Réseaux TCP/IP, sécuriser son réseau d'entreprise
Tutorat en option

Formation en ligne - 6h45
Réf : 4QY - Prix 2024 : 95CHF HT

Ce cours en ligne a pour objectif de vous donner les connaissances nécessaires pour sécuriser un réseau d'entreprise. Il s'adresse à toute personne disposant de connaissances sur les réseaux locaux et le protocole TCP/IP. La pédagogie s'appuie sur un auto-apprentissage séquencé par actions de l'utilisateur sur l'environnement à maîtriser.

OBJECTIFS PÉDAGOGIQUES

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

Connaître les bases de la sécurité des réseaux TCP/IP

Maîtriser les réseaux locaux et le protocole TCP/IP

Sécuriser l'architecture d'un réseau TCP/IP

Utiliser les VPN (réseaux privés virtuels)

Identifier les failles sur un réseau TCP/IP

PÉDAGOGIE ET PRATIQUES

Une évaluation tout au long de la formation grâce à une pédagogie active mixant théorie, exercice, partage de pratique et gamification. Un service technique est dédié au support de l'apprenant. La formation est diffusée au format SCORM (1.2) et accessible en illimité pendant 1 an.

ACTIVITÉS DIGITALES

Démonstrations, cours enregistrés, partages de bonnes pratiques, fiches de synthèse.

PARTICIPANTS

Public souhaitant sécuriser un réseau d'entreprise.

PRÉREQUIS

Connaissances sur les réseaux locaux et le protocole TCP/IP.

COMPÉTENCES DU FORMATEUR

Les experts qui ont conçu la formation et qui accompagnent les apprenants dans le cadre d'un tutorat sont des spécialistes des sujets traités. 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. 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

La progression de l'apprenant est évaluée tout au long de sa formation au moyen de QCM, d'exercices pratiques, de tests ou d'échanges pédagogiques.
Sa satisfaction est aussi évaluée à l'issue de sa formation grâce à un questionnaire.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : documentation et support de cours, exercices pratiques d'application et corrigés des exercices, études de cas ou présentation de cas réels. ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une attestation de fin de formation est fournie si l'apprenant a bien suivi la totalité de la formation.

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.

LE PROGRAMME

dernière mise à jour : 06/2023

1) Appréhender la sécurité des réseaux TCP/IP

- 5 piliers de la sécurité informatique.
- Quelques méthodes d'analyse de risque.
- Exemple d'approche en couches.
- Sauvegarde des données.
- PRA (plan de reprise d'activité) et PCA (plan de continuité d'activité).
- Quelques points législatifs.
- Sécurité réseau, bilan des faiblesses.

2) Consolider ses connaissances sur les réseaux TCP/IP

- Trame Ethernet.
- Terminologie relative aux paquets.
- Quatre couches - le protocole ARP.
- Classes du protocole IP.
- Notation CIDR.
- Réseau IP auquel on appartient.
- Protocole IP.
- Routage et tables de routage.
- Exemple de réseaux TCP/IP - Calculs.

- Protocole ICMP.
- Comparaison entre les protocoles UDP et TCP.
- Ports de la couche transport.
- Identification des applications.
- Utilitaire TCPView.
- Utilitaire Telnet.

3) Identifier les failles classiques sur un réseau TCP/IP

- Ingénierie sociale.
- Analyse des ports ouverts.
- Programmes furtifs : codes malveillants.
- Programmes furtifs : mouchards.
- Vulnérabilité du Wi-FI. Systèmes de chiffrement.
- VPN Tunneling pour sécuriser une borne Wi-Fi.
- Attaque sur la couche IP : usurpation d'adresse MAC.
- Attaques de type refus de services (DDOS).
- Failles de la couche IP. Attaque sur la fragmentation.
- DHCP Proofing.
- Utilisation des messages ICMP.
- Connexion TCP et attaque Syn Flood.
- Détournement de connexion IP.
- Protocole FTP.
- Modes FTP Actifs et Passifs.
- Failles basiques de SMTP.
- Structure du système DNS et résolution de nom.
- Transfert de zone.

4) Sécuriser l'architecture d'un réseau TCP/IP

- Gestion des communications.
- Détection d'intrusion.
- Routeur filtrant et pare-feu.
- Proxy et reverse proxy.
- Adresses IP privées.
- Traduction NAT.
- Principes de la DMZ.

5) Utiliser les VPN (réseaux privés virtuels)

- Principe et utilisation des VPN.
- Grands types de VPN.
- PPTP et L2TP.
- IPSec et NAT Transversal.
- Sécurité d'un réseau privé virtuel.
- VPN et mise en quarantaine.
- Protocoles d'authentification.
- Démonstration : mettre en œuvre un VPN nomade.