(Télé-)présentiel Cours Officiel Formation certifiante

Configuring F5 Advanced WAF (Web Application Firewall)

Objectifs

- Décrire le rôle du système BIG-IP en tant que proxy complet dans un réseau de distribution d'applications
- Provisionnement du pare-feu d'application Web avancé F5
- Définir un WAF (pare-feu d'application Web)
- Décrire comment le pare-feu d'application Web avancé F5 protège une application web en sécurisant les types de fichiers, les URL et les paramètres
- Définir les paramètres d'apprentissage, d'alarme et de blocage relatifs à la configuration du le pare-feu d'application Web avancé F5
- Définir les signatures d'attaque et expliquer pourquoi la simulation des signatures d'attaque est importante
- Déployer des campagnes de menace pour se protéger contre les menaces du CVE
- Configurer le traitement de la sécurité au niveau des paramètres d'une application web
- Déployer le pare-feu d'application Web avancé F5 en utilisant le générateur automatique de politiques
- Régler une politique manuellement ou permettre l'élaboration automatique d'une politique
- Intégrer les résultats d'un scan des vulnérabilités d'applications tierces dans une politique de sécurité
- Configurer l'obligation de connexion pour le contrôle des flux
- Atténuer les risques d'attaque de type « credential stuffing »
- Configurer la protection contre les attaques par la force brute
- Déployer une défense avancée contre le « scraping » web, tous les robots connus et les autres agents automatisés
- Déployer DataSafe pour sécuriser les données côté client

Pré-requis

- Il n'y a pas de pré-requis spécifique à la technologie F5 pour ce cours.
- Une expérience de LTM n'est pas requise
- Une connaissance préalable du WAF n'est pas nécessaire.

Certification

Cette formation prépare à la certification 303-ASMTECHNOLOGY SPECIALIST

Public

Ce cours est destiné au personnel SecOps responsable du déploiement, du réglage et de la maintenance quotidienne de l'Adv. WAF F5. Les participants obtiendront un niveau fonctionnel d'expertise avec l'Advanced WAF F5, y compris la politique de sécurité complète et la configuration des profils, l'évaluation des clients et les types d'atténuation appropriés.

Programme de la formation

Paramétrage de BIG-IP

- Introduction du système BIG-IP
- Mise en place initiale du système BIG-IP
- Archivage de la configuration du système BIG-IP
- Exploiter les ressources et les outils du support du F5

Traitement du trafic avec BIG-IP

- Identification des objets de traitement du trafic BIG-IP
- Comprendre les profils
- Aperçu des politiques locales en matière de trafic
- Visualisation du flux de requêtes HTTP

Concepts d'application web

- Aperçu du traitement des demandes d'application web
- Pare-feu d'application Web : Protection de la couche 7
- Contrôles de sécurité de la couche 7
- Aperçu des éléments de communication sur le web
- Aperçu de la structure des requêtes HTTP
- Examen des réponses HTTP
- Comment F5 Advanced WAF analyse les types de fichiers, les URL et les paramètres
- Utilisation du serveur mandataire HTTP

Déploiement de stratégies de sécurité

- Définir l'apprentissage
- Comparaison des modèles de sécurité positifs et négatifs
- Le déroulement du déploiement
- Affectation de la stratégie au serveur virtuel
- Flux de travail pour le déploiement : Utilisation des paramètres avancés
- Configurer les technologies de serveur
- Définir les signatures d'attaques
- Visualiser les requêtes
- Contrôles de sécurité offerts par le déploiement rapide
- Définir les signatures d'attaques

Personnalisation des stratégies et intrusions

- Traitement du trafic après déploiement
- Catégorisation des intrusions
- Classement des intrusions : évaluation des menaces
- Définir les étapes et la mise en oeuvre
- Définir le mode d'exécution
- Définition de la période de préparation de l'application
- Révision de la définition de l'apprentissage
- Définir les suggestions d'apprentissage
- Choisir l'apprentissage automatique ou manuel
- Définir les paramètres d'apprentissage, d'alarme et de blocage
- Configuration de la page de réponse de blocage

Signatures d'attaques et vagues d'attaques

- Définir les signatures d'attaques
- L'essentiel sur les signatures d'attaques
- Création de signatures d'attaques définies par l'utilisateur
- Définir des modes d'édition simples et avancés
- Définir les jeux de signatures des attaques
- Définir les pools de signatures d'attaques
- Comprendre les signatures et la mise en scène des attaques
- Mise à jour des signatures d'attaques
- Définir les vagues de menace
- Déploiement contre les vagues de menace

Elaboration d'une stratégie de sécurité

- Définir et apprendre les composantes de la politique de sécurité
- Définir une wildcard
- Définir le cycle de vie de l'entité
- Choisir le programme d'apprentissage
- Comment apprendre : Jamais (wildcard uniquement)
- Comment apprendre : Toujours
- Comment apprendre : Sélectif
- Révision de la période de préparation à l'application de la législation : Entités
- Visualisation des suggestions d'apprentissage et de l'état des étapes
- Définir le score d'apprentissage
- Définition des adresses IP de confiance et de non confiance

Sécurité des cookies et autres entêtes

- L'objectif des cookies F5 Advanced WAF
- Définition des cookies autorisés et obligatoires
- Sécurisation des en-têtes HTTP

Rapports et enregistrements

- Visualisation des données de synthèse sur la sécurité des applications
- Rapports : Construisez votre propre vue
- Rapports : Graphique basé sur les filtres
- Statistiques sur la force brute et le web scrapping
- Visualisation des rapports sur les ressources
- Conformité PCI : PCI-DSS 3.0
- Analyse des requêtes
- Visualisation des journaux dans l'utilitaire de configuration
- Configuration de la journalisation des réponses

Traitement des paramètres avancés

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

Construire des stratégies automatiques

- Aperçu de l'élaboration automatique des stratégies
- Définir des modèles qui automatisent l'apprentissage
- Définir le relâchement des stratégies
- Définir le resserrement des politiques

- Définir la vitesse d'apprentissage : l'échantillonnage du trafic
- Définir les changements de site de suivi

Intégration de scanner de vulnérabilité

- Intégration du scanner
- L'importation de vulnérabilités
- Résoudre les vulnérabilités
- Utilisation du fichier XSD du scanner XML générique

Déployer des stratégies à plusieurs niveaux

- Définir une politique parente
- Définition de l'héritage
- Cas d'utilisation du déploiement de la politique parente

Contrôle à l'ouverture de session et réduction des attaques par force brute

- Définition des pages de connexion pour le contrôle des flux
- Configuration de la détection automatique des pages de connexion
- Définir les attaques par force brute
- Configuration de la protection contre les attaques par force brute
- Atténuation de la force brute à la source
- Définition de l'attaque sur les informations d'identification
  Atténuer les attaques sur les informations d'identification

Le traçage des sessions

- Définir le traçage des sessions
- Configuration des actions en cas de détection d'une intrusion

Atténuation des attaques sur la couche 7

- Définir les attaques par déni de service
- Définir le profil de protection du DDoS
- Vue d'ensemble de la protection du DDoS basée sur le TPS
- Création d'un profil d'enregistrement du DDoS
- Appliquer les mesures d'atténuation du TPS
- Définir la détection comportementale et la détection basée sur le stress

Défense avancée contre les robots

- Classer les clients avec le profil Bot Defense
- Définir les signatures des robots
- Définition de l'empreinte F5
- Définir des modèles de profil de défense des robots
- Définir la protection des micro-services

Chiffrement des formulaires avec DataSafe

- Cibler les éléments de la livraison des demandes
- Exploitation du modèle d'objet document
- Protection des applications utilisant DataSafe
- L'ordre des opérations pour la classification des URL

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.