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

Mis à jour le 08/10/2024

S'inscrire

Formation PacketFence

2 jours (14 heures)

Notre formation PacketFence vous propose une immersion complète dans cette solution open source de gestion des accès réseau (NAC), spécialement conçue pour sécuriser et contrôler les connexions dans des environnements hétérogènes.

PacketFence permet d'automatiser la détection et la gestion des équipements réseau, d'assurer un contrôle d'accès basé sur les rôles et d'offrir des portails captifs pour l'authentification des utilisateurs, ce qui en fait un outil incontournable pour les administrateurs réseau et les équipes de sécurité informatique.

Grâce à sa compatibilité avec les principaux équipements réseau (Cisco, Aruba, etc.), PacketFence s'intègre facilement à des infrastructures existantes tout en permettant une gestion fine de la sécurité, allant de la détection d'anomalies à l'isolement des périphériques suspects.

Durant cette formation, vous apprendrez à installer, configurer et gérer PacketFence, à intégrer la solution avec vos équipements réseau, et à définir des politiques de sécurité avancées pour mieux protéger vos ressources critiques.

Vous découvrirez également comment utiliser PacketFence pour surveiller les incidents en temps réel et appliquer des sanctions automatiques aux violations des règles de sécurité réseau.

Cette formation vous permettra de développer des compétences clés pour renforcer la sécurité de votre infrastructure réseau tout en optimisant la gestion des utilisateurs et des périphériques connectés.

Comme pour toutes nos formations, elle sera accompagnée des dernières ressources et des meilleures pratiques du domaine.

Objectifs

- Maîtriser les principes de base de PacketFence et son installation
- Gérer les utilisateurs, périphériques et invités via le portail captif
- Intégrer PacketFence avec les équipements réseau
- Configurer et appliquer des politiques de sécurité réseau basées sur les rôles
- Surveiller et maintenir PacketFence

Public visé

- Administrateurs réseau
- Ingénieurs en sécurité
- Techniciens systèmes et réseaux
- Responsables informatiques

Pré-requis

- Connaissance de base des réseaux TCP/IP
- Expérience en gestion de réseaux ou sécurité informatique
- Familiarité avec les concepts d'accès réseau (VLAN, 802.1X) et les équipements réseau (commutateurs, routeurs)
- Une expérience avec les outils RADIUS et LDAP est un plus

PROGRAMME DE NOTRE FORMATION PACKETFENCE

Introduction à PacketFence

- Présentation de la sécurité réseau et de la gestion des accès
- Objectifs de PacketFence : contrôle d'accès, gestion des invités, isolation des périphériques
- Historique et évolution de PacketFence
- Cas d’utilisation dans les environnements réseau
- Fonctionnalités principales : détection des anomalies, portail captif, intégration avec les équipements
- Prérequis techniques pour l’installation de PacketFence

Installation et configuration initiale

- Préparation de l'environnement serveur pour PacketFence (OS, matériels)
- Installation de PacketFence via les paquets et les sources
- Paramètres de base : adresses IP, certificats SSL et DNS
- Configuration des interfaces réseau (gestion, isolation, enregistrement)
- Connexion au serveur PacketFence et découverte de l'interface web d’administration
- Vérification du bon fonctionnement initial

Gestion des utilisateurs et des périphériques

- Création et gestion des utilisateurs dans PacketFence
- Utilisation des rôles et des permissions pour les utilisateurs
- Gestion des périphériques : ajout, suivi et audits
- Introduction au portail captif pour l’authentification des utilisateurs
- Gestion des invités et inscription automatique des périphériques
- Utilisation des API pour l'intégration avec les systèmes externes

Intégration avec les équipements réseau

- Intégration avec les commutateurs et points d’accès (Cisco, Aruba, etc.)
- Configuration du mode VLAN dynamique pour la segmentation réseau
- Introduction à la gestion du 802.1X et RADIUS avec PacketFence
- Utilisation des ACL pour la gestion de l’accès réseau
- Surveillance des périphériques sur le réseau : détection et réponse
- Dépannage des connexions avec les équipements réseau

Politiques de sécurité et d'accès réseau

- Définition des politiques de sécurité basées sur les rôles et les profils
- Gestion des violations et des sanctions : quarantaine, blocage
- Configuration des règles de sécurité
- Introduction aux méthodes d’authentification : SSO, LDAP, RADIUS
- Gestion des certificats et des méthodes de sécurité avancées
- Implémentation de la surveillance en temps réel et des alertes

Surveillance et maintenance du réseau

- Utilisation des journaux d’activité pour la surveillance et l'audit
- Surveillance des incidents et gestion des alertes en temps réel
- Stratégies de dépannage des incidents réseau liés à PacketFence
- Mise à jour et maintenance de PacketFence (correctifs et nouvelles versions)
- Sauvegarde et restauration de la configuration PacketFence
- Étapes pour la mise en production et bonnes pratiques de déploiement

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.