F5 - Configuration d'Advanced WAF : Web Application Firewall

Sécuriser les applications Web

Présentiel ou en classe à distance

4 jours (28 h) Réf.: SE72

Idéal en Distanciel

Avec des réseaux informatiques inter connectés, les menaces visant les applications et les données sont omniprésentes. Avec Advanced WAF, F5 Networks propose une solution de protection des applications Web contre les attaques par force brute, par extraction de contenu de sites Web (le "web scraping") ou encore par déni de service ("DDoS" au niveau de la couche 7). Cette formation très pratique d'une durée de 4 jours permettra aux participants d'acquérir l'expertise nécessaire pour détecter, atténuer et prévenir les attaques basées sur le protocole HTTP qui ciblent les applications Web.

A qui s'adresse cette formation ?

Pour qui

- Personnel SecOps responsable du déploiement, du réglage et de la maintenance quotidienne de F5 Advanced WAF

Prérequis

- Il est conseillé d'avoir suivi la formation "F5 - Administration BIG-IP" (SE70) ou être certifié Administrateur BIG-IP F5
- Il est conseillé d'avoir suivi les formations en ligne gratuites suivantes : "Premiers pas avec BIG-IP" et "Premiers pas avec BIG-IP Application Security Manager)" pour les participants ayant une expérience limitée en matière d'administration et de configuration BIG-IP

Programme

1 - Configuration du système BIG-IP

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

2 - Traitement du trafic avec BIG-IP

- Identification des objets de traitement de trafic BIG-IP
- Comprendre les profils
- Aperçu des stratégies de trafic local

- Visualiser le flux de requêtes HTTP

3 - Concepts liés aux applications Web

- Présentation du traitement des demandes d'application 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 requêtes HTTP
- Examen des réponses HTTP
- Comment F5 Advanced WAF analyse les types de fichiers, les URL et les paramètres
- Utilisation du proxy HTTP Fiddler

4 - Vulnérabilités des applications Web

- Une taxonomie des attaques : le paysage des menaces
- Exploits communs contre les applications Web

5 - Déploiement des stratégies de sécurité

- Définir l'apprentissage
- Comparaison des modèles de sécurité positifs et négatifs
- Le workflow de déploiement
- Attribution 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 proposés par le déploiement rapide
- Définition des signatures d'attaque

6 - Réglage des stratégies et infractions

- Traitement du trafic post-déploiement
- Comment les infractions sont catégorisées
- Taux d'infraction : échelle de menace
- Définir la mise en scène et l'application
- Définir le mode d'application
- Définir la période de préparation à l'application
- Revoir la définition de l'apprentissage
- Définir des suggestions d'apprentissage
- Choisir l'apprentissage automatique ou manuel
- Définition des paramètres d'apprentissage, d'alarme et de blocage
- Interpréter le résumé de l'état de préparation à l'application
- Configuration de la page de réponse de blocage

7 - Signatures d'attaque et campagnes contre les menaces

- Définition des signatures d'attaque
- Les bases de la signature d'attaque
- Création de signatures d'attaque définies par l'utilisateur
- Définition des modes d'édition simples et avancés
- Définition des ensembles de signature d'attaque
- Définition des pools de signature d'attaque
- Comprendre les signatures d'attaques et la mise en scène des attaques
- Mise à jour des signatures d'attaque
- Définition des campagnes contre les menaces
- Déploiement de campagnes contre les menaces

8 - Élaboration d'une stratégie de sécurité positive

- Définition et apprentissage des composants de stratégie de sécurité
- Définition du joker (Wildcard)
- Définir le cycle de vie de l'entité
- Choisir le programme d'apprentissage
- Comment apprendre : Jamais (joker 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 d'avancement
- Définition du score d'apprentissage
- Définition d'adresses IP approuvées et non approuvées
- Comment apprendre : Compact

9 - Sécurisation des cookies et autres en-têtes

- Le but des cookies WAF avancés F5
- Définition des cookies autorisés et appliqués
- Sécuriser les en-têtes HTTP

10 - Rapports visuels et journalisation

- Affichage des données récapitulatives de sécurité des applications
- Rapports : créer votre propre vue
- Rapports : graphique basé sur des filtres
- Statistiques sur la force brute et le Web Scraping
- Affichage des rapports de ressources
- Conformité PCI : PCI-DSS 3.0
- Analyse des demandes
- Installation et destination de la journalisation locale
- Affichage des journaux dans l'utilitaire de configuration
- Définition du profil de journalisation
- Configuration de la journalisation des réponses

11 - Projet de Lab 1

12 - Gestion avancée des paramètres

- Définition des types de paramètres
- Définir des paramètres statiques
- Définir les paramètres dynamiques
- Définition des niveaux de paramètres
- Autres considérations relatives aux paramètres

13 - Élaboration automatique de stratégies

- Vue d'ensemble de l'élaboration automatique de stratégies
- Définition de modèles qui automatisent l'apprentissage
- Définition du relâchement des stratégies
- Définition du resserrement des stratégies
- Définition de la vitesse d'apprentissage : échantillonnage du trafic
- Définition des modifications du site de suivi

14 - Intégration du scanner de vulnérabilité d'applications Web

- Intégration de la sortie du scanner
- Importer des vulnérabilités
- Résolution des vulnérabilités
- Utilisation du fichier XSD du scanner XML générique

15 - Déploiement de stratégies en couches

- Définir une stratégie parent
- Définir l'héritage
- Cas d'utilisation du déploiement de la stratégie parent

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

17 - Reconnaissance avec suivi de session

- Définition du suivi de session
- Configuration des actions en cas de détection de violation

18 - Atténuation DoS de la 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

19 - Bots Defense avancés

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

20 - Chiffrement de formulaire à l'aide de DataSafe

- Ciblage des éléments de la livraison d'applications
- Exploiter le modèle d'objet de document
- Protection des applications à l'aide de DataSafe
- L'ordre des opérations pour la classification des URL

21 - Révisions et laboratoires finaux

- Projet de laboratoire final (Option 1) - Scénario de production
- Projet de laboratoire final (Option 2) - Gestion du trafic avec les stratégies de trafic local de couche 7

Les objectifs de la formation

- Savoir provisionner le pare-feu d'application Web avancé F5
- Comprendre comment déployer F5 Advanced Web Application Firewall à l'aide du modèle Rapid Deployment (et d'autres modèles)
- Définir les paramètres d'apprentissage, d'alarme et de blocage en fonction de la configuration du pare-feu d'application Web avancé F5
- Savoir comparer la mise en oeuvre des stratégies de sécurité positives et négatives et expliquer les avantages de chaque
- Apprendre à configurer le traitement de sécurité au niveau des paramètres d'une application Web
- Comprendre comment configurer la protection contre les attaques par force brute
- Savoir déployer Advanced Bot Defense contre les web scrapers, les bots connus et d'autres agents automatisés
- Apprendre à déployer DataSafe pour sécuriser les données côté client

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- L'alternance de cours théorique, de travaux pratiques et de d'échanges permettra aux participants d'acquérir les compétences nécessaires à la détection et à la prévention des attaques sur les applications Web.
- La qualité d'une formation officielle (support de cours en anglais).
- 97% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.