Programme de cours
Sécurité de vos applications Web

Durée : 4 jours soit 28 heures

Référence : IF-SECAPP

Public visé :

- Responsable sécurité
- Chef de projets
- Développeur Web
- Administrateur de serveur Web

Pré-requis :

- Connaissances en administration Linux ou Windows
- Connaissances des réseaux et protocoles TCP/IP

Objectifs pédagogiques :

- Évaluer les risques internes et externes liés à l'utilisation d'Internet
- Identifier les différentes solutions pour mettre en oeuvre la sécurité d'un serveur Web
- Comprendre comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
- Être capable de mettre en oeuvre une politique de sécurité fiable sur un serveur Apache ou IIS

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant
Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.
Après
Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)
Enfin
Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 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 ?

Module 2 : 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.

Module 3 : 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.

Atelier : Installation et utilisation de l'analyseur réseau Wireshark. Utilisation d'un proxy d'analyse HTTP spécifique.

Module 4 : Les vulnérabilités des applications Web

- Pourquoi les applications Web sont-elles plus exposées ?
- Les risques majeurs des applications Web selon l'OWASP (Top Ten 2010).
- 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…).

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

Module 5 : 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 ?

Module 6 : 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.

Atelier : Mise en oeuvre de SSL sous IIS et Apache. Attaques sur les flux HTTPS avec sslstrip et sslsnif.

Module 7 : 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).

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

Module 8 : 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… ?

Module 9 : L'authentification des utilisateurs

- L'authentification via HTTP : Basic Authentication et Digest Authentication ou par l'application (HTML form).
- L'authentification forte : certificat X509 client, Token SecurID, ADN digital Mobilegov…
- Autres techniques d'authentification par logiciel : CAPTCHA, Keypass, etc.
- Attaque sur les mots de passe : sniffing, brute force, phishing, keylogger.
- Attaque sur les numéros de session (session hijacking) ou sur les cookies (cookie poisoning).
- Attaque sur les authentifications HTTPS (fake server, sslsniff, X509 certificate exploit…).

Atelier : Attaque “Man in the Middle” sur l'authentification d'un utilisateur et vol de session (session hijacking).

Module 10 : Le firewall “applicatif”

- Reverse-proxy et firewall applicatif, détails des fonctionnalités.
- Quels sont les apports du firewall applicatif sur la sécurité des sites Web ?
- Insérer un firewall applicatif sur un système en production. Les acteurs du marché.

Atelier : Mise en oeuvre d'un firewall applicatif. Gestion de la politique de sécurité. Attaques et résultats.