BiGso
3 rue Jules Raimu
31200 TOULOUSE
Email: nibizard@bigso.fr
Tel: 05 62 80 43 66

F5- Configuring F5 Advanced WAF (previously licensed as ASM) v16.1

Dans ce cours de 4 jours, les étudiants acquièrent une compréhension fonctionnelle de la façon de déployer, d'ajuster et d'utiliser F5 Advanced Web Application Firewall pour protéger leurs applications Web contre les attaques HTTP.

Durée : 28.00 heures (4.00 jours)

Profils des stagiaires

- Ce cours est destiné au personnel SecOps responsable du déploiement, du réglage et de la maintenance quotidienne de F5 Adv. WAF. Les participants obtiendront un niveau d'expertise fonctionnel avec F5 Advanced WAF, y compris une politique de sécurité complète et une configuration de profil, une évaluation du client et des types d'atténuation appropriés.
- • Une expérience avec LTM n'est pas requise.
- • Une connaissance préalable du WAF n'est pas requise.

Prérequis

- Les connaissances et l'expérience générales suivantes en matière de technologie de réseau sont recommandées avant de suivre un cours dirigé par un instructeur F5 Global Training Services :
- • Encapsulation du modèle OSI
- • Routage et commutation
- • Ethernet et ARP
- • Concepts TCP/IP
- • Adressage IP et sous-réseau
- • NAT et adressage IP privé
- • Passerelle par défaut
- • Pare-feu réseau
- • LAN contre WAN

Objectifs pédagogiques

- Décrire le rôle du système BIG-IP en tant que périphérique proxy complet dans un réseau de distribution d'applications
- Configurer 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
- Déployez F5 Advanced Web Application Firewall à l'aide du modèle Déploiement rapide (et d'autres modèles) et définissez les contrôles de sécurité inclus dans chaque
- Définir les paramètres d'apprentissage, d'alarme et de blocage en ce qui concerne la configuration du pare-feu d'applications Web avancé F5
- Définir les signatures d'attaque et expliquer pourquoi la mise en scène des signatures d'attaque est importante
- Déployer des campagnes de menaces pour vous protéger contre les menaces CVE
- Opposer la mise en œuvre positive et négative de la politique de sécurité et expliquer les avantages de chacune
- Configurer le traitement de la sécurité au niveau des paramètres d'une application Web
- Déployer F5 Advanced Web Application Firewall à l'aide du Générateur automatique de stratégies
- Régler une stratégie manuellement ou autoriser la création automatique de stratégies
- Intégrer la sortie de l'analyseur de vulnérabilités d'applications tierces dans une stratégie de sécurité
- Configurer l'application de connexion pour le contrôle de flux
- Atténuer le bourrage d'informations d'identification
- Configurer la protection contre les attaques par force brute
- Déployez Advanced Bot Defense contre les scrapers Web, tous les bots connus et autres agents automatisés

BiGso
3 rue Jules Raimu
31200 TOULOUSE
Email: nibizard@bigso.fr
Tel: 05 62 80 43 66

Contenu de la formation

- Chapitre 1 : 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
- Chapitre 2 : Traitement du trafic avec BIG-IP
  - Identification des objets de traitement du trafic BIG-IP
  - Présentation des profils
  - Vue d'ensemble des politiques de circulation locales
  - Visualiser le flux de requêtes HTTP
- Chapitre 3 : Vue d'ensemble 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
  - Vue d'ensemble de la structure de requête HTTP
  - Examen des réponses HTTP
  - Comment F5 Advanced WAF analyse les types de fichiers, les URL et les paramètres
  - Utilisation du proxy HTTP Fiddler
- Chapitre 4 : Vulnérabilités des applications Web
  - Une taxonomie des attaques : le paysage des menaces
  - Exploits courants contre les applications Web
- Chapitre 5 : Déploiements de stratégies de sécurité : concepts et terminologie
  - Définir l'apprentissage
  - Comparaison des modèles de sécurité positifs et négatifs
  - Flux de travail de déploiement
  - Affectation d'une stratégie au serveur virtuel
  - Workflow de déploiement : utilisation des paramètres avancés
  - Configurer les technologies de serveur
  - Définition des signatures d'attaque
  - Affichage des demandes
  - Contrôles de sécurité offerts par un déploiement rapide
- Chapitre 6 : Réglage des politiques et violations
  - Traitement du trafic post-déploiement
  - Comment les violations sont classées
  - Taux de violation : une échelle de menace
  - Définition de la mise en scène et de l'application
  - Définition du mode d'application
  - Définition de la période de préparation à l'application
  - 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
  - Configuration de la page de réponse de blocage
- Chapitre 7 : Signatures d'attaque et campagnes contre les menaces
  - Définition des signatures d'attaque
  - Principes de base de la signature d'attaque
  - Création de signatures d'attaque définies par l'utilisateur
  - Définition de modes d'édition simples et avancés
  - Définition des ensembles de signatures d'attaque
  - Définition des pools de signatures d'attaque
  - Présentation des signatures et la mise en scène des attaques
  - Mise à jour des signatures d'attaque
  - Définition des campagnes contre les menaces

BiGso
3 rue Jules Raimu
31200 TOULOUSE
Email: nibizard@bigso.fr
Tel: 05 62 80 43 66

- Déploiement de campagnes contre les menaces

- Chapitre 8 : Élaboration d'une politique de sécurité positive
  - Définition et apprentissage des composants de stratégie de sécurité
  - Définition du caractère générique
  - Définition du cycle de vie de l'entité
  - Choisir le programme d'apprentissage
  - Comment apprendre : Jamais (Wildcard uniquement)
  - Comment apprendre : Toujours
  - Comment apprendre : Sélectif
  - Examen de la période de préparation à l'application : entités
  - Affichage des suggestions d'apprentissage et de l'état de la préparation
  - Définition du score d'apprentissage
  - Définition d'adresses IP approuvées et non approuvées
  - Comment apprendre : Compact
- Chapitre 9 : Sécurisation des cookies et autres rubriques d'en-têtes
  - Le but des cookies WAF avancés F5
  - Définition des cookies autorisés et appliqués
  - Sécuriser les en-têtes HTTP
- Chapitre 10 : Rapports visuels et journalisation
  - Affichage des données récapitulatives de sécurité des applications
  - Rapports : créez votre propre point de vue
  - Reporting: graphique basé sur des filtres
  - Statistiques de Brute Force 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
- Chapitre 11 : Projet de laboratoire 1
- Chapitre 12 : 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
- Chapitre 13 : Élaboration automatique de politiques
  - Définition de modèles qui automatisent l'apprentissage
  - Définition du relâchement de la politique
  - Définition du resserrement des politiques
  - Définition de la vitesse d'apprentissage : échantillonnage du trafic
  - Définition des modifications du site de suivi
- Chapitre 14 : Intégration de l'Analyseur de vulnérabilités d'application Web
  - Intégration de la sortie du scanner
  - Importer des vulnérabilités
  - Résolution des vulnérabilités
  - Utilisation du fichier XSD du scanner XML générique
- Chapitre 15 : Déploiement de stratégies en couches
  - Définition d'une politique parentale
  - Définir l'héritage
  - Cas d'utilisation de déploiement de stratégie parent
- Chapitre 16 : 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
  - Configuration de la protection contre la force brute

BiGso
3 rue Jules Raimu
31200 TOULOUSE
Email: nibizard@bigso.fr
Tel: 05 62 80 43 66

- Atténuation de la force brute basée sur la source
- Définition du remplissage des informations d'identification
- Atténuer le bourrage des informations d'identification

- Chapitre 17 : Reconnaissance avec suivi de session
  - Définition du suivi de session
  - Configuration des actions en cas de détection de violation
- Chapitre 18 : Atténuation du déni de service de couche 7
  - Définition des attaques par déni de service
  - Définition du profil de protection DoS
  - Présentation de la protection DoS basée sur TPS
  - Création d'un profil de journalisation DoS
  - Application des atténuations TPS
  - Définition de la détection comportementale et basée sur le stress
- Chapitre 19 : Défense de bots avancée
  - Classification des clients avec le profil Bot Defense
  - Définition des signatures de bot
  - Définition de l'empreinte digitale F5
  - Définition des modèles de profil Bot Defense
  - Définition de la protection des microservices
- Chapitre 20 : Projets finaux

Organisation de la formation

Equipe pédagogique
Nicole BIZARD
Responsable formation
06 14 78 61 01
nibizard@bigso.fr

Moyens pédagogiques et techniques

- Modalité : Formation réalisée en présentiel ou à distance selon la formule retenue
- Méthode : Un formateur expert, une conférence, des ateliers pratiques et des discussions sur les différents outils de pare-feu d'applications Web avancés F5
- Documentées : Support projeté et remis en début ou fin de formation en PDF ou téléchargeable
- Les salles du centre sont équipées d'un paperboard, d'un vidéo projecteur et de PC portables.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Questionnaire de pré-évaluation avant le stage
- Questionnaire d'évaluation de la satisfaction en fin de stage
- Feuille de présence émargée par demi-journée par les stagiaires et le formateur
- Attestation de fin de formation
- Questionnaire d'évaluation des acquis à 30/90 jours

Accessibilité

La formation est accessible aux personnes à mobilité réduite.
Une étude des conditions d'accès et des moyens de compensation sera réalisé en amont à l'inscription afin d'identifier plus précisément les conditions de réalisation et de faisabilité de la formation.
Vous pouvez trouver toutes les informations nécessaires sur notre site : https://bigso.fr/accueil/formations/

Maj. Le 12/12/2022