Date de publication : 31/01/2024

Formation : Tests d'intrusion, organiser son audit

Cours pratique - 4j - 28h00 - Réf. TEI
Prix : 2890 € H.T.

4,6 / 5

Clé en main

Formation éligible au financement Mobilités

Le test d'intrusion ou Pentest, est une intervention technique qui permet de déterminer le réel potentiel d'intrusion et de destruction d'un pirate sur une infrastructure SI. Ce cours présente la démarche et les outils pour effectuer ce type de test et rédiger de manière professionnelle le rapport final d'audit.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Acquérir une méthodologie pour organiser un audit de sécurité de type test de pénétration sur son SI
- Rédiger un rapport final suite à un test d'intrusion
- Formuler des recommandations de sécurité

Public concerné

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux. Auditeurs amenés à faire du Pentest.

Prérequis

Bonnes connaissances de la sécurité informatique (matériel, architectures réseau, architectures applicatives). Expérience requise.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Après une première journée dédiée aux rappels et à la préparation de l'environnement, les journées suivantes seront consacrées à la réalisation des tests d'intrusion en situation réelle.

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux. Auditeurs amenés à faire du Pentest.

PRÉREQUIS

Bonnes connaissances de la sécurité informatique (matériel, architectures réseau, architectures applicatives). Expérience requise.

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.

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.

Programme de la formation

1 Les menaces

- Evolution de la sécurité des SI.
- Etat des lieux de la sécurité informatique.
- L'état d'esprit et la culture du hacker.
- Quels risques et quelles menaces ?

2 Méthodologie de l'audit

- Le contexte règlementaire.
- L'intérêt d'effectuer un test d'intrusion, un Pentest, les différents types de Pentest.
- Comment intégrer le test d'intrusion dans un processus de sécurité général.
- Apprendre à définir une politique de management de la sécurité et d'un Pentest itératif.
- Organiser et planifier l'intervention. Comment préparer le référentiel ?
- La portée technique de l'audit. Réaliser le Pentest.

Travaux pratiques

Réaliser un audit.

3 Les outils de Pentest

- Quels outils utiliser ? Sont-ils vraiment indispensables ?
- La prise d'information. L'acquisition des accès.
- L'élévation de privilèges. Le maintien des accès sur le système.
- Les outils de Scan et de réseau.
- Les outils d'analyse système et d'analyse Web.
- Les outils d'attaque des collaborateurs.
- Quel outil pour le maintien des accès ?
- Les frameworks d'exploitation.

Travaux pratiques

Manipulation d'outils de Pentest. Utilisation d'outils de scan.

4 Rédaction du rapport

- Collecter les informations.
- Préparation du document et écriture du rapport.
- L'analyse globale de la sécurité du système.
- Décrire les vulnérabilités trouvées.
- Formuler les recommandations de sécurité.

Réflexion collective

Réalisation d'un rapport suite à un test d'intrusion.

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 formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation 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 participant 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

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Mises en situation

- Interception de flux HTTP ou HTTPS mal sécurisés.
- Test d'intrusion sur une adresse IP.
- Test d'intrusion d'applications client-serveur : FTP , DNS , SMTP.
- Tests d'intrusion d'applications Web (SQL Injection, XSS , vulnérabilité d'un module PHP et d'un CMS).
- Tests d'intrusion interne : compromission via une clé USB piégée et via un PDF malicieux.

Travaux pratiques
Les participants vont auditer un réseau d'entreprise sur la base d'un scénario d'un cas réel.

Parcours certifiants associés

Pour aller plus loin et renforcer votre employabilité, découvrez les parcours certifiants qui contiennent cette formation :

- Parcours certifiant Manager la cybersécurité des systèmes, applications et bases de données - Réf. ZCN

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle.
Découvrez-les sur notre page Comment financer sa formation ou contactez votre conseiller formation.

Financement par les OPCO

- Adhérents Mobilités, découvrez les avantages négociés par votre OPCO en cliquant ici

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.
Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.
Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Dates et lieux

CLASSE À DISTANCE
2026 : 31 mars, 2 juin, 22 sep.

PARIS LA DÉFENSE
2026 : 2 juin, 22 sep.