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

Mis à jour le 15/11/2024

S'inscrire

Formation Certification KLCP™ (PEN-103)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF AVEC LE COURS PEN-103

2 jours (14 heures)

PRÉSENTATION

Vous souhaitez démontrer vos compétences en sécurité offensive et maîtriser les outils de Kali Linux ? Notre formation à la certification KLCP (PEN-103) vous permettra d'acquérir une large gamme de compétences et de connaissances essentielles pour les tests de pénétration et la sécurité informatique.

Au cours de cette formation, vous apprendrez à utiliser et configurer Kali Linux, à exploiter manuellement des vulnérabilités, et à mener des tests de pénétration complets. Vous développerez des compétences approfondies en reconnaissance, scanning, exploitation et post-exploitation de cibles.

Cette formation vous enseignera également à sécuriser les systèmes et réseaux, à utiliser des outils avancés de Kali Linux pour l'analyse de réseaux et les tests de sécurité, et à comprendre les concepts clés de la sécurité informatique.

Après avoir suivi notre préparation, vous serez prêt à passer la certification Kali Linux Certified Professional (KLCP).

OBJECTIFS

- Comprendre et utiliser les outils de Kali Linux pour les tests de sécurité
- Reconnaître et exploiter les vulnérabilités réseau et web
- Maîtriser les concepts de base de la sécurité informatique
- Exécuter des tests de pénétration complets, de la reconnaissance à la post-exploitation
- Obtenir la certification Kali Linux Certified Professional (KLCP)

PUBLIC VISÉ

- Pentesters
- Hackers éthiques
- Administrateurs système et réseau
- Développeurs et architectes techniques
- Analystes en sécurité informatique

Pré-requis

- Connaissance de base de Linux et des systèmes d'exploitation
- Connaissance de base des réseaux informatiques
- Maîtrise de l’anglais technique

Pré-requis logiciels

- **Kali Linux** --> Téléchargeable ici

Note : Ambient IT n’est pas propriétaire de KLCP™, cette certification appartient à OffSec ® Services LLC.

PROGRAMME DE NOTRE FORMATION CERTIFICATION KLCP™

INTRODUCTION À WEB-103

- Présentation de la certification PEN-103 et de ses objectifs
- Compréhension des concepts de base de la sécurité informatique
- Reconnaître l'état d'esprit nécessaire à un professionnel de la sécurité
- Introduction aux concepts de la triade de la sécurité : Confidentialité, Intégrité, Disponibilité (CIA)
- Terminologie clé et caractéristiques uniques du domaine
- Introduction aux outils de base de Kali Linux
- Vue d'ensemble des laboratoires et configuration du VPN

DÉMARRAGE AVEC LES OUTILS DE BASE

- Modification et configuration du fichier /etc/hosts
- Tests de validation des modifications du fichier d'hôtes
- Introduction aux proxys et utilisation de Burp Suite
- Utilisation de Nmap pour le scanning et l’exécution de scripts NSE
- Concept de listes de mots et leur utilisation avec Gobuster
- Utilisation de Wfuzz pour la découverte de fichiers et de répertoires
- Utilisation de hakrawler pour le crawling et le spidering

TESTS DE PÉNÉTRATION WEB

- Introduction aux concepts de test de pénétration web
- Identification et exploitation des vulnérabilités XSS (Cross-Site Scripting)
- Utilisation de JavaScript pour exfiltrer des données
- Exploitation des serveurs réfléchis et stockés XSS
- Introduction et exploitation des attaques CSRF (Cross-Site Request Forgery)
- Compréhension et exploitation des politiques CORS faibles
- Étude de cas sur l’exploitation des vulnérabilités web

SCANS ET ANALYSE DES RÉSEAUX

- Introduction aux outils de scanning de réseau
- Utilisation avancée de Nmap pour la découverte et l’énumération
- Analyse des paquets réseau avec Wireshark
- Surveillance des connexions réseau avec Netstat et lsof
- Tests de performance réseau avec iperf et hping
- Configuration et utilisation des outils WiFi (aircrack-ng suite)
- Analyse des vulnérabilités réseau avec OpenVAS

SÉCURITÉ ET ADMINISTRATION SYSTÈME

- Concepts de sécurité et administration de base sous Linux
- Gestion des utilisateurs et des permissions
- Configuration des pare-feux (iptables, ufw)
- Cryptographie : utilisation de GPG et OpenSSL
- Sécurisation des services réseau (SSH, FTP, Web)
- Audit de sécurité et journalisation avec syslog
- Outils avancés de sécurité (Metasploit Framework)

TECHNIQUES D'EXPLOITATION ET POST-EXPLOITATION

- Introduction aux techniques d’exploitation
- Utilisation de Metasploit pour l'exploitation des vulnérabilités
- Techniques d'exploitation manuelles et scripts
- Maintien de l'accès et élévation de privilèges
- Mouvement latéral et persistance sur les systèmes compromis
- Exfiltration de données et contournement des mesures de sécurité
- Techniques de nettoyage et anti-forensic

PRATIQUES ET SIMULATIONS

- Mise en place d’un environnement de laboratoire sécurisé
- Simulation de scénarios de test de pénétration réalistes
- Exercices pratiques avec les outils de Kali Linux
- Participation à des challenges Capture The Flag (CTF)
- Analyse de cas réels d’incidents de sécurité
- Révisions et préparation à l’examen KLCP
- Session de questions et réponses pour clarification et révisions finales

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.