Formation Configuring F5 Advanced WAF: Web Application Firewall

(previously licensed as ASM)

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

Dans ce cours de 4 jours, les étudiants acquièrent une compréhension fonctionnelle du déploiement, du réglage et de l'utilisation de F5 Advanced Web Application Firewall pour protéger leurs applications web contre les attaques basées sur le protocole HTTP. Le cours comprend des cours magistraux, des travaux pratiques et des discussions sur les différents outils de F5 Advanced Web Application Firewall pour détecter et atténuer les menaces provenant de multiples vecteurs d'attaque tels que le web scraping, le déni de service de la couche 7, la force brute, les bots, l'injection de code et les exploits de type "zero day".

Référence	WGAC-BIG-AWF-CFG
Durée	4 jours (28h)
Tarif	3 800 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 17 au 20 décembre 2024

VOIR TOUTES LES DATES

Objectifs

| Décrire le rôle du système BIG-IP en tant que proxy complet dans un réseau de livraison d'applications
| Dimensionner le pare-feu d'application Web avancé F5
| Définir un pare-feu d'application Web
| Décrire comment F5 Advanced Web Application Firewall protège une application web en sécurisant les types de fichiers, les URL et les paramètres
| Déployer F5 Advanced Web Application Firewall à l'aide du modèle de déploiement rapide (et d'autres modèles) et définir les contrôles de sécurité inclus dans chacun d'eux.
| Définir les paramètres d'apprentissage, d'alarme et de blocage dans le cadre de la configuration de F5 Advanced Web Application Firewall
| Définir les signatures d'attaques et expliquer pourquoi la mise en scène des signatures d'attaques est importante.
| Déployer des campagnes de lutte contre les menaces pour se protéger contre les menaces CVE
| Comparer la mise en oeuvre d'une politique de sécurité positive et négative et expliquer les avantages de chacune d'entre elles
| Configurer le traitement de la sécurité au niveau des paramètres d'une application web
| Déployer F5 Advanced Web Application Firewall à l'aide de l'outil Automatic Policy Builder
| Ajuster une politique manuellement ou permettre l'élaboration automatique d'une politique
| Intégrer les résultats d'un scanner de vulnérabilité d'application tiers dans une politique de sécurité
| Configurer l'application du login pour le contrôle du flux
| Atténuer le bourrage d'informations d'identification (credential stuffing)
| Configurer la protection contre les attaques par force brute
| Déployer une défense avancée contre les robots racleurs de sites web, tous les robots connus et autres agents automatisés

Public

| Tout étudiant ayant une expérience limitée de l'administration et de la configuration BIG-IP

Prérequis

| Encapsulation du modèle OSI

| Routage et commutation
| Ethernet et ARP
| Notions TCP/IP
| Adressage IP et sous-réseaux
| NAT et adressage IP privé
| Passerelle par défaut
| Pare-feu réseau
| LAN vs WAN

Programme de la formation

Présentation du système BIG-IP
| Configuration initiale du système BIG-IP
| Archivage de la configuration du système BIG-IP
| Exploitation des ressources et outils d'assistance F5

Traitement du trafic avec BIG-IP
| Identifier les objets de traitement du trafic de BIG-IP
| Comprendre les profils
| Vue d'ensemble des politiques de trafic locales
| Visualisation du flux de requêtes HTTP

Présentation du traitement des applications Web
| Pare-feu d'application Web : Protection de la couche 7
| Contrôles de sécurité de la couche 7
| Vue d'ensemble des éléments de communication Web
| Aperçu de la structure des requêtes HTTP
| Examen des réponses HTTP
| Comment F5 Advanced WAF analyse les types de fichiers, les URL et les paramètres
| Utilisation du proxy HTTP Fiddler

Vue d'ensemble des vulnérabilités des applications Web
| Une taxonomie des attaques : Le paysage des menaces
| Exploits courants contre les applications Web

Déploiement de politiques de sécurité : Concepts et terminologie
| Définir l'apprentissage
| Comparaison des modèles de sécurité positifs et négatifs
| Le processus de déploiement
| Affectation d'une politique à un serveur virtuel
| Processus de déploiement : Utilisation des paramètres avancés
| Configurer les technologies du serveur
| Définition des signatures d'attaque
| Visualisation des demandes
| Contrôles de sécurité offerts par le déploiement rapide

Optimisation des politiques et violations
| Traitement du trafic après le déploiement
| Comment les violations sont-elles classées ?
| Classement des violations : Une échelle de menace
| Définition de la mise en scène et de l'application
| Définition du mode d'application de la loi
| Définition de la période de préparation à l'application de la loi
| Revoir la définition de l'apprentissage
| Définition des suggestions d'apprentissage
| Choix de l'apprentissage automatique ou manuel
| Définition des paramètres d'apprentissage, d'alarme et de blocage
| Interprétation du résumé de l'état de préparation à l'exécution
| Configuration de la page de réponse de blocage

Utilisation des signatures d'attaques et des campagnes de menaces
| Définition des signatures d'attaque
| Notions de base sur les signatures d'attaque
| Création de signatures d'attaque définies par l'utilisateur
| Définition des modes de modification simple et avancé
| Définition des ensembles de signatures d'attaque

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

| Définition des pools de signatures d'attaque
| Comprendre les signatures d'attaque et la mise en scène
| Mise à jour des signatures d'attaque
| Définition des campagnes de lutte contre les menaces
| Déploiement des campagnes de menaces

Élaboration d'une politique de sécurité positive
| Définition et apprentissage des composants de la politique de sécurité
| Définition du joker
| Définition du cycle de vie des entités
| Choix du schéma d'apprentissage
| Comment apprendre : Jamais (Wildcard uniquement)
| Comment apprendre : Toujours
| Comment apprendre : Sélectif
| Examen de la période de préparation à l'exécution : Entités
| Affichage des suggestions d'apprentissage et de l'état d'avancement
| Définition du score d'apprentissage
| Définition des adresses IP fiables et non fiables
| Comment apprendre : Compact

Sécurisation des cookies et autres sujets d'en-tête
| Objectif de F5 Cookies de l'Advanced WAF
| Définition des cookies autorisés et forcés
| Sécurisation des en-têtes HTTP

Rapports visuels et journalisation
| Visualisation des données de synthèse sur la sécurité des applications
| Rapports : Créez votre propre vue
| Rapports : Graphique basé sur des filtres
| Statistiques sur la force brute et le grattage de sites web
| Visualisation des rapports sur les ressources
| Conformité PCI : PCI-DSS 3.0
| Analyse des demandes
| Facilités et destinations de la journalisation locale
| Visualisation des journaux dans l'utilitaire de configuration
| Définition du profil de journalisation
| Configuration de la journalisation des réponses

Projet de laboratoire 1
Gestion avancée des paramètres
| Définition des types de paramètres
| Définition des paramètres statiques
| Définition des paramètres dynamiques
| Définition des niveaux de paramètres
| Autres considérations relatives aux paramètres

Élaboration automatique des politiques
| Définition de modèles qui automatisent l'apprentissage
| Définition de l'assouplissement de la politique
| Définition du resserrement de la politique
| Définir la vitesse d'apprentissage : échantillonnage du trafic
| Définition du suivi des modifications du site

Intégration avec les scanners de vulnérabilité des applications Web
| Intégration des résultats des scanners
| Importation de vulnérabilités
| Résolution des vulnérabilités
| Utilisation du fichier XSD du scanner XML générique

Déployer des politiques en couches
| Définition d'une politique parent
| Définition de l'héritage
| Cas d'utilisation du déploiement d'une politique mère

Application des règles de connexion et atténuation de la force brute
| Définition des pages de connexion pour le contrôle des flux
| Configuration de la détection automatique des pages de connexion
| Définition des attaques par force brute
| Configuration de la protection contre la force brute
| Atténuation des attaques par force brute à la source
| Définition du bourrage d'informations d'identification
| Atténuation du bourrage d'informations d'identification

Reconnaissance avec suivi de session
| Définition du suivi de session
| Configuration des actions en cas de détection d'une violation

Atténuation des dénis de service de la couche 7
| Définition des attaques par déni de service
| Définition du profil de protection contre les dénis de service
| Vue d'ensemble de la protection contre les dénis de service basée sur le TPS
| Création d'un profil de journalisation des dénis de service
| Application des atténuations TPS
| Définition de la détection comportementale et de la détection basée sur le stress

Défense avancée contre les bots
| Classification des clients avec le profil de défense anti-bot
| Définition des signatures de bots
| Définition de F5 Fingerprinting
| Définition des modèles de profil de défense contre les robots
| Définition de la protection des microservices

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.