Tests d'intrusion : Techniques et pratiques avancées

DOMAINE : *PenTest*
CATEGORIE : *Tests d'intrusion*

MISE A JOUR LE 13/01/2025

Descriptif

De nos jours, la sécurité informatique est devenue un enjeu de taille pour les **entreprises**. En effet, ces deux dernières années, **70% des cyberattaques** ont visé des **sociétés** pouvant causer des désagréments allant du vol de données jusqu'à la mise en danger des vies humaines. Il est indispensable que le tissu **industriel** se protège contre les **cybermenaces**.

Cette formation est conçue pour vous fournir les **compétences** et les connaissances nécessaires pour identifier, **exploiter et corriger** les **vulnérabilités** des systèmes d'information.

Les tests de pénétration, également connus sous le nom de **pentests**, sont une composante essentielle de la sécurité informatique. Ils permettent de simuler des **attaques réelles** afin de tester la robustesse des systèmes de sécurité d'une **organisation**. En suivant cette formation, vous apprendrez à planifier et exécuter des tests de pénétration de manière éthique et **professionnelle**, en utilisant les outils et **techniques** les plus **avancés** du domaine.

Informations

Référence	**CY-PT-TITPA**

Publics concernés

Administrateur réseau, développeur logiciel ou tout professionnel de la sécurité souhaitant approfondir ses connaissances

Formateur

Expert certifié en cybersécurité

Prérequis

Avoir des connaissances de base en sécurité, en réseau, en système d'exploitation et savoir rédiger des scripts

Certification préparée

Aucune

Objectifs

- Comprendre les principes **fondamentaux** des tests de pénétration.
- Apprendre à **planifier** et **organiser** des tests de pénétration
- Maîtriser les **outils** liés au **PenTest** tels que *Metasploit* et *Nmap*.
- Savoir **exploiter les vulnérabilités** des réseaux, systèmes et applications.
- **Analyser** les résultats des tests et rédiger des **rapports** détaillés.

Type de session

Intra-entreprise, **inter-entreprise** (en présentiel ou à distance)

Durée	4 jours (28 heures)
Date	À la demande
Tarif	2.450 € H.T
Effectif	12 participants max
Niveau	**Intermédiaire**
Délai d'accès	**3 semaines**

Programme

1) Planifier et organiser son travail

- Comprendre les concepts de gouvernance, de risque et de conformité
- Appliquer les bons outils et méthodologies en fonction de l'environnement client
- Comprendre le concept de hacking éthique

2) Collecte d'informations et analyse de vulnérabilité

- Effectuer une reconnaissance passive
- Effectuer une reconnaissance active
- Analyser les résultats d'une reconnaissance
- Rechercher des vulnérabilités

3) Attaques et exploitation

- Rechercher et appliquer des attaques sur des réseaux filaires
- Rechercher et appliquer des attaques basées sur des applications
- Rechercher et appliquer des attaques basées sur les technologies cloud
- Mettre en œuvre des attaques sur des IoT

4) Les autres types d'attaques

- L'engineering social
- Les attaques physiques

5) Les techniques post-exploitation

- Les outils permettant la post-exploitation
- L'escalade de privilèges
- Mise en œuvre de malware

6) Retranscrire les analyses

- Savoir communiquer son analyse
- Recommander les corrections appropriées
- Savoir communiquer les démarches post-analyse

7) Développement logiciel et pentests

- Structure interne d'une application
- L'analyse de code
- Initiation au scripting
- Les principaux outils

Ce programme peut être adapté pour des sessions plus courtes, plus longues ou selon des besoins spécifiques

Modalités pédagogiques

Nous mettons en œuvre des modalités pédagogiques **variées** afin de maintenir l'attention des participants. Cette formation s'appuiera sur :

- Une alternance théorie (35%) et pratique (65%).
- Des mises en situation réelle, études de cas et échanges de pratiques.
- Des mises à disposition d'outils numériques interactifs, collaboratifs et participatifs.

À la fin de la formation, toutes les ressources pédagogiques seront **mises à disposition** pour tous les participants via leur espace dédié.

Modalités d'évaluation et de suivi

Les acquis de l'action de formation sont **évalués** à partir des productions des participants lors des études de cas et à partir de quiz et exercices réguliers.

Un questionnaire **d'autoévaluation** au regard des objectifs de la formation vous sera transmis avant le début de la formation et à la fin de celle-ci, vous permettant ainsi de mesurer votre progression en fin de formation.

Information sur l'accessibilité

Nous remercions les personnes qui auraient des **besoins spécifiques** de nous le signaler dès leur inscription. Quel que soit le type de handicap, nous pouvons adapter certaines de nos modalités de formation en étudiant ensemble vos besoins. Pour toutes questions, merci de contacter notre **référent handicap** :

- Par mail à handicap@ghdeformation.fr
- Ou par téléphone au +33 06 78 84 71 24