Sécurité des Applications Web (niveau 1)

Réf. SEC-WEB-01

Description de la formation

L'accès non autorisé aux serveurs de l'entreprise constitue une menace significative. Il est crucial de maîtriser et d'implémenter les technologies et solutions nécessaires pour sécuriser les applications mises en œuvre, en mettant un accent particulier sur les applications vulnérables telles que les services extranet et les systèmes de messagerie. Cette formation, orientée vers des solutions pratiques, vous fournira les outils essentiels pour protéger un service en ligne, en s'appuyant sur des cas réels d'attaques et les stratégies de défense correspondantes.

Détails de la Formation

Prérequis

Connaissance des fondamentaux en informatique (réseaux, systèmes Windows et Linux, applications) avec des notions en cybersécurité. Manipulation autonome pour taper des commandes Linux.

Matériel requis

Le stagiaire doit avoir accès à un ordinateur qui possède un clavier, souris, écran, connexion Internet, un micro et une caméra. Sur cet ordinateur, un navigateur Web doit déjà être installé et configuré pour se connecter à distance sur la machine virtuelle donnée par le formateur. Les liens et identifiants seront donnés au début de la formation. L'accès à l'environnement de test sera effectué par le navigateur web (port TCP/443).

Durée

3 jours (21 heures)

Public concerné

Développeurs, architectes, consultants, administrateurs systèmes et réseaux.

Documents fournis à la fin de la formation

Il est remis aux stagiaires :
• Le plan de déroulement de la formation
• Le support de formation et les énoncés des exercices au format PDF
• Le code source des exercices et des solutions
• Les fichiers créés dans la machine virtuelle par le participant (selon demande)

Moyens pédagogiques

Pour une formation en distanciel, nous utiliserons la visioconférence et des démonstrations en direct. Nous alternerons régulièrement théorie et pratique : chacun dispose d'un poste de travail virtuel Kali Linux pour mettre en pratique au fur et à mesure les notions abordées. Pour une formation en présentiel, les participants auront également accès à une machine virtuelle Kali Linux accessible à distance. Plus de détails en annexe.

Modalités d'évaluation

Les participants seront évalués par des : quiz, exercices pratiques et QCM de validation.

Accessibilité

Formation en ligne accessible avec des outils d'assistance sur demande.

Conditions inscription

Inscription préalable nécessaire, au moins 2 semaines avant le début de la formation.

Programme de la Formation

JOUR 1 : Introduction et Constituants d'une application Web

Matin :
- Introduction aux statistiques et évolution des failles liées au Web (OWASP).
- Evolution des attaques protocolaires et applicatives.
- Le monde des hackers : identité, motivations, et moyens.

Après-midi :
- Composants d'une application N-tiers.
- Serveur frontal HTTP : rôle et faiblesses.
- Risques intrinsèques des composants.
- Principaux acteurs du marché.
- Travaux pratiques : Utilisation de l'analyseur réseau Wireshark et utilisation d'un

proxy d'analyse HTTP (Burp Suite Community).

JOUR 2 : Le protocole HTTP et Les vulnérabilités des applications Web

Matin :
- Détails du protocole HTTP (TCP, PDU, en-têtes, status, cookies, authentifications, HTTP Request Smuggling et HTTP Response splitting).
- Travaux pratiques : Analyse du protocole HTTP.

Après-midi :
- Exposition aux risques des applications Web.
- Les risques majeurs selon l'OWASP.
- Attaques XSS, injections et attaques sur les sessions.
- Vulnérabilités du frontal HTTP et attaques sur configuration standard.
- Travaux pratiques : Attaque XSS, exploitation de faille sur le frontal HTTP, contournement d'authentification par injection SQL.

JOUR 3 : Sécurisation, Firewall et Développement sécurisé

Matin :
- Firewall réseau dans la protection d'applications HTTP.
- Sécurisation des flux avec SSL/TLS.
- Configuration du système et des logiciels pour la sécurité.
- Travaux pratiques : Mise en œuvre de SSL sous Apache et Nginx, attaques sur les flux HTTPS.

Après-midi :
- Principe du développement sécurisé.
- L'authentification des utilisateurs.
- Le firewall "applicatif".
- Travaux pratiques : Attaque "Man in the Middle" sur l'authentification, mise en œuvre d'un firewall applicatif (mod_security sur Apache).

Sessions en INTRA (dans votre entreprise) également possibles, veuillez nous contacter.

Session en langue française par défaut, anglais possible sur demande.

Contact

Courriel : contact@coditrust.com

Formateur et référant handicap : Anthony DESSIATNIKOFF

Annexe : Environnement technique

Chaque participant aura un accès direct à sa machine virtuelle Kali Linux à jour avec tous les outils déjà installé pour ne pas perdre du temps au début de la formation.

Les exercices seront effectués dans un réseau fermé entre les participants et le formateur. Plusieurs machines volontairement vulnérables sont présentes pour être ciblées par les participants comprenant des serveurs et applications différentes pour varier les techniques.

Captures d'écran des machines Kali Linux :