Formation Configuring F5 Advanced WAF (Web Application Firewall)

Objectifs de la formation F5 WAF

Cette formation officielle F5 WAF, Web Application Firewall, précédemment connu sous l'appelleation ASM (Application Security Manager), permet aux participants d'acquérir l'expertise nécessaire pour détecter, atténuer et prévenir les attaques basées sur le protocole HTTP qui ciblent les applications Web. Se déroulant sur quatre jours, cette formation axée sur les travaux pratiques débute au niveau le plus simple pour apprendre à configurer et mettre en œuvre rapidement une politique de sécurité des applications, avant de passer à des configurations plus complexes.

Cette formation se compose d'analyses détaillées et d'exercices pratiques permettant d'apprendre à protéger les applications Web contre les attaques par force brute, le « web scraping » (ou extraction de contenu de sites Web), les attaques DDoS au niveau de la couche 7 et autres vecteurs d'attaques actuels.

À l'issue de la formation, les participants seront capables de :

- Différencier les modèles de sécurité négative des modèles de sécurité positive
- Configurer le mode de protection le plus adapté à leurs applications Web

La formation se déroule sur la version 14.1 de BIG IP.

À qui s'adresse cette formation ?

Public :

Cette formation s'adresse aux administrateurs réseaux et sécurité chargés de l'installation et de la maintenance quotidienne du module Application Security Manager.

Prérequis :

Pour suivre ce stage F5 WAF, il faut obligatoirement avoir suivi la formation Administrateur BIG-IP (F101) dans une version V12 minimum ou être certifié administrateur TMOS (validation des certifications 101 et 201).
Les terminologies réseaux, les notions de routage, de switching, d'adressage IP font aussi partie des connaissances demandées.

Contenu du cours F5 WAF

Provisionnement des ressources pour le pare-feu d'applications Web avancé F5

Traitement du trafic avec BIG-IP Local Traffic Manager (LTM)

Concepts d'application Web

Vulnérabilités des applications Web

Déploiement de la stratégie de sécurité

Réglage de la stratégie de sécurité

Signatures d'attaque

Renforcement positif de la sécurité

Sécurisation des cookies et autres en-têtes

Création de rapports et journalisation

Rôles d'utilisateur

Modification, fusion et exportation de stratégies

Gestion avancée des paramètres

Utilisation de modèles d'application

Utilisation du Générateur de stratégies automatique

Intégration avec les scanners de vulnérabilité Web

Application de la connexion et suivi de session

Atténuation de la force brute

Suivi de session

Détection et atténuation du grattage Web

Application de la géolocalisation et exceptions d'adresse IP

Utilisation des stratégies parent et enfant

Protection DoS de couche 7

Pare-feu d'applications Web avancé F5 et iRules à l'aide de profils de contenu pour les applications AJAX et JSON

Détection avancée des bots et défense proactive des bots