TCP/IP - Mise en œuvre d'un réseau sécurisé

Informatique

Sécurité logicielle

Référence : 3-SR-TCP
Durée : 4 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1400 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

- Concevoir et mettre en oeuvre des réseaux TCP/IP.
- Principes et techniques d'interconnexion et d'administration.
- Mise en oeuvre des principales applications de TCP/IP

Prérequis

Avoir des notions d'administration système.

Public concerné

Professionnels de la sécurité, les administrateurs, les ingénieurs réseau, technicien informatique

Contenu pédagogique

VPN: Assurer des communications sûres dans un environnement hostile

- Organisations étendues et mobilité
- Menaces sur les communications
- Objectifs de la sécurité des communications

Réseaux Virtuels Privés

- Qu'est ce qu'un VPN ?
- Quelles utilisations ?
- Comment construire ou acquérir un VPN?

Première approche de la cryptographie

- Transformation des messages - chiffrement et déchiffrement
- Deux types de chiffrement
- Signatures numériques
- Certificats numériques
- Implantation des protections
- Vieillissement et révocation automatique et manuelle des clés

Gestion de clés publiques (PKI)

- Objectif de la PKI
- Caractéristiques et éléments de la PKI
- Exemples de PKI

Première approche de l’encapsulation et de l’étiquettage

- TCP/IP et le modèle OSI
- Serial Line Interface Protocol (SLIP), "Point to point protocole" (PPP), "Point to point Tunneling Protocol" (PPTP)
- Level 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP)
- Multiprotocol Label Switching (MPLS)
- Protocole de réservation de ressource (RSVP), services différenciés (DiffServ), et services intégrés IETF (IntServ)

Sécurité du protocole IP (Ipsec)

- Qu'est ce que l´Ipsec ?
- Association de sécurité (SA), Base de données de sécurité (SADB), Base de données des procédures (SPD)
- Mode opératoire et services de sécurité d'Ipsec
- Phases et échange de clés Internet (IKE)
- Risques et limites d'IPSEC
- Principaux matériels/logiciels permettant de créer des VPN IPSEC

Sécurité des couches applicatives : SSL, SSH et TLS

- Qu'est ce que SSL/TLS ?
- Mode opératoire et services de sécurité de SSL/TLS
- Risques et limites de SSL/SSH
- Principaux matériels/logiciels permettant de créer des VPN SSL/TLS/SSH

Modèles propriétaires : LEAP/WPA/VNC/...

- La sécurité nécessaire des communications sans fils
- Des solutions cryptographiques propriétaires controversées
- Quelle harmonisation ?

Architecture de communications sécurisées

- Applications à servir, répartition des risques, politique, et architecture
- Lieu d'installation des services de protection
- Sécurité des communications et disponibilité
- Approche de choix de solutions

Gestion et maintenance des communications sécurisées

- Principes pour maintenir et gérer des communications sécurisées
- Recherche et correction des fautes
- Performance
- Gestion des clés
- Directions futures
- Services de sécurité dans IPV6

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants sous forme de réunion - discussion.
- Utilisation de cas concrets issus de l'expérience professionnelle.
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- Feuille de présence signée en demi-journée.
- Evaluation des acquis tout au long de la formation.
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55