Organisme de formation : ENDKOO, 4 Rue de la charité 69002 LYON, France sous le numéro SIRET 83475061400028. Enregistré sous le n° de déclaration d'activité :84691626269

ENDKOO›

Nom de la formation:	Formation DECOUVERTE Kali Linux 1/2 journée
Résumé de la formation:	Cette formation d'une demi-journée est destinée aux utilisateurs débutants de Kali Linux qui souhaitent comprendre les fonctionnalités de base de l'outil et utiliser les fonctionnalités avancées pour effectuer des tests de sécurité. La formation inclura des séances théoriques et des exercices pratiques pour permettre aux participants de mettre en pratique les compétences acquises.
Matériel :	Pour suivre la formation, les participants auront besoin d'un ordinateur avec une connexion internet et d'une installation de Kali Linux.
Pour qui :	Cette formation est destinée aux utilisateurs débutants de Kali Linux qui souhaitent comprendre les fonctionnalités de base de l'outil et utiliser les fonctionnalités avancées pour effectuer des tests de sécurité.
Enjeu :	Apprendre à utiliser les outils de Kali Linux pour effectuer des tests de sécurité sur les systèmes cibles. Apprendre à utiliser des outils d'analyse de sécurité professionnels pour tester la sécurité de votre réseau et de vos systèmes. Apprendre à utiliser Kali Linux pour effectuer des audits de sécurité, des tests d'intrusion et des pentests. Comprendre les concepts de base de la sécurité informatique et des vulnérabilités courantes. Apprendre à utiliser les outils de Kali Linux de manière efficace pour maximiser les résultats. Apprendre à utiliser les différents outils de Kali Linux en combinaison pour effectuer des analyses de sécurité complètes. Comprendre les risques associés à l'utilisation de Kali Linux et comment les éviter. Apprendre les meilleures pratiques de sécurité pour utiliser Kali Linux de manière éthique.
Prérequis :	Avoir une certaine aisance en informatique et de savoir utiliser un ordinateur de manière générale. Savoir naviguer sur internet et de savoir utiliser les navigateurs web courants. Il est conseillé d'avoir une bonne compréhension de base de l'anglais pour comprendre la documentation et les tutoriels disponibles. Avoir une certaine curiosité pour la cybersécurité et les outils d'analyse de sécurité. Il est souhaitable d'avoir une expérience dans les systèmes d'exploitation Linux, car Kali Linux est basé sur Debian Linux. Il est souhaitable d'avoir une bonne compréhension des concepts de sécurité tels que les vulnérabilités, les exploits et les outils d'analyse de sécurité. Etre disposé à apprendre de nouveaux concepts et de nouvelles technologies.
Objectifs :	A la fin de la formation, les participants seront en mesure d'utiliser les outils de Kali Linux pour effectuer des analyses de ports, des analyses de vulnérabilités, des cracks de mots de passe et des analyses de réseau sur les systèmes cibles.
Durée :	1/2 journée (3.5h)
Points forts et méthodes :	La formation est conçue pour être pratique et interactive, avec des exercices pratiques pour tester les compétences acquises. Les participants auront également l'occasion de

	mettre en pratique les compétences acquises dans un environnement de groupe. Le formateur est spécialisé dans le numérique depuis 2003. Méthodologie avec théorie à 50% et pratique à 50% (exercices en lignes)
Modalités :	Formation à distance uniquement via Microsoft Teams
Délais d'accès :	Formation intra entreprise – Délais à négocier avec l'entreprise dont inférieur à 2 mois
Support pédagogique :	Un support pédagogique et une palette d'exercice sera remis à chaque participant
Les modalités d'évaluations des acquis :	En début et en fin de formation, les stagiaires h/f réalisent un test de positionnement (auto évaluation) via GoogleForms de leurs connaissances et compétences en liens avec les objectifs de la formation. L'écart entre les 2 évaluations permet de mesurer leurs acquis.
Accessibilité aux personnes handicapées :	Le support de formation est disponible en format numérique, il est accessible aux personnes handicapées en utilisant des outils d'accessibilité.
Les modalités d'évaluations de la satisfaction et suivi de la prestation	Dans le cadre de notre démarche qualité, toutes nos formations font l'objet d'une évaluation « à chaud » (en fin de formation) et « à froid » (4 mois après la fin de la formation) par stagiaire h/f. Une feuille d'émargement sera signée par demie journée pour chaque stagiaire ainsi que pour le formateur qui justifiera la présence des participants.
Tarifs :	445€HT
Programme de formation:	Introduction à Kali Linux (30 minutes) :
	But: Donner aux participants une compréhension de base de Kali Linux, y compris ses fonctionnalités, son utilisation et ses outils de piratage éthique.
	Exercice : Installation de Kali Linux en utilisant VirtualBox
	Navigation de base de Kali Linux (45 minutes) :
	But: Apprendre aux participants à naviguer dans le système d'exploitation Kali Linux et à utiliser les commandes de base.
	Exercice : Utilisation des commandes de base pour naviguer dans le système de fichiers de Kali Linux
	Outils de sécurité de Kali Linux (1 heure) :
	But: Présenter aux participants les différents outils de sécurité de Kali Linux et leur utilisation pour tester la sécurité des réseaux.
	Exercice : Utilisation de Nmap pour scanner les ports d'un système cible.

ENDKOO›

	Attaques de réseau de base avec Kali Linux (45 minutes) :
	But: Apprendre aux participants les différentes méthodes d'attaque de réseau de base et comment les utiliser avec Kali Linux.
	Exercice : Utilisation de Metasploit pour exploiter une vulnérabilité de sécurité dans un système cible.
	Conclusion (15 minutes) :
	Résumé de la formation et des points clés appris.
	Questions et réponses.