Sécurité des réseaux et Internet

Durée : 3 jours Référence : SECRI

Cette formation permet de répondre aux impératifs de sécurité des communications de l'entreprise et intégrer la sécurité dans l'architecture d'un système d'information. Elle englobe une analyse détaillée des menaces et des moyens d'intrusion ainsi que des techniques spécifiques de sécurité, solutions et produits.

Contenu

- Introduction
- Outils et méthodes d'intrusion via TCP-IP
- Sécurisation des postes clients
- Sécurisation du sans-fil (Wi-fi et Bluetooth)
- Technologie firewall/proxy
- Techniques cryptographiques
- Sécurisation des Intranet/Extranet
- Réseaux Privés Virtuels (VPN)
- Sécurisation des applications
- Gestion et supervision active de la sécurité

Participants

Responsables sécurité, développeurs, concepteurs et administrateurs réseau / système.

Pré-requis

Connaissances des réseaux et des systèmes.

Programme

Introduction

- Concepts : risque, menaces, vulnérabilité...
- Evolution de la cybercriminalité.
- Nouveaux usages (Web 2.0, virtualisation, Cloud Computing...) et risques associés.
- Nouvelles techniques d'attaque et contre-mesures.

Outils et méthodes d'intrusion via TCP-IP

- Les attaques par le stack IP.
- Les attaques applicatives (DNS, HTTP, SMTP, etc.).
- Utilisation d'un code mobile malveillant.
- Comprendre les techniques des hackers.
- Les sites (CERT, Security focus/bugtraq, CVE...).

Sécurisation des postes clients

- Les menaces : backdoor, virus, spyware, rootkit...
- Le rôle du firewall personnel et ses limites.
- Les logiciels anti-virus/anti-spyware : comparatif.
- Linux et Open Office vs Windows et MS Office
- Les attaques par les documents PDF.
- Comment sécuriser les périphériques amovibles.
- Contrôle de conformité de Cisco NAC, MS NAP.
- La sécurité intégrée dans Windows 7 (AppLocker, Bitlocker, UAC, DirectAccess...).

Sécurisation du sans-fil (Wi-fi et Bluetooth)

- Technologies de réseaux sans fil (standards 802.11).
- Attaques spécifiques (Wardriving, failles WEP et EAP).
- Sécurité des bornes (SSID, Filtrage MAC).
- Vulnérabilités WEP. Faiblesse de l'algorithme RC4.
- Le standard de sécurité IEEE 802.11i (WPA et WPA2).
- Authentifier des utilisateurs (EAP, certificats, token...).
- Les différentes méthodes Cisco LEAP, EAP-TLS, PEAP...
- Attaque sur les hotspots Wi-fi (Rogue AP).
- Attaques spécifiques sur Bluetooth (Bluebug...)
- Comment se protéger efficacement contre les attaques ?
- Audit et surveillance du réseau. Outils d'audit.

Technologie firewall/proxy

- Serveurs proxy, reverse proxy, masquage d'adresse.
- Filtrage. Firewall et proxy : quelle complémentarité ?
- Principe des firewalls, périmètre fonctionnel.
- La mise en place de solutions DMZ.

- Sécurité liée à l'adressage.
- Evolution de l'offre Firewall (appliance, VPN, IPS, UTM...).
- Notion de " dé-périmétrisation " du forum Jericho.
- Utilisation des firewalls dans la protection des environnements virtuels.

Techniques cryptographiques

- Terminologie, principaux algorithmes. Législation et contraintes d'utilisation en France et dans le monde.
- Algorithmes à clé publique : Diffie Hellman, RSA...
- Scellement et signature électronique : MD5, MAC...
- Mots de passe, token, carte à puce, certificats ou biométrie
- Authentification forte : logiciels (S/key), cartes à puces, calculettes d'authentification.
- Sécurisation des clés de chiffrement (PFS, TPM...).
- Evaluation des systèmes d'authentification : Radius, Tacacs+, Kerberos, X509.
- Compléter l'authentification par l'intégrité et la confidentialité de vos données.

Sécurisation de Intranet/Extranet

- Les architectures à clés publiques.
- Les attaques sur SSL/TLS (sslstrip, sslnif...).
- Un serveur de certificat interne ou public ? En France ou aux USA ? A quel prix
- Comment obtenir des certificats ? Comment les faire gérer ?
- Les risques liés aux certificats X509. L'apport des certificats X509 EV.
- Annuaire LDAP et sécurité.
- Architectures "3A" (authentification, autorisation, audit) : SSO, Kerberos, OSF/DCE et ECMA Tacacs.

Réseaux Privés Virtuels (VPN)

- Analyse du besoin, conception et déploiement.
- La création d'un VPN site à site via Internet.
- IPSec. Les modes AH et ESP, IKE et la gestion des clés.
- Les produits compatibles IPSec, l'interopérabilité.
- Surmonter les problèmes entre IPSec et NAT.
- Les VPN SSL (quel intérêt par rapport à IPSec).
- Les produits VPN SSL, l'enjeu de la portabilité.
- Le VPN avec DirectAccess sous Windows 7.
- Les offres VPN Opérateurs. VPN IPSec ou VPN MPLS

Sécurisation des applications

- Les principales techniques d'attaque des applications (buffer overflow, XSS, SQL Injection, vol de session...).
- Le processus SDL (Security Development Lifecycle).
- Utilisation de la technique de " fuzzing ".
- Les outils de revue de code orientés sécurité.
- Le Firewall applicatif (WAF).
- Solution WAF Open source avec Apache en reverse proxy et mod_security.
- Les critères d'évaluation d'un WAF selon le Web Application Security Consortium (WASC).
- Le hardening et la vérification d'intégrité temps réel.

Gestion et supervision active de la sécurité

- L'apport des normes ISO 27001 et ISO 27002.
- Les tableaux de bord Sécurité. La norme ISO 27004.
- Les missions du RSSI dans le suivi de la sécurité.
- Les audits de sécurité (techniques ou organisationnels).
- Les tests de vulnérabilité ou tests d'intrusion.
- Les outils Sondes IDS, Scanner VDS, Firewall IPS.
- Consigner les preuves et riposter efficacement.
- Mettre en place une solution de SIM.
- Se tenir informé des nouvelles vulnérabilités.
- Gérer les mises à niveaux.
- Savoir réagir en cas d'incidents.
- Les services indispensables : où les trouver.
- Démonstration

Intrusion dans un service Web en ligne. Exemple d'un serveur HTTPS et d'un tunnel de sécurité de type IPSec. Protection avancée d'un service Web ; détection des attaques et parades en temps réel. Usage d'un IPS.