Nessus, conduire un audit de vulnérabilités

Cours Pratique de 2 jours - 14h
Réf : NES - Prix 2024 : 1 660€ HT
Le prix pour les dates de sessions 2025 pourra être révisé

Nessus est une solution de référence pour auditer les vulnérabilités d'un système d'information. Vous apprendrez dans ce cours à mener un audit de vulnérabilités sur les réseaux, les applications Web, les systèmes d'exploitation, les équipements et les injections de différents types de codes malveillants.

OBJECTIFS PÉDAGOGIQUES

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

Installer et configurer Nessus

Utiliser le client Nessus

Conduire un audit de vulnérabilités avec Nessus

Conduire un audit de configuration de systèmes Windows et Linux

LE PROGRAMME

dernière mise à jour : 01/2018

1) Contexte et positionnement de Nessus

- Terminologie et référentiels relatifs aux vulnérabilités (CVE, CWE, CVSS, AWS, CERT...).
- Audit de sécurité versus audit de vulnérabilités et test de pénétration.
- Positionnement des différents outils et approches de sécurité : la détection d'intrusions, le scanner.
- Les outils d'audit de vulnérabilités (Snort, Suricata, Nessus, OpenVas, Qualys, Acunetix...).
- Le scan de vulnérabilités réseaux, systèmes et applications (outils, démarche et limites).
- Présentation des produits Nessus.
- Le mode de fonctionnement client/serveur.
- La configuration et scan de base de réseaux.

Travaux pratiques : Installation, configuration et scan de base de réseaux.

2) Composants et architectures de Nessus

- Architecture et fonctionnalités de Nessus.
- L'intégration des plug-ins : gestion et conception de plug-ins.
- Le déploiement de manager, agent.
- La gestion des licences.

Travaux pratiques : Configuration et paramétrages. Gestion et conception de plug-ins.

3) Politique : conception et analyse

- Définition d'une politique de scan basique.
- Définition et gestion d'une politique de découverte (hôte, port, service).
- Création, configuration et planification d'un scan de vulnérabilité avancé.
- Opérations de scan de vulnérabilités : scans d'applications Web vulnérables, scans actifs, scans authentifiés.
- Audit de vulnérabilités d'applications Web.

PARTICIPANTS

Techniciens, administrateurs systèmes et réseaux et auditeurs amenés à faire du "PenTest".

PRÉREQUIS

Connaissances de base en réseaux et sécurité.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. 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 qu'ils enseignent. 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

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

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.

- Conception d'une politique de sécurité.
Travaux pratiques : Conception d'une politique de sécurité et d'audit de vulnérabilités. Mise en œuvre d'une plateforme Web et audit de vulnérabilités d'applications Web.

4) Audit de configuration et de vulnérabilités : mise en œuvre et analyse
- Principes de l'audit de configuration.
- Introduction à l'audit de conformité.
- Principes des audits de systèmes : Windows, Linux/Unix.
- Audit de système, d'environnement virtuel.
- Le reporting et l'analyse des vulnérabilités.
Travaux pratiques : Audit de configuration de systèmes Windows et Linux.

LES DATES

CLASSE À DISTANCE
2024 : 02 déc.

2025 : 24 mars, 30 juin, 29 sept., 27 nov.

PARIS
2025 : 17 mars, 23 juin, 22 sept., 20 nov.