

Introduction générale

Contexte d'étude :

De nos jours, la plupart des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau local. Ce réseau permet d'échanger des données entre les divers collaborateurs internes et externes à l'entreprise.

La possibilité de travail collaboratif apportée par un réseau local constitue un premier pas. L'étape suivante concerne le besoin d'ouverture du réseau local vers le monde extérieur, c'est à dire internet. En effet, une entreprise n'est jamais complètement fermée sur elle-même. Il est par exemple nécessaire de pouvoir partager des informations avec les clients de l'entreprise.

Ouvrir l'entreprise vers le monde extérieur signifie aussi laisser des portes ouvertes à divers acteurs étrangers. Ces portes peuvent être utilisées pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise (piratage de données, destruction,...).

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire qui doit être comporté un composant essentiel qui est le pare-feu (firewall). Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr.

Les pare-feux sont un des plus vieux équipements de sécurité ils ont été soumis à de nombreuses évolutions. Dernière mouture de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul le trafic du HTTP passe par le port TCP 80. Ces pare-feux d'entreprise utilisent la technique de filtrage de contenu nommé «inspection des paquets profondément » "Deep Packet Inspection", cette technologie permet d'examiner le contenu de chaque paquet .Pour inspecter profondément le paquet, le pare-feu doit être capable de lire le contenu de chaque paquet, qui implique l'inspection de trafic crypté qui est un grave déficit de sécurité dans les pare-feux.

Problématique :

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, mais pour des raisons de sécurité on a besoin de crypter le trafic échangé ; par l'implémentation d'un tunnel crypté pour la circulation sécurisée des données, malheureusement des contenus malveillants peuvent dissimuler dans le trafic crypté, donc la question qui se pose est : comment aider le pare-feu pour l'inspection et l'analyse de ce type de trafic ?

Objectif :

Pour résoudre le problème d'inspection de trafic crypté, une technique nommée « homme au milieu confiant » "trusted man-in-the-middle" est exploitée.

L'attaque de l'homme au milieu (HDM) ou *man in the middle attack* (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. En inspirant du mécanisme de cette attaque pour renforcer le pare-feu par un module « trusted man-in-the-middle (TMITM) » « Homme au milieu confiant » capable d'inspecter le trafic crypté.

Ce travail étudie spécialement le trafic crypté par le protocole SSL/TLS chez le pare-feu. La fonctionnalité principale de ce protocole est la garantie (théoriquement) de la confidentialité et l'intégrité des données échangées entre deux utilisateurs. Il permet aussi de garantir l'identité du serveur et du client à l'aide des certificats.

La fonctionnalité du module d'inspection de trafic SSL, décrypte, inspecte et ré-encrypte de manière transparente le trafic crypté SSL pour permettre aux services de sécurité de s'appliquer à tout le trafic traversant les pare-feux, cependant ces fonctions vont consommer les ressources de calcul du pare-feu et réduire son efficacité.

Pour cela on va proposer un module d'inspection d'une seule session SSL, qui va intervenir juste au niveau du sous protocole handshake, pour obtenir la clé de session, et éviter le double encryptage de données.

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.

Organisation du mémoire :

Ce mémoire est articulé autour de quatre chapitres :

Nous commençons notre mémoire par une introduction générale qui fixe l'objectif assigné à ce travail.

Dans le premier chapitre on va présenter les pare-feux d'une manière générale, leurs fonctionnalités et leurs catégories, et à la fin de ce chapitre on va décrire précisément le problème de pare-feu avec le trafic crypté SSL.

Le deuxième chapitre présente le protocole SSL et son principe de fonctionnement et ses sous protocoles qu'ils sont aidés à l'organisation de fonctionnement, et enfin une petite explication de PKI (Public Key Infrastructure), cette infrastructure joue un rôle très important dans la gestion des clés SSL.

Le module d'inspection de trafic crypté qui constitue le corps de notre travail fait l'objet du troisième chapitre, en commençant par une présentation d'attaque Man In The Middle, et puis le sniffer Trusted Man In The Middle pour inspecter le trafic crypté, afin d'optimiser les opérations de cryptages notre module d'inspection va modifier seulement

Introduction générale

les messages de **handshake** pour obtenir la clé de session, cette dernière est commune entre les trois membres : le serveur, le firewall et le client.

Le dernier chapitre c'est l'étape de réalisation. Il présente notre module d'inspection implémenté et son environnement de développement.

Pour terminer nous présentons une conclusion générale concernant la conception du système et ses résultats.