

# Sécurité systèmes et réseaux - Niveau 2

3 j (21 heures)

Ref : SSR2

## Public

Responsable sécurité, Architecte sécurité, Direction informatique, Ingénieur/Consultant systèmes et réseaux, Administrateur réseaux

## Pré-requis

Bonnes connaissances de TCP/IP et de la sécurité des réseaux d'entreprise

## Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue  
Exposés, cas pratiques, synthèse, assistance post-formation pendant trois mois  
Un poste par stagiaire, vidéoprojecteur, support de cours fourni à chaque stagiaire

## Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur  
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires  
Questionnaire d'évaluation de la satisfaction en fin de stage  
Auto-évaluation des acquis de la formation par les stagiaires  
Attestation de fin de formation

Cette formation vous permettra de mesurer le niveau de sécurité de votre système d'information au moyen d'outils de détection d'intrusions, de détection de vulnérabilités, d'audit... Elle vous apportera la connaissance de solutions avancées pour maintenir et faire évoluer dans le temps le niveau de sécurité souhaité au regard de vos besoins. Les travaux pratiques proposés permettront d'acquérir les compétences nécessaires à l'installation, la configuration et l'administration des applications les plus utilisées dans le domaine de la sécurité.

## Objectifs

Mesurer le niveau de sécurité de votre système d'information  
Maintenir et faire évoluer dans le temps le niveau de sécurité souhaité  
Configurer et administrer les applications les plus utilisées dans le domaine de la sécurité

## Programme détaillé

### 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, Nsl, 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 Authenticator, 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

## **DETECTER 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

## **VERIFIER L'INTEGRITE D'UN SYSTEME**

---

- 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 oeuvre de NESSUS (état, fonctionnement, évolution)

## **GERER LES EVENEMENTS DE SECURITE**

---

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 SECURITE DES RESEAUX WI-FI**

---

Comment sécuriser un réseau Wi-Fi ?  
Les faiblesses intrinsèques des réseaux Wi-Fi  
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 ?

## **LA SECURITE DE LA TELEPHONIE 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 SECURITE 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 oeuvre contre le SPAM

