



ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

Formation Test d'intrusion : expert

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

Théoriciens, passez votre chemin ! Cette formation de 5 jours est résolument orientée vers la pratique des tests d'intrusion. Elle est composée de 40% de cours et 60% d'exercices de simulation en environnement virtualisé. A l'issue de cette formation, vous saurez utiliser les méthodes et les outils vous permettant de découvrir et exploiter les vulnérabilités des systèmes d'information.

- | mettre en place un lab de pentest,
- | réaliser une veille en vulnérabilités,
- | mener des actions de repérage, prise d'information et social engineering,
- | effectuer des scans de réseaux simples ou en mode "stealth",
- | identifier et exploiter des vulnérabilités réseau (ex : man in the middle, DDoS...),
- | découvrir les méthodes et outils d'exploitation de vulnérabilités système (ex : Metasploit),
- | identifier et exploiter des vulnérabilités web (XSS, SQL...).

Référence	TI15
Durée	5 jours (35h)
Tarif	à partir de 3 500 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

- | Découvrir les vulnérabilités impactant les systèmes d'information.
- | Appréhender et mettre en oeuvre les techniques utilisées par les attaquants.
- | Maîtriser son risque et organiser la défense de son système d'information.

Public

- | RSSI, DSI
- | consultants en sécurité,
- | ingénieurs, techniciens,
- | administrateurs systèmes & réseaux,
- | développeurs

Prérequis

- | Connaissances de base en système, réseau et développement.
- | Connaissance de l'environnement Linux conseillée.

Programme de la formation

Introduction

- | Présentation de la formation
- | Rappels vocabulaire technique

Veille

- | Introduction à la veille technique
- | Sites & outils de veille

Prise d'information

- | Passive
- | Active
- | TP : Prise d'information

Ingénierie sociale

Etude de cas concret

Scan Réseau

- | Rappels protocole TCP/IP
- | Fonctionnement scanner de port
- | TP : Utilisation scanner de port

Vulnérabilités réseaux

- | Homme du milieu
- | Déni de service
- | TP : Exploitation de vulnérabilité réseau

Scanner de vulnérabilité

- | Fonctionnement scanner de vulnérabilité
- | TP : Utilisation scanner de vulnérabilité

Vulnérabilités systèmes

- | Présentation de Metasploit
- | TP : Exploitation de vulnérabilités système
- | Contournement d'anti-virus

Vulnérabilités clientes

- | Elévation de privilège
- | Attaques physiques

Vulnérabilités clientes

- | Injection de code client (XSS)
- | Cross-Site Request Forgery

Vulnérabilités serveurs

- | Injection SQL
- | Local file inclusion (LFI)
- | Faille d'upload

Exercice pratique : Mise en situation

- | Plateforme d'entraînement imitant un réseau d'entreprise.
- | Exploitation des vulnérabilités en environnement réel

Informations pratiques

Il est demandé aux stagiaires de se munir d'un ordinateur portable et d'installer l'outil gratuit "Virtual Box".

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Accessibilité



Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.

Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.