Sécurité : Mener un audit - Méthode d'audit d'un SI

Référence : **SECAUDSI** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi les formations SECHSB - Hacking et Sécurité : les fondamentaux et SECHSA - Hacking et Sécurité : avancé ou posséder les connaissances et compétences équivalentes. • Connaissance des systèmes Linux et Windows.

PROFIL DES STAGIAIRES

• Consultants en sécurité. • Développeurs. • Ingénieurs / Techniciens.

OBJECTIFS

• Bien délimiter un audit, connaître les méthodes existantes. • Connaître les règles et les engagements d'un audit, et ses limitations. • Les outils nécessaires pour réaliser un audit. • Mettre en place une situation d'audit. • Quelles sont les méthodologies reconnues.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

JOUR 1

Introduction aux tests d'intrusion

- Définition du test d'intrusion
- L'intérêt du test d'intrusion
- Les phases d'un test d'intrusion : Reconnaissance - Analyse des vulnérabilités - Exploitation - Gain et maintien d'accès - Comptes rendus et fin des tests

Règles et engagements

- Portée technique de l'audit : Responsabilité de l'auditeur - Contraintes fréquentes - Législation : Articles de loi - Précautions usuelles

Les types de tests d'intrusion

- Externe
- Interne

Méthodologie

- Utilité de la méthodologie
- Méthodes d'audit
- Méthodologies reconnues

Particularités de l'audit

- d'infrastructure classique
- d'infrastructure SCADA
- web
- de code

JOUR 2

Les outils d'audit de configuration (SCAP, checklists, etc.)

Les outils d'audit de code

- Outils d'analyse de code
- Outils d'analyse statique
- Outils d'analyse dynamique

Les outils de prise d'information

- Prise d'information : Sources ouvertes - Active
- Scanning : Scan de ports - Scan de visibilité

Les outils d'attaque

- Outils réseau
- Outils d'analyse système
- Outils d'analyse web
- Frameworks d'exploitation
- Outils de maintien d'accès

JOUR 3

Étude de cas

- Application de la méthodologie et des outils sur un cas concret

Les livrables

- Évaluation des risques
- Impact, potentialité et criticité d'une vulnérabilité
- Organiser le rapport
- Prestations complémentaires à proposer