Prise en main de KALI Linux

DOMAINE : *Hacking étique*
CATEGORIE : *Offensive*

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 vise à fournir aux participants une introduction complète à **Kali Linux**. Cette distribution, très populaire est spécialisée dans les campagnes de **tests d'intrusion** (PenTest) et d'audit de sécurité.

Les participants seront en mesure de **configurer et mettre en œuvre** Kali Linux pour identifier et **exploiter** les vulnérabilités des systèmes informatiques.

Cette formation est un excellent **point d'entrée** à toute personne souhaitant s'initier au **PenTest**.

Informations

Référence	**CY-HE-KALI**

Publics concernés

Toute personne souhaitant approfondir ses connaissances en tests d'intrusion

Formateur

Expert certifié en cybersécurité

Prérequis

Avoir les connaissances de bases en réseau et être familier avec l'utilisation de la ligne de commande

Certification préparée

Aucune

Objectifs

- Être initié aux **tests de pénétration**.
- Savoir mettre en œuvre un **environnement Kali** Linux.
- Savoir **collecter** des données sur un **réseau**.
- Savoir rechercher et **exploiter** des vulnérabilités.

Type de session

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

Durée	3 jours (21 heures)
Date	À la demande
Tarif	1.550 € H.T
Effectif	12 participants max
Niveau	**Intermédiaire**
Délai d'accès	**3 semaines**

Programme

1) Introduction à Kali Linux

- Pourquoi utiliser Kali
- Différences avec les autres distributions
- Principales utilisations
- Cadre légal et éthique

2) Installation et configuration

- Installation à partir d'une image ISO
- Utilisation en mode Live-CD
- Mise en œuvre d'une machine virtuelle
- Installation sur architecture ARM
- Créer une image Kali personnalisée

3) Préparation de son environnement de test

- Configuration de base de Kali Linux
- Gestion des paquets
- Configuration du réseau

4) Présentation des outils de sécurité

- La collecte d'information
- L'analyse des vulnérabilités
- L'exploitation des failles

5) Exploitation des vulnérabilités

- Exploitation avec Metasploit
- Mise en œuvre de payloads
- Prise de contrôle à distance et élévation des privilèges

6) Technique d'analyse réseau

- Analyse du trafic avec Wireshark
- Le MAC spoofing et le changement d'adresse MAC
- Technique d'attaque Man in the Middle

7) La sécurité des réseaux sans fil

- Introduction à la sécurité des réseaux sans fil
- Le matériel compatible avec Kali pour les tests Wifi
- Mise en œuvre des outils Aircrack-ng et Reaver
- Analyse et contre-mesures

8) Attaques par force brute

- Principe de fonctionnement
- Mise en œuvre des outils Patator et THC-Hydra
- Attaque sur les services SSH, FTP et HTTP
- Les mesures de protection contre les attaques par force brute

9) Mise en pratique réelle

- Présentation du laboratoire de test
- Mise en œuvre de différentes attaques sur le système fictif
- Initiation au forensique et retour d'expérience
- Savoir effacer ses traces
- Bonnes pratiques

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 (55%).
- 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