SÉCURITÉ SYSTÈMES ET RÉSEAUX PERFECTIONNEMENT

Public	Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.
Durée	4 jours - 28 heures
Pré-requis	Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise.
Objectifs	Mesurer le niveau de sécurité du système d'information Utiliser des outils de détection d'intrusions, de détection de vulnérabilités et d'audit Renforcer la sécurité du système d'information Connaitre le fonctionnement d'une architecture AAA (Authentication, Autorization, Accounting) Mettre en œuvre SSL/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
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.

RAPPELS

- Le protocole TCP/IP.
- La translation d'adresses.
- L'architecture des réseaux.
- Le firewall : avantages et limites.
- Les proxys, reverse-proxy : la protection applicative.
- Les zones démilitarisées (DMZ).

LES OUTILS D'ATTAQUE

- Paradigmes de la sécurité et classification des attaques.
- Principes des attaques : spoofing, flooding, injection, capture, etc.
- Librairies : Libnet, Libpcap, Winpcap, Libbpf, Nasl, lua.
- Outils : Scapy, Hping, Ettercap, Metasploit, Dsnif, Arpspoof, Smurf.

LA CRYPTOGRAPHIE, APPLICATION

- Les services de sécurité.
- Principes et algorithmes cryptographique (DES, 3DES, AES, RC4, RSA, DSA, ECC).
- Certificats et profils spécifiques pour les divers serveurs et clients (X509).
- Protocole IPSEC et réseaux privés virtuels (VPN).
- Protocoles SSL/TLS et VPN-SSL. Problématiques de compression des données.

ARCHITECTURE AAA (AUTHENTICATION, AUTORIZATION, ACCOUNTING)

- Le réseau AAA : authentification, autorisation et traçabilité.
- One Time Password : OTP, HOTP, Google Authentificator, SSO (Protocole Kerberos).
- La place de l'annuaire LDAP dans les solutions d'authentification.
- Les module PAM et SASL.
- Architecture et protocole Radius (Authentication, Autorization, Accounting).
- Les attaques possibles.
- Comment se protéger ?

DÉTECTER LES INTRUSIONS

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (Nmap) et applicatifs (Web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise ?
- Panorama du marché, étude détaillé de SNORT.

VÉRIFIER L'INTÉGRITÉ D'UN SYSTÈME

- Les principes de fonctionnement.
- Quels sont les produits disponibles ?
- Présentation de Tripwire ou AIDE (Advanced Intrusion Detection Environment).
- L'audit de vulnérabilités.
- Principes et méthodes et organismes de gestion des vulnérabilités.
- Site de référence et panorama des outils d'audit.
- Définition d'une politique de sécurité.
- Etude et mise en œuvre de Nessus (état, fonctionnement, évolution).

GÉRER LES ÉVÉNEMENTS DE SÉCURITÉ

- Traitement des informations remontées par les différents équipements de sécurité.
- La consolidation et la corrélation.
- Présentation de SIM (Security Information Management).
- Gestion et protocole SNMP : forces et faiblesses de sécurité.
- Solution de sécurité de SNMP.

LA SÉCURITÉ DES RÉSEAUX WIFI

- Comment sécuriser un réseau WiFi ?
- Les faiblesses intrinsèques des réseaux WiFi.
- Le SSID Broadcast, le MAC Filtering, quel apport ?
- Le WEP a-t-il encore un intérêt ?
- Le protocole WPA, première solution acceptable.
- Implémentation WPA en mode clé partagée, est-ce suffisant ?
- WPA, Radius et serveur AAA, l'implémentation d'entreprise.
- Les normes 802.11i et WPA2, quelle solution est la plus aboutie aujourd'hui ?
- Injection de trafic, craquage de clés WiFi.

LA SÉCURITÉ DE LA TÉLÉPHONIE SUR IP

- Les concepts de la voix sur IP. Présentation des applications.
- L'architecture d'un système VoIP.
- Le protocole SIP, standard ouvert de voix sur IP.
- Les faiblesses du protocole SIP.
- Les problématiques du NAT.
- Les attaques sur la téléphonie sur IP.
- Quelles sont les solutions de sécurité ?

LA SÉCURITÉ DE LA MESSAGERIE

- Architecture et fonctionnement de la messagerie.
- Les protocoles et accès à la messagerie (POP, IMAP, Webmail, SMTP, etc.).
- Problèmes et classifications des attaques sur la messagerie (spam, fishing, usurpation de l'identité, etc.).
- Les acteurs de lutte contre le SPAM.
- Les méthodes, architectures et outils de lutte contre le SPAM.
- Outils de collecte des adresses de messagerie.
- Les solutions mises en œuvre contre le SPAM.

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 : 13/09/2022