Fortinet – FortiWeb NSE 6 (Préparation à la certification NSE 6)

Date et durée

Code formation : NSE6-2FR
Durée : 3 jours
Nombre d'heures : 21 heures

Formation avec préparation à la certification

Description

Le FortiWeb de Fortinet est un programme de pare-feu applicatif, ayant pour but d'optimiser la sécurité des applications Web face aux différentes menaces informatiques. Cette formation vous apprendra à déployer et maîtriser les fonctionnalités de FortiWeb afin de protéger vos applications Web. Elle fait partie du cursus de préparation pour l'obtention de la **certification Fortinet NSE6**

Objectifs

Cette formation a pour objectif **de vous enseigner la gestion de la sécurité des applications Web avec FortiWeb**. Après une compréhension approfondie des principes de sécurité, vous apprendrez à gérer les différents types de menace informatique en opérant les configurations de base de FortiWeb, en mettant en place le pare-feu et en résolvant les problèmes survenant sur le serveur FortiWeb. Cette formation comprend un ensemble de modules théoriques et d'exercices pratiques pour appliquer en situation concrète vos nouvelles compétences techniques. Elle fait partie du cursus de préparation à l'examen de **certification Fortinet NSE 6**.
A l'issue de cette formation, vous saurez :

- Identifier et prévenir les différents risques pouvant sévir sur les couches applicatives.
- Faire face aux formes de piratage telles que le défacement ou les attaques par déni de service.
- Agir face aux vulnérabilités et exploits zero day tout en préservant le trafic direct.
- Gérer la compatibilité rétroactive des applications avec OWASP Top 10 2013 et PCI DSS 3.0.
- Assurer une sécurité optimale de vos serveurs et applications Web hébergées en identifiant leurs failles et faiblesses.
- Renforcer la protection des applications HTTP et XML avec FortiGate et FortiWeb.
- Gérer le fonctionnement des protocoles FTP et SSH en évitant le contournement accidentel des scans.
- Paramétrer les options de blocage et de rapports pour FortiADC ou FortiGate externe et FortiAnalyzer.
- Gérer la charge dans un pool de serveurs.
- Maîtriser la protection des applications nues : protocoles SSL/TLS, authentification et contrôle d'accès sophistiqué.
- Etablir la liste noire des suspects.
- Résoudre les problèmes de flux de trafic.
- Diagnostiquer les faux positifs.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

La participation à cette formation implique de :

- Maîtriser les concepts de couches OSI et de protocole HTTP.
- Connaître les fondamentaux du langage HTML et JavaScript.
- Connaître la base d’un langage de page dynamique côté serveur, tel que PHP.
- Savoir utiliser le transfert de port FortiGate.

Public

Cette formation s’adresse aux professionnels IT impliqués dans l’administration de FortiWeb.

Cette formation s'adresse aux profils suivants

Administrateur système
Directeur des Systèmes d'Information (DSI)
Ingénieur système

Programme

Module 1 : Vue d’ensemble
Module 2 : Configurer FortiWeb
Module 3 : Intégrer le SIEM externe
Module 4 : Intégrer les répartiteurs de charge et SNAT
Module 5 : Défacement et attaques par déni de service
Module 6 : Signature, assainissement et auto-apprentissage
Module 7 : Secure Sockets Layer (SSL) et Transport Layer Security (TLS)
Module 8 : Authentifier et contrôler l’accès
Module 9 : La norme PCI DSS 3.0
Module 10 : Mise en cache et compression
Module 11 : Réécrire et rediriger
Module 12 : Résoudre les problèmes
Module 13 : Diagnostiquer avec FortiWeb