Mistralcom Formation
la formation autrement

PROGRAMME SÉCURITÉ SYSTÈMES ET RÉSEAUX – NIVEAU 1

OBJECTIFS : Ce stage pratique vous montrera comment mettre en œuvre les principaux moyens de sécurisation des systèmes et des réseaux. Après avoir étudié quelques menaces pesant sur le système d'information, vous apprendrez le rôle des divers équipements de sécurité dans la protection de l'entreprise afin d'être en mesure de concevoir une architecture de sécurité et de réaliser sa mise en œuvre.

- Connaître les failles et les menaces des systèmes d'information
- Maîtriser le rôle des divers équipements de sécurité
- Concevoir et réaliser une architecture de sécurité adaptée
- Utiliser des outils de détection de vulnérabilités : scanners, sondes IDS
- Mettre en œuvre les principaux moyens de sécurisation des réseaux
- Sécuriser un système Windows et Linux

PUBLIC CONCERNÉ/PRÉREQUIS : Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux. Bonnes connaissances en réseaux et systèmes.

DURÉE : 4 jours (28 heures)

METHODE PÉDAGOGIQUE : Alternance d'exposés théoriques et d'exercices pratiques. Ceux-ci permettront l'évaluation de la formation par rapport aux objectifs.

SUIVI ET ÉVALUATION : Mise en situation pratique des élèves – Fiche individuelle d'évaluation de la formation – Remise en fin de formation d'une attestation individuelle de stage.

Accessibilité aux personnes en situation de handicap : Nous consulter.
Délais d'accès à la formation : Les inscriptions sont possibles 15 jours avant la formation.

CONTENU

1. RISQUES ET MENACES

- Introduction à la sécurité.
- État des lieux de la sécurité informatique.
- Le vocabulaire de la sécurité informatique.
- Attaques "couches basses".
- Forces et faiblesses du protocole TCP/IP.
- Illustration des attaques de type ARP et IP Spoofing, TCP-SYNflood, SMURF, etc.
- Déni de service et déni de service distribué.
- Attaques applicatives.
- Intelligence gathering.
- HTTP, un protocole particulièrement exposé (SQL injection, Cross Site Scripting, etc.).
- DNS : attaque Dan Kaminsky.

Mistralcom Formation - SARL au capital de 1000 euros - Siège social: Z.A. 1 rue des Artisans 68280 SUNDHOFFEN
Téléphone: 03 67 68 02 00 - formation@mistralcom.fr
SIRET: 833 971 765 00015 - APE: 8559B
Crédit Mutuel Bartholdi Colmar: FR76 1027 8032 0000 0216 2290 130

2. ARCHITECTURES DE SECURITE

- Quelles architectures pour quels besoins ?
- Plan d'adressage sécurisé : RFC 1918.
- Translation d'adresses (FTP comme exemple).
- Le rôle des zones démilitarisées (DMZ).
- Exemples d'architectures.
- Sécurisation de l'architecture par la virtualisation.
- Firewall : pierre angulaire de la sécurité.
- Actions et limites des firewalls réseaux traditionnels.
- Evolution technologique des firewalls (Appliance, VPN, IPS, UTM...).
- Les firewalls et les environnements virtuels.
- Proxy serveur et relais applicatif.
- Proxy ou firewall : concurrence ou complémentarité ?
- Reverse proxy, filtrage de contenu, cache et authentification.
- Relais SMTP, une obligation ?

3. SECURITE DES DONNEES

- Cryptographie.
- Chiffrements symétrique et asymétrique. Fonctions de hachage.
- Services cryptographiques.
- Authentification de l'utilisateur.
- L'importance de l'authentification réciproque.
- Certificats X509. Signature électronique. Radius. LDAP.
- Vers, virus, trojans, malwares et keyloggers.
- Tendances actuelles. L'offre antivirale, complémentarité des éléments. EICAR, un "virus" à connaître.

4. SECURITE DES ECHANGES

- Sécurité Wi-Fi.
- Risques inhérents aux réseaux sans fil.
- Les limites du WEP. Le protocole WPA et WPA2.
- Les types d'attaques.
- Attaque Man in the Middle avec le rogue AP.
- Le protocole IPSec.
- Présentation du protocole.
- Modes tunnel et transport. ESP et AH.
- Analyse du protocole et des technologies associées (SA, IKE, ISAKMP, ESP, AH...).
- Les protocoles SSL/TLS.
- Présentation du protocole. Détails de la négociation.
- Analyse des principales vulnérabilités.
- Attaques sslstrip et sslsnif.
- Le protocole SSH. Présentation et fonctionnalités.
- Différences avec SSL.

5. SECURISER UN SYSTEME, LE "HARDENING"

- Présentation.
- Insuffisance des installations par défaut.
- 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.
- Configuration du noyau.
- Système de fichiers.
- Gestion des services et du réseau.

6. AUDIT ET SECURITE AU QUOTIDIEN

- Les outils et techniques disponibles.
- Tests d'intrusion : outils et moyens.
- Détection des vulnérabilités (scanners, sondes IDS, etc.).
- Les outils de détection temps réel IDS-IPS, agent, sonde ou coupure.
- Réagir efficacement en toutes circonstances.
- Supervision et administration.
- Impacts organisationnels.
- Veille technologique.
- Etude de cas
- Etude préalable.
- Analyse du besoin.
- Elaborer une architecture.
- Définir le plan d'action.
- Déploiement.
- Démarche pour installer les éléments.
- Mise en œuvre de la politique de filtrage.