Réseau et Sécurité
Correction TP - Casse de mot de passe WPA2

Questions préliminaires

1) Il s'agit d' un fichier contenant une liste de mots ou de combinaisons de mots susceptibles d'être utilisés comme mots de passe. Dans une attaque par dictionnaire, l'outil de cassage de mot de passe teste successivement chaque mot du dictionnaire sur une clé chiffrée pour tenter de trouver la bonne.

2) Le PC ne possède pas de carte Wi-Fi active. Cela signifie qu'il ne peut pas capturer les paquets émis sur les réseaux sans fil ni analyser le trafic Wi-Fi environnant.

1.1 Analyse avec mot de passe faible

aircrack-ng -w french_passwords_top20000.txt wpa2_handshake_strong_password.pcap

a-b) Le mot de passe correct est "marseille". Le temps et le nombre de clés testées dépendent de la façon dont Aircrack-ng parcourt la wordlist. La ligne `[00:00:03] 19888/20000 keys tested (7492.69 k/s)` signifie ici : 3 secondes écoulées et 19 888 clés testées.

1.2 Analyse avec mot de passe fort

aircrack-ng -w french_passwords_top20000.txt wpa2_handshake_strong_password.pcap

a) 20 000 mots de passe — indiqué par `20000/20000 keys tested`.

b) ≈ 2 secondes (affiché `[00:00:02]`)

c) Non, le mot de passe n'a pas été trouvé. La sortie affiche `KEY NOT FOUND` et cela signifie que la liste testée (les 20 000 entrées) a été entièrement parcourue sans obtenir de correspondance. Le mot de passe ne fait donc pas partie du dictionnaire.

1.3 Importance des mots de passe robustes

Plus un mot de passe est long et mélange **majuscules, minuscules, chiffres et caractères spéciaux**, moins il a de chances d'apparaître dans un dictionnaire (qui contient surtout des mots courants et leurs variantes), et plus il mettra de temps à être deviné par brute-force.