[Exploitation/Cracking] Wifi

Introduction

Cette page décrit des méthodologies et des outils pour compromettre des réseaux utilisant le protocole Wifi.

Aircrack-ng

Certainement l'outil le plus célèbre pour pirater des réseaux wifi, il est aussi celui demandant le plus de ressources.

Il requiert une carte wifi supportant l'injection de paquet et le mode moniteur et une puissance de calcul suffisante pour casser le mot de passe par la suite.

En effet, l'objectif va être d'envoyer un paquet de *désauthentification* pour récupérer un **handshake** contenant le hash du mot de passe du wifi qu'on appelle **psk**.

Une fois le hash capturé, il ne reste plus qu'à lancer une attaque hors-ligne sur celui-ci pour obtenir le mot de passe en clair.

Le temps de cracking peut être plus ou moins long selon la puissance de calcul disponible et la complexité du mot de passe.

Fern

WiFiPumpkin3

Anciennement nommé EvilGinx, cet outil est en mesure de créer des faux points d'accès wifi permettant de piéger des utilisateurs du réseau wifi cible en espérant récupérer le mot de passe du réseau wifi par des attaques phishing exécutées en local.

Revision #3
Created 2 September 2023 12:18:41 by Elieroc
Updated 3 May 2024 15:52:05 by Elieroc