Semestre 2 **Licence 3 Ingénierie Informatique** Cours Sécurité des Réseaux

TP3 : Hachage en ligne de mots de passe

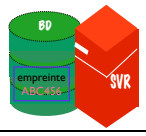
But du TP

- Utilser des outils en ligne pour hacher

Hachage et attaques sur les mots de passe

Beaucoup de sites comme google, amazon, jumia etc… stockent leurs mots de passe hachés.

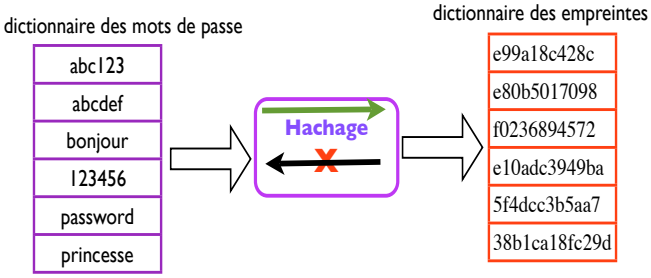
Nom	Prénom	Login	Mot de passe
Sarr	Malick	msarr	e10adc3949ba59abbe56e057f20f883e
Diatta	Eveline	ediatta	e80b5017098950fc58aad83c8c14978e
Fall	Modou	mfall	e99a18c428cb38d5f260853678922e03



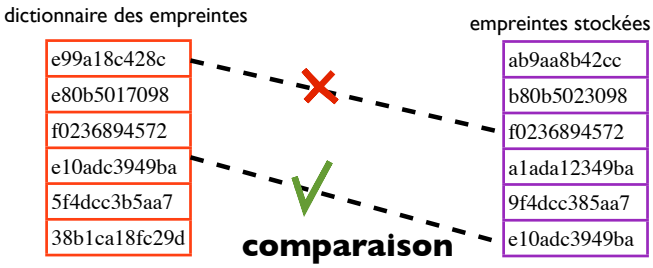
L'objectif de cet exercice pratique est de comprendre comment mener l'attaque par dictionnaire et l'attaque par force brute sur les mots de passe.

Attaque par dictionnaire :

1- à partir d'un dictionnaire, le hacker génère des milliers d'empreintes et obtient un dictionnaire d'empreintes.



2- Les empreintes du dictionnaire sont comparées avec celles stockées dans la base de données des mots de passe. Cela suppose que le Hacker a accès à la base de données.



Lab

On considère un système d'authentification par mot de passe qui utilise les règles suivantes :

- les mots de passes doivent être constitués de lettres minuscules a, b ou/et des chiffres 0 et 1.
- un mot de passe doit compter exactement 4 caractères (lettre(s) et chiffre(s)).

1- Vous devez mener une **attaque par dictionnaire** : en disposant du dictionnaire de données du Tableau 1 et des empreintes stockées dans la base de données (Tableau 2), trouver le mot de

passe d'un utilisateur sachant que MD5 est utilisée pour le calcul des empreintes ? Utiliser le générateur de hachage en ligne suivant : https://www.tools4noobs.com/online_tools/hash/

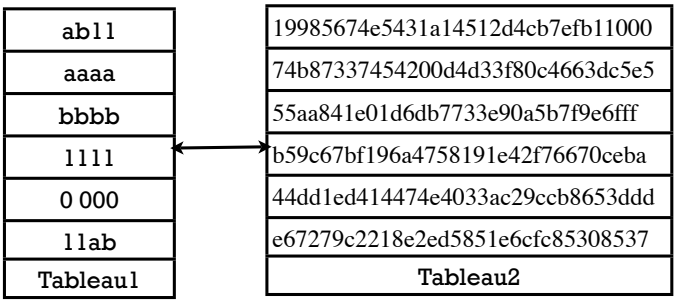


Tableau1
ab11
aaaa
bbbb
1111
0 000
11ab

Tableau2
19985674e5431a14512d4cb7efb11000
74b87337454200d4d33f80c4663dc5e5
55aa841e01d6db7733e90a5b7f9e6fff
b59c67bf196a4758191e42f76670ceba
44dd1ed414474e4033ac29ccb8653ddd
e67279c2218e2ed5851e6cfc85308537

2- Vous devez mener une attaque par **force brute** : établir le tableau de l'ensemble des mots de passe que le hacker doit essayer pour accéder au système ?
3- Sachant que vous ne disposez d'un accès qu'à la base de données (via des requêtes SQL par exemple) des empreintes (Tableau 2), trouvez le mot de passe de 3 utilisateurs si MD5 est utilisée pour générer les empreintes ? Utiliser le crackeur de mots de passe en ligne suivant : https://crackstation.net/.
4- Aller sur le site https://www.tools4noobs.com/online_tools/hash/ et générer l'empreinte de du mot de passe « bonjour ». Utiliser cette empreinte précédemment générée sur le site https://crackstation.net/. Afin de retrouver le mot de passe « bonjour »
5- Choisir un mot passe complexe (qui probablement n'existe pas dans aucun dictionnaire), répéter les étapes de la question 4 afin de montrer que le site https://crackstation.net/.n'inverse pas la fonction de hachage mais utilise plutôt une base de données d'empreintes.