

Conclusion générale

Dans ce mémoire nous avons implémenté un outil permet de décrypter le trafic chiffré en prend comme un cas d'étude le chiffrement SSL/TLS.

Le besoin de choisir ce protocole est que ce dernier est supporté par la majorité des protocoles applicatifs grâce à ses services de sécurité basés sur des moyens cryptographiques : Authentification, Confidentialité, et Intégrité des données.

Cependant des attaquants peuvent exploiter cet avantage pour faire passer des données malveillantes (Virus,...) cryptées, donc un antivirus ou un pare-feu est incapable d'inspecter ce type de trafic, alors il laisse passer tous le trafic crypté.

Donc ce travail essaye de trouver des solutions à ce problème.

Notre solution donnée par l'utilisation d'une technique nommée "Trusted Man In The Middle avec la modification de messages **handshake**". Cette technique permet de récupérer les clés de chiffrement de deux partenaires avant l'établissement de la communication pour donner au sniffer une possibilité de décryptage de trafic échangé.

Alors notre objectif dans ce travail est double :

- Inspection du trafic crypté SSL.
- Optimisation des opérations d'encryptage et de décryptage au sein de notre module d'inspection.

Et comme une démonstration nous allons développer une application prototype. Cette application analyse les paquets cryptés d'une communication entre un client et un serveur.