Formation Cybersécurité, tester ses environnements

Attaquer, détecter, collecter et analyser

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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.

Référence	CTE
Durée	3 jours (21h)
Tarif	2 390 €HT
Repas	repas inclus

Objectifs

| 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

Public

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

Prérequis

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

Programme de la formation

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 oeuvre de différentes attaques Web en conditions réelles côté serveur et côté client.

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 oeuvre de SNORT, écriture de signature d'attaques.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

- du 24 au 26 novembre 2024
- du 9 au 11 décembre 2024*
- du 16 au 18 décembre 2024*
- du 3 au 5 mars 2025
- du 16 au 18 juin 2025
- du 18 au 20 août 2025

PARIS

- du 17 au 19 novembre 2024
- du 16 au 18 décembre 2024
- du 24 au 26 février 2025
- du 24 au 26 mars 2025
- du 2 au 4 juin 2025
- du 11 au 13 août 2025

VOIR TOUTES LES DATES

(*) session confirmée

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.).
| 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.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.