réf. sc11

SECURITE SYSTEMES ET RESEAUX MISE EN OEUVRE

INFORMATIONS

CONTACT

03 88 47 10 96
mfo@metaformose.org

A QUI S'ADRESSE LA FORMATION ?

- Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

MÉTHODES ET OUTILS PÉDAGOGIQUES

- Formation en présentiel, interactive axées ur la pratique pour une meilleure compréhension et application
- Supports vidéo et exercices
- Documents informatiques et papiers

PREREQUIS

- Utilisation courante de Windows et des équipements constitutifs d'un réseau

NOMBRE DE PARTICIPANTS

2 à 8 personnes

DURÉE DE L'INTERVENTION

5 journées soit 35 heures
9h-12h30 et 13h30h-17h

EVALUATION

- Contrôle des connaissances en cours de formation, tests, questionnaires
- Fiche d'évaluation et de satisfaction stagiaire
- Attestation individuelle de formation

INTERVENANTS

- Formateurs seniors experts en sécurité et cloud

LES OBJECTIFS DE LA FORMATION

» Savoir concevoir et réaliser une architecture de sécurité adaptée
» Pouvoir mettre en oeuvre les principaux moyens de sécurisation des réseaux
» Disposer d'une première approche sur la sécurisation des serveurs
» Découvrir en quoi la cryptographie est utile pour sécuriser les échanges d'informations

LE PROGRAMME DE LA FORMATION

1. L'environnement

- Le périmètre (réseaux, systèmes d'exploitation, applications)
- Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
- Les risques
- La protection
- La prévention
- La détection

2. Les attaques

- Les intrusions de niveau 2 : au niveau du commutateur d'accès ou du point d'accès sans-fil
- Les intrusions de niveau 3 (IP) : IP spoofing, déni de service, scanSniffer, man-in-the-middle, les applications stratégiques (DHCP, DNS, SMTP), les applications à risques (HTTP)
- Les attaques logiques : virus, ver, cheval de Troie, spyware, phishing, le craquage de mot de passe
- Les attaques applicatives : sur le système d'exploitation ou sur les applications (buffer overflow)

3. Les protections

- Au niveau des commutateurs d'accès : port sécurisé sur mac-adresse, utilisation du protocole 802.1x, VLAN Hopping, DHCP Snooping, IP source guard, ARP spoofing, filtre BPDU, root guard
- Au niveau sans-fil : mise en place d'une clé WEP, de WPA, de WPA 2 (802.1i)
- Au niveau IP : les pare-feux applicatifs, spécialisés, sur routeur, state full (inspection des couches au dessus de 3), les UTM, les proxys
- Protection des attaques logiques : les anti-virus, les anti spyware, le concept NAC
- Protection des attaques applicatives : hardening des plates-formes Microsoft et Unix, validations des applicatifs

4. Monitoring et prévention

- Sondes IDS
- SysLog Serveur
- Exploitations des logs
- IPS : boîtiers dédiés, fonctionnalité du routeur

5. Exemples d'architectures

- Exemple d'une entreprise mono-site
- Connexion des nomades
- Exemple d'entreprise multi-site

6. La sécurité des échanges, la cryptographie

- L'objectif du cryptage et fonctions de base
- Les algorithmes symétriques
- Les algorithmes asymétriques
- Les algorithmes de hashing
- Les méthodes d'authentification (pap,chap,Kerberos)
- Le HMAC et la signature électronique
- Les certificats et la PKI
- Les protocoles SSL IPSEC S/MIME
- Les VPN (réseau privé virtuel) site à site et nomades