Sécurité : Test d'intrusion - mise en situation d'audit

Référence : **SECPNT** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Avoir suivi le cours SECHSA ou posséder les connaissances et compétences équivalentes.

PROFIL DES STAGIAIRES

• Administrateurs systèmes / réseaux. • Consultants en sécurité. • Ingénieurs / Techniciens.

OBJECTIFS

• Apprendre à rédiger un rapport d'audit professionnel. • Mettre en application vos compétences techniques des cours SECHSB/HSA dans le cadre d'une intervention professionnelle. • Organiser une procédure d'audit de sécurité de type test de pénétration sur son SI. • Se mettre en situation réelle d'Audit.

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

Méthodologie de l'audit

• La première journée sera utilisée pour poser les bases méthodologiques d'un audit de type test d'intrusion
• L'objectif principal étant de fournir les outils méthodologiques afin de mener à bien un test d'intrusion

Objectifs et types de PenTest

• Qu'est-ce qu'un PenTest ?
• Le cycle du PenTest?
• Différents types d'attaquants
• Types d'audits (Boite Noire, Boîte Blanche, Boîte Grise)
• Avantages du PenTest
• Limites du PenTest
• Cas particuliers (Dénis de service, Ingénierie sociale)

Aspect règlementaire

• Responsabilité de l'auditeur
• Contraintes fréquentes
• Législation : articles de loi
• Précautions
• Points importants du mandat

Exemples de méthodologies et d'outils

• Préparation de l'audit : Déroulement - Cas particuliers (Habilitations - Dénis de service - Ingénierie Sociale)
• Déroulement de l'audit : Reconnaissance, Analyse des vulnérabilités, Exploitation, Gain et maintien d'accès, Comptes rendus et fin des tests

Éléments de rédaction d'un rapport

• Importance du rapport

- Composition : Synthèse générale, Synthèse technique
- Evaluation de risque
- Exemples d'impacts
- Se mettre à la place du mandataire
- Une revue des principales techniques d'attaques et outils utilisés sera également faite afin de préparer au mieux les stagiaires à la suite de la formation

JOURS 2, 3 et 4

- Une mise en situation d'audit sera faite afin d'appliquer sur un cas concret les outils méthodologiques et techniques vus lors de la première journée
- L'objectif étant de mettre les stagiaires face à un scénario se rapprochant le plus possible d'un cas réel, un réseau d'entreprise
- Le système d'information audité comportera diverses vulnérabilités (Web, Applicatives, etc.) plus ou moins faciles à découvrir et à exploiter. L'objectif étant d'en trouver un maximum lors de l'audit et de fournir au client les recommandations adaptées afin que ce dernier sécurise efficacement son système d'information
- Pour ce faire, le formateur se mettra à la place d'un client pour qui les stagiaires auront à auditer le système d'information. Ces derniers seront laissés en autonomie et des points méthodologiques et techniques seront régulièrement faits par le formateur afin de guider les stagiaires tout au long de la mise en situation
- Le formateur aura un rôle de guide afin de : faire profiter les stagiaires de son expérience de terrain, mettre en pratique la partie théorique de la première journée, d'élaborer un planning, d'aider les stagiaires à trouver et exploiter les vulnérabilités présentes, formater les découvertes faites en vue d'en faire un rapport pour le client

JOUR 5

- Le dernier jour est consacré au rapport
- La rédaction de ce dernier et les méthodes de transmission seront abordées

Préparation du rapport

- Mise en forme des informations collectées lors de l'audit
- Préparation du document et application de la méthodologie vue lors du premier jour

Écriture du rapport

- Analyse globale de la sécurité du système
- Description des vulnérabilités trouvées

Transmission du rapport

- Précautions nécessaires
- Méthodologie de transmission de rapport
- Que faire une fois le rapport transmis ?