TLS/SSL, installation, configuration et mise en œuvre

Cours Pratique de 2 jours - 14h
Réf : LSL - Prix 2024 : 1 660€ HT

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 œuvre côté client et serveur au sein d'échanges à sécuriser.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Mettre en œuvre le protocole TLS

Configurer de manière forte et sécurisée les clients et serveurs TLS

Analyser le trafic TLS

Connaître les attaques sur TLS

LE PROGRAMME

dernière mise à jour : 01/2018

1) 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.

2) Certificats et signature numérique

- Signature numérique.
- Attaques sur les clés publiques.
- Certificats et mise en œuvre des clés PKCS12.
- Profils de certificats pour TLS.

Travaux pratiques : Conception de certificats (côté client et serveur) et des PKCS12 du côté client.

3) 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.

4) Configuration et mise en œuvre du protocole TLS

- Configuration du côté client et serveur.
- Configuration pour authentification simple du serveur.
- Mise en œuvre des certificats, paramétrages des algorithmes de chiffrement du côté serveur.

PARTICIPANTS

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

PRÉREQUIS

Connaissances de base en informatique et en réseaux.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Authentification du serveur, configuration des magasins de certificats.
Travaux pratiques : Configuration et mise œuvre de TLS du côté serveur Web Apache.

5) 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 œuvre des extensions, analyse de performances.

6) 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 œuvre d'attaques sur TLS. Configuration et mise en œuvre de DTLS.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 11 juil., 14 oct.	2024 : 04 juil., 07 oct.