Sécurité des SI Risques et Protection avancés

Durée : 5 jours Référence : SECSI2

Cette Formation présente les problèmes de sécurité des SI. Elle vise à apporter aux participants une vision globale des risques sur les réseaux et les systèmes d'information en général. Prendre connaissance des différentes attaques sur les SI, leur fonctionnement et être capable de se protéger. Acquérir la maitrise globale permettant de conduire les projets et faire le bon choix de son outillage sécurité.

Contenu

- Introduction à la sécurité des systèmes d'information
- Partie 1 : Réseaux IP et risques associés
- Partie 2 : Outils et moyens de prévention et de détection

Participants

Responsable sécurité, ingénieur et administrateur sécurité, Chef de projet sécurité, architecte, développeur et Responsable informatique.

Pré-requis

Très bonnes connaissances du fonctionnement des protocoles TCP-IP. Connaître les principes fondamentaux et les concepts réseaux.

Programme

Introduction à la sécurité des systèmes d'information

- Définitions et principes généraux
- Critères généraux de la sécurité des SI
- Cadre normatif (BS17799, ISO-2700x)

Partie 1 : Réseaux IP et risques associés

Concepts fondamentaux

- Le protocole IP (TTL, DF…)
- Le protocole TCP (drapeaux U,A,P,R,S,F)
- Le protocole UDP, ICMP

Techniques d'attaques et d'intrusion

- Phases d'une attaque et attaquants
  - Les différents profils d'attaquants, Les phases d'une attaque
- Phase de découverte d'environnements
  - Scans de ports, Détection d'OS et d'application, Détection de pare-feu
  - WarDialing, Découverte de réseaux Wifi/Bluetooth

  Atelier Nmap: Découverte de l'outilNmap, Utilisation des commandes de base, lancement d'opération de découverte et de scan réseaux

Intrusion/Exploitation

- Ecoute réseau, Cassage de mots de passe, Dénis de service
- Attaques au niveau 2 OSI: ARP Spoofing, MAC flooding, MAC Duplicating,…
- Attaques au niveau supérieur OSI: SYN Flooding, Buffer Overflow, Cross Site Scripting, SQL Injection
- DoS, DDoS, …
- Attaques DNS, Attaques Wifi/Bluetooth

Atelier Hping, ARP spoofing, … : Découverte de l'outil Hping et des ces multiples usages

Découverte de la distribution Kali Linux (BackTrack)

Malwares

- Les types, les méthodes de propagations et les évolutions

Partie 2 : Outils et moyens de prévention et de détection

Méthodologie d'analyse de risques

- Généralités
- CC (ISO 15408 / 1999) et autres méthodes d'évaluation
- La méthode EBIOS

Cryptographie

- Introduction
- Cryptographie
  - Symétrique, asymétrique, hachage, hmac…
  - DES, 3DES, AES, IDEA…
  - RSA, ElGamal (DSA), …
  - SHA-1, SHA-256, MD5, Hmac
- Formats et encodages
  - Base64, ASN.1, BER, …
  - Public-Key Cryptography Standards (PKCS)
- Certification numérique
  - Présentation du standard X509 et X509v3
  - Autorités de certifications (CA)
  - Signature électronique et authentification
  - Certificats personnels et clés privées
  - Exportation et importation de certificats
- L'architecture PKI

Atelier Openssl : Découverte de l'outil Openssl, génération de clés, de hash, de certificats, d'autorité de certification …

Sécurité périmétrique

- Filtrage et proxifiation : Pare Feu (Statefull, stateless), Proxy
- Architectures : DMZ, Zonnage et cloisonnement
- VPN : PPTP, L2TP, IPSec, SSL/TLS...
- **Atelier OpenVPN**: Mise en place d'un tunnel IPSec avec OpenVpn, configuration (clé pré-partagé, certificats...)

Sécurité des réseaux internes

- Antivirus, VLAN, 802.1X
- Systèmes de quarantaine
- Wifi (WEP, WPA, 802.11i,…)

Authentification et chiffrement des données

- Méthodes d'authentification : Simple (login,mdp), OTP, securID, clés…
- Protocoles d'authentification : Challenge/response, RADIUS, Kerberos, TACACS+
- Chiffrement : Fichier, disque, courier (PGP, SecurityBox,TrueCrypt, GnuPG, S/MIME..)
- Usage des certificats et de la cryptographie

Atelier Openssl : Génération, import et export de certificats

Détection d'intrusion

- Traçabilité & Logs
- Contrôle d'intégrité
- IDS/IPS, HIDS, NIDS
- Réaction aux incidents (GDI)
- **Etude de cas**: Présentation de l'outil Nessus

Sécurité des applications

- Contexte
- Technologie WEB
- Architecture WEB et protocole http
- Firewall applicatif (WAF)
- Sécurité Web Services (WS-security, XML encryption, XML signature…)
- Audit et tests d'applications Web