Sécurité des applications Web

Cours Pratique de 3 jours - 21h
Réf : SER - Prix 2024 : 2 390€ HT

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.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Identifier les vulnérabilités les plus courantes des applications Web

Comprendre le déroulement d'une attaque

Mettre en place des mesures de sécurisation simples pour les applications Web

Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS

Tester la sécurité de ses applications Web

TRAVAUX PRATIQUES

Des sites en ligne sécurisés et protégés (firewall multi-DMZ) seront déployés, une accélération SSL, un proxy d'analyse du protocole HTTP, un injecteur de flux HTTP(S), une authentification forte par certificat, des outils d'attaques sur les flux HTTPS...

PARTICIPANTS

Administrateurs réseaux, systèmes, Webmaster.

PRÉREQUIS

Connaissances de base en systèmes, réseaux et d'Internet.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 03/2024

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 ?

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.

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.

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

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 2021).
- 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.

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 ?

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.

Travaux pratiques : Mise en œuvre de SSL (Apache ou IIS). Attaques sur les flux HTTPS avec sslstrip et sslsnif.

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).

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

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... ?

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

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.
Travaux pratiques : Mise en œuvre d'un firewall applicatif. Gestion de la politique de sécurité. Attaques et résultats.

LES DATES

CLASSE À DISTANCE	LILLE	PARIS
2024 : 08 juil., 21 oct.	2024 : 08 juil., 21 oct.	2024 : 01 juil., 14 oct.