Siège Social : 13 chemin de Fardeloup
13600 LA CIOTAT. Téléphone :04 42 62 84 10
FAX : 04 92 77 01 59

Email : sales@digital-network.net

Bureaux : 120 Avenue du Marin Blanc ZI Les Paluds - 13685 AUBAGNE
www.digital-network.net
www.securite-reseaux.com

Sarl capital Variable 8.000 € -
RCS MARSEILLE 434 254 942 – APE : 722C
www.dns-fr.com
www.dnsi.info

Les stratégies de mot de passe

La sécurité d'un système d'information dépend de chacun de nous.

Auteur : Christophe Casalegno <christophe.casalegno@digital-network.net>

Le **mot de passe**, quelque chose de si simple, si usuel qu'on en oublie très souvent l'importance. Boites emails, comptes shell, applications web, intranet, le mot de passe est partout.

L'importance du mot de passe est souvent sous estimée. On trouve ainsi de nombreux systèmes ou des efforts considérables de sécurité ont été effectués, alors que les stratégies de mots de passe, définies le plus souvent sur le papier au sein de la politique de sécurité ou de la charte d'utilisation du système d'information, sont rarement **vérifiées et appliquées**.

Un cracker souhaitant devenir maître d'un système d'information, cherchera dans un premier temps à obtenir un compte au sein du système ou de l'application cible, puis cherchera à élever son niveau de privilèges jusqu'à obtenir ceux dont il a besoin pour accomplir sa tâche.

Le premier compte obtenu, est souvent un compte utilisateur « mineur » ne disposant pas de privilèges particuliers, et où en conséquence, aucune stratégie de mot de passe particulière aura été appliquée.
Nom, prénom, mot usuel ou familier, le mot de passe d'un point considéré à tort comme non sensible (ex : mot de passe d'une secrétaire, d'un compte invité ou autre), constitue une faiblesse critique dans un système d'information.

Il existe pourtant quelques règles simples permettant d'obtenir un mot de passe d'une solidité tout à fait convenable. La première règle en matière de mots de passe est de ne jamais choisir un mot « réel », c'est à dire que l'on puisse trouver dans un dictionnaire (utilisés pour les attaques de type brute forcing sur un ou plusieurs comptes).

Tous les composés chimiques, noms propres, etc... sont bien entendu également à proscrire (les dictionnaires utilisés dans le brute forcing contiennent en effet également de type de de mot).

Le brute forcing s'explique assez simplement : Sachant que l'on connaît l'algorithme de codage des mots de passe, il suffit alors de l'appliquer à des dictionnaires choisis astucieusement (on en trouve une multitude sur Internet et il est très facile d'en composer soi même), de crypter chaque mot du dictionnaire avec l'algorithme utilisé par le système de cryptage des mots de passe et de comparer le résultat avec l'existant.

Il est également possible d'utiliser du brute force dit « direct » en s'adressant directement au service d'authentification et en simulant un envoie via le protocole adapté du login et du mot de passe.

En utilisant une technique de bruteforcing sur un fichier, 20% des mots de passes sont cassés dans une moyenne d'une heure. Il est donc capital de choisir son mot de passe avec le plus grand sérieux.

Il convient de d'effectuer ce choix avec la plus grande attention, car il n'est jamais possible de connaître les informations dont le pirate dispose. Soyez donc vigilants et n'utilisez aucune information personnelle (numéro de sécurité sociale, immatriculation, prénom de votre petite amie, etc...).

Ne donner votre mot de passe à PERSONNE. Le mot de passe est un secret uniquement entre vous et le système, personne d'autres de doit être en mesure de l'utiliser et surtout pas votre voisin de bureau...

Cette règle vaut dans toutes les situations, et le téléphone n'est pas une exception (de plus il est plus dur d'être certain de l'identité de son interlocuteur au téléphone que de visu).

Il existe heureusement quelques techniques simples et efficaces permettant de générer un mot de passe solide. Un livre entier ne suffirait pas à toutes les énumérer, nous allons donc voir les plus simples et les plus efficaces. Attention, la sécurité d'un mot de passe est également relative à l'algorithme de cryptage utilisé.

I] La phrase mnémonique

Cette méthode très simple permet de construire de bons mots de passe que vous pourrez retrouver facilement en cas d'oubli ou de perte.

Prenons l'exemple suivant : « Hier, ma femme est allée faire les courses. »

Maintenant gardons uniquement les initiales de cette phrase, nous obtenons alors : Hmfeaflc
C'est bien mais ce n'est pas suffisant. Un bon mot de passe contient non seulement les majuscules, des minuscules mais également des chiffres et caractères spéciaux.

Prenons le cas d'une autre phrase : La Ciotat et Aubagne, sont deux villes !
Effectuons la même opération mais gardons la ponctuation. Nous pouvons également remplacer le mot « deux » par le chiffre équivalent et le mot « et » par le signe correspondant ce qui donne :

La Ciotat et Aubagne, sont deux villes ! -> LC&A,s2v!

Voilà qui est mieux, ce mot de passe sera assez solide pour la plupart des utilisations et restera assez simple à retenir grâce à la phrase mnémonique.

Cette méthode est efficace mais il faut arriver à un mot de passe d'un minimum de 8 caractères.

II] La méthode par substitution

Cette méthode qui fait partie des plus simple, est pourtant l'une des plus efficace. Il suffit d'apprendre par coeur une chaîne de caratères comme par exemple « !*+._& ».

Ensuite d'appliquer sur un mot cette chaîne, soit en intercalant après chaque lettre un

caractère de la chaîne soit en remplaçant par ex une lettre sur deux par la dite chaîne.

Par exemple le mot Digital4 peut devenir :

Digital4 --> !D*i+g.i_t&a!l*4 ou encore Digital4 --> D!g*t+l.

Libre à vous d'utiliser les variantes que vous souhaitez en ayant une préférence pour l'utilisation combinée des caratères spéciaux, chiffres, majuscules et minuscules au sein d'un même mot de passe.

III] Autres méthodes

On pourrait écrire des centaines de pages sur la fabrication de mots de passe surs, des techniques les plus simples aux plus sophistiquées. N'hésitez pas à inventer votre propre méthode : celle qui vous conviendra le mieux. Mais n'oubliez jamais les règles essentielles énoncées plus haut :

- Un mot de passe est TOP SECRET
- Il ne doit en aucun cas être un mot réel
- Il doit comporter un minimum de 8 caratères
- Il doit être composé de lettres minuscules et majuscules, de chiffres et de cractères spéciaux.

IV] Optimiser la sécurité

Bien que le mot de passe représente un maillon parmi les plus importants de la chaîne « sécuritaire », un bon mot de passe n'est évidement pas suffisant pour protéger efficacement ses données. Afin qu'une stratégie de mot de passe soit efficace il faut :

- Ne jamais faire transiter le mot de passe en clair sur le réseau
- Etre sur que l'on s'adresse bien au bon système d'information
- Etre attentif au moindre message d'alerte et/ou avertissement (ex ssh/ssl)
- Que la sécurité de la machine sur laquelle est tapé le mot de passe soit garantie
- Utiliser un système de cryptage sur les couches concernées afin d'éviter tout risque d'hijacking (vol de session sans besoin du mot de passe).

Certains prétendent également que le mot de passe est une technique révolue face aux divers autres types d'authentification existants (pki, biométrie, systèmes jettables, etc...).

Pourtant les tests d'intrusion que j'effectue au quotidien montrent le contraire : si le remplacement de l'authentification classique par un système biométrique par ex peut dérouter un pirate, il n'est en rien plus sécurisé qu'un simple login/pass, nous verrons cela plus en détail dans un prochain document consacré à la faiblesse des systèmes d'authentification alternatifs et centralisés.

Christophe Casalegno | Directeur Technique | Groupe Digital Network
Consultant spécialisé en sécurité réseaux/systèmes, techniques intrusives et infoguerre
---
Institut International des Hautes Etudes de la cybercriminalité
Centre International de Recherches et D'Etudes sur le Terrorisme et l'Aide aux Victimes du Terrorisme
Consultant permanent pour le magazine « Le Confidentiel »