Sécurité des serveurs web initiation

Durée	2 Jours - (16 Heures)	Modalité d'accès	Aucun
Pré-requis	Connaissances de base en systèmes, réseaux et d'internet	Date	Voir convention
Public	Administrateurs réseaux, systèmes, webmaster	Lieu	Voir convention
Intervenants	Formateurs experts en web programmation sécurité	Délai d'accès	Définir avec l'entreprise
Nb participants	1 à 5	Accessibilité	L'organisme de formation étudiera l'adaptation des moyens de la prestation pour les personnes en situation de handicap
Prix	Voir convention	Obligations réglementaires	Aucune

Méthode pédagogique :
Chaque apport théorique est suivi d'une phase de mise en pratique à travers des exercices appropriés ou de projet « métier » en relation avec l'activité du stagiaire. Mise en application des savoirs faire et techniques apprises.

Outil pédagogique :
Supports papiers

Évaluation :
Exercices de validation en continu et des appréciations tout au long de la formation : une note en pourcentage avec QCM d'entrée et QCM de sortie

Validation :
Attestation de fin de stage

OBJECTIF

Identifier les vulnérabilités les plus courantes des applications web - Comprendre le déroulement d'une attaque - Tester la sécurité de ses applications Web - Configurer un serveur web pour chiffrer le trafic Web avec HTTPS

PROGRAMME

JOUR 1 :

Introduction
- Statistiques et évolution des failles liées au Web selon IBM X-Force et OWASP.
- Evolution des attaques protocolaires et applicatives.
- Le monde des hackers : qui sont-ils ? Quels sont leurs motivations, leurs moyens ?

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 TCP, HTTP, persistance et pipelining.
- Les PDU 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.
- Attaques protocolaires HTTP Request Smuggling et HTTP Response splitting.

Travaux pratiques
- Installation et utilisation de l'analyseur réseau Wireshark. Utilisation d'un proxy d'analyse HTTP spécifique.

Les vulnérabilités des applications Web
- Pourquoi les applications Web sont-elles plus exposées ?
- Les risques majeurs des applications Web selon l'OWASP (Top Ten 2017).
- Les attaques «Cross Site Scripting» ou XSS - Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
- Les attaques en injection (Commandes injection, SQL Injection, LDAP injection...).
- Les attaques sur les sessions (cookie poisonning, session hijacking...).
- Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...).
- Attaques sur les configurations standard (Default Password, Directory Transversal...).

Travaux pratiques
- Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http. Contournement d'une authentification par injection de requête SQL.

Le firewall réseau dans la protection d'applications 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 ?

JOUR 2

Sécurisation des flux avec SSL/TLS
- Rappels des techniques cryptographiques utilisées dans SSL et TLS.
- Gérer ses certificats serveurs, le standard X509.
- Qu'apporte le nouveau certificat X509 EV ?
- Quelle autorité de certification choisir ?
- Les techniques de capture et d'analyse des flux SSL.
- Les principales failles des certificats X509.
- Utilisation d'un reverse proxy pour l'accélération SSL.
- L'intérêt des cartes crypto hardware HSM.

Travaux pratiques
- Mise en œuvre de SSL sous IIS et Apache. Attaques sur les flux HTTPS avec sslstrip et sslsnif.

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. Apache ou 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... ?