TLS/SSL INSTALLATION CONFIGURATION ET MISE EN œUVRE

Public	Techniciens et administrateurs systèmes et réseaux, architectes sécurité et responsables sécurité.
Durée	2 jours - 14 heures
Pré-requis	Connaissances de base en informatique et en réseaux.
Objectifs	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
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Planning	Du 08/09/2025 au 09/09/2025
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

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.

CERTIFICATS ET SIGNATURE NUMÉRIQUE

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

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.

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.
- Authentification du serveur, configuration des magasins de certificats.

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).

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.

DÉPLOIEMENT DES SOLUTIONS DE SÉCURITÉS POUR LES PROTOCOLES SUIVANTS :

- Déploiement Syslog Secure
- Deploiement d'un serveur de temps sécurisé.
- Email
- Tp mise en œuvre LDAPS sur un controleur de domaine, principe des autorité racines et secondaires

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation