Sécurité des applications WEB

Durée : 3 jours

Les objectifs :

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie. Résolument pragmatique, ce stage vous apportera les clés de la protection d'un service en ligne à partir d'exemples concrets d'attaques et de ripostes adaptées.

Participants de cette formation sécurite Web

Responsable sécurité. Directeur informatique. Ingénieur système et réseaux. Architecte sécurité. Chef de projet Web, Développeur Internet. Webmaster.

Pré-requis de cette formation sécurite Web

Connaissances de base des réseaux TCP/IP et d'Internet.

Travaux pratiques

Des sites en ligne sécurisés et protégés (firewall multi-DMZ) seront déployés, une sonde IDS Snort, une protection avancée Apache en reverse Proxy furtif et filtrant, une accélération SSL, une authentification forte par certificat, un contrôle d'intégrité type Tripwire, ….

Programme de cette formation sécurite Web

Introduction

- Présentation du contexte en quelques chiffres.
- Le projet " honeynet " et ses enseignements.
- Les attaques les plus courantes.

Constituants d'une application Web

- Les éléments d'une application N-tiers.
- Le serveur frontal HTTP, son rôle et ses faiblesses.
- Les risques intrinsèques de ces composants.
- Les acteurs majeurs du marché.

Le protocole HTTP en détail

- Rappels sur connexion TCP, http, persistance et pipelining.A
- Les PDUs GET, POST, PUT, DELETE. HEAD et TRACE.
- Champs de l'en-tête, codes de status 1xx à 5xx.
- Redirection, hôte virtuel, proxy cache et tunneling.
- Les cookies, les attributs, les options associées.
- Les authentifications (Basic, Improved Digest...).
- L'accélération http, proxy, le Web balancing.

Travaux pratiques

Installation et utilisation de l'analyseur réseau Ethereal. Utilisation d'un proxy spécifique Achille.

Les risques inhérents aux services Web

- Pourquoi les services Web sont-ils plus exposés ? SQL Injection et Buffer Overflow. Code Red, détail du fonctionnement. Vol de session par cookie poisonning. Manipulation des champs et risques associés.

Travaux pratiques

Exploitation de la faille " Unicode ". Contournement d'une authentification par SQL Injection. Cookie et vol de session. Cross Site Scripting.

Le firewall réseau dans la protection d'application HTTP

- Le firewall réseau, son rôle et ses fonctions.
- Combien de DMZ pour une architecture N-Tiers.
- Pourquoi le firewall réseau n'est pas apte à assurer la protection d'une application Web.

Confidentialité des informations

- Rappels des techniques cryptographiques.
- Sécurité du transport d'informations avec HTTPS.
- Gérer ses certificats serveurs, le standard X509.
- Quelle autorité de certification choisir ?
- Accélérateurs SSL : comment choisir.

Travaux pratiques

Mise en œuvre de S.S.L. sous IIS et Apache.

Configuration du système et des logiciels

- La configuration par défaut, le risque majeur.
- Règles à respecter lors de l'installation d'un système d'exploitation. Linux ou Windows, l'importance du système. Pourquoi Apache plus que IIS ? Comment configurer Apache et IIS pour une sécurité optimale ? Le cas du Middleware et de la base de données. Les V.D.S. (Vulnerability Detection System).

Travaux pratiques

Procédure de sécurisation du frontal Web (Apache ou IIS).

Principe du développement sécurisé

- Sécurité du développement, quel budget ?
- La sécurité dans le cycle de développement.
- Le rôle du code côté client, sécurité ou ergonomie ?
- Le contrôle des données envoyées par le client.
- Lutter contre les attaques de type " Buffer Overflow ".
- Les règles de développement à respecter ?
- Comment lutter contre les risques résiduels : Headers, URL Malformée, Cookie Poisoning…

L'authentification des utilisateurs

- Connexion anonyme et authentification applicative. Systèmes à mot de passe " en clair ", par challenge, crypté. Les attaques sur mots de passe. SecurID, une alternative intéressante contre le vol des mots de passe. Les standards PKCS, l'apport de la PKI. Le rôle de l'annuaire LDAP.

Travaux pratiques
Déploiement d'un annuaire LDAP. Génération de certificats X509 pour l'authentification. Mise en place d'un portail WebSSO (firewall applicatif) et transfert de l'identification.

Le firewall " applicatif "
- Le firewall applicatif, une technologie naissante. Reverse-proxy et firewall applicatif, détails des fonctionnalités standard. Quels sont les apports de firewall applicatif sur la sécurité des sites Web. Comment peut-on insérer un firewall applicatif sur un système en production ? Les acteurs du marché.

Travaux pratiques
Mise en œuvre d'un firewall applicatif. Gestion de la politique de sécurité. Réédition des attaques précédentes et résultats.

Supervision de la sécurité
- La supervision, élément fondamental de la sécurité. Quels sont les composants à auditer, les événements à risque ? Les sondes de détection d'intrusions (I.D.S.). Le contrôle d'intégrité du système de fichiers. Gérer les alertes. La supervision doit-elle être externalisée ?

Démonstration
I.D.S. Open Source Snort.

Conclusion
- Architecture de sécurité complète pour un service Web à risque.
- Le budget approximatif des éléments de sécurité.
- Web Services, XML Encryption et SOAP, quels risques dans les applications futures ?