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 DEBUTANTE sur Kali Linux 3 journées
Résumé de la formation:	Cette formation de 3 jours (7 heures par jour) 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 :	3 jours (21 heures)
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 :	2500€HT
Programme de formation:	Jour 1 :
	Présentation de Kali Linux (1 heure) : Présentation de l'outil, des fonctionnalités et des concepts de base
	But: Comprendre les fonctionnalités de base de Kali Linux et son utilisation pour les tests de sécurité
	Exercice: Installation de Kali Linux sur un ordinateur virtuel
	Utilisation de la ligne de commande (2 heures) : Apprentissage des étapes de base de l'utilisation de la ligne de commande, utilisation des commandes fondamentales.
	But: Apprendre à utiliser les commandes de base pour naviguer dans l'interface de Kali Linux
	Exercice: Utilisation de commandes de base pour naviguer dans le système de fichiers et afficher les informations système
	Jour 2:
	Utilisation des outils de reconnaissance de ports (3 heures) : Apprentissage des étapes de l'analyse des ports, utilisation des outils Nmap et Zenmap
	But: Comprendre les étapes pour analyser les ports d'un système cible
	Exercice: Analyse des ports d'une machine cible

	Utilisation des outils d'analyse de vulnérabilité (2 heures) : Apprentissage des étapes de l'analyse des vulnérabilités, utilisation des outils OpenVAS et Nessus.
	But: Comprendre les étapes pour analyser les vulnérabilités d'un système cible
	Exercice: Analyse des vulnérabilités d'une machine cible
	Jour 3:
	Utilisation des outils de cracking de mot de passe (3 heures) : Apprentissage des étapes de cracking de mots de passe, utilisation des outils John the Ripper et Hashcat.
	But: Comprendre les étapes pour cracker les mots de passe d'un système cible
	Exercice: Cracking de mots de passe d'un compte utilisateur
	Utilisation des outils d'analyse de réseau (2 heures)
	Apprentissage des étapes de l'analyse de réseau, utilisation des outils Wireshark et Tcpdump
	But: Comprendre les étapes pour analyser les paquets réseau d'un système cible
	Exercice: Analyse des paquets réseau d'un système cible