400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

SÉCURITÉ SYSTÈMES ET RÉSEAUX CODE2UTF('8211',0) MISE EN OEUVRE

CODE STAGE : S-RES

OBJECTIFS

Savoir concevoir et réaliser une architecture de sécurité adaptée
Mettre en oeuvre les principaux moyens de sécurisation des réseaux
Disposer dcode2utf('8217',0)une première approche sur la sécurisation des serveurs
Découvrir les obligations légales inhérentes à la sécurité

DURÉE

5 jours

PUBLIC

Toute personne en charge de la sécurité dcode2utf('8217',0)un système dcode2utf('8217',0)information ou intervenant sur le réseau ou la mise en place de serveurs dcode2utf('8217',0)entreprises

PRÉ-REQUIS

Utilisation courante de Windows et des équipements constitutifs dcode2utf('8217',0)un réseau

PROGRAMME

1. Lcode2utf('8217',0)ENVIRONNEMENT
Le périmètre (réseaux, systèmes dcode2utf('8217',0)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 dcode2utf('8217',0)accès ou du point dcode2utf('8217',0)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 dcode2utf('8217',0)exploitation ou sur les applications (buffer overflow)

3. LES PROTECTIONS
Au niveau des commutateurs dcode2utf('8217',0)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 dcode2utf('8217',0)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 Dcode2utf('8217',0)ARCHITECTURES
Exemple dcode2utf('8217',0)une entreprise mono-site
Connexion des nomades
Exemple dcode2utf('8217',0)entreprise multi-site

6. LA SÉCURITÉ DES ÉCHANGES, LA CRYPTOGRAPHIE
Lcode2utf('8217',0)objectif du cryptage et fonctions de base
Les algorithmes symétriques
Les algorithmes asymétriques
Les algorithmes de hashing
Les méthodes dcode2utf('8217',0)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) de site à site et nomades

SQLI INSTITUT

400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE