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

Mis à jour le 27/05/2024

S'inscrire

Formation Nessus

3 jours (21 heures)

Présentation

Savez-vous que Nessus est la référence n° 1 pour l'évaluation des vulnérabilités ? Notre formation Nessus vous apprendra à utiliser cette technologie conçue pour la surface d'attaque moderne.

Durant ce cours, vous explorez plusieurs fonctionnalités telles que la détection de vulnérabilités , la cartographie réseau, l'automatisation des scans ainsi que la gestion des correctifs.

Nessus vous permettra de dépasser le cadre de vos assets IT en renforçant vos applications web, en obtenant de la visibilité sur votre surface d'attaque et en sécurisant votre infrastructure cloud.

L'évaluation des vulnérabilités ne sera jamais aussi simple, intuitive et facile avec cette technologie. Nessus est déployable sur une grande variété de plateformes pour résoudre toutes les erreurs efficacement.

Comme pour toutes nos formations, notre formation Nessus vous présentera sa toute dernière version et ses nouveautés (à la date de rédaction de l'article : Nessus 10.7.2).

Objectifs

- Maîtriser le déploiement et la configuration de Nessus
- Appliquer les meilleures pratiques en sécurité informatique et gestion des vulnérabilités
- Configurer et gérer des scanners avancés et surveiller leur performance

Public visé

- Auditeurs
- Administrateurs système

- Ingénieurs en sécurité

Pré-requis

- Compréhension des réseaux informatiques et des concepts de sécurité
- Expérience de base en configuration et en administration système

PROGRAMME DE NOTRE FORMATION NESSUS

INTRODUCTION À NESSUS

- Présentation de Nessus et de son positionnement dans la sécurité informatique
- Notes de version et nouveautés
- Exigences système, matérielles et logicielles
- Gestion de la politique SELinux en mode Enforcing
- Compréhension des exigences de licence

DÉPLOIEMENT

- Configuration des ports nécessaires pour Nessus
- Configuration des pare-feu basés sur l'hôte
- Support d'IPv6 et limitations de NAT
- Interaction avec les logiciels antivirus et avertissements de sécurité

INSTALLATION DE NESSUS

- Installation sur différentes plateformes : Linux, Windows, macOS, Raspberry Pi
- Déploiement de Nessus en tant qu'image Docker
- Validation de l'installation et résolution des problèmes courants

CONFIGURATION DE NESSUS

- Installation des différentes versions de Nessus : Essentials, Professional, Expert, Manager
- Processus d'activation et liaison avec Tenable VM, Nessus Manager et Security Center
- Gestion du code d'activation et mise à jour des plugins

GESTION DE NESSUS HORS LIGNE

- Procédures d'installation et de mise à jour hors ligne
- Mise à jour manuelle de Nessus Manager sur un système hors ligne
- Gestion de l'entrepôt d'audit hors ligne

SCANS ET MODÈLES DE SCANS

- Création et gestion des scans
- Compréhension des résultats des scans et des politiques de scan
- Utilisation des plugins et création de rapports personnalisés
- Exercices pratiques de scan

SCANS D'APPLICATIONS WEB AVEC NESSUS

- Introduction au balayage des applications Web avec Nessus
- Configuration des scans spécifiques aux applications Web
- Identification des vulnérabilités web courantes

CONFIGURATION DES SCANNERS ET PARAMÈTRES AVANCÉS

- Configuration du serveur LDAP avec Tenable Nessus Manager
- Réglages avancés du serveur proxy et SMTP
- Utilisation d'une autorité de certification personnalisée (CA)

SURVEILLANCE ET DÉBOGAGE AVANCÉ

- Surveillance du scanner Nessus
- Techniques de débogage avancé et la capture de paquets
- Gestion des notifications et des comptes utilisateurs

SÉCURITÉ INFORMATIQUE ET GESTION DES VULNÉRABILITÉS

- Meilleures pratiques en matière de sécurité informatique et gestion des vulnérabilités
- Importance de la conformité aux normes de sécurité
- Exercices pratiques pour renforcer l'application des connaissances

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.