Correction PROF - TD Mots de passe v2023-24

Liens divers :
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033928007

1 Ex. 1 - Digicode d'un bâtiment

Q.1.1. Combien y a-t-il de combinaisons possibles ? 10 000 (10 puissance 4) on va de 0000 à 9999

Q.1.2. Nbr de combinaisons possibles ? 12 symboles puissance 6 = 2 985 984

Q.1.3. Conclusion ?. . .Le deuxième mot de passe est plus sûr, il protégera le digicode de l'attaque par force brute contrairement au premier. Mais il est plus compliqué à retenir. Le choix du mot de passe dépend du niveau de sécurité du bâtiment et de qui peut y accéder (immeuble d'habitation ou datacenter…)

2 Ex. 2 - Code d'une carte bancaire

Q.2.1. Combien y a-t-il de codes possibles ? . . . 10 000

Q.2.2. Le voleur a-t-il des chances de réussir l'attaque par force brute ? NON, il y a 3 tentatives de saisie autorisées

3 Ex. 3 – Site web de la banque postale

Q.3.1. Combien y a-t-il de mots de passe possibles ? 10 puissance 6 = 1 million

Q.3.2. moyens de protection ? . . . le compte est bloqué au bout de 3 tentatives max.

(Il y a aussi le temps de latence de réponse du serveur qui empêcherait l'attaque en un temps raisonnable, sauf si plusieurs requêtes effectuées en simultané.)

Autres réponses proposées par les élèves : authentification à double facteur (envoi de SMS ou autre). Bloquer une adresse IP suspecte qui fait plein de connexions

4 Ex. 4 - Mot de passe du réseau du lycée

Q.4.1. Combien y a-t-il de mots de passe possibles ?

26 symboles puissance 6 … = 26 puissance 6 = 308 915 776

Q.4.2. Est-ce que Windows a une protection contre ce type d'attaque ?
Seuil de verrouillage (au bout d'un certain nombre d'essais le compte est verrouillé) .
Durée de verrouillage (le compte est verrouillé un certain temps).
Temps d'attente (latence) entre deux essais.

5 Temps nécessaire pour casser un mot de passe

Q.5.1 Combien de temps (en moyenne) faut-il à la machine pour casser les mots de passe suivants :

- 123456789 : immédiat
- votre mot de passe du lycée : immédiat
- P@ZZw0rD : 3 jours
- 1ère recommandation ANSSI : : 575 145 ans
- 2ème recommandation : + 5 milliards d'années

Q.5.2. Vous avez pu constater que le mot de passe du réseau du lycée n'est pas robuste. Est-ce un problème ?

Non le risque de piratage est limité. Le réseau n'est pas accessible depuis internet. De plus il n'y a pas vraiment de données confidentielles à voler. (quoique il y a l'accès possible à la messagerie.)

Un mot de passe plus long serait difficile à retenir pour les jeunes élèves.

Le système choisi (mot de passe de 6 lettres n'ayant aucun sens) est donc un compromis entre la sécurité et la facilité d'utilisation.

6 Phrase de passe

6.1 -

Bobigny est dans le 93

B0b1gny_3st_d@ns_l3_93

J’adore C# et PHP

J’@d0r3_C#_&_PHP

6.2 - phrases de passe:

Mon mot de passe est un secret bien gardé depuis 25 ans !

Mm2pe1sbgd25a !

Les rançongiciels ont enregistré une augmentation de 36 % entre 2016 et 2017 (source Wikipedia)

Lroe1a236%e2016&2017(sW)

Les quatre opérations de base de ma nouvelle calculatrice Texas Instruments sont : + - * /

L4o2b2mncTIs :+-*/