DIGITAL NETWORK

Siège: 13 chemin de Fardeloup

13600 La Ciotat

Siret: 43425494200015

APE: 722 Z

www.digital-network.org

www.dnsi.info



Laboratoires : 120 Avenue du Marin Blanc, ZI Les Paluds,

13685 Aubagne

www.digital-internetwork.net www.securite-reseaux.net

Les stratégies de mots de passe

Auteur: Brain Override | Christophe Casalegno | Digital Network http://www.digital-network.org | http://www.digital-internetwork.org | UIN: 103408553 christophe.casalegno@digital-network.org

La sécurité des systèmes d'information de votre entreprise dépend de chacun de vous.

En effet, la **stratégie** la plus fréquente chez les **crackers**, cherchant à prendre le contrôle d'un système, consiste tout d'abord à usurper l'identité d'un utilisateur ; puis, dans un deuxième temps, à utiliser les **failles connues du système** pour devenir super utilisateur.

Dans la plupart des systèmes, en particulier sous **Windows NT et UNIX**, lorsque le pirate a réussi à trouver une paire "**login/mot de passe**" valide, plus rien ne peut plus l'arrêter tant qu'il n'est pas détecté.

Le choix du mot de passe constitue donc une étape essentielle de la protection d'un système informatique.

La première règle en matière de **mot de passe**, est de ne jamais choisir un mot "réel", c'est à dire que l'on peut trouver dans un dictionnaire.

Tous les composés chimiques, noms propres sont bien entendu également à proscrire : En effet, la méthode la plus utilisée consiste à faire des **essais systématiques** à partir de dictionnaires.

Sachant que l'on connaît l'**algorithme de codage des mots de passe,** il suffit alors de l'appliquer à des dictionnaires choisis astucieusement sur **internet**, (il y en a en dans de nombreuses langues), ou de le composer soi—même et de comparer le résultat à chacune des entrées du fichier système contenant les **mots de passe**, qu'on a réussi à extraire au préalable.

En utilisant cette technique, on arrive à casser en moyenne plus de 20% des mots de passe d'un fichier en moins d'une heure.

Dans ces cas là, même changer le mot de passe une fois par jour n'est pas une mesure suffisante!

Voilà pourquoi il est très important de bien choisir son mot de passe.

Attention: une chaine n'est jamais plus solide que son maillon le plus faible.

Certains croient en effet à tort, que leur **mot de passe**, ne concernant qu'un poste de travail sans importance n'a pas d'intérêt...

CECI EST TOTALEMENT FAUX!!

C'est d'ailleurs comme cela, que de nombreuses attaques réussissent :

Le pirate s'attaque d'abord à un système du réseau sous-protégé, puis de là, en exploitant les failles du système, acquiert des privilèges plus importants, jusqu'à être super-utilisateur. Et là, tout devient possible pour lui! N'oubliez donc pas que la sécurité des systèmes d'information est l'affaire de tous. Techniciens, administrateurs, secretaire ou pdg, tout le monde est concerné.

Recommandations.

Attention, vous ne savez jamais les informations dont le **pirate** dispose. Tout comme vous ne savez jamais qui il peut être

Soyez donc vigilant, n'employez **aucune information personnelle** (n°SS, n° immatriculation, prénom de votre chien, ou de votre petite amie.).

Pour récapituler, votre **mot de passe** ne doit donc pas être un mot qui existe ni quoi que ce soit ayant un rapport avec votre vie personnelle.

Il ne faut également JAMAIS noter son mot de passe où que ce soit!

Pour finir, n'ayez confiance en personne : Le mot de passe est un secret uniquement entre vous et la machine, personne d'autre et surtout pas votre voisin de bureau...

Ne donnez également jamais votre **mot de passe** au téléphone sans être sûr à 100 % de l'identité de votre interlocuteur, et encore... Si vous utiliser l'email, utiliser de préférence un outil comme gnupg pour être sur que seule la personne concernée obtient son mot de passe.

Le Choix du mot de passe.

Après ces quelques recommandations, vient le difficile choix du mot de passe.

Il existe plusieurs méthodes pour composer un bon mot de passe. Nous allons en passer quelques unes en revue...

A- La phrase mnémonique.

Cette méthode, très simple, permet de construire de bons mots de passe que vous pourrez retrouver assez facilement en cas d'oubli. Tout d'abord retenez une phrase simple comme : "Hier, ma femme est allée faire les courses."

Maintenant, ne prenons que les initiales de ces mots : "**Hmfeaflc**", c'est déjà pas mal mais pas encore assez compliquéé car il n'y a que des lettres dans le mot de passe.

Une attaque dite "**Brute Force**", c'est à dire en essayant toutes les combinaisons possibles aurait donc eu raison de ce mot en trop peu de temps.

Nous allons donc garder la ponctuation et, mettre une lettre sur deux, en majuscule, ce qui nous donne : "H,mFeAfLc".

Pour finir, nous allons transformer une lettre sur quatre, en la remplaçant par le nombre équivalent de sa position dans l'alphabet :

"H,mF5AfL3" C'est déjà pas mal!

Rien ne vous empêche d'utiliser des caractères spéciaux comme :

La Ciotat et Aubagne sont des villes! -> LC&A19dv!

Libre à vous également de compter ou non les caractères spéciaux comme des lettres. Cette méthode améliore déjà considérablement la sécurité des mots de passe, surtout lorsque le mot fait au moins 8 lettres.

B- La méthode par substitution

La méthode par substitution est très simple et pourtant est l'une des plus efficaces :

Vous apprenez par coeur une chaine de caractère comme :

"!*+/_&", ces caractères remplaceront les voyelles du mot que vous avez choisi.

Ex: Télévision --> T!1*v+s/n, vous pouvez encore complexifier en mettant une majuscule pour 2 consonnes:

T!l*V+s/N

Autre exemple : Armoires--->ArMoireS-->!rM*+r/S

Tous les mots de passe générés par cette méthode peuvent être considérés comme relativement robustes.

C- Autres méthodes

On pourrait écrire des centaines de pages concernant la fabriquation de mots de passe solides comme taper une chaine de caractères aléatoirement et l'apprendre par coeur, etc...

N'hésitez pas à inventer votre propre méthode, mais n'oubliez jamais les règles essentielles ennoncées avant :

- Un mot de passe est TOP SECRET
- Il ne doit pas être un mot "réel"
- Il doit comporter au moins 8 caractères et ne doit pas être constitué que de lettres ou de chiffres.

Optimiser la sécurité

Maintenant que vous avez choisi un mot de passe que personne ne pourra trouver, vous vous croyez sûrement à l'abri des pirates les plus tenaces...

Et bien il n'en est rien! En effet si un cracker en veut vraiment à vos systèmes, il pourra décrypter votre mot de passe en utilisant une attaque dite "BRUTE FORCE", qui consiste à essayer toutes les solutions possibles : "AAAAAAA, AaAAAAAA, etc...

Cependant, réussir à craquer un bon mot de passe de cette façon, demande du temps et de la puissance.

Malgré tout, cela reste donc du domaine du possible. Un pirate ingénieux, peut par exemple se servir d'une multitude de systèmes qu'il a piraté sur **Internet** et sur lesquels il a implanté un "cheval de Troie", qui aura pour rôle de contribuer au calcul de votre mot de passe.

L'idéal est de changer de mot de passe tous les jours, cependant, on peut limiter ce changement, selon le besoin réel en sécurité, afin que la «convivialité» ne soit pas trop affectée.

96 heures offre un excellent rapport, mais vous pouvez allonger ce temps jusqu à une semaine voire un mois. Tout dépend du niveau de confidentialité nécessaire à vos informations.

N'oubliez pas que plus des 2/3 des malveillances sont internes. Mais également qu'il faut susciter un intérêt assez important chez le pirate pour qu'il s'intéresse à vous.

Une petite entreprise de fruits et légumes a beaucoup moins de chance d'attirer les malveillances qu'une société faisant de la recherche ou une entreprise où circulent de grosses sommes d'argent.

Pour finir, nous dirons cependant que lorsque le problème du mot de passe se pose vraiment, il y a souvent de biens plus gros problèmes à corriger...

Christophe Casalegno | Digital Network

http://www.digital-network.org | http://www.dnsi.info
http://www.digital-internetwork.net | UIN: 103408553

CAMPAGNE INTERNATIONALE CONTRE LES PEDOPHILES
http://www.bouclier.org/campagne