F5 BIG-IP v16.x – Configuration avancée WAF

Référence
THIS3214

Durée
4 jours / 28 heures

Prix HT / stagiaire
3650€

Programme *(Mis à jour le 21/02/2024)*

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

Objectifs pédagogiques
- 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 Stufing »
- 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.

Niveau requis
- Avoir suivi le cours BIG-IP ADM « F5 BIG-IP v16.x – Administration », avoir validé les certi?ications 101 et 201 ou avoir les connaissances équivalentes.

- 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 paramètre

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