Date de publication : 05/12/2024

Formation : F5 - Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

Cours officiel F5-TRG-BIG-AWF-CFG, préparation aux certifications F5

Cours pratique - 4j - 28h00 - Réf. WA1

Avec cette formation, vous disposerez d'une compréhension fonctionnelle de la manière de déployer, de régler et d'utiliser F5 Advanced Web Application Firewall pour protéger vos applications web contre les attaques basées sur le protocole HTTP. Entre théorie et mise en pratique, vous aborderez les différents outils de F5 Advanced Web Application Firewall pour détecter et atténuer les menaces provenant de multiples vecteurs d'attaque tels que le web scraping, le déni de service de la couche 7, la force brute, les bots, l'injection de code et les exploits de type "zero day".

PARTICIPANTS

Administrateurs de sécurité et de réseau qui seront responsables de l'installation, du déploiement, de l'optimisation et de la maintenance quotidienne du F5 Advanced Web Application Firewall.

PRÉREQUIS

Posséder la certification "F5 Certified BIG-IP Administrator" ou un niveau de connaissances équivalent. Il est recommandé d'avoir des connaissances ou une expérience générale en technologies réseau.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Décrire le rôle du système BIG-IP en tant que proxy complet dans un réseau de distribution d'applications
- Dimensionner le F5 Advanced Web Application Firewall
- Définir un pare-feu d'application Web
- Expliquez comment F5 Advanced WAF protège les applications web via la sécurité des fichiers, URL et paramètres
- Déployer F5 Advanced Web Application Firewall à l'aide du modèle de déploiement rapide
- Définir les contrôles de sécurité inclus dans chacun d'eux
- Définir les paramètres d'apprentissage, d'alarme et de blocage dans le cadre de la configuration de F5 Advanced WAF
- Définir les signatures d'attaque et expliquer l'importance de la mise en scène des signatures d'attaque
- Déployer des campagnes de lutte contre les menaces pour se protéger contre les menaces CVE
- Comparer les politiques de sécurité positives et négatives et détailler les avantages distincts de chaque approche
- Configurer le traitement de la sécurité au niveau des paramètres d'une application web
- Déployer F5 Advanced Web Application Firewall à l'aide de l'éditeur de politique automatique
- Ajuster une politique manuellement ou permettre l'élaboration automatique d'une politique
- Intégrer les résultats d'un scanner de vulnérabilité d'application tiers dans une politique de sécurité
- Configurer l'application de la connexion pour le contrôle du flux
- Atténuer le bourrage d'informations d'identification (credential stuffing)
- Configurer la protection contre les attaques par force brute
- Déploiement d'une défense avancée contre les robots et autres agents automatisés
- Déployer DataSafe pour sécuriser les données côté client

Public concerné

Administrateurs de sécurité et de réseau qui seront responsables de l'installation, du déploiement, de l'optimisation et de la maintenance quotidienne du F5 Advanced Web Application Firewall.

Prérequis

Posséder la certification "F5 Certified BIG-IP Administrator" ou un niveau de connaissances équivalent. Il est recommandé d'avoir des connaissances ou une expérience générale en technologies réseau.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

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.
- 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.
- Analyse les types de fichiers, les URL et les paramètres.
- Utilisation du proxy HTTP Fiddler.

4 Vulnérabilités des applications web

- Présentation 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 processus de déploiement.
- Attribution d'une stratégie au serveur virtuel.
- 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 Optimisation des stratégies et infractions

- Traitement du trafic post-déploiement.
- Les catégories d'infractions.
- Echelle 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.
- Notions de base sur les signatures 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), toujours et sélectif..
- Examen de la période de préparation à l'application.
- 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

- Objectif des cookies du F5 Advanced WAF.
- 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 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.

12 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.
- Définition des modifications du site de suivi.

13 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.

14 Déploiement de stratégies en couches

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

15 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.

16 Reconnaissance avec suivi de session

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

17 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.

18 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.

19 Chiffrement des formulaires 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.

Options

Certification : 230 € HT

Cette formation prépare à la certification "F5 Certified Technology Specialist, BIG-IP ASM".
Comment passer votre examen ?

L’option de certification se présente sous la forme d’un voucher ou d’une convocation qui vous permettra de passer l’examen à l’issue de la formation.