F5 BIG-IP - Offre officielle

F5 BIG-IP v16.x - Configuration avancée WAF

4 jours (28h00) | ★★★★½ 4,6/5 | BIGIP-ASM | Certification F5 Certified Technology Specialist ASM (303) (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Décrire le rôle du système BIG-IP en tant que périphérique proxy complet dans un réseau de distribution d'applications
- Configurer le Web Application Firewall (WAF) avancé F5
- Définir un WAF
- Décrire comment le WAF avancé F5 protège une application Web en sécurisant les types de fichiers, les URL et les paramètres
- Déployer le WAF avancé F5 en utilisant le template de déploiement rapide (et d'autres templates) et définir les contrôles de sécurité inclus dans chacun d'entre eux
- Définir les paramètres d'apprentissage, d'alarme et de blocage relatifs à la configuration du WAF avancé F5
- Définir les signatures d'attaques et expliquer pourquoi la mise à disposition des signatures d'attaques est importante
- Déployer des campagnes de menace pour vous protéger contre les menaces CVE (Common Vulnerabilities and Exposures)
- Mettre en contraste la mise en oeuvre positive et négative de la politique de sécurité et expliquer les avantages de chacune d'entre elles
- Configurer le traitement de la sécurité au niveau des paramètres d'une application Web
- Déployer le WAF avancé F5 en utilisant Automatic Policy Builder
- Régler une politique manuellement ou autoriser l'élaboration automatique d'une politique
- Intégrer les résultats d'un scanner de vulnérabilités d'applications tierces dans une politique de sécurité
- Configurer l'application de la connexion pour le contrôle des flux
- Atténuer le "Credential Stuffing"
- Configurer la protection contre les attaques de force brute
- Déployer une défense avancée de bots contre les "Web Scrapers", tous les bots connus et d'autres agents automatisés.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir suivi le cours BIGIP-ADM "F5 BIG-IP v16.x - Administration", avoir validé les certifications 101 et 201 ou avoir les connaissances équivalentes. Avoir des connaissances et de l'expérience dans les domaines suivants : encapsulation du modèle OSI, routage et switching, Ethernet et ARP (Address Resolution Protocol), concepts TCP/IP, adressage IP et subnetting, NAT et adressage IP privé, gateway par défaut, firewalls de réseau et LAN vs WAN.

Public concerné

Professionnels SecOps responsables du déploiement, du réglage et de la maintenance quotidienne du WAF avancé F5.

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

Présentation du système BIG-IP

- Configuration initiale du système BIG-IP
- Archivage de la configuration du système BIG-IP
- Tirer parti des ressources et des outils de support F5

Traitement du trafic avec BIG-IP

- Identification des objets de traitement du trafic BIG-IP
- Présentation des profils
- Vue d'ensemble des stratégies de trafic local
- Visualisation du flux de requêtes HTTP

Vue d'ensemble du traitement des applications Web

- Pare-feu d'application Web : protection de couche 7
- Contrôles de sécurité de couche 7
- Vue d'ensemble des éléments de communication Web et de la structure de requête HTTP
- Examen des réponses HTTP
- Comment le WAF avancé F5 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

Déploiements de stratégies de sécurité : concepts et terminologie

- Définition de l'apprentissage
- Comparaison des modèles de sécurité positifs et négatifs
- Flux de travail de déploiement
- Affectation d'une stratégie à un serveur virtuel
- Workflow de déploiement : utilisation des paramètres avancés
- Configurer les technologies serveur
- Définition des signatures d'attaques
- Affichage des demandes
- Contrôles de sécurité offerts par un déploiement rapide

Réglage de la politique et violations

- Traitement du trafic post-déploiement
- Comment les violations sont catégorisées
- Taux de violation : une échelle de menace
- Définition
  - De la mise en scène et de l'application
  - Du mode d'application
  - De la période de préparation à l'application de la loi
- Révision de la définition de l'apprentissage
- Définition des suggestions d'apprentissage
- Choisir 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'application de la loi
- Configuration de la page de réponse de blocage

Utilisation des signatures d'attaques et des campagnes de menaces

- Définition
  - Des signatures d'attaques
  - De modes d'édition simples et avancés
  - De jeux de signatures d'attaques
  - Des pools de signatures d'attaques
- Principes de base de la signature d'attaques
- Création de signatures d'attaques définies par l'utilisateur
- Présentation des signatures d'attaques et de la mise en scène
- Mise à jour des signatures d'attaques
- Définition des campagnes de menaces
- Déploiement de campagnes de menaces

Elaboration de politiques de sécurité positives

- Définition et apprentissage des composants de la stratégie de sécurité
- Définition du caractère générique et du cycle de vie de l'entité
- Choisir le programme d'apprentissage
- Comment apprendre :
  - Jamais (caractère générique uniquement)
  - Toujours
  - Sélectif
- Examen de la période de préparation à l'application de la loi : entités
- Affichage des suggestions d'apprentissage et de l'état de la mise en scène
- Définition du score d'apprentissage
- Définition d'adresses IP approuvées et non approuvées
- Comment apprendre : Compact

Sécurisation des cookies et autres rubriques d'en-tête

- Le but des cookies du WAF avancé F5
- Définition des cookies autorisés et appliqués
- Sécurisation des en-têtes HTTP

Rapports visuels et journalisation

- Affichage des données récapitulatives de la sécurité des applications
- Création de rapports : créez votre propre vue
- Rapports : graphique basé sur des filtres
- Statistiques de force brute et de Web Scraping
- Affichage des rapports de ressources
- Conformité PCI : PCI-DSS 3.0
- Analyse des demandes
- Installations et destinations locales d'exploitation forestière
- Affichage des journaux dans l'utilitaire de configuration
- Définition du profil de journalisation
- Configuration de la journalisation des réponses

Gestion avancée des paramètres

- Définition
  - Des types de paramètres
  - Des paramètres statiques
  - Des paramètres dynamiques
  - Des niveaux de paramètres
- Autres considérations relatives aux paramètres

Elaboration automatique de politiques

- Définition

- De modèles qui automatisent l'apprentissage
- De l'assouplissement de la politique
- Du resserrement des politiques
- De la vitesse d'apprentissage : échantillonnage du trafic
- Des modifications du site de suivi

Intégration aux analyseurs de vulnérabilités des applications Web

- Intégration de la sortie du scanner
- Importation et résolution des vulnérabilités
- Utilisation du fichier XSD de l'analyseur XML générique

Déploiement de stratégies en couches

- Définition
  - D'une stratégie parent
  - De l'héritage
- Cas d'utilisation du déploiement de la stratégie parent

Application de la connexion et atténuation de la force brute

- Définition des pages de connexion pour le contrôle de flux
- Configuration de la détection automatique des pages de connexion
- Définition des attaques par force brute
- Brute Force Protection Configuration
- Atténuation de la force brute à la source
- Définition et atténuation du bourrage d'informations d'identification (Credential Stuffing)

Reconnaissance avec suivi de session

- Définition du suivi de session
- Configuration des actions lors de la détection des violations

Atténuation du déni de service de couche 7

- Définition
  - Des attaques par déni de service
  - Du profil de protection DoS
- Vue d'ensemble de la protection DoS basée sur TPS
- Création d'un profil de journalisation DoS
- Application des mesures d'atténuation TPS
- Définition de la détection comportementale et basée sur le stress

Défense avancée des bots

- Classification des clients avec le profil Bot Defense
- Définition
  - Des signatures de bot
  - De l'empreinte digitale F5
  - Des modèles de profil Bot Defense
  - De la protection des microservices

Certification (en option)

- L'achat du voucher (à prévoir en supplément) devra se faire directement par le stagiaire, via le portail de certification F5
- Le passage de l'examen se fera (ultérieurement) en présentiel uniquement (dans un centre agréé Pearson Vue ou Prometric)
- L'examen (en anglais) s'effectue en ligne, et durera en moyenne 1h30

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et/ou, en fin de formation, par une certification éditeur (proposée en option)

Les + de la formation

Le support de cours et les labs sont en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.