

## Test d'intrusion : Mise en situation d'Audit

### Le PenTest par la pratique



#### Description

Ce cours vous apprendra à mettre en place une véritable procédure d'audit de type Pen Test ou Test d'Intrusion sur votre S.I.

Les stagiaires sont plongés dans un cas pratique se rapprochant le plus possible d'une situation réelle d'entreprise.

En effet, le PenTest est une intervention très technique, qui permet de déterminer le potentiel réel d'intrusion et de destruction d'un pirate sur l'infrastructure à auditer, et de valider l'efficacité réelle de la sécurité appliquée aux systèmes, au réseau et à la confidentialité des informations.

Vous y étudierez notamment l'organisation et les procédures propres à ce type d'audit ; ainsi qu'à utiliser vos compétences techniques (des compétences équivalentes aux cours HSF et HSA recommandées) et les meilleurs outils d'analyse et d'automatisation des attaques (outils publics ou privés développés par nos équipes) pour la réalisation de cette intervention.

#### Informations générales

Code : PNT

Durée : 3 jours

Participants : 10 Maximum

Prix

#### Public

- Consultants en sécurité
- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux

#### Pré-requis

- Niveau cours HSF/HSA

#### Moyens

- Support de cours
  - 80% d'exercices pratiques
  - 1 PC par personne / Internet
  - Environnement Virtualisé
- Windows de démonstration (Windows 2003 ...), et Linux.

#### Objectifs

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

#### Jour 1 : Méthodologie de l'Audit

##### Qu'est ce qu'un Pen Test ?

L'intérêt d'un PenTest  
Intégration d'un PenTest dans un Processus de sécurité général  
Définition de la politique de management sécurité et PenTest itératif.  
Organiser son intervention  
Préparer le référentiel  
La portée technique de l'Audit  
Réaliser le PenTest  
La prise d'information  
Acquisition d'accès  
Elévation de privilèges  
Maintien des accès sur le système  
Les traces de l'intrusion

##### Les Outils de PenTest

Les outils de Scan  
Les outils Réseaux  
Les outils d'analyse Système  
Les outils d'analyse Web  
Les outils d'attaque des collaborateurs  
Les outils de maintien des accès  
Les framework d'exploitation

#### Jour 2 : Mise en Situation d'audit

##### Mise en Situation d'Audit

Les stagiaires vont auditer sur la base d'un scénario se rapprochant le plus possible d'un cas réel, un réseau d'entrepri-se.

La journée est une succession de découvertes de vulnérabilités et d'exploitation de celles-ci en vue de pénétrer le réseau cible.

#### Jour 2 : Mise en Situation d'Audit (suite)

La partie théorique de la journée précédente est mise en pratique.

Le formateur guidera tout au long de l'audit les stagiaires et leur fera profiter de son expérience terrain.

Elaboration du planning

Répartition des tâches

#### Jour 3 : Mise en Situation d'audit (suite)

##### Préparation du rapport

Collecte des informations  
Préparation du document

##### Ecriture du rapport

Analyse globale de la sécurité du système  
Description des vulnérabilités trouvées  
Définition des recommandations de sécurité

##### Synthèse générale sur la sécurité du système

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