TLS/SSL, installation, configuration et mise en oeuvre

★★★★★

PL-51 **2 Jours (14 Heures)**

Description

Le standard TLS (Transport Layer Secure) est le protocole le plus déployé pour la sécurisation des échanges applicatifs. Ce cours vous apportera une bonne connaissance de l'architecture, du protocole et des services de sécurité de TLS. Vous le mettrez en oeuvre côté client et serveur au sein d'échanges à sécuriser.

À qui s'adresse cette formation ?

Pour qui

Techniciens et administrateurs systèmes et réseaux, architectes sécurité et responsables sécurité.

Prérequis

Aucun

Les objectifs de la formation

- Mettre en oeuvre le protocole TLS Configurer de manière forte et sécurisée les clients et serveurs TLS Analyser le trafic TLS Connaître les attaques sur TLS

Programme de la formation

Cryptographie et services de sécurité

- Terminologie et principes cryptographiques.
- Principaux algorithmes de cryptographie et leurs usages dans TLS : AES, DHE, ECC, RSA, DSA.
- Fonction de hachage (MD5, SHA1, SHA2, SHA3) avec et sans clé (Hmac).
- Modes opératoires de cryptographie.
- Cryptanalyse et attaque sur les fonctions cryptographiques.
- Services de sécurité : confidentialité, authentification, intégrité.
- Travaux pratiques Chiffrement et déchiffrement à base de OpenSSL et cryptanalyse.

Certificats et signature numérique

- Signature numérique.
- Attaques sur les clés publiques.
- Certificats et mise en oeuvre des clés PKCS12.
- Profils de certificats pour TLS.
- Travaux pratiques Conception de certificats (côté client et serveur) et des PKCS12 du côté client.

Architecture et services de TLS

- Positionnement des différentes versions : SSLv3, TLS1.
- 0, TLS1.
- 1, TLS1.
- 2.
- Architecture, protocole et services de sécurité, échanges TLS.
- Configuration des cipher suites.
- Travaux pratiques Configuration d'un client TLS et analyse de trafic TLS.

Configuration et mise en oeuvre du protocole TLS

- Configuration du côté client et serveur.
- Configuration pour authentification simple du serveur.
- Mise en oeuvre des certificats, paramétrages des algorithmes de chiffrement du côté serveur.
- Authentification du serveur, configuration des magasins de certificats.
- Travaux pratiques Configuration et mise oeuvre de TLS du côté serveur Web Apache.

Services avancés du protocole TLS

- Extensions et fonctionnalités de TLS.
- Différents modes d'authentification : certificat OpenPGP, PSK.
- Ticket et réouverture de session.
- Benchmarking de session.
- Configuration du client TLS (PKCS12).
- Travaux pratiques Configuration des clients et serveurs TLS pour une authentification forte et mutuelle.
- Mise en oeuvre des extensions, analyse de performances.

Analyse de sécurité et perspectives du protocole TLS

- Attaques sur le protocole TLS.
- Bonnes pratiques, contrôle des configurations.
- Présentation du protocole DTLS.
- Présentation de la future version de TLS 1.
- 3.
- Travaux pratiques Audit du protocole TLS.
- Mise en oeuvre d'attaques sur TLS.
- Configuration et mise en oeuvre de DTLS.