F5 BIG-IP v14 - Configuration avancée WAF

Référence BIGIP-ASM
Durée 4 jours (28 heures)
Certification F5 Certified Technology Specialist ASM (303) (non incluse)
Appréciation des résultats Évaluation qualitative de fin de stage
Modalité et moyens pédagogique Démonstrations – Cas pratiques – Synthèse et évaluation des acquis

À l'issue de ce stage vous serez capable de :

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

Niveau requis

Avoir suivi le cours BIGIP-ADM "F5-BIGIP v14 - Administration" et avoir validé les certifications 101 et 201. Avoir une bonne connaissance des terminologies réseaux et sécurité, notions de routage, switching et d'adressage IP.

Public concerné

Administrateurs réseaux et sécurité chargés de l'installation et de la maintenance quotidienne du module Application Security Manager.

Cette formation :

- est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation ;
- bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Approvisionnement de ressources pour le trafic avancé F5 de Web Application Firewall (WAF)

Traitement avec les concepts d'application Web BIG-IP Local Traffic Manager (LTM)

Vulnérabilités des applications Web

La politique de sécurité

- Déploiement
- Mise au point

Signatures des attaques

Mettre en place la sécurité positive

Sécurisation des cookies et autres headers

Rapports et enregistrements

Différence de politique, regroupement et exportation

Gestion avancée des paramètres

Utilisation de modèles d'application

Utilisation du générateur automatique de stratégies

Intégration avec les scanners de vulnérabilités Web

Mise en application de la connexion

Atténuation de la force brutale

Suivi des sessions

Détection et atténuation du Web scraping

Exceptions relatives à la géolocalisation et à l'adresse IP

Utilisation des politiques parent et enfant

Protection DoS de la couche 7

Web Application Firewall F5 avancé et iRules

Utilisation des profils de contenu pour les applications avancées Ajax et JSON

Bot Detection et la défense proactive Bot Defense

Les + de la formation

L'examen de certification (proposé en option) est en anglais.