

Mis à jour le 11/12/2023

S'inscrire

# Formation HackTheBox : Le perfectionnement en cybersécurité

3 jours (21 heures)

## Présentation

Découvrez notre formation sur la plateforme n°1 de perfectionnement en cybersécurité qu'est HackTheBox. Vous utiliserez tous les outils nécessaires pour améliorer continuellement vos capacités dans le domaine de la sécurité informatique.

Durant ce cours, approfondissez vos connaissances en piratant toute une série de machines différentes. Vous serez amenés à utiliser divers outils tels que Nmap, Metasploit ou John The Ripper pour vos actions.

Vous apprendrez des concepts de base tels que les [tests d'intrusion](#), les termes et les technologies communs ou les transferts de fichiers.

À l'issue de cette formation, les meilleures pratiques vous seront enseignées en matière de découverte des failles d'un système, d'erreur de configuration d'une base de données ou de mauvaise implémentation de formulaire d'upload.

Comme dans toutes nos formations, celle-ci vous sera présentée avec les toutes [dernières nouveautés](#) d'HackTheBox.

## Objectifs

- Comprendre l'environnement d'HackTheBox
- Analyser et identifier les failles de sécurité d'un système
- Maîtriser différents types d'attaques
- Savoir attaquer des systèmes de sécurité

## Public visé

- Pentesteurs
- Hackers éthiques
- Développeurs
- Chefs de projets
- Techniciens SSI

## Pré-requis

- Connaissance de Linux
- Connaissance de base sur des réseaux, des systèmes, de la sécurité
- Notion sur le pestesting

## Programme de la formation HackTheBox

### Introduction

- Qu'est-ce que HackTheBox ?
- Initiation à la sécurité informatique
- Termes communs
- Naviguer sur la plateforme HTB
- Premiers pas avec une distribution Pentest

### Empreintes

- Principes de dénombrement
- Énumération basée sur l'infrastructure
- Protocoles de gestion à distance Windows et Linux
- SNMP
- SMTP
- IPMI

### Processus de test de pénétration

- Présentation des tests d'intrusion
- Collecte d'informations
- Évaluation de la vulnérabilité
- Preuve de concept
- Pratique

### Attaque de mot de passe

- Présentation de l'outil John The Ripper
- Mutations de mot de passe
- Recherche d'informations d'identification dans Windows

- Chasse aux identifiants sous Linux
- Stockage des identifiants
- Attaques Pass the Hash
- Attaquer LSASS
- Attaquer Active Directory et NTDS.dit

## Attaque des services communs

- Concept d'attaques
- Recherche d'informations sensibles
- Exécution de code à distance
- Les vulnérabilités

## Attaquer les réseaux d'entreprises

- Accès initial
- Compromis d'Active Directory
- Service d'énumération et d'exploitation
- Collecte d'informations externe et interne

## Injection de commande

- Introduction aux injections de commande
- Identification des filtres
- Contournement des filtres d'espace
- Contournement des commandes sur liste noire
- Masquer les commandes avancées

## Transfert de fichiers

- Diverses méthodes de transfert de fichiers
- Transférer des fichiers avec du code
- Capture de fichiers via HTTP/S
- Méthodes courantes de détection

## Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

## Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant

d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

## Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

## Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

## Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

## Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.