**Mot de passe**

Le mot de passe est souvent un point faible de la sécurité.

**Conseils**

* minimum de 9 caractères
* contient un symbole de chacun des trois groupes

|  |  |
| --- | --- |
| **Groupe** | **Exemples** |
| 26 lettres majuscules et 26 lettres minuscules | A B C ... Z et a b c ... z |
| 10 chiffres | 0 1 2 3 4 5 6 7 8 9 |
| 32 symboles différents des lettres et des chiffres | ` ~ ! @ # $ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . / |

* doit être assez différent de votre mot de passe précédent
* ne doit pas contenir votre nom ou votre nom d'usager
* ne doit pas être un mot du dictionnaire

|  |  |  |
| --- | --- | --- |
| **longueur du****mot de passe** | **nombre de****mot de passe si N=94** | **calcul le nombre de mot de passe** |
| 6 | 689 869 781 056 | N = nombre de caractères possibleL = longueur du mot de passeM = nombre de mot de passeM = N**L** |
| 7 | 64 847 759 419 264 |
| 8 | 6 095 689 385 410 816 |
| 9 | 572 994 802 228 616 704 |
| 10 | 53 861 511 409 489 970 176 |

Si le mot de passe complexe expire après 60 jours et a une longueur de

* 7 caractères, il faut **12 509 212** de tentatives par seconde pour le trouver
* 8 caractères, il faut **1 175 865 928** de tentatives par seconde pour le trouver

**Site internet pour valider si le mot de passe est sécuritaire**

* <https://www.microsoft.com/security/pc-security/password-checker.aspx> (utilisé pour faire le tableau plus bas, mais n’existe plus)
* <https://password.kaspersky.com/> (alternative pour avoir une meilleure idée)

Le temps nécessaire pour trouver un mot de passe est influencé par

* la longueur du mot de passe
* l'ensemble des caractères utilisés pour le mot de passe
* l'algorithme utilisé pour encrypter le mot de passe ("LM hash" ou "NT hash")
* la puissance de calcul

Les résultats dans le tableau sont calculés en supposant que le processeur évalue 10 millions de mot de passe par seconde.

Le tableau affiche le temps maximum pour trouver le mot de passe.

|  |  |  |  |
| --- | --- | --- | --- |
| **Longueur du****mot de passe** | **52 caractères / position** | **62 caractères / position** | **94 caractères / position** |
| 1 | **moins d'une seconde** | **moins d'une seconde** | **moins d'une seconde** |
| 2 | **moins d'une seconde** | **moins d'une seconde** | **moins d'une seconde** |
| 3 | **moins d'une seconde** | **moins d'une seconde** | **moins d'une seconde** |
| 4 | **moins d'une seconde** | **moins d'une seconde** | **moins d'une seconde** |
| 5 | **38.02 secondes** | **1.53 minutes** | **12.23 minutes** |
| 6 | **32.95 minutes** | **1.58 heures** | **19.16 heures** |
| 7 | **1.19 jours** | **4.08 jours** | **75.06 jours** |
| 8 | **61.87 jours** | **252.71 jours** | **19.33 années** |
| 9 | **8.82 ans** | **42.93 ans** | **1 816.95 années** |
| 10 | **458.38 ans** | **2 661.40 ans** | **170 793.73 années** |
| 11 | **23 835.82 ans** | **165 006.85 ans** | **16 054 610.83 ans** |
| 12 | **1 239 462.86 ans** | **10 230 424.79 ans** | **1 509 133 418.36 ans** |
| 13 | **64 452 068.55 ans** | **634 286 337.10 ans** | **141 858 541 325.91 ans** |
| 14 | **3 351 507 564.49 ans** | **39 325 752 900.36 ans** | **13 334 702 884 635.80 ans** |

* Il y a 65 millions d’années, les dinosaures ont tous disparu de la surface de la Terre.
* L'âge de la Terre est d'environ 5 milliards d'années.
* L'âge de l'univers est d'environ 13.8 milliards d'années.

**La longueur maximale d'un mot de passe est de 127 caractères.**

**En décembre 2012, Jeremi Gosney a démontré qu'il pouvait tester 350 x 109 mots de passe à la seconde avec son cluster de 5 serveurs, de 25 cartes graphique RADEON et du logiciel "ocl-Hashcat Plus".**

**Avec ce système, il est possible de trouver un mot de passe de 8 caractères peut importe sa complexité (majuscule, minuscule, chiffre, caractères spéciaux) en 5.5 heures.**

**Le fichier SAM**

Les informations concernant les utilisateurs locaux sont enregistrées dans le fichier SAM (Securtiy Account Manager) de l'ordinateur.

* C:\Windows\System32\config\SAM

Le SID d'un administrateur se termine toujours par 500.

S-1-5-21-1220945662-1326574676-1177238915-**500**

**Algorithme "LM hash"**

* Cet algorithme est utilisé depuis Windows 3.11
* Son fonctionnement est très primitif

**La méthode de chiffrement "Lan Manager Hash" est considérée faible.**

Un mot de passe "LM hash" a 2 contraintes:

* Le mot de passe ne peut pas avoir plus de 14 caractères.
* Le mot de passe doit contenir que des caractères ASCII imprimable.

Mode de fonctionnement:

1. Le mot de passe est converti en majuscule.
2. Si le mot de passe a une longueur inférieure à 14 caractères il est complété par des caractères NULL. Le code ASCII du caractère NULL est 0.
3. Le mot de passe est découpé en 2.

Si le deuxième bloc est constitué de 7 caractères NULL alors les 8 derniers octets codés seront toujours identiques à la valeur **AA D3 B4 35 B5 14 04 EE**

**note: l'algorithme ajoute un bit de parité**

1. Les 2 textes chiffrés sont concaténés pour créer une chaîne de 16 octets qui devient le "LM hash".

**Algorithme "NT hash"**

* Depuis Windows Vista, "NT hash" est utilisé par défaut pour l’authentification locale.

**La méthode de chiffrement "NT Hash" est considérée plus forte.**

Le "NT hash" a plusieurs avantages par rapport au "LM hash"

* Le mot de passe du "NT hash" peut avoir jusqu’à 127 caractères
* En plus des caractères ASCII, les caractères UNICODE peuvent être utilisés.
* Il prend en considération la casse.
* Utilise l'algorithme MD4.

**Logiciels pour trouver le mot de passe Administrateur local**

1. **Vous n’avez légalement pas le droit de vous introduire dans l’ordinateur de quelqu’un d’autre.**
2. **Vous devez donc tester ces logiciels sur votre machine ou avoir l’autorisation de son propriétaire.**
3. **Dans le cours B22 vous devez demander l'autorisation du professeur avant d'utiliser ces logiciels.**

Les logiciels pour trouver les mots de passe utilisent plusieurs techniques:

* "dictionary" teste des mots du dictionnaire
* "hybrid" teste des mots du dictionnaire avec des variations
* "brute force" teste de façon exhaustive les mots de passe

"**Ophcrack LiveCD 3.6.0**" est disponible sur le site "**http://ophcrack.sourceforge.net**".

* ophcrack-vista-livecd-3.6.0.iso

cracks NT hashes (Windows Vista and 7)

* ophcrack-xp-livecd-3.6.0.iso

cracks LM hashes (Windows XP and earlier)



Il s’agit d’un CD basé sur la distribution Linux "Slitaz", la version compatible avec Windows Vista et Windows 7 contient des tables avec des valeurs "NT hashes".

La compagnie vend des bases de données pour trouver les mots de passe (NT hash) de Windows Vista et Windows 7.

* La base de données "Vista eightXL" dont la taille est de 2 TO, contient tous les mots de passe de 8 caractères de long.

note: chaque caractère du mot de passe fait parti d'un ensemble de 94 caractères

Le site internet "http://www.objectif-securite.ch/ophcrack.php" permet de trouver rapidement un mot de passe alphanumérique à partir d'une valeur "LM Hash".



Mot de passe = AAAaaa111

LM Hash = 06B46A2246BED7705D3872C04445E010

**Logiciels pour changer le mot de passe Administrateur local**

1. **Vous n’avez légalement pas le droit de vous introduire dans l’ordinateur de quelqu’un d’autre.**
2. **Vous devez donc tester ces logiciels sur votre machine ou avoir l’autorisation de son propriétaire.**
3. **Dans le cours B22 vous devez demander l'autorisation du professeur avant d'utiliser ces logiciels.**

Il reste cependant une attaque efficace, une clé USB ou un CD contenant un mini système d'exploitation.

Le CD "Offline NT Password & Registry Editor" contient une mini-distribution Linux qui permet de réinitialiser le mot de passe des comptes locaux.

**Pour éviter de corrompre le compte d'un l'utilisateur vous devez effacer son mot de passe.**

* Offline NT Password & Registry Editor (gratuit)

http://pogostick.net/~pnh/ntpasswd

**cd140201.iso est compatible avec Windows 8.1 32 bits et 64 bits**

La solution de Microsoft utilise une version de Windows PE avec plusieurs outils.

* Microsoft Diagnostics and Recovery Toolset 8.1 (pour Windows 8.1)
* Microsoft Diagnostics and Recovery Toolset 8.0 SP1 (pour Windows 8)
* Microsoft Diagnostics and Recovery Toolset 8.0 (pour Windows 8)
* Microsoft Diagnostics and Recovery Toolset 7.0 (pour Windows 7)
* Microsoft Diagnostics and Recovery Toolset 6.5 (pour Windows 7)
* Microsoft Diagnostics and Recovery Toolset 6.0 (pour Windows Vista)
* Microsoft Diagnostics and Recovery Toolset 5.0 (pour Windows XP)

Locksmith est l'outil qui permet de remplacer le mot de passe

**Pour se protéger:**

**On doit modifier le BIOS de l'ordinateur pour empêcher le démarrage de l'ordinateur avec un périphérique amovible.**

**Logiciels pour changer le mot de passe "Administrateur de domaine"**

Il existe des logiciels pour changer le mot de passe "Administrateur de domaine".

Asunsoft Windows Password Geeker Advanced

* http://www.asunsoft.com

**Logiciels pour ne pas demander de mot de passe**

Kon-Boot modifie le noyau du système lorsqu'il démarre pour éviter d'utiliser le processus d'authentification Windows. Le redémarrage de l'ordinateur rétablira le contenu original du noyau de Windows et ses procédures d'authentification.

Kon-Boot est disponible sur le site http://www.kon-boot.com

note: la version gratuite est valide pour Windows XP

**Conseils pour augmenter la sécurité**

La "Stratégie de groupe locale" permet de modifier plusieurs paramètres afin d'augmenter la sécurité.

**On peut appliquer des restrictions sur les mots de passes**

Configuration ordinateur

Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégies de mot de passe

Voici les paramètres à modifier:

* Conserver l'historique des mots de passe = 24
* Durée de vie maximale du mot de passe = 30 jours
* Longueur minimale du mot de passe = 9
* Le mot de passe doit respecter des exigences de complexités = Activé

On doit savoir qu'un utilisateur qui a un mot de passe valide comme MDPsecret1 peut modifier son mot de passe à chaque 30 jours pour MDPsecret2 jusqu'à MDPsecret24 !!!

Il existe des logiciels pour la gestion des mots de passe.

Par exemple, le nouveau mot de passe d'un utilisateur doit avoir X pourcentage de différence avec les vieux mots de passe.

**Password Complexity Manager**

http://www.tools4ever.com

**Password Policy Enforcer**

http://www.anixis.com

**On peut verrouiller un compte après un nombre N de tentatives.**

Configuration ordinateur

Paramètres Windows / Paramètres de sécurité / Stratégies de comptes / Stratégie verrouillage du compte

Voici les paramètres à modifier:

* Durée de verrouillage des comptes = 60 minutes
* Réinitialiser le compteur de verrouillages du compte après = 10 minutes
* Seuil de verrouillage du compte = 5 tentatives d'ouvertures de session non valides

**On peut renommer le compte Administrateur**

Configuration ordinateur

Paramètres Windows / Paramètres de sécurité / Stratégies locales / Options de sécurité

Voici le paramètre à modifier:

* Comptes: renommer le compte administrateur

**Enregistreur de frappes (keyboard logger)**

Un "keyboard logger" sauvegarde toutes les touches appuyées sur le clavier.

Un employeur peut obtenir des preuves lorsqu'un employé abuse d'internet à des fins personnelles.

**KeyLogger Flash USB (http://www.keelog.com)**

* s'installe entre le clavier et le port USB
* pas besoin d'installer de pilote
* invisible pour le système d'exploitation de l'ordinateur



**KeyLogger Flash PS/2 (http://www.keelog.com)**

* s'installe entre le clavier et le port PS/2



**KeyGhost Security Keyboard (http://www.keyghost.com)**

* est un "keyboard logger" qui est caché dans un clavier

**Lecteur d'empreintes digitales**

Un lecteur d'empreintes digitales permet de s'authentifier à Windows, de s'authentifier à un site web, ...



"FingerPrint Reader" de Microsoft est compatible avec Windows Vista

 

Vous devez utiliser des mots de passe qui ne sont pas faciles à trouver.

On peut acheter un lecteur d'empreintes digitales externe.

On peut acheter un clavier avec un lecteur d'empreintes digitales intégré.

On peut acheter un ordinateur professionnel avec TPM 1.2 et un lecteur d'empreintes digitales intégré:

* HP fournit le logiciel "HP ProtectTools"
* Dell fournit le logiciel "Wave EMBASSY Trust Suite"

**Carte à puce (smart card)**

La carte à puce utilise une authentification forte à deux facteurs:

1. vous devez avoir votre carte à puce
2. vous devez connaître votre NIP

Une carte à puce permet de s'authentifier à Windows, de s'authentifier à une session de "Bureau à distance", ...

|  |  |
| --- | --- |
| **Carte à puce** | **Clé USB de type "carte à puce"** |
| untitled1.pngVotre ordinateur a besoin d'un lecteur de cartes à puce. | untitled1.pngVotre ordinateur n'a pas besoin d'un lecteur de cartes à puce. |

Vous devez activer le service **SCardSrv** "%SystemRoot%\System32\SCardSvr.exe" mais dans la liste des services il a le nom "Carte à puce" (Smart card).

Pour ouvrir une session sur un ordinateur avec une carte à puce vous insérez votre carte à puce dans le lecteur de carte à puce et vous tapez le N.I.P. lorsque vous y êtes invité par l'ordinateur.

 

**Stratégie de sécurité locale (secpol.msc)**

Paramètres de sécurité / Stratégies locales / Options de sécurité

Ouverture de session interactive: comportement lorsque la carte à puce est retirée

* Aucune action
* Verrouiller la station de travail
* Forcer la fermeture de session
* Déconnecter en cas de session Terminal Server

**Si l'ordinateur est membre d'un domaine Windows, c'est le serveur qui va gérer les certificats de sécurité pour les cartes à puce.**

**Si la carte mère d'un ordinateur professionnel contient un contrôleur de sécurité "Trusted Platform Module" (TPM 1.2) c'est l'ordinateur qui va gérer les cartes à puce.**

On peut acheter un lecteur de carte à puce externe.

On peut acheter un clavier avec un lecteur de carte à puce intégré.

On peut acheter un ordinateur professionnel avec TPM 1.2 et un lecteur de carte à puce intégré:

* HP fournit le logiciel "HP ProtectTools"
* Dell fournit le logiciel "Wave EMBASSY Trust Suite"

**OTP (One-Time Password)**

Il faut installer un logiciel sur le serveur de la compagnie pour générer les codes en synchronisation dans le temps.



Un nouveau code est généré à chaque 60 secondes !!!

Ensuite l'utilisateur entre le "passcode" pour accéder à l'ordinateur, au site Web de la compagnie, ...



**Comment ça marche**

Lors de la première utilisation:

* vous devez choisir votre NIP

exemple: 1982

* vous devez entrer votre nom d'utilisateur et le code de 6 chiffres qui est présentement affiché sur l'appareil (RSA SecurID)

exemple: MSMITH et 449054

* vous devez confirmer le NIP deux fois
* vous devez entrer votre nom d'utilisateur et le "passcode"

ATTENTION, à partir de ce moment le passcode correspond à votre NIP + les 6 chiffres affichés à l'écran de l'appareil (RSA SecurID) donc 1982449054