Sécurité des applications Web

-Réference: **PL-62** -Durée: **3 Jours (21 Heures)**

Les objectifs de la formation

A qui s'adesse cette formation ?

POUR QUI :

- Administrateurs réseaux, systèmes, Webmaster.

Programme

- **Introduction**
  - Analyse des thèmes de l'examen.
  - Propositions de méthodes.
  - Pratiquer le découpage des réseaux.
  - Construire des compétences de dépannage en s'appuyant sur des scénarios.
  - Mise en situation Séance intensive de test dans des conditions proches de l'examen avec exploitation collective des résultats.
- **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.

Programme

- 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 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.
  -).
  - 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 ?

- **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.

Programme

- Utilisation d'un reverse proxy pour l'accélération SSL.
- L'intérêt des cartes crypto hardware HSM.
- Travaux pratiques Mise en oeuvre 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.
  - ?

- **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.
  -).
  -

Programme

Travaux pratiques Attaque "Man in the Middle" sur l'authentification d'un utilisateur et vol de session (session hijacking).

- **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.
  - Travaux pratiques Mise en oeuvre d'un firewall applicatif.
  - Gestion de la politique de sécurité.
  - Attaques et résultats.

(+212) 5 22 27 99 01

(+212) 6 60 10 42 56

Contact@skills-group.com

Nous sommes à votre disposition :
De Lun - Ven 09h00-18h00 et Sam 09H00 – 13H00

Angle bd Abdelmoumen et rue Soumaya, Résidence Shehrazade 3, 7éme étage N° 30
Casablanca 20340, Maroc