Kali Linux, démarrer l'analyse de la sécurité de son infrastructure

Formation en ligne - 1h15
Réf : 4DJ - Prix 2024 : 95CHF HT

Ce cours en ligne a pour objectif de vous apprendre à installer et à utiliser la distribution Kali Linux, regroupant l'ensemble des outils nécessaires pour réaliser des tests de sécurité. Il s'adresse à toute personne devant réaliser des tests de sécurité informatique dans son entreprise. La pédagogie s'appuie sur un auto-apprentissage séquencé par actions de l'utilisateur sur l'environnement à maîtriser. Une option de tutorat vient renforcer l'apprentissage.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Installer et utiliser la distribution Kali Linux

Analyser les vulnérabilités avec Nessus

Tester votre réseau avec Macchanger ou Macof

Comprendre le concept de Man in The Middle, ainsi que les outils d'attaque par force brute.

Gérer la sécurisation d'un réseau WiFi

PÉDAGOGIE ET PRATIQUES

Une évaluation tout au long de la formation grâce à une pédagogie active mixant théorie, exercice, partage de pratique et gamification. Un service technique est dédié au support de l'apprenant. La formation est diffusée au format SCORM (1.2) et accessible en illimité pendant 1 an.

ACTIVITÉS DIGITALES

Démonstrations, cours enregistrés, partages de bonnes pratiques, quiz, fiches de synthèse.

PARTICIPANTS

Personnes devant réaliser des tests de sécurité informatique dans leur entreprise.

PRÉREQUIS

Connaissances sur l'utilisation d'un système Linux.

COMPÉTENCES DU FORMATEUR

Les experts qui ont conçu la formation et qui accompagnent les apprenants dans le cadre d'un tutorat sont des spécialistes des sujets traités. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

La progression de l'apprenant est évaluée tout au long de sa formation au moyen de QCM, d'exercices pratiques, de tests ou d'échanges pédagogiques.
Sa satisfaction est aussi évaluée à l'issue de sa formation grâce à un questionnaire.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : documentation et support de cours, exercices pratiques d'application et corrigés des exercices, études de cas ou présentation de cas réels.
ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une attestation de fin de formation est fournie si l'apprenant a bien suivi la totalité de la formation.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

LE PROGRAMME

dernière mise à jour : 06/2023

1) Découverte de Kali Linux

- L'intérêt de Kali Linux.
- Les différents modes.
- Le Black Hat et le White Hat.
- La législation pour l'exécution des tests.

2) Installation de Kali Linux

- Introduction.
- Installation de Kali Linux sur une machine virtuelle.
- Mise à jour de la distribution Kali Linux.
- Présentation de l'environnement.

3) Configuration de Kali Linux

- Modification de la langue du clavier.
- Réglage de la résolution de l'écran.
- Réglages réseau.
- Mise à jour de la distribution.

4) Découverte des vulnérabilités
- Présentation des tests de vulnérabilité du système.
- Présentation des outils du marché.
- Présentation de Nessus.

5) Installation et utilisation de Nessus
- Présentation de la maquette de test.
- Installation de Nessus.
- Utilisation de Nessus sur la maquette réseau.
- Création de rapports.

6) Prise en main de Kali Linux et du réseau
- Présentation du principe de Man in the Middle.
- Changement d'une adresse MAC.
- Découverte du MAC spoofing.
- Réalisation d'une analyse DNS.

7) Utilisation des outils réseau
- Installation et utilisation de MAC Changer.
- Installation et utilisation de Macof.
- Installation et utilisation de DNSmap.
- Installation et utilisation de THC-IPv6 Attack Toolkit.

8) Découverte de l'attaque par force brute avec Kali Linux
- Présentation du principe de l'attaque par force brute.
- Présentation des méthodes d'attaque par force brute.

9) Utilisation d'outils d'attaque par force brute
- Installation et utilisation de Patator.
- Installation et utilisation de Thc-Hydra et Hydra-gtk.

10) Gestion de la sécurité WiFi
- Sécurisation d'un réseau WiFi.
- Présentation du matériel WiFi compatible avec Kali Linux.
- Découverte du WiFi Honey.
- Présentation des outils.