TP– SYNTHÈSE INFORMER LES UTILISATEURS

Thomas Grzesinski

I.CYBERCAFÉ

Outil recommandé

Le responsable du cyber-café devrait *configurer un Proxy.*

Définition proxy: Un proxy est un serveur intermédiaire qui sépare les utilisateurs, des sites Web sur lesquels ils naviguent. Les serveurs proxy assurent différents niveaux de fonctionnalité, de sécurité et de confidentialité, selon votre type d'utilisation, vos besoins ou la politique de votre entreprise.

Utilisé un serveur proxy est idéale pour avoir une vision de sécurité plus avancé sur son réseau

PROXY

L’outil peut fonctionner de différentes façons:

-*En faisant une Liste de contrôle d’accès (ACL)*:Cette méthode permet d’intégrer dans une liste des sites qui sont autorisées a être accessibles ou non, généralement ces sites sont basés sur des adresses IP, des noms de domaines.

-*Du filtrage par URL*: Donner des motifs d’URL qui correspondent aux sites que vous souhaitez autoriser ou non

-*Filtrage basé sur les catégories*: Certains proxys utilisent une base de données de catégories de sites web. Vous pouvez choisir de bloquer ou d'autoriser l'accès à des catégories spécifiques de sites (par exemple, les réseaux sociaux, les sites de jeu, etc.).

PROXY

-*Contrôle d'accès basé sur l'utilisateur* : Certains proxys peuvent être configurés pour autoriser ou bloquer l'accès en fonction de l'utilisateur. Cela signifie que l'accès à certains sites peut être restreint en fonction des informations d'identification de l'utilisateur.

-*Filtrage basé sur le contenu* : Le filtrage basé sur le contenu peut être utilisé pour bloquer des sites en fonction du type de contenu qu'ils présentent. Par exemple, vous pouvez bloquer l'accès à des sites contenant du contenu pour adultes.

-*Journalisation et rapports* : Les proxys peuvent également enregistrer les activités, ce qui permet aux administrateurs de suivre les sites auxquels les utilisateurs accèdent. Cela peut aider à identifier les sites qui posent problème et à ajuster les règles en conséquence.

PROXY

L’avantage du proxy c’est qu’il peut donc *bloquer l’accées a certaines URL qui peuvent rediriger vers des sites ou se trouve un malware*.

Il peut notamment analyser le contenu de fichiers téléchargés, que ce soit aussi dans les pièces jointes ou par e-mails. Et si le fichier est malveillant le proxy va le bloquer

Il fait aussi des analyses heuristique ou ici la méthode consiste de détecter des comportements suspects qi pourraient indiquer la présence de malware. Cela peut inclure la surveillance des activités réseau ou la détection de modèles de comportement malveillant.

CONTRÔLE À DISTANCE DES POSTES

Contrôle des postes a distance

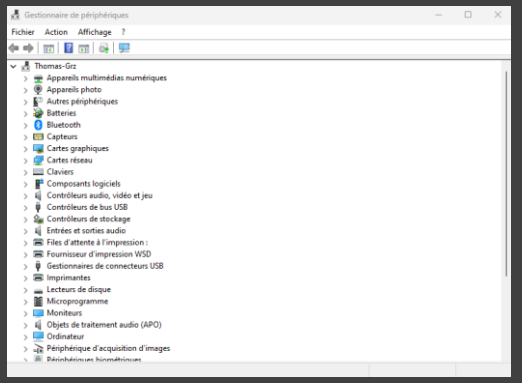
Il existe *trois méthodes* :

-*Première méthode* installer le logiciel *ManaEngine* ce logiciel peut:

-*Bloquer ou limiter l'utilisation des périphériques* (souris, lecteur de disque, CD-ROM, périphérique de stockage amovible, les disquettes, le Bluetooth, les images, les imprimantes, et les modem)

-*Prévenir des activités de téléchargement non autorisées ou la possibilité d'injecter un malware dangereux dans le réseau*.

-*Deuxième méthode* allez dans le « *gestionnaire de périphériques* » de votre machine
Et *cliquez sur le périphérique que vous souhaitez désactivez*

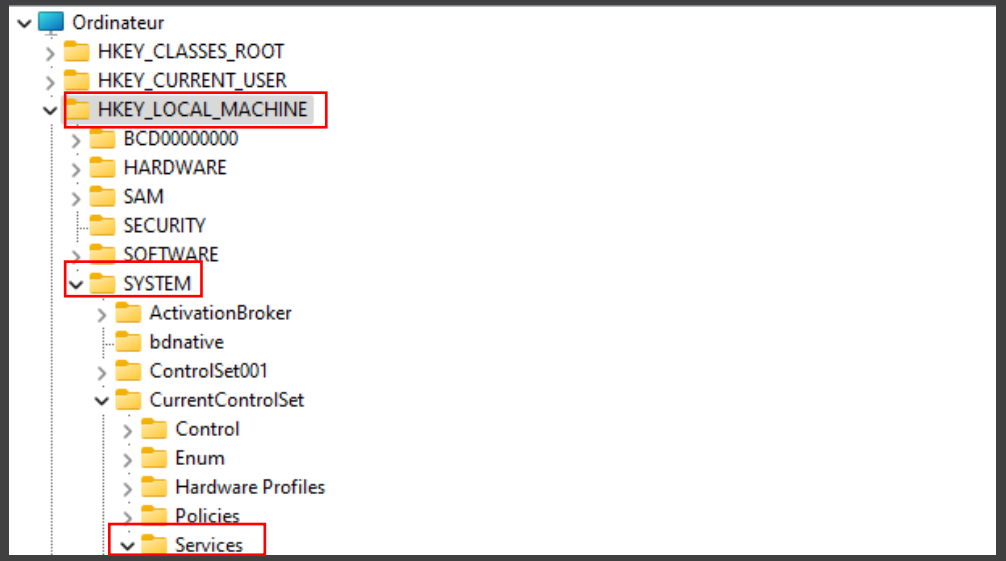


Contrôle des postes à distance

-*Dernière méthode* allez dans la barre de recherche Windows et tapez « *Regedit* »

Regedit est un fichier standard Windows, avec lequel vous pouvez exécuter l'éditeur de registre propre à Windows

Une fois que vous êtes dans Regedit suivez ce chemin :

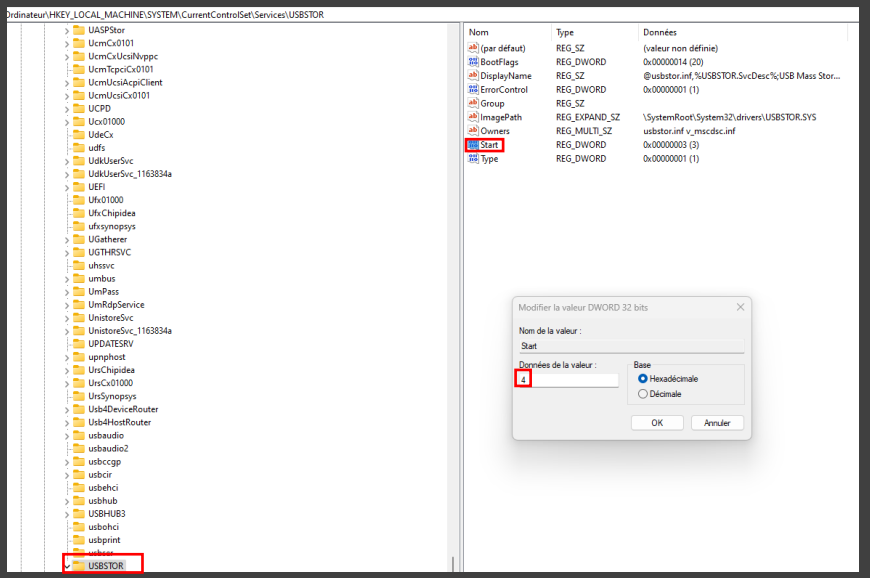


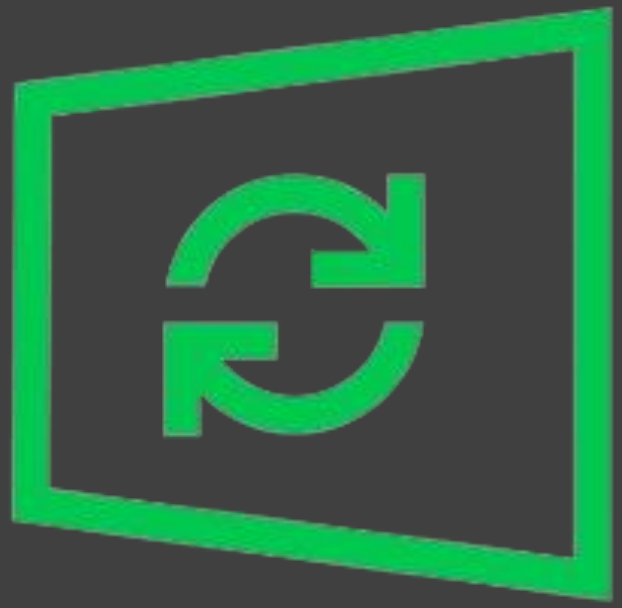
Contrôle des postes a distance

Allez jusque au *dossier USBSTOR* et cliquez sur « *Start* »et mettez-y la *valeur 4*.

La valeur 4 permet empêchera l'utilisation de clé USB au moment du redémarrage de votre PC, si vous voulez autoriser l'utilisation de clé USB insérer la valeur 3 et redémarrer votre PC

Pour que ceci reste permanent
Il faut faire en sorte que soit *effectué* depuis *le compte administrateur*, pour que *les comptes utilisateurs ne puissent pas modifier cette valeur*





WINDOWS UPDATE

Windows UPDATE

Pour avoir la dernière version du système d'exploitation Windows, il vous suffit d'allez dans

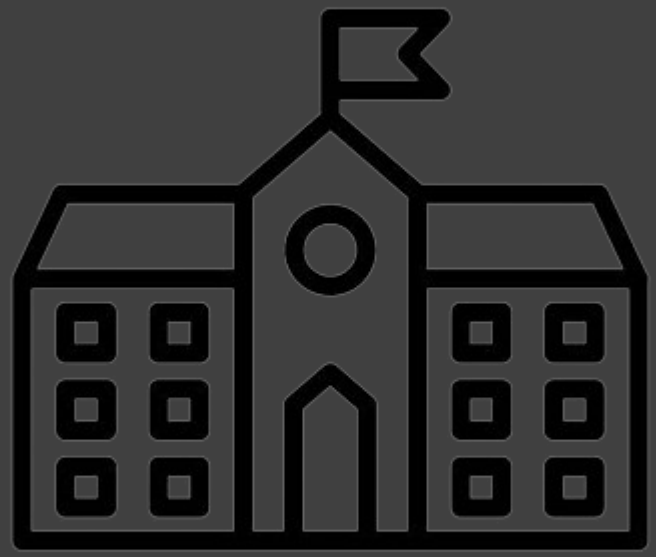
La barre de recherche *Windows > Paramètres> systèmes>mise a jour et sécurité > Windows update puis faites rechercher une mise a jour*

Une mise à jour s'effectuera si il y en a une.

Les mises à jour permettent :

- *De corriger les bugs rencontrer avec la dernière mise a jour*
- *Ajouter de nouvelles fonctionnalités*
- *Empêcher les cybercriminels d'utiliser des failles de sécurité de votre OS pour vous pirater et vous dérober des données personnelles/sensibles*

Vous pouvez aussi *télécharger des logiciels d'antivirus telle que Bitdefender qui sont la pour rajouter une protection supplémentaire sur votre ordinateur et empêcher que votre machine ne soit infecté*



II-LYCÉE

L'ANSII mot de passe: création

Selon l'ANSII lors de la création des mots de passe vous devez:

Créer un mot de passe minium de 15 caractères car le niveau de sensibilité sera de Fort à très fort

Niveau de sensibilité	Longueur minimale en nombre de caractères	Taille de clé équivalente en bits [5]
Faible à moyen	Entre 9 et 11	≈ 65
Moyen à fort	Entre 12 et 14	≈ 85
Fort à très fort	Au moins 15	≥ 100

De plus ce mot de passe doit être *composé d'un jeu de caractères pour qu'il soit le plus complexe possible exemple : 96Akz%>ocheval*

La notion de complexité d'un mot de passe désigne usuellement le choix du jeu de caractères dans lequel les caractères composant un mot de passe sont choisis. Ces jeux de caractères peuvent être assez variés concernant leur taille et composition (caractères numériques, alphanumériques, en minuscules, en majuscules, comprenant des caractères spéciaux, etc). Plus la taille du jeu de caractères est grande plus le nombre de mots de passe possibles est grand.

L’ANSSI mot de passe: Création

Les coffres-forts de mot de passe sont aussi un bon moyen de générer des mots de passe longs et complexes sans avoirs besoins de les mémoriser ou même d’en prendre connaissance) et de les stocker de manière sécuriser

Afin de permettre aux utilisateurs l’emploi de mots de passe robustes, il est important de mettre à leur disposition des outils dédiés, comme les coffres-forts de mots de passe. Les coffres-forts de mots de passe (*Keepass* [29] est un exemple) permettent, entre autres, de générer des mots de passe longs et complexes (sans avoir besoin de les mémoriser ni même d’en prendre connaissance) et de les stocker de manière sécurisée.

L'ANSII mot de passe: Robustesse

Lors de la création des mots de passe *assurez-vous que les mots de passe subissent un contrôle automatisé et systématique de la robustesse des mots de passe au moment de leur création ou de leur renouvellement.*

Voici les exemples:

- mettre en place des mécanismes automatiques et systématiques permettant de vérifier que les mots de passe respectent bien les règles définies dans la politique de sécurité des mots de passe ;
- comparer les mots de passe lors de leur création à une base de données répertoriant les mots de passe les plus utilisés ou bien ceux qui ont été compromis (par exemple les dictionnaires recensant les mots de passe les plus utilisés ou bien encore les dictionnaires inclus dans les outils de « cassage » de mots de passe comme *JohnTheRipper* [1]) ;
- repérer les mots de passe contenant des motifs (ou des répétitions de motifs) spécifiques (comme une suite de chiffre telle que « 12345 », la suite des premières lettre des claviers comme « azerty », etc) ;
- repérer les mots de passe contenants des informations personnelles saisies lors de la création du compte, comme les noms et prénoms ou encore les dates de naissance ;
- lors d'un renouvellement du mot de passe, interdire la réutilisation d'un mot de passe parmi les X derniers mots de passe déjà utilisés.

L’ANSII mot de passe: Durée

Les mots de passe ont un délai d’expiration*, en effet les mots de passe en entreprise sont obligés d’être changé tous les 3 mois minimum* pour éviter que les utilisateurs ne créent des comptes avec le même mot de passe avec un chiffre en plus comme par exemple « toto » et « toto1 »

La durée de mot de passe dépend aussi de l’utilisateur si c’est l’administrateur qui détient les droits d’accès il devra changer son mot de passe plus régulièrement que les autres pour éviter les tentatives d’intrusion

Il est recommandé d’imposer un délai d’expiration sur les mots de passe des comptes très sensibles comme les comptes administrateurs.

Pour des comptes peu sensibles, imposer un délai d’expiration trop court (3 à 6 mois par exemple) peut se révéler contre-productif étant donné les comportements des utilisateurs observés lorsqu’ils sont soumis à ce type de contrainte. En revanche, pour les comptes très sensibles comme les comptes à privilèges, conserver un délai d’expiration des mots de passe reste une bonne mesure à mettre en œuvre.

L'ANSII mot de passe: Stockage des mots de passe

Les mots de passe doivent-être stocké de façon a ce que l'on ne garde seulement les empreintes. Car en cas d'attaque au lieu que les hackers trouvent directement les mots de passe, seulement les empreintes de mots de passe seront visibles

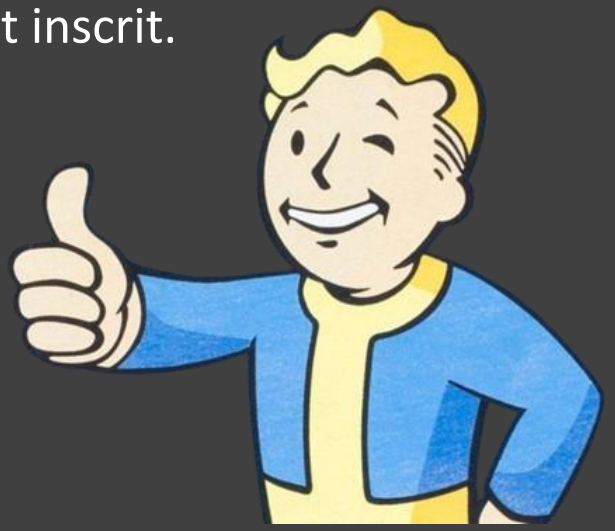
Le stockage des mots de passe des utilisateurs par le vérifieur doit être réalisé de manière sécurisée. En effet, en cas de compromission de cette base (cette base a été récupérée ou rendue publique par un attaquant), les mots de passe seront directement révélés s'ils sont stockés en clair. Ainsi, ce sont les empreintes des mots de passe qu'il faut conserver plutôt que les mots de passe eux-mêmes. Le stockage des mots de passe en clair doit être absolument proscrit. Ces empreintes, aussi appelées hachés, sont le résultat d'une fonction de hachage cryptographique (comme les familles SHA2 ou SHA3) appliquée aux mots de passe. Ces fonctions de hachage cryptographique semblent au premier abord de bons outils pour stocker les mots de passe, car elles ont, en particulier, la propriété d'être à sens unique : retrouver le mot de passe originel à partir d'une empreinte est extrêmement difficile.

Utilisateur BTS SIO Bonnes pratiques

Durant ces deux années deux BTS les élèvent de SIO doivent donc:

-*Utiliser les mots de passe (ou phrases de passe) robustes*, c'est à-dire suffisamment longs et complexes pour résister aux attaques par recherche exhaustive et n'étant pas un mot du dictionnaire (ou une citation ou phrase connue) pour résister aux attaques par dictionnaire.

-*utiliser un mot de passe différent pour chaque service* auquel l'utilisateur est inscrit.



Utilisateur BTS SIO Bonnes pratiques

-*utiliser un coffre-fort de mots de passe* permettant facilement de générer des mots de passe robustes et différents pour chaque service, facilitant la mise en œuvre de la recommandation

-*adopter les bons réflexes de protection des mots de passe*. Par exemple, il est impératif de ne pas écrire ses mots de passe sur une note sous le clavier, de ne pas créer un fichier « mot de passe » sur le poste utilisateur, de ne pas s'envoyer ses mots de passe par courriel, etc. L'utilisation d'outils comme les coffres forts de mots de passe est à privilégier.

Utilisateur BTS SIO Bonnes pratique

-*utiliser un mot de passe robuste pour accéder à sa messagerie électronique*. En particulier, il faut privilégier l'utilisation d'une méthode d'authentification multi facteur lorsque cela est disponible

-*ne pas construire son mot de passe à partir d'informations personnelles comme les noms et prénoms ou encore la date de naissance*, car si une personne connait des informations sur vous elle va commencer par essayer d'utiliser des mots de passe avec votre date de naissance ou le nom de votre chien par exemple

Utilisateur BTS SIO Bonnes pratique

-*modifier les mots de passe par défaut et modifier son mot de passe tous les 3 mois*

-Utiliser une authentification, une procédure par laquelle un système informatique certifie l'identité d'une personne ou d'un ordinateur. Le but de cette procédure étant d'autoriser la personne à accéder à certaines ressources sécurisées. Ceci peut se faire a l'aide d'un texto que vous recevez avec un code et vous devez entrer

La méthode passphrase

Définition de passphrase: Une phrase secrète ou phrase de passe (en anglais : passphrase) est un mot de passe d'un nombre important de caractères. On parle de phrase de passe plutôt que de mot de passe parce que la phrase de passe contient souvent des suites de mots qui ressemblent parfois à une phrase pour des raisons mnémotechniques.

Et il existe deux méthodes pour définir un mot de passe par passphrase:

Première méthode

La première méthode est la méthode mnéomique:

Dans cette approche, la passphrase est formée en utilisant des mots faciles à mémoriser. Ces mots peuvent être choisis pour former une phrase significative ou simplement une série de mots aléatoires. L'idée est de créer une séquence de mots qui a du sens pour vous, facilitant ainsi la mémorisation.

Par exemple, une passphrase mnémonique pourrait être : "CascadeRougeChienSoleil".

Deuxième méthode

La deuxième méthode est la méthode aléatoire crée une passphrase en utilisant des caractères aléatoires, y compris des lettres majuscules, des minuscules, des chiffres et des caractères spéciaux. Ces passphrases sont générées de manière aléatoire à l'aide de générateurs de mots de passe ou d'algorithmes.

Par exemple, une passphrase aléatoire pourrait ressembler à : "K#t9pLz!2qYsRvX".

ATTENTION !

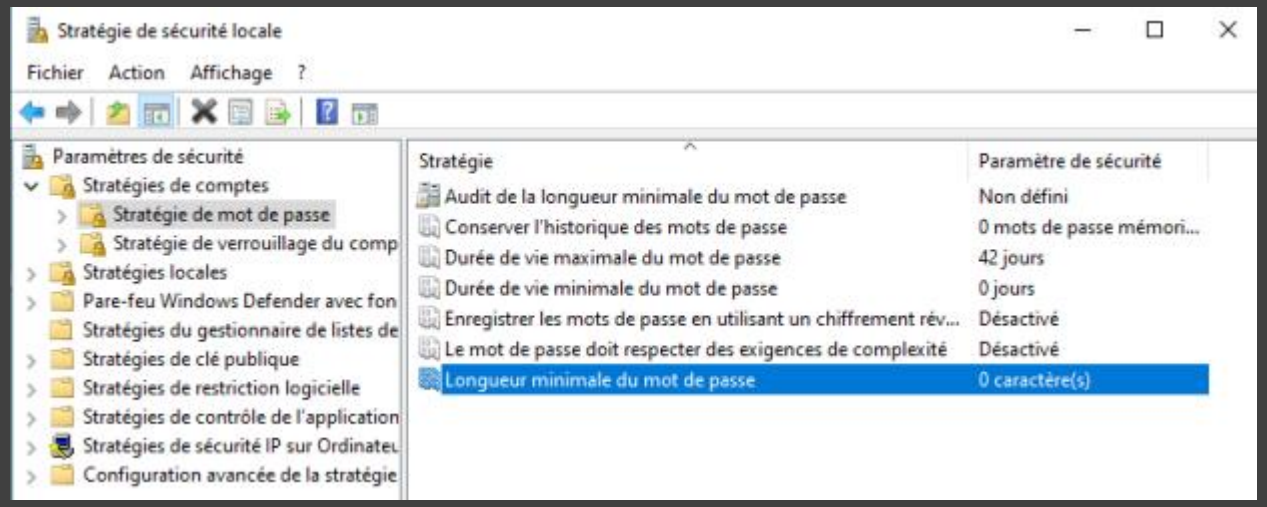
Lors de la création de votre mot de passe vous ne devez surtout pas:

-*Notez vos identifiants sur un post-it et le laissez sur votre bureau* car les utilisateurs pourront faire n'importe quoi sur votre machine et ce sera de votre faute.

-*Ne pas partager vos identifiants sur les réseaux à vos amis ou les envoyez par mail* car les utilisateurs pourront faire n'importe quoi et ce sera de votre faute et il y peut y avoir usurpation d'identité

-*Ne pas donner à un ami même ou à un collègue de confiance vos identifiants pour qu'il puisse se connecter à votre machine sans votre présence* car les utilisateurs pourront faire n'importe quoi sur votre machine et ce sera de votre faute.

-*Réutiliser le même mot de passe et login partout*, si vous venez a vous faire pirater vos codes d'identification se sera très simple pour un cybercriminel d'accéder a vos réseaux/mail et voler vos données



STRATÉGIE DE SÉCURITÉ LOCALE

Stratégie de sécurité locale

-*Audit de la longueur minimale du mot de passe*: Ce paramètre de sécurité détermine la longueur minimale du mot de passe pour laquelle les évenements d'avertissement de longueur du mot de passe sont émis. Ce paramètre peut être configuré de 1 à 128

-*Conserver l'historique des mots de passe*: Ce paramètre de sécurité détermine le nombre de nouveaux mot de passe uniques devant être associés à un compte d'utilisateur avant qu'un ancien mot de passe puisse être réutilisé. La valeur doit être comprise entre 0 et 24 mots de passe

-Durée de vie maximale du mot de passe: Ce paramètre de sécurité détermine la période (en jours) pendant laquelle un mot de passe peut être utilisé avant que le système oblige l'utilisateur à le changer

Stratégie de sécurité locale

-*Durée de vie minimale du mot de passe*: Ce paramètre de sécurité détermine la période minimale (en jours) d'utilisation d'un mot de passe avant que l'utilisateur puisse le changer. Vous choisissez une valeur comprise entre 1 et 998 jours, ou vous pouvez permettre des changements immédiats en spécifiant la valeur 0

-*Enregistrer les mots de passe en utilisant un chiffrement réversible*: Ce paramètre de sécurité détermine si le système d'exploitation stocke les mots de passe en utilisant un chiffrement réversible

-*Le mot de passe doit respecter des exigences de complexité*: Ce paramètre de sécurité détermine si les mots de passe doivent respecter des exigences minimales

Stratégie de sécurité locale

- *Longueur minimale du mot de passe*: Ce paramètre de sécurité détermine le nombre minimale de caractères que le mot de passe d'un compte d'utilisateur peut contenir

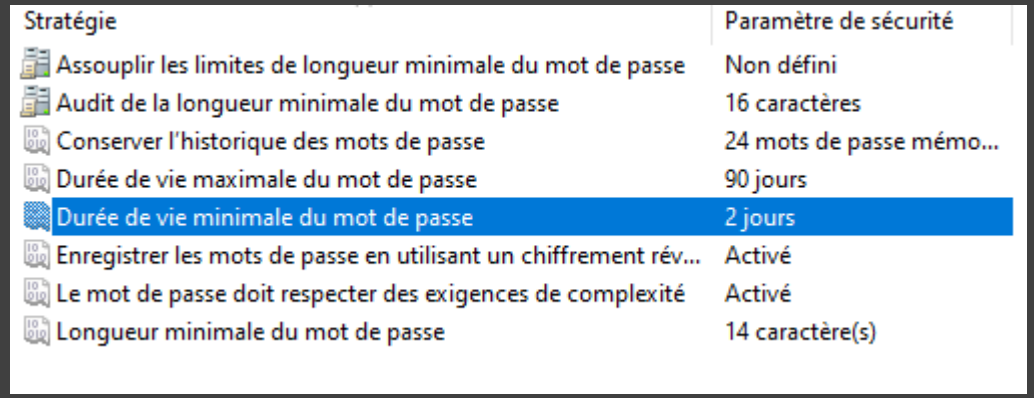
Stratégie de sécurité locale

Pour pouvoir modifier et imposer les valeurs que vous souhaitez, sur votre compte Administrateur vous devez:

Allez dans la barre des tâches -> Ecrire Stratégie de sécurité locale -> Stratégies de compte ->

Stratégie de mot de passe -> modifier les valeurs que vous souhaitez

Le mieux est de programmé votre stratégie de sécurité locale comme ceci :



Stratégie de sécurité locale

En effet mettre 16 caractères a l'audit de la longueur minimale du mot de passe permet déjà de respecter les règle de l'ANSII sur la longueur de mot de passe.

Conserver l'historique des mots de passe permettra de ne pas réutiliser autant de mot de passe souhaité pour un utilisateur donc 24 sont suffisant

Pour la durée de vie maximal de mot de passe du mot de passe il faut obligatoirement mettre 90 jours (trois mois) pour respecter les règles recommandés de L'ANSII et donc mettre minimum 2 jours pour la durée de vie minimale de mot de passe

Activé « Enregistrer les mots de passe en utilisant un chiffrement réversible » et « Le mot de passe doit respecter des exigences de complexité » Pour chiffrer votre mot de passe et qu'il ne puisse pas être déchiffré et qu'il respecte les exigences de complexité posé

Et pour finir imposé minium une longueur de mot de passe de 14 caractères pour respecter les règles recommandés de l'INSAA même si 16 serait beaucoup mieux (on ne peut imposer jusque 14)

III. KEEPASS

KEEPASS

KEPPASS est un gestionnaire de mots de passe open source gratuit, qui vous aide à gérer vos mots de passe de manière sécurisée. Vous pouvez stocker tous vos mots de passe dans une seule base de données, verrouillée avec une clé principale. Il vous suffit donc de mémoriser une seule clé principale pour déverrouiller toute la base de données. Les fichiers de la base de données sont cryptés à l'aide des algorithmes de cryptage les meilleurs et les plus sécurisés actuellement connus (AES-256, ChaCha20 et Twofish)

KEEPASS

Installer le logiciel de KEEPPAS sur leur site internet officiel: https://keepass.info

Le logiciel permet de de sauvegarder un ensemble de mot de passe dans une base de données chiffrée sous la forme d'un fichier dont l'extension .kdb ou .kdbx selon la version. Ce fichier de base de données s'ouvre avec un mot de passe maître et/ou avec d'autres méthodes d'authentification comme un fichier clé.

Keepass

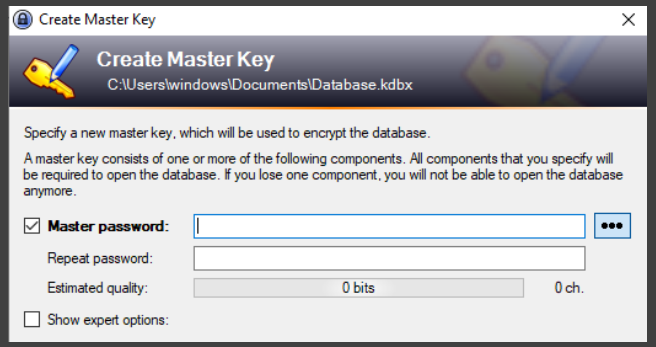
Pour créer cette base de donnée vous devez:

Cliquer sur File -> New -> Créer la nouvelle base de données et y données un mot de passe maître .

Ce mot de passe maître permettra d'accéder à votre base de données de mot de passe

ATTENTION ce sera le seul mot de passe

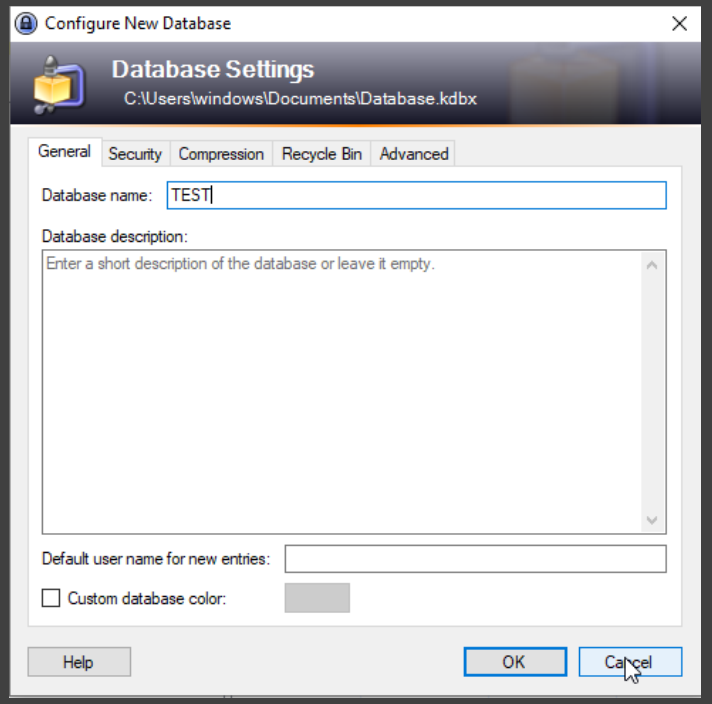
a connaître par cœur !



Les bits sont là pour aider l'utilisateur à savoir à quoi correspond leur mot de passe en nombre de bits « un mot de passe de 16 symboles puisant dans une table de 36 caractères a une taille de clé de 83 bits ; ce score passe à 91 bits si l'on utilise un même mot de passe de 16 caractères qui a été créé via une table de 52 caractères »

Keepass

Donnez un nom à cette base de données



Keepass

Pour ajouter un nouveau mot de passe à enregistrer:

Cliquez sur le logo en haut à gauche sur Add Entry

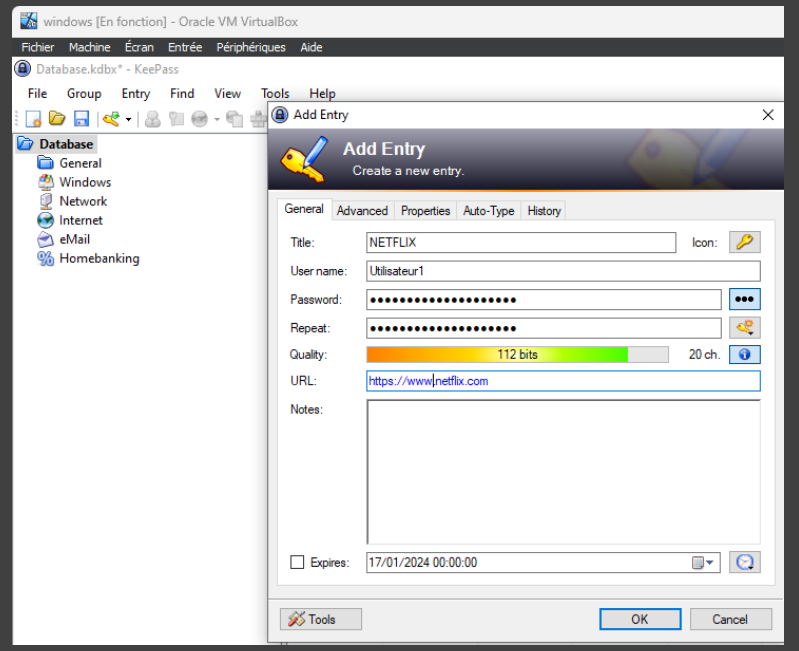
Si c'est pour un compte NETFLIX par exemple *écrivez le dans Title*

Attribuez le nom d'utilisateur du compte

Le mot de passe peut être générer par vous-même ou aléatoirement

Entrez aussi l'URL du site pour un accès plus rapide

Faites Ok



Keepass Avantages/Désavantages

Avantages	Désavantages
Avoir nos mots de passe chiffré	Pour accéder nos mot de passe il faut a tout pris avoir une copie de la base sur un disque dur externe/clé usb
Avoir nos mot de passe sauvegardé	Interface un peu trop vielle
Pas obligé de retenir tout les mots de passe	Complexe d'utilisation au début
Possibilité d'avoir une très grande complexité de mot de passe	
Gratuit	
Disponible sur tout les OS	