Cybersécurité, tester ses environnements
attaquer, détecter, collecter et analyser

Cours Pratique de 3 jours - 21h
Réf : CTE - Prix 2024 : 2 390€ HT

Cette formation avancée vous apprendra les techniques indispensables pour mesurer le niveau de sécurité de votre Système d'Information. A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à élever le niveau de sécurité de votre réseau.

OBJECTIFS PÉDAGOGIQUES

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

Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques

Mesurer le niveau de sécurité de votre Système d'Information

Réaliser un test de pénétration

LE PROGRAMME

dernière mise à jour : 07/2022

1) Les attaques Web

- OWASP : organisation, chapitres, Top10, manuels, outils.
- Découverte de l'infrastructure et des technologies associées, forces et faiblesses.
- Côté client : clickjacking, CSRF, vol de cookies, XSS, composants (flash, java). Nouveaux vecteurs.
- Côté serveur : authentification, vol de sessions, injections (SQL, LDAP, fichiers, commandes).
- Inclusion de fichiers locaux et distants, attaques et vecteurs cryptographiques.
- Evasion et contournement des protections : exemple des techniques de contournement de WAF.
- Outils Burp Suite, ZAP, Sqlmap, BeEF.

Mise en situation : Présentation et prise en main des environnements, outils. Mise en œuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

2) Détecter les intrusions

- Les principes de fonctionnement et méthodes de détection.
- Les acteurs du marché, panorama des systèmes et applications concernés.
- Les scanners réseaux (Nmap) et applicatifs (Web applications).
- Les IDS (Intrusion Detection System).
- Les avantages de ces technologies, leurs limites.
- Comment les placer dans l'architecture d'entreprise ?
- Panorama du marché, étude détaillé de SNORT.

Mise en situation : Présentation et prise en main des environnements, outils. Installation, configuration et mise œuvre de SNORT, écriture de signature d'attaques.

3) La collecte des informations

- L'hétérogénéité des sources. Qu'est-ce qu'un événement de sécurité ?
- Le Security Event Information Management (SIEM). Les événements collectés du SI.
- Les journaux système des équipements (firewalls, routeurs, serveurs, bases de données, etc.).

PARTICIPANTS

Responsables, architectes sécurité. Techniciens et administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances en sécurité SI, réseaux, systèmes (en particulier Linux).

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.

- La collecte passive en mode écoute et la collecte active.

Mise en situation : Démarche d'une analyse de log. La géolocalisation d'une adresse. La corrélation de logs d'origines différentes, visualiser, trier et chercher les règles.

LES DATES

CLASSE À DISTANCE
2024 : 22 avr., 15 juil., 28 oct., 09 déc.

PARIS
2024 : 08 juil., 21 oct., 16 déc.