

Tests d'intrusion, mise en situation d'audit



PL-52 4 Jours (28 Heures)

Description

Le test d'intrusion, ou "PenTest", est une intervention technique qui permet de déterminer le réel potentiel d'intrusion et de destruction d'un pirate sur une infrastructure SI. Ce stage présente la démarche et les outils pour effectuer ce type de test et rédiger de manière professionnelle le rapport final d'audit.

À qui s'adresse cette formation ?

Pour qui

Responsable, architecte sécurité. Techniciens et administrateurs systèmes et réseaux. Auditeur amené à faire du "PenTest".

Prérequis

Aucun

Les objectifs de la formation

- Acquérir une méthodologie pour organiser un audit de sécurité de type test de pénétration sur son SI
- Evaluer les risques que court un système informatique face à une intrusion externe
- Réaliser un rapport final suite à un test d'intrusion
- Formuler des recommandations de sécurité

Programme de la formation

Introduction

- Evolution de la sécurité des SI.
- Etat des lieux de la sécurité informatique.
- L'état d'esprit et la culture du hacker.
- Quels risques et quelles menaces ?

Méthodologie de l'audit

- Qu'est-ce qu'un "PenTest" ? L'intérêt d'effectuer un test d'intrusion.
- Comment intégrer le test d'intrusion dans un processus de sécurité général.
- Apprendre à définir une politique de management de la sécurité et d'un "PenTest" itératif.
- Organiser et planifier l'intervention.
- Comment préparer le référentiel ? La portée technique de l'audit.
- Réaliser le "PenTest".
- La prise d'information.
- L'acquisition des accès.
- L'élévation de privilèges.
- Le maintien des accès sur le système.
- Les traces de l'intrusion.

Les outils de "PenTest"

- Quels outils utiliser ? Les outils de Scan et de réseau.
- Les outils d'analyse système et d'analyse Web.
- Les outils d'attaque des collaborateurs.
- Quel outil pour le maintien des accès ? Les frameworks d'exploitation.
- Mise en situation Les participants vont auditer un réseau d'entreprise sur la base d'un scénario se rapprochant le plus possible d'un cas réel.

Vulnérabilités et exploitation

- Découverte de nouvelles vulnérabilités.
- Comment les exploiter ? Réaliser le planning.
- La répartition des tâches.
- Travaux pratiques Identifier les nouvelles vulnérabilités.
- Exemple de réalisation d'un planning.

Le rapport final

- L'importance de la préparation du rapport.
- La collecte des informations.
- Préparation du document et écriture du rapport.
- L'analyse globale de la sécurité du système.
- Comment décrire les vulnérabilités trouvées ? Formuler les recommandations de sécurité.
- La synthèse générale sur la sécurité du système.
- Transmettre le rapport.
- Les précautions nécessaires.
- Que faire une fois le rapport transmis ? Réflexion collective Réalisation d'un rapport suite à un test d'intrusion.

Les équipements réseaux et le sans-fil

- Les vulnérabilités des composants du réseau.
- Comment les identifier ? Exploiter une faille liée à un composant.
- Le réseau sans fil.
- Les faiblesses du réseau Wi-Fi.
- Les actions de suivi.