+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 24/04/2024

S'inscrire

# Formation Kali Linux

3 jours (21 heures)

## Présentation

Notre formation Kali Linux vous offre une opportunité unique de maîtriser la distribution Linux spécialisée dans la sécurité informatique et le piratage éthique.

Kali Linux vous donne accès à une multitude d'outils de sécurité avancés et à jour, permettant d'effectuer des tests de sécurité, des audits et des analyses approfondies des réseaux et des systèmes informatiques.

Au cours de cette formation, nous vous guiderons à travers les aspects essentiels de Kali Linux, depuis ses bases jusqu'à ses applications avancées dans des scénarios professionnels.

Nous aborderons en détail son architecture, les méthodes d'installation et de configuration, ainsi que l'utilisation pratique de ses outils et de ses fonctionnalités. Vous apprendrez également les bonnes pratiques en matière de sécurité et de piratage éthique.

Comme pour toutes nos formations, notre formation Kali Linux vous présentera sa toute dernière version et ses nouveautés (à la date de rédaction de l'article : Kali Linux 2024).

## Objectifs

- Comprendre l'importance de Kali Linux en cybersécurité et les différences entre les pratiques Black Hat et White Hat.
- Savoir installer, configurer et sécuriser une installation de Kali Linux
- Maîtriser l'utilisation des outils de scan tels que Nmap et Nessus
- Apprendre les principes de base de l'exploitation des vulnérabilités avec Metasploit

## Public visé

- Pentesters

- Analystes en sécurité
- Administrateurs système

## Pré-requis

- Connaissances de base en informatique et en systèmes d'exploitation Linux
- Familiarité avec les concepts de sécurité informatique
- Capacité à utiliser la ligne de commande Unix/Linux
- Une expérience de développement logiciel serait bénéfique

## PROGRAMME DE NOTRE FORMATION KALI LINUX

### INTRODUCTION À KALI LINUX

- Présentation de Kali Linux et son importance en cybersécurité
- Différences entre les pratiques Black Hat et White Hat
- Aperçu des différents modes d'utilisation de Kali Linux
- Cadre légal des tests d'intrusion et de sécurité
- Orientation sur la structure du programme de formation

### INSTALLATION ET CONFIGURATION DE KALI LINUX

- Procédure d'installation de Kali Linux sur une machine virtuelle
- Configuration initiale et mise à jour du système
- Personnalisation de l'environnement de travail
- Réglages réseau et connexion à Internet
- Sécurisation de l'installation de Kali Linux

### DÉCOUVERTE DES VULNÉRABILITÉS AVEC KALI LINUX

- Introduction aux tests de vulnérabilité des systèmes
- Utilisation des outils de scan tels que Nmap et Nessus
- Interprétation des résultats et identification des failles
- Création de rapports de vulnérabilités
- Bonnes pratiques dans la gestion des vulnérabilités

### TECHNIQUES D'ANALYSE RÉSEAU

- Fondamentaux du réseau et utilisation des commandes de base
- Pratique de l'attaque Man in the Middle (MitM)
- Techniques de MAC spoofing et changement d'adresse MAC
- Analyse de trafic avec Wireshark
- Utilisation d'outils réseau spécifiques à Kali Linux

### EXPLOITATION DES VULNÉRABILITÉS

- Principes de base de l'exploitation de failles
- Utilisation de Metasploit pour l'exploitation des vulnérabilités
- Élaboration de payloads et écoute des connexions entrantes
- Prise de contrôle à distance et élévation des privilèges
- Documentation et rapport après exploitation

### ATTAQUES PAR FORCE BRUTE

- Compréhension des attaques par force brute et leurs implications
- Installation et utilisation de Patator et Thc-Hydra
- Configuration des attaques contre différents services (SSH, FTP, HTTP)
- Mesures de protection contre les attaques par force brute
- Analyse des résultats et mesures correctives

### SÉCURITÉ DES RÉSEAUX SANS FIL

- Introduction à la sécurité des réseaux WiFi
- Présentation du matériel compatible avec Kali Linux pour les tests WiFi
- Utilisation des outils comme Aircrack-ng et Reaver
- Techniques de sécurisation et prévention des attaques sur les réseaux sans fil
- Mise en place d'une attaque de test et analyse des contre-mesures

### SCRIPTING ET AUTOMATISATION

- Introduction au scripting avec Bash et Python
- Automatisation des tâches répétitives avec des scripts
- Développement d'outils personnalisés pour les tests de sécurité
- Gestion des résultats avec des scripts et des outils de reporting
- Exercices pratiques de scripting appliqués à la cybersécurité

### RÉVISIONS ET MISE EN PRATIQUE

- Révision des concepts clés et des outils étudiés durant la formation
- Mise en place d'un laboratoire de test pour la pratique des techniques apprises
- Simulation d'une évaluation de sécurité sur un système fictif
- Retour d'expérience et discussion sur les cas pratiques
- Conseils pour la veille technologique et la progression continue en cybersécurité

## 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.