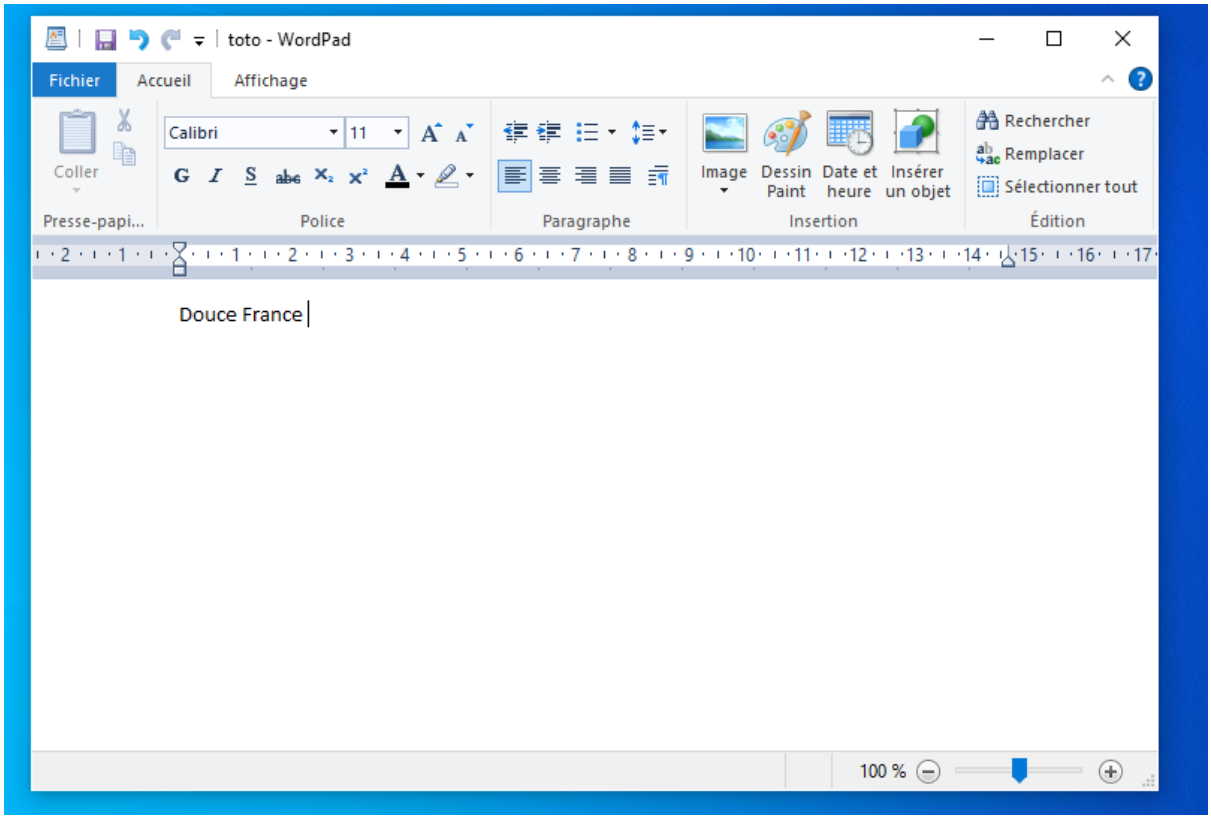
TP2-Mewo-SISR2-KLEIN Vincent

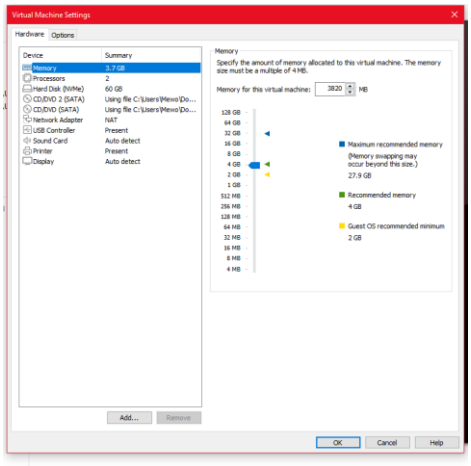
Mettons-nous en condition

J'ai fait un Fichier Toto.txt avec un bloc note

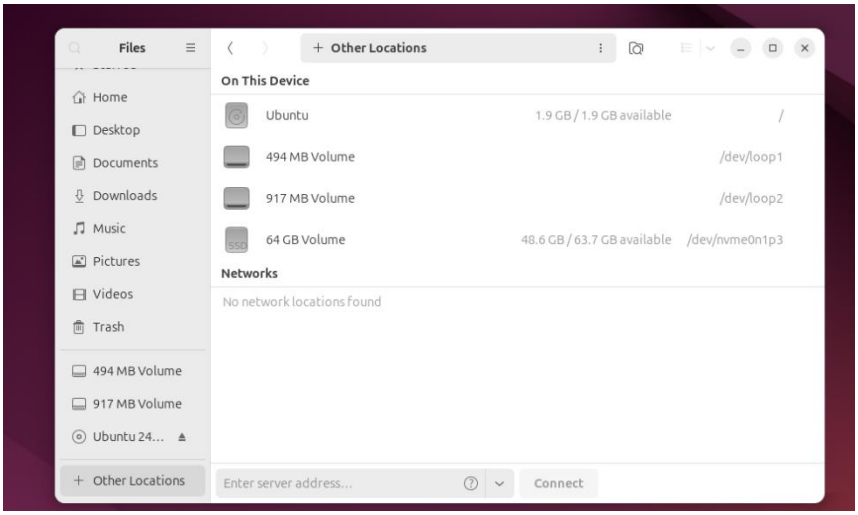


Continuer notre expérience

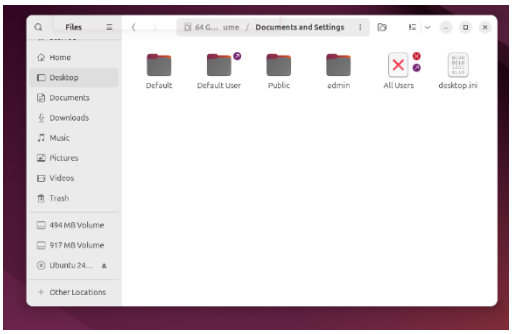
Pour boot un système linux sur notre VM Windows 10 Il faut ouvrir les settings



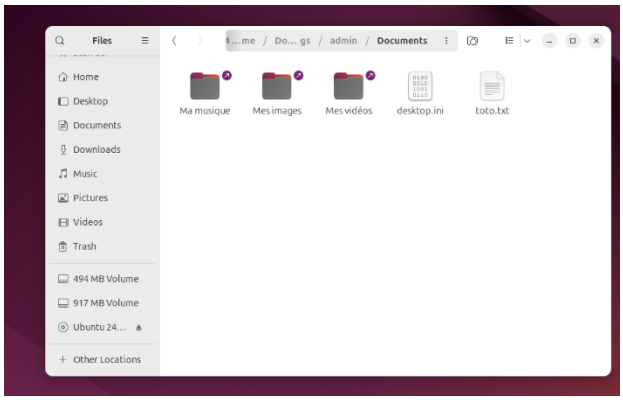
Puis aller dans option et changer le Work dictory (attention il faut être en BIOS car UEFI intègre des systèmes de sécurité plus élaboré) et mettre le chemin d'accès à l'image ISO du système linux à utiliser

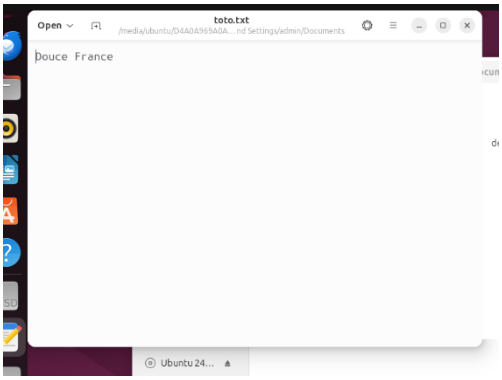


Appuyer sur Other location et le disc 64



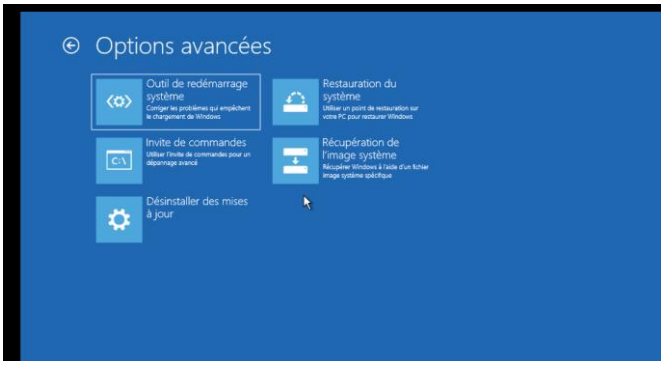
Aller sur les répertoires admin et documents et là on l'a



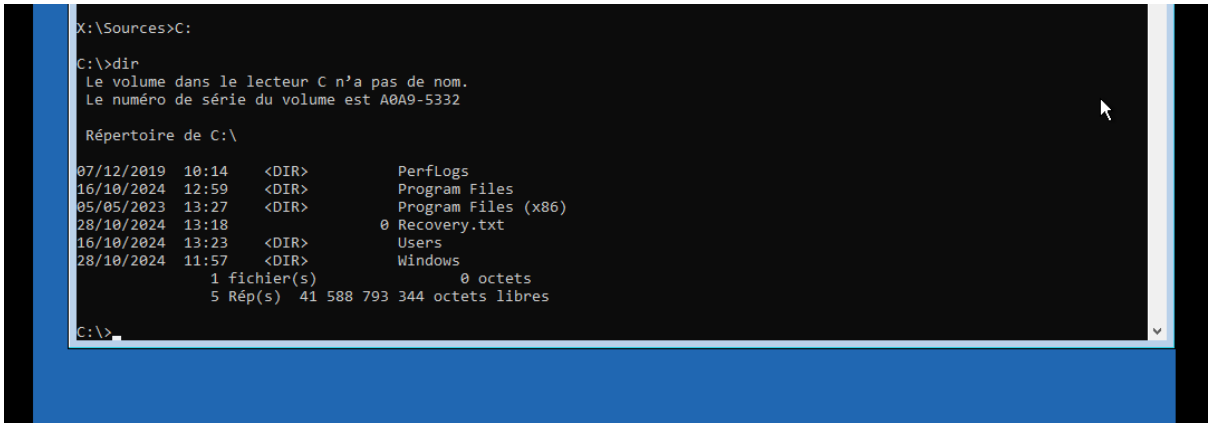


Pour la récupération de mot de passe je vais utiliser la méthode 2 b en utilisant la faille Windows

Etape 1
Je commence à faire réparer l'ordinateur ce qui me permet de pouvoir avoir accès à l'invite de commande à la suite d'avoir cliqué sur dépannage.

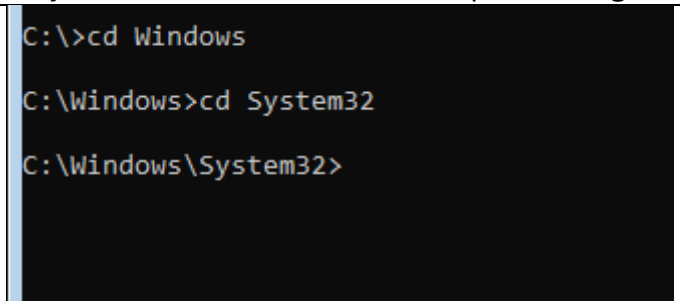


Etape 2
On doit mettre la ligne de commande C: pour accéder au disque dur

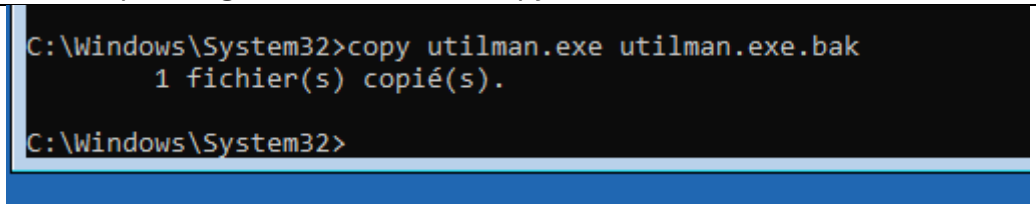


Etape 3

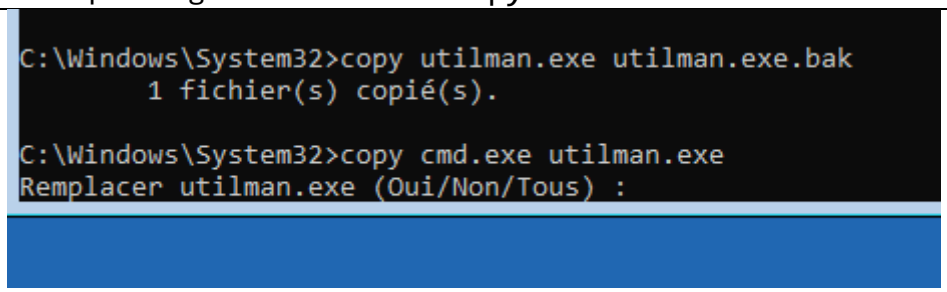
Mettre la ligne de commande cd windows puis cd System 32 (pour rappel cd veut dire change directory c'est une commande utiliser pour changer de répertoire)



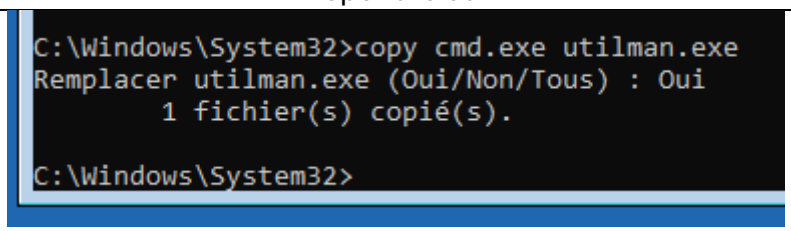
Etape 4
Taper la ligne de commande copy utilman.exe utilman.exe.bak



Etape 5
Taper la ligne de commande `copy cmd.exe Utilman.exe`



Etape 6
Répondre oui



Etape 7
Redémarré l'ordi en appuyant la touche Windows et U
Normalement ça affiche une invite de commande

Chez moi ça n'a pas marché il fallait relancer une installation qui au passage ne marcher pas. J'ai installé une VM Windows 7 et réinstaller un VM Windows 10 pour mes autres cours

Avec Windows 7 pour accéder au CMD au lieu des option ergonomique il faut spammer la touche F2 et reset la configuration data ça reprend l'installation. Ne faut pas démarrer l'installation faut clique sur réparer son ordinateur

C’est une réelle découverte qui peut servir si on a besoin

C’est génial ces techniques nous permet de faire tellement de chose plus ou moins bien, plus ou moins légal comme redonner accès au session a des utilisateur ayant oublié leur mot de passe mais aussi donné accès à la session admin, donner plus de pouvoir de configuration de l’ordinateur, à des personnes malveillante

Enfin

-Ces techniques permet 2 utilisations d’un compte utilisateur ou admin :

_La légal pour redonner l’accès au compte utilisateur/admin au personne qui ont oublié leur mot de passe utilisateur/admin ou pour réparer un ordinateur dont on n’a pas le mot de passe utilisateur/admin. Et puis l’accès au terminal sans entrer dans une session utilisateur et admin doit permettre surement de faire des réparations

_La illégal pour récupérer de la data (des données en français) comme voulait faire Elliot dans cet extrait de la Saison 4 épisode 3 de la série Mr.robot. Ainsi que d’ajouter du code malveillant en rentrant sur la session admin

-On peut peut-être mettre une multi authentification. Le principe d’une multi authentification comme la double authentification permet à l’utilisateur qui veut se connecter de recevoir sur un autre compte (email, SMS…) un code à retranscrire. Si on n’a pas accès au téléphone et au mail on ne peut pas retranscrire le code et ça en bloque l’accès.

Voici comment activer la double authentification selon le centre d’aide de Windows (https://support.microsoft.com/fr-fr/account-billing/proc%C3%A9dure-d-utilisation-de-la-v%C3%A9rification-en-deux-%C3%A9tapes-avec-votre-compte-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4)

Etape 1 Connexion au compte Microsoft

Etape 2 Allez dans la rubrique option de sécurité avancé

Etape 3 Activez la double authentification

Comme autre méthode j’ai choisi le chiffrement du Bios avec BitLocker

Etape 1 Installer Bitlocker après l'avoir mis dans le server manager

Etape 2 Désactiver le TPM

Etape 3 Ouvrir les parametre de machine et crée une disquette bitlocker.flp

Etape 4 Formater la disquette

Etape 5 Lancer une fenêtre DOS avec la commande cscript c:WindowsSystem32manage-bde.wsf -on C: -rp -sk A: Pour avoir les droits admin

Etape 6 Vérifier que dans le bios « Removable Device est bien en dernière position dans la liste

Etape 7 Relancer la machine

Etape 8 Dans le panneau de configuration lancer Bitlocker Drive Encryption

En cas de problème on peut utiliser l'outil Microsoft Bitlocker Drive Tool Preparation

J'ai voulu essayer les 2 méthode en installant Windows 10 sur une VM de mon ordinateur perso mais ce n'était pas la même version que j'ai installé en cours. J'ai installé la version professionnel N. Il me demande de me connecter via mon compte Microsoft et ils mettent une autre sécurité nativement via un code PIN. Donc si on n'a pas le code pin on n'a pas accès à l'ordinateur. Pour moi la plus simple des méthodes reste la double authentification mais il reste une faille c'est si le pirate ou le réparateur a accès au SMS ou à la boite mail de l'utilisateur ça lui donne quand même accès au compte. Toutes les méthodes ont une faille sinon personne ni même l'utilisateur aurait accès à son compte

- On a la même faille sur linux on doit appuyer sur la touche e au démarrage pour afficher le terminal. J'ai essayé sur une VM Kali, comme je veux essayer cet OS avant la fin du support de Windows 11, pour voire si Linux est mieux que Windows pour moi. Je ne suis pas encore arrivé ma VM continue son démarrage normal

Petit plus sur les méthodes de craquer un mot de passe

Source : https://www.youtube.com/watch?v=YI-6nZFxwNg

https://www.youtube.com/watch?v=1J_qJfRPv-g

https://www.presse-citron.net/10-outils-utilises-par-les-hackers-pour-cracker-les-mot-de-passe-ou-comment-mieux-securiser-les-votres/

https://www.leblogduhacker.fr/se-proteger-des-6-tech-pour-trouver-un-mot-de-passe/

Attaque brute de force

La plus simple tester toutes les combinaisons possibles mais ça peut être long et difficile surtout si l'utilisateur a mis un bon mot de passe. Il y a aussi des algorithmes comme partagé sur Github qui permet d'accéléré cette méthode. La parade le reCAPTCHA qui détecte par exemple si c'est un humain ou un robot clique sur le reCAPTCHA sans image ni lettre à retranscrire. Mais toutefois selon ma deuxième source des comptes arrive encore à se faire cracké avec ce procédé comme le compte de Théresa May ancienne première ministre britannique. Avec cette source de prévention on apprend l'ancien code secret de la bombe nucléaire américaine (qui au passage était très simple, ce qui représente un certain gros danger pour tous on peut demander au japonais ce que peut produire de se prendre une bombe nucléaire), le mot de passe du compte admin de Facebook…

La troisième source liste 10 logiciels pouvant être utilisé pour les crackeurs

La social enginerie (ingénierie sociale en français) est une technique visant à manipuler des gens pour qu'ils puissent en pansant faire du bien divulguer le mot de passe ou de la data sensible. Il faut sensibiliser sur ce grand risque d'ordre humain. Si

on donne son mot de passe il est bien, comme dit la quatrième source, de le changer. Une autre façon de s'en protéger c'est de se méfier des gens que l'on ne connait pas. Le Phishing est un exemple de ce procédé rendre un mail attrayant pour que l'utilisateur clique sur les liens d'un faux site pour qu'ils mettent son mot de passe.

Les malwares

Avec un malware de type keylogger le pirate reçoit tout ce que tape l'utilisateur. Les façons de s'en prémunir utiliser un logiciel anti keylogger, éviter de se connecter a son compte en dehors de son ordinateur, utiliser des clavier virtuelle.

Les tables Rainbow

C'est une méthode plus technique qui consiste à de nombreuse liste prés-hashé. Le hash est une technique de chiffrement à sens unique aucun algorithme peu revenir en arrière. Les tables rainbow sont comparable aux techniques brutes de force a différence que ce n'est pas en texte brute mais sur le principe du hachage. Il n'existe pas trop de moyens de s'en prémunir à part de mettre en place des mots de passe considéré comme fort et invulnérable à durée humaine (actuellement sans compter sur la puissance de calcul des ordinateurs quantiques car ce n'est pas des ordinateurs qui sont populaire, ca reste encore une technologie en phase de test)

Deviner le mot de passe

Parfois un indice se révèle lorsque qu'on a eu trop de saisi incorrect. Ainsi que les questions de sécurité. Pour s'en prémunir mettre des indices assez vaseux qui permet de définir qu'une partie du mot de passe ou ne pas mettre de la data qui peut être facilement retrouver tel que les noms de famille, son lieu de naissance, le nom de son animal de compagnie… La meilleure technique de création de mot de passe c'est la méthode de Monsieur Jobard, de prendre les paroles de sa musique préférée faire un pattern en remplaçant des lettre par des chiffres et des caractère spéciaux et de faire des petites modifications sur le pattern suivant le site sur lequel on est