TD 1 – Contrôle d'accès logique

Exercice 1 :

1- Citer trois critères permettant de construire un mot de passe "solide".

2- Pourquoi est-il conseillé de changer périodiquement un mot de passe ? (expliquer en 2 lignes max)

3- Dire à quel domaine de sécurité (physique, logique, applicative, d'exploitation ou de télécommunication) appartient chacune des situations suivantes :

a. Sauvegarde des données
b. Mise à jour de php sur le serveur
c. Changement d'un mot de passe
d. Onduleur
e. Marquage du matériel
f. https
g. Test et validation
h. Plan de secours et de sauvegarde

4. Expliquer que veut-on dire par la dernière situation "Plan de secours et de sauvegarde".

Exercice 2 :

1. Un fichier Unix F1 a les droits d'accès suivants : 764. Expliquer.
   En affichant les droits d'accès au fichier F2, Aline et Bob obtiennent 760. Aline s'aperçoit qu'elle peut lire ce fichier mais pas Bob.
2. Répondre aux questions suivantes par "Oui" ou par "Non"
   a- Le fichier peut appartenir à Aline
   b- Le fichier peut appartenir à Bob
   c- Aline et Bob ne sont pas du même groupe.
3. Expliquer la réponse à la question "c" ci-dessus.
4. Les droits d'accès à un fichier F1 pour un certain utilisateur sont 700, ceux d'un autre fichier F4 sont 750. Dites quel fichier est plus important que l'autre pour l'utilisateur en expliquant votre réponse.

Exercice 3 :

On voudrait créer des mots de passe de 10 caractères. On dispose pour cela d'un alphabet de 70 caractères (les lettres A..Z, a..z, les chiffres 0..9 ainsi que 8 autres caractères du code ASCII).

1. Quel est le nombre de mots de passes différents qu'on peut générer.
2. Calculer ce nombre si on décide que le premier caractère du mot de passe doit être une lettre alphabétique.
3. Si une machine peut tester tous les codes calculés à la question 1 en une heure, combien de codes doit-elle alors tester en une seconde.

Exercice 4 :

On veut générer des mots de passe en utilisant la méthode suivante:

- La longueur du mot de passe est de 8 caractères;
- Le mot de passe contient les 26 lettres de l'alphabet (avec une différence entre les minuscules et les majuscules), les chiffres de 0 à 9, et les caractères _ et #;
- Les 2 premiers caractères sont générés aléatoirement, le premier n'est pas un chiffre;
- Les 3 caractères suivants correspondent à l'une des syllabes suivantes :

toi	*pla*	*mon*	*flo*	*cou*	*gou*	*ner*	*men*	*ore*	*lie*

- Les 3 derniers caractères sont générés aléatoirement en utilisant les chiffres 0 à 9.

1. Quel est le nombre de mots de passe différents qu'on peut construire.
2. Si une personne connaît les détails précédents pour la génération des mots de passe, combien lui faut de temps au maximum pour trouver un mot de passe en utilisant un programme qui peut tester 1000 mots de passe par seconde? Préciser ce temps en (heures, minutes, secondes).

Exercice 5 :

On voudrait générer automatiquement des mots de passe en utilisant l'algorithme suivant:

- Chaque mot de passe contient 8 caractères
- Il doit obligatoirement commencer par une lettre alphabétique
- Il peut contenir les lettres a..z, A..Z et les chiffres 0..9
- Chaque caractère du mot de passe sera choisi aléatoirement

1. Combien de mots de passe différents pourrait-on alors créer ?
2. L'algorithme pourrait-il fournir le même mot de passe 2 fois ? Si oui, quelle est alors la probabilité pour que ça se produise ?

Exercice 6 :

On se propose de générer des mots de passe en utilisant la méthode suivante :

— Le mot de passe commence par les 3 premières lettres du nom de la personne;

— Suit sa taille en centimètres;

— Enfin sa date de naissance au format JJMMAAAA.

On suppose que la taille varie entre 1m40 et 2m40 et l'année de naissance de 1900 à 2007.

1. Combien de mots de passe différents peut-on créer ?
2. Critiquer cette méthode.

Exercice 7

On s'intéresse ici à des mots de passe de longueur égale à 8 lettres alphabétiques (mais il y a une différence entre les majuscules et les minuscules).

1- Quelle est la faiblesse de ce type de mots de passe ? à quel type d'attaque est-il sensible ?

2- Combien de mots de passes différents peut-on créer ?

3- Si on considère qu'on dispose d'un ordinateur permettant de tester 10000 mots de passe par seconde, combien de temps faudra-t-il au maximum pour trouver un mot de passe dans notre cas ? (utiliser l'unité de temps la plus adéquate)

4- Supposons que la première lettre du mot de passe soit connue, recalculer le temps de la question 3

5- Proposer une méthode permettant de diminuer le temps trouvé à la question3.

Exercice 8 :

1. Est-il conseillé d'utiliser le même mot de passe pour tous ses comptes e-mail? Donnez 3 raisons.
2. On voudrait construire des mots de passe assez faciles à retenir. Pour cela, on prend un ensemble de 10 syllabes. Les mots de passe seront construits en concaténant deux syllabes distinctes, suivies d'un nombre aléatoire sur 2 chiffres (00 à 99).
   a. Combien de mots passe différents pourra-t-on alors construire ? Détaillez la réponse.

b. Que pensez-vous de cette méthode.

3. Expliquez brièvement la méthode d'authentification utilisée par les DAB (Distributeurs Automatique des Billets de banques).

Exercice 9 :

On veut confronter les quatre possibilités de contrôle d'accès à savoir : Matrice d'autorisation, ACL, Unix et C-Liste Aux situations suivantes :

- User1 désire que ses fichiers soit lisibles par quiconque sauf user2
- User3 et user4 souhaitent partager seulement entre eux l'accès total à quelques fichiers.
- User5 désire que certains de ses fichiers soient publics.

Quelles sont vos propositions ?

Exercice 10 :

«Un employé télécharge de la musique par un système *peer-to-peer* pendant ses heures de travail. Il reçoit malencontreusement une copie du virus "I LOVE YOU" qui se propage automatiquement sous forme de courrier électronique à tous ses collègues. Le serveur de messagerie interne étant doté d'un antivirus, la pièce jointe est heureusement automatiquement éliminée.»

Quels sont les principes de base ignorés dans l'architecture de sécurité informatique de cette entreprise.

Exercice 11 :

On désigne par R le taux de transmission (en caractères par seconde) de la saisie de signes sur un clavier au système, N le nombre de caractères d'un mot de passe, S la taille de l'alphabet (nombre de signes) utilisé pour composer le mot de passe, D le délai en secondes imposé après un essai infructueux de mot de passe. On suppose qu'un mot de passe est composé de caractères choisis au hasard dans l'alphabet.

1. Définir une formule permettant de calculer le temps nécessaire pour trouver un mot de passe.

2. Calculer le temps correspondant aux données suivantes :

- D = 0, R = 5, N = 6, S = 26
- D = 0, R = 5, N = 7, S = 26

Exercice 12 :

La clé la plus utilisée auparavant dans les réseaux WiFi était de type WEP (Wireless Equivalent Privacy). Sa longueur est souvent de 13 caractères ASCII imprimables.
Une fois les 13 caractères définis, la méthode WEP rajoute 3 caractères ASCII aléatoires cette fois-ci pour obtenir la clé complète.

1- Sachant que chaque caractère est codé sur 8 bits, quelle est la longueur (en bits) de la clé complète ?
2- Le nombre de caractères ASCII imprimables est égal à 95. Quel est alors le nombre total de clés WEP complètes possibles ?
3- On dispose d'un ordinateur permettant d'analyser 1000 clés à la seconde. Combien lui faudra-t-il de temps pour analyser le nombre trouvé en 2. Exprimez le résultat en hh :mm :ss.
4- Combien devra être la vitesse (clés/seconde) de l'ordinateur pour analyser toutes les clés possibles en moins de 3 heures ?