TP CH4 TD1

Table des matières

I. Introduction

Dans le cadre de la politique de sécurité mise en place par l'entreprise, M. Brillat a demandé la réalisation d'un audit de sécurité.
L'objectif de ce travail est d'évaluer l'efficacité de la sensibilisation des utilisateurs, notamment en testant la solidité de leurs identifiants de connexion à travers des tentatives réelles de cassage de mots de passe.

II. Préparation de Windows

En suivant le guide de configuration fourni, j'ai préparé une machine virtuelle sous Windows 10.
Trois comptes utilisateurs ont été créés, chacun avec un niveau de sécurité différent :

1. **ENEDIS** : mot de passe faible (moins de 8 caractères) → *judo63*
2. **MSA** : mot de passe intermédiaire (plus de 8 caractères) → *aurillac15*

3. **CLIC** : mot de passe complexe choisi librement (exemple : *P@ssw0rd!2025*)

Extraction des empreintes (hashes)

Pour récupérer les empreintes des mots de passe, j'ai commencé par désactiver la protection en temps réel de Windows, puis j'ai exécuté l'outil **FGDUMP** avec les droits administrateur.

- Les fichiers **SAM** et **SYSTEM** ont été extraits correctement
- Un fichier nommé **127.0.0.1.pwdump** a été généré sur le bureau
- À l'aide de **Notepad++**, j'ai nettoyé ce fichier afin de ne conserver que les lignes correspondant aux comptes ENEDIS, MSA et CLIC

Enfin, j'ai téléchargé et préparé l'archive **vista_proba_free.zip**, contenant les Rainbow Tables nécessaires pour la suite du TP.

III. Configuration de Kali Linux

La machine virtuelle a ensuite été redémarrée sur l'image ISO *Live* de **Kali Linux**.

Commandes et actions réalisées :

1. Passage du clavier en AZERTY avec la commande :
   setxkbmap fr
2. Identification de la partition Windows à l'aide de :
   fdisk -l
   La partition la plus volumineuse (exemple : /dev/sda2) correspond à Windows.
3. Recherche du fichier de hashes en naviguant dans :
   /media/kali/[UUID]/Users/Administrateur/Desktop/
   afin de retrouver le fichier **127.0.0.1.pwdump**.

IV. Tests avec John The Ripper

L'outil **John The Ripper** a été utilisé en ligne de commande pour effectuer différents types d'attaques sur les mots de passe, en précisant le format **NT**.

4.1 Attaque « Single Crack » (mode simple)

Cette méthode se base sur les informations liées au compte (nom d'utilisateur, nom complet, etc.) pour tenter de deviner le mot de passe.

- Commande utilisée :
  john --single 127.0.0.1. pwdump
- Résultat :
  Le mot de passe du compte **ENEDIS (judo63)** n'a pas été trouvé immédiatement avec cette méthode. Bien qu'il soit très faible, il ne correspond pas directement à une variation du nom du compte.

4.2 Attaque par dictionnaire (Wordlist)

J'ai ensuite utilisé une liste de mots de passe courants afin de tester les combinaisons les plus répandues.

- Commande utilisée :
  john --wordlist=/usr/share/wordlists/rockyou.txt --format=NT 127.0.0.1. pwdump
- Résultats :
  - **ENEDIS (judo63)** : mot de passe cassé, car présent dans les dictionnaires classiques
  - **MSA (aurillac15)** : mot de passe également cassé. Malgré une longueur supérieure à 8 caractères, le schéma « nom de ville + numéro » est très prévisible et souvent intégré aux dictionnaires hybrides

4.3 Attaque par force brute (Incremental)

Pour le dernier compte restant, j'ai lancé une attaque par force brute.

- Commande utilisée :
  john --incremental --format=NT 127.0.0.1.pwdump
- Résultat :
  Cette attaque est très longue à exécuter. En utilisant la commande john --show, j'ai pu constater l'avancement du processus.
  Le compte **CLIC**, disposant d'un mot de passe complexe, n'a pas été cassé durant le temps du TP.

[Description de la capture d'écran n°2]
Terminal affichant les résultats de John The Ripper avec les mots de passe trouvés *judo63* (ENEDIS) et *aurillac15* (MSA), suivis du message *Session completed*.

V. Tests avec Ophcrack

Pour compléter l'audit, j'ai utilisé l'outil graphique **Ophcrack**.

Procédure suivie :

1. Lancement d'Ophcrack
2. Chargement du fichier **PWDUMP** généré sous Windows
3. Installation de la table **vista_proba_free** via le bouton *Install*
4. Lancement du cassage des mots de passe avec *Crack*

Observations

Ophcrack a retrouvé les mots de passe des comptes **ENEDIS** et **MSA** en seulement quelques secondes.
Les Rainbow Tables se révèlent très efficaces contre les mots de passe alphanumériques simples ou sans caractères spéciaux complexes, quelle que soit leur longueur, tant qu'ils restent couverts par la table utilisée.

[Description de la capture d'écran n°3]
Interface d'Ophcrack affichant les barres de progression à 100 %, avec les mots de passe *judo63* et *aurillac15* visibles en clair dans la colonne *NT Pwd*.

VI. Conclusion

Cet audit de sécurité montre que la majorité des mots de passe considérés comme « moyens » restent vulnérables face aux attaques actuelles.

Critères pour renforcer la sécurité des mots de passe (Question 6)

D'après les tests réalisés, un mot de passe robuste doit respecter les critères suivants :

1. **Une longueur suffisante** : au minimum 12 caractères pour ralentir efficacement les attaques par force brute
2. **Une vraie complexité** : utilisation combinée de majuscules, minuscules, chiffres et caractères spéciaux afin de contrer les Rainbow Tables standards

3. **Aucune logique sémantique** : éviter les noms propres, villes ou dates (comme pour le compte MSA), car ces éléments sont ciblés en priorité par les attaques par dictionnaire