GROUPE DATA-FLAQ'S TECHNOLOGIES INC.

FORMATION

SECURITE INFORMATIQUE

TECHNOLOGIES INC.

A BAMAKO, MALI

Sommaire

Formation Sécurité Informatique

Best

Objectifs pédagogiques

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
Mettre en œuvre les principaux moyens de sécurisation des réseaux
Utiliser des outils de détection de vulnérabilités : scanners, sondes IDS
Sécuriser un système Windows et Linux

Participants

Responsable, architecte sécurité. Techniciens et administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances en réseaux et systèmes.

Travaux pratiques

Mise en œuvre d'une solution de proxy HTTP sous Windows ou Linux, d'une solution antivirale sur les flux réseaux. Conception et mise en œuvre d'une architecture multi-firewalls, multi-DMZ. Mise en œuvre des techniques fondamentales de sécurisation du système d'exploitation.

PROGRAMME DE FORMATION

» Risques et menaces

- Introduction à la sécurité.
- Etat 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.

Travaux pratiques

Installation et utilisation de l'analyseur réseau Wireshark. Mise en oeuvre d'une attaque applicative.

» Architectures de sécurité

- 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 ?

Travaux pratiques

Mise en oeuvre d'un proxy Cache/Authentification.

» Sécurité des données

- 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.

Travaux pratiques

Déploiement d'un relais SMTP et d'un proxy HTTP/FTP Antivirus.
Mise en oeuvre d'un certificat serveur.

» Sécurité des échanges

- 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.

Travaux pratiques

Réalisation d'une attaque Man in the Middle sur une session SSL.
Mise en œuvre d'IPSec mode transport/PSK.

» Sécuriser un système, 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.

Travaux pratiques

Exemple de sécurisation d'un système Windows et Linux.

» Audit et sécurité 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.

Travaux pratiques

Elaboration d'une maîtrise de flux.