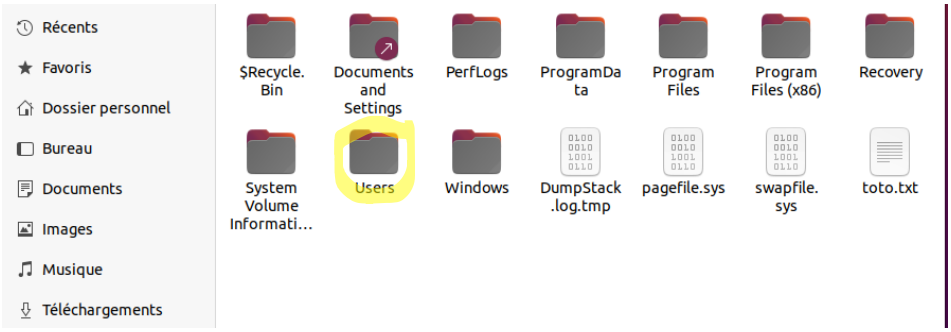

Figure 11

- Ici nous constatons qu'il y a tous les fichiers de notre VM enregistré, nous voyons un dossier avec le nom de notre VM, pour mon cas, je clique sur le dossier « Selim » afin de récupérer les données de ma VM.

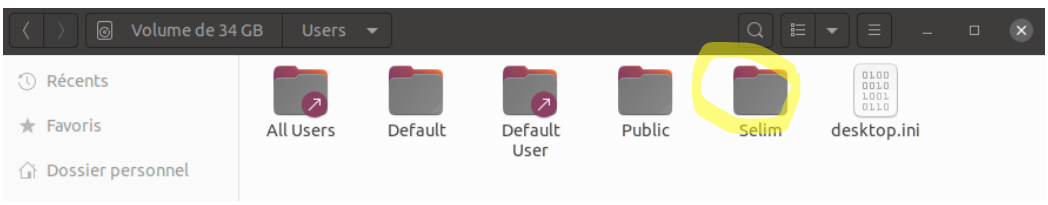

Figure 12

- Choisir « Desktop » (bureau) pour cette étape, pour qu'on puisse accéder au dossier enregistré dans le bureau de notre VM.

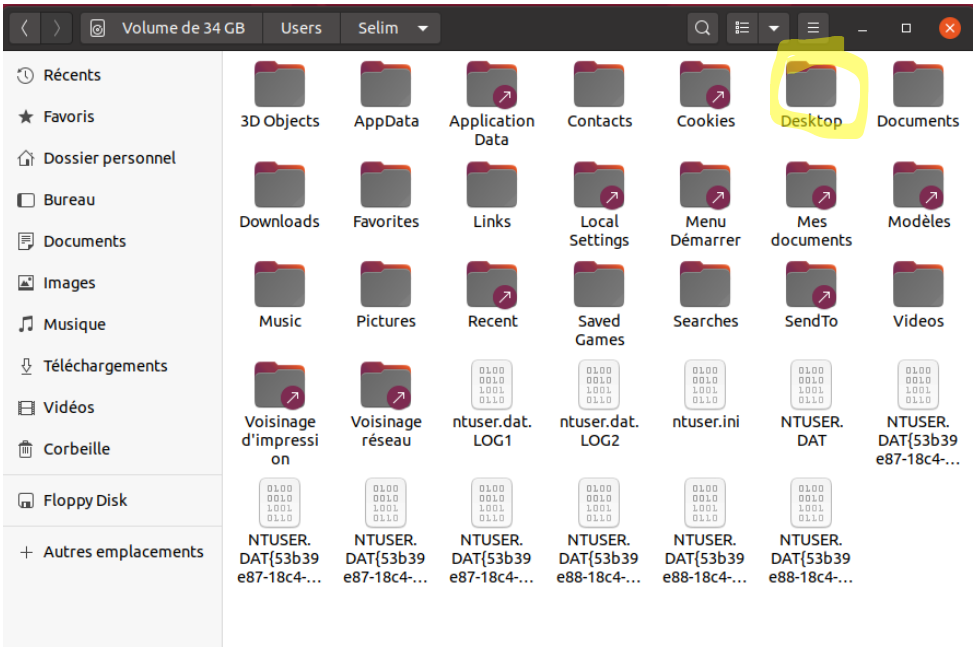

Figure 13

- Nous constatons que nous pouvons accéder à notre document enregistré sur notre bureau et voir le contenu de celui-ci en lecture seule, on peut le copier sur le bureau de cette session pour le modifier.

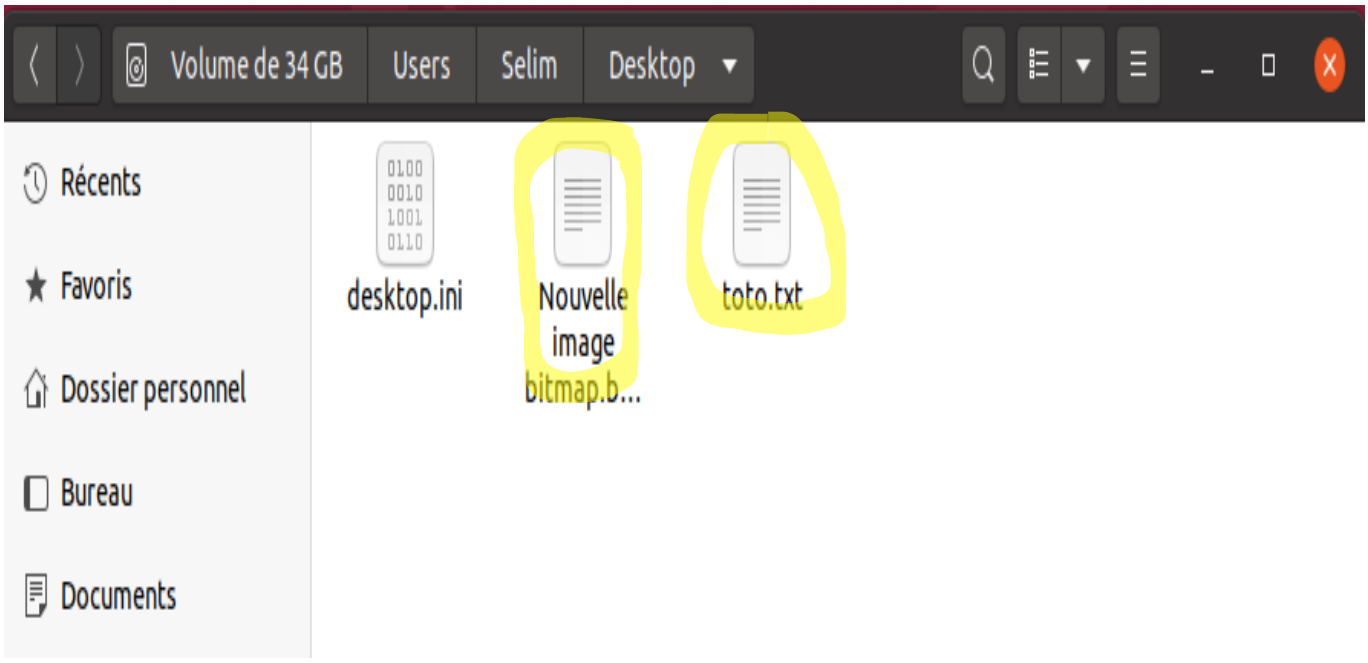

Figure 14 : les deux fichiers qui étaient enregistrés sur W10.

Conclusion.

- Comme nous pouvons le constater la sécurité est très faible, il faudra trouver des solutions pour que cela soit plus sécurisé et il y a plusieurs solutions :
- Protéger son bios avec un mot de passe,
- Chiffrée son disque dur avec un BitLocker,
- Choisir la 2éme génération lors de l'installation de Windows.

Protection face aux attaques.

(⚠ATTENTION ! SI vous lancez cette procédure, le disque sera chiffré cela veut dire que si vous perdez votre clé de récupération ou le mot de passe de votre session toutes les données seront inutilisables même si une personne externe essaye d'accéder à vos données personnelles⚠).

- On commence, aller sur → Démarrer → Panneau de configuration → Système et sécurité → Chiffrement de lecteur BitLocker → Activer BitLocker.

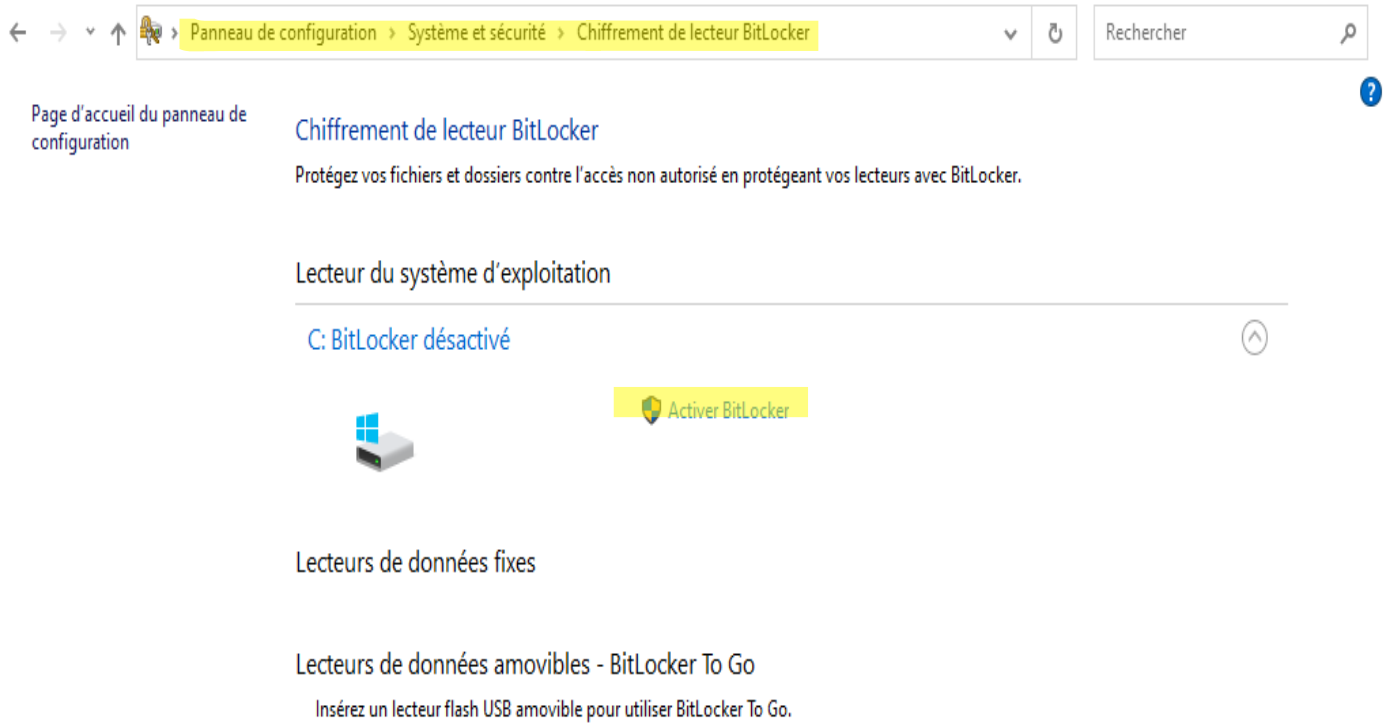

Figure 15 : activation du BitLocker

- Il y a deux choix : « Insérer une clé USB » et « Entrer un mot de passe ».
- Pour cette étape je choisis le mot de passe.

Figure 16

- Entrer le mot de passe que vous souhaitez pour protéger le BitLocker.

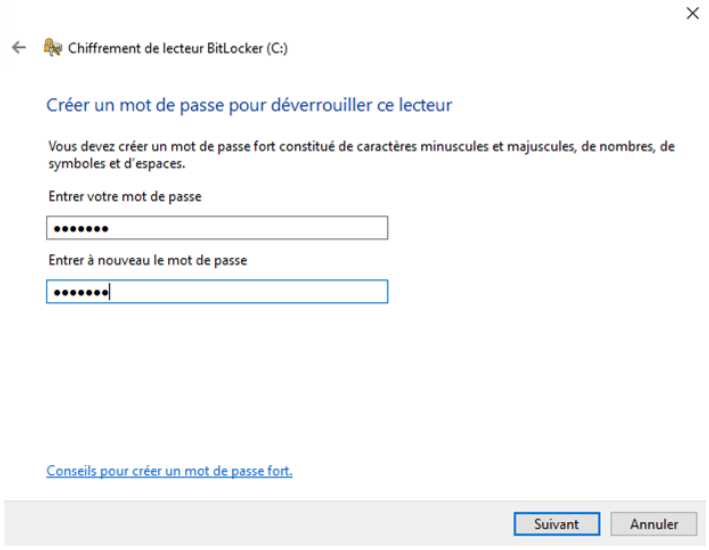

Figure 17 : choisir le mdp pour le BitLocker

- Choisir « Enregistrer dans un fichier » et « imprimer la clé de récupération » un PDF sera à récupérer.

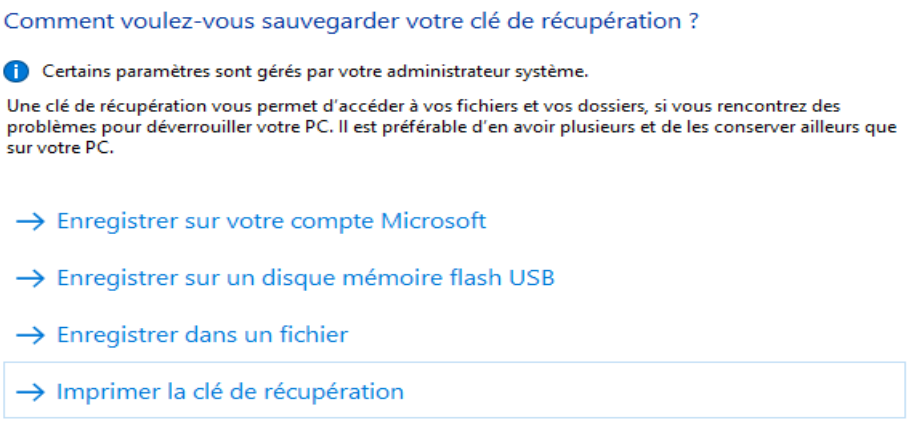

Figure 18

- Il faut l'enregistrer sur un lecteur amovible, une clé USB par exemple.

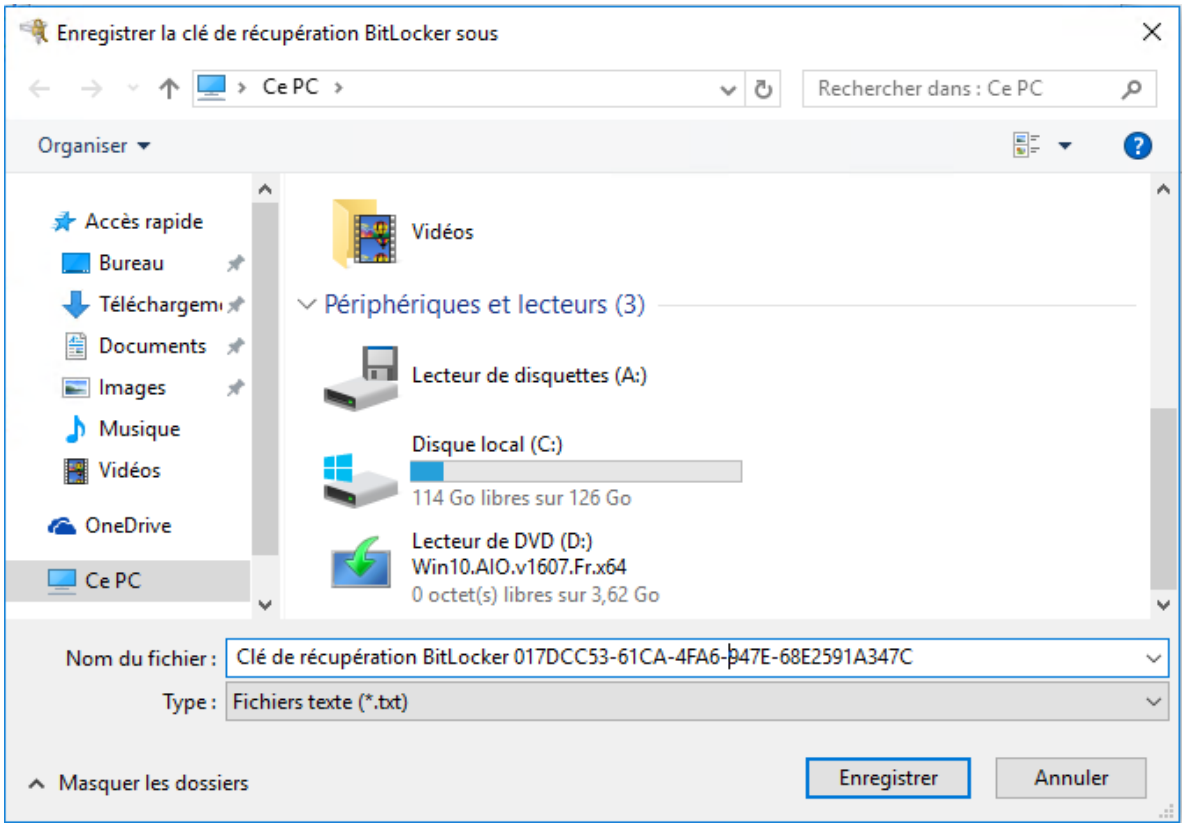

Figure 19

- Voici le PDF avec notre identificateur et notre clé de récupération.

Clé de récupération du chiffrement de lecteur BitLocker

Pour vérifier qu'il s'agit de la clé de récupération appropriée, comparez le début de l'identificateur suivant avec la valeur d'identification affichée sur votre PC.

Identificateur :

29FF4852-E8DF-4AD2-87D1-608B5282B219

Si l'identificateur ci-dessus correspond à celui affiché sur votre PC, utilisez la clé suivante pour déverrouiller le lecteur.

Clé de récupération :

449746-293667-443388-091729-240515-114147-617584-430331

Si l'identificateur ci-dessus ne correspond pas à celui affiché sur votre PC, cette clé ne permet pas de déverrouiller le lecteur.
Essayez une autre clé de récupération ou accédez à https://go.microsoft.com/fwlink/?LinkID=260589 pour obtenir une aide supplémentaire.

Figure 20

- Voici l'image sur laquelle nous tombons lorsque l'on souhaite suivre la méthode de l'intrusion à Windows et changer le mot de passe, le BitLocker est bien configuré donc nous sommes sécurisées des personnes malveillantes.

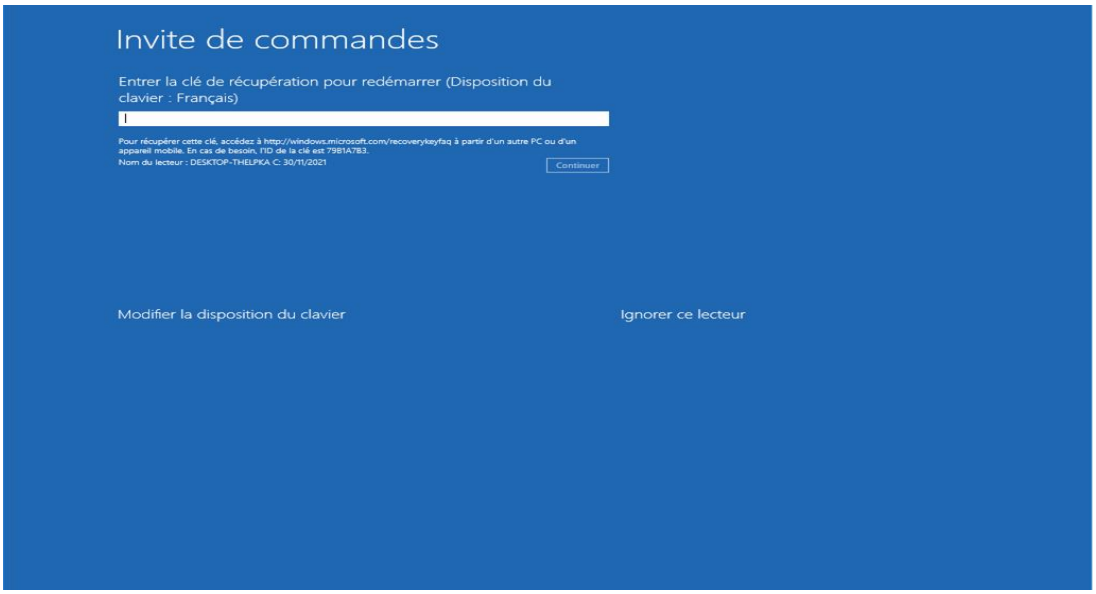

Figure 21

- Cette procédure peut être effectué sur Linux et Mac Os.
- Le lien qui nous permet d'avoir le tuto pour Linux est : https://guide.ubuntu-fr.org/desktop/user-forgottenpassword.html

Le lien qui nous permet d'avoir le tuto pour Mac Os est : https://www.debutersurmac.fr/mac-os-x-2/mac-os-x/comment-retrouver-le-mot-de-passe-principal-de-mon-mac/

- Sur l'image ci-dessous nous voyons un exemple de réinitialisation du mot de passe sous Ubuntu.

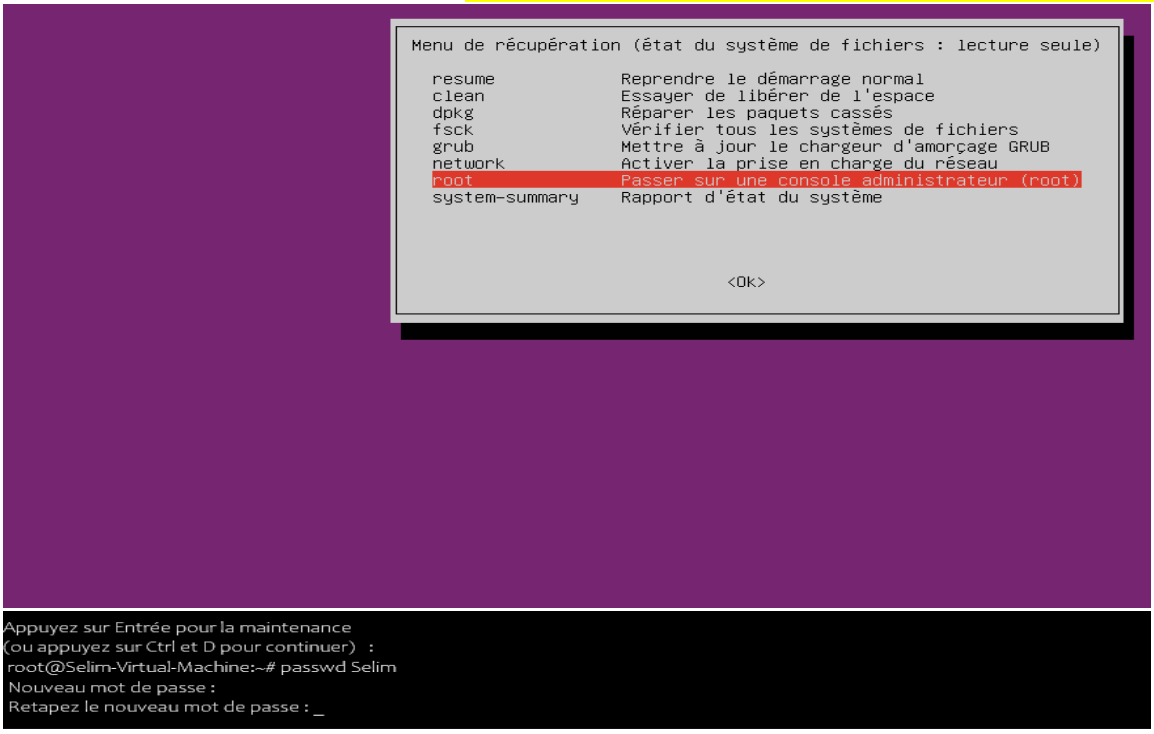

Figure 22

Mise en place du mot de passe BIOS.

- Cette sécurité s'effectue lors du démarrage de l'ordinateur (Impossible sur un VM).
- L'image ci-dessous est une représentation du Bios
- Pour accéder au Bios cela dépend de la marque de votre PC, renseignez-vous sur internet pour savoir comment accéder au bios de votre PC.
- Donc pour effectuer une sécurité de notre ordinateur suivait les étapes suivantes :

➔ Aller sur l'onglet « Security » → « Set Supervisor Password » → « Enter New Password » pour mettre un mot de passe de sécurité au bios.

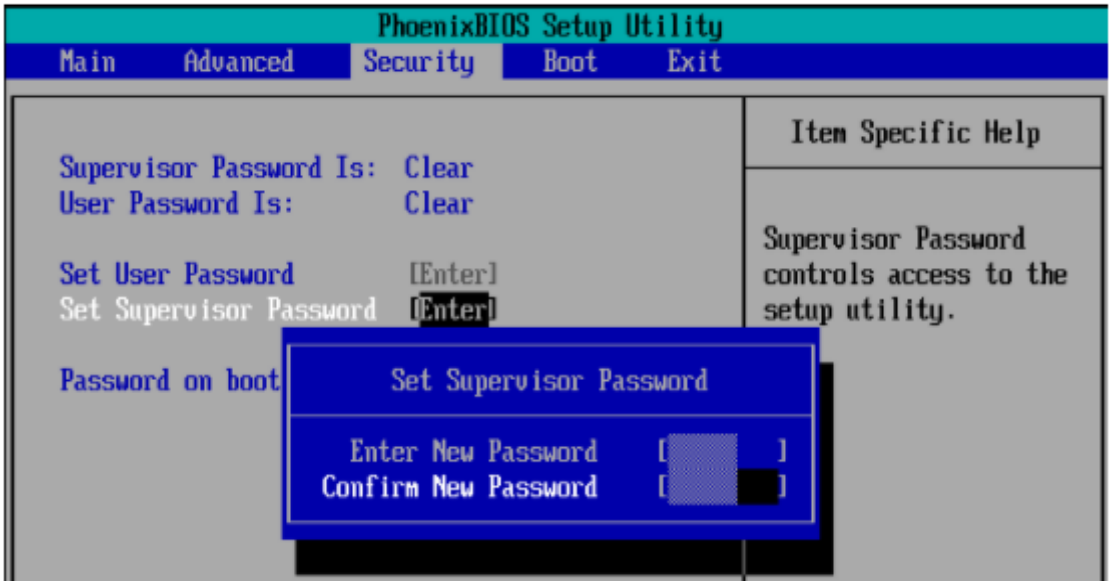

Figure 23 : paramètre du Bios

➔ Aller sur l'onglet « Security » → « Password on boot » → « Enabled » afin que le système mis en place demande un mot de passe lors du démarrage du PC pour être en toute sécurité et être protégé.

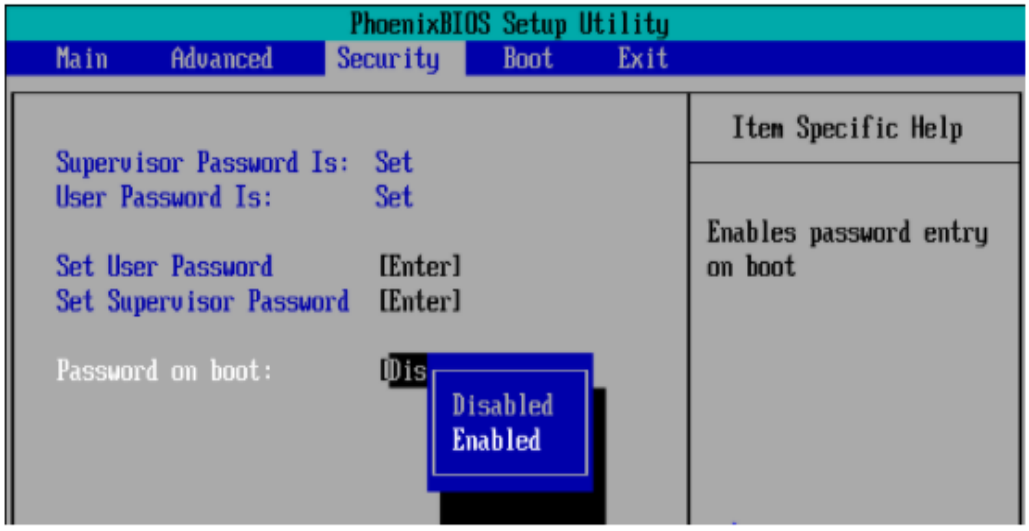

Figure 24

- Enregistré la configuration et quitté le Bios :

➔ « Exit » → « Exit Saving Changes » → « Yes ».

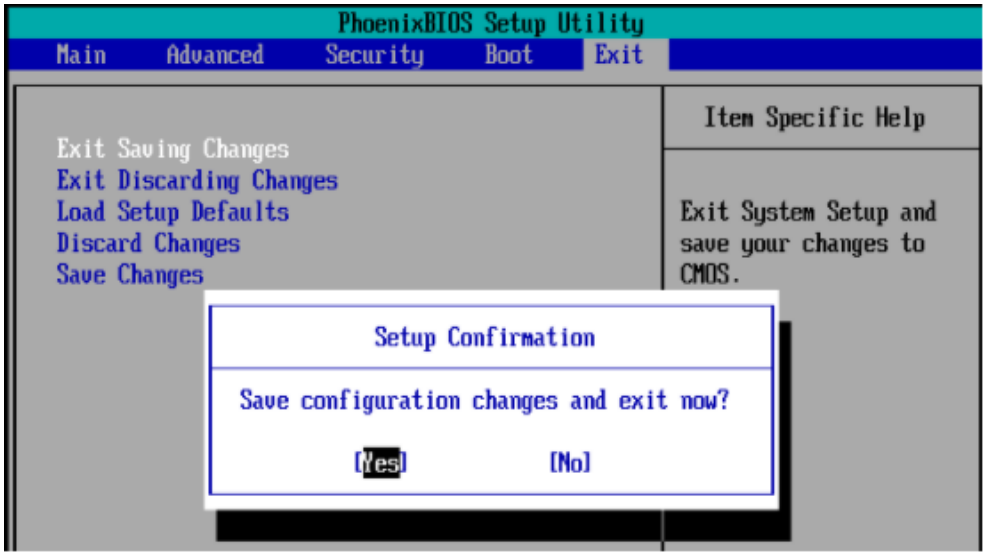

Figure 25

- Lorsque l'on démarre notre PC, nous voyons qu'un mot de passe est demandé.

Figure 26 : le mdp du Bios mis en place.

Conclusion.

- On peut en conclure qu'avec ces sécurités nous sommes protégés face aux attaques, cela ne veut pas dire que nous sommes protégés à 100%, l'informatique est une technologie avec toujours une faille disponible, mais les étapes précédentes nous protègent contre de nombreuses attaques.

(⚠ Les numéros en gris sur le côté droit de certaines pages, ce sont les indications des différentes étapes inscrit dans le sommaire. ⚠)