Tests d'intrusion, organiser son audit

Cours Pratique de 4 jours - 28h
Réf : TEI - Prix 2024 : 2 790€ HT

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 stage 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 l'apprenant 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

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.

LE PROGRAMME

dernière mise à jour : 03/2020

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.

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.

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.

- 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.

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.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 28 mai, 09 juil., 22 oct.	2024 : 21 mai, 02 juil., 15 oct.