LES BASES DE LA SÉCURITÉ SYSTÈMES ET RÉSEAUX

Public	Techniciens et administrateurs systèmes et réseaux.
Durée	3 jours - 21 heures
Pré-requis	Bonnes connaissances en réseaux et sécurité. Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité.
Objectifs	Connaître les failles et les menaces des systèmes d'information Maîtriser le rôle des divers équipements de sécurité Mettre en œuvre les principaux moyens de sécurisation des réseaux
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
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.

LE MÉTIER D'INTÉGRATEUR SÉCURITÉ

- Quel est le métier de l'intégrateur sécurité ?
- Quelles sont ses compétences ?
- Participer au maintien en conditions optimales de sécurité des OS.
- Intégrer, déployer et maintenir des solutions de sécurité.
- Les solutions de sécurité essentielles.

RISQUES ET MENACES

- Introduction à la sécurité.
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP SYN Flood, SMURF, etc.
- Déni de service et déni de service distribué.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- Les attaques sur le DNS.

ARCHITECTURES DE SÉCURITÉ

- Quelles architectures pour quels besoins ?
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité.
- Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Reverse proxy, filtrage de contenu, cache et authentification.

SÉCURITÉ DES DONNÉES

- Cryptographie.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services cryptographiques.
- Authentification de l'utilisateur.
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.

SÉCURITÉ DES ÉCHANGES

- Sécurité WiFi.
- Les limites du WEP. Le protocole WPA et WPA2.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Le protocole SSH. Présentation et fonctionnalités.

SÉCURISER UN SYSTÈME, LE "HARDENING"

- Critères d'évaluation (TCSEC, ITSEC et critères communs).
- Sécurisation de Windows.
- Gestion des comptes et des autorisations.
- Contrôle des services.
- Configuration réseau et audit.
- Sécurisation de Linux.

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

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

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

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 27/02/2024