Résumé

La sécurité d'un réseau informatique sans-fil, ou réseau WiFi, est un sujet d'actualité récurrent lors de ces dernières années. Le thème de mon Travail de Maturité est de comprendre le WEP (*Wired Equivalent Privacy*), un des systèmes d'encryptage du WiFi, et d'en démontrer ses faiblesses.

La présentation du système d'encryptage de mon Travail de Maturité expliquera d'abord de manière générale le fonctionnement du réseau WiFi et ensuite de manière plus détaillée les caractéristiques techniques du WEP, ses défaillances et les attaques possibles à l'encontre de celui-ci.

Pour illustrer la théorie de mon document, la partie pratique consistera en une tentative de pénétration de mon réseau personnel sécurisé par un système d'encryptage WEP. Cette partie pratique contiendra la présentation de la plateforme de tests, des programmes et des lignes de code utilisés, avec à chaque fois une illustration des résultats obtenus. En finalité, je vous démontrerai que le WEP, surnommé de nos jours *Weak Encryption Protocol* (Faible protocole d'encryptage) par les ingénieurs informaticiens, est obsolète et que sa clé d'encryptage peut être découverte facilement en quelques minutes.

En conclusion, la faiblesse du système d'encryptage WEP montre qu'un hacker peut pénétrer facilement dans un réseau informatique, modifier ou lire les fichiers et ainsi engendrer de lourdes conséquences pour la confidentialité des données de l'entreprise utilisant ce système de protection.

Aujourd'hui, l'utilisation de nouvelles méthodes de protection, plus fiables, tel le WPA et le WPA2 (*WiFi Protection Access*) permet de protéger plus efficacement un réseau informatique.