Formation Fortinet FortiWeb

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

Dans cette formation d'une durée de trois jours, vous apprendrez à déployer, à configurer et à dépanner le pare-feu d'application Web de Fortinet : FortiWeb. Les formateurs vous présenteront les concepts-clés liés à la sécurisation des applications web. Ils vous proposeront des exercices en laboratoire, vous permettant d'explorer les fonctionnalités de protection et de performances de FortiWeb. Vous travaillerez sur des simulations d'attaques utilisant des applications web réelles. À partir de simulations du trafic, vous apprendrez à répartir la charge des serveurs virtuels sur les serveurs réels, tout en appliquant des paramètres logiques, en inspectant le flux et en sécurisant les cookies de session HTTP.

Référence	NSE6-2
Durée	3 jours (21h)
Tarif	3 450 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 4 au 6 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Identifier les menaces guettant les couches applicatives
| Lutter contre les défacements et attaques par déni de service
| Prévenir les attaques 0-day sans perturber le trafic direct
| Rendre les applications rétroactivement compatibles avec OWASP Top 10 2013 et PCI DSS 3.0
| Découvrir les vulnérabilités de vos serveurs et applications Web hébergées pour une protection personnalisée et efficace.
| Configurer FortiGate avec FortiWeb, pour une sécurité renforcée des applications HTTP et XML
| Empêcher le contournement accidentel des scans, tout en autorisant les protocoles FTP et le SSH
| Configurer le blocage et le reporting pour un FortiADC ou FortiGate externe, et pour FortiAnalyzer
| Choisir le mode de fonctionnement adéquat
| Équilibrer la charge au sein d'un pool de serveurs
| Sécuriser les applications « nues » : protocoles SSL/TLS, authentification et contrôle d'accès sophistiqué.
| Façonner FortiWeb pour protéger vos applications spécifiques.
| Dresser une liste noire des suspects : hackers, participants aux attaques DDoS et gratteurs de contenu.
| Effectuer un dépannage en cas de problème liés au flux du trafic (y compris le flux FTP/SSH).
| Diagnostiquer les faux positifs et personnaliser les signatures
| Optimiser les performances

Public

| Professionnels des réseaux et de la sécurité chargés de l'administration et l'assistance FortiWeb.

Prérequis

| Connaissance des couches OSI et du protocole HTTP
| Maîtrise de base des langages HTML et JavaScript, ainsi que d'un langage de page dynamique côté serveur (par exemple, PHP)
| Maîtrise de base du transfert de port FortiGate

Programme de la formation

Introduction
Configuration de base
Intégration SIEM externe
Intégration répartiteurs de charge et SNAT
Défacement et attaques par déni de service
Signatures, assainissement et auto-apprentissage
SSL et TLS
Authentification et contrôle d'accès
Conformité à la norme PCI DSS 3.0
Mise en cache et compression
Réécriture & redirections
Résolution des problèmes
Diagnostic

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.