Développez vos talents
Certifiez vos compétences

Offre éditeurs

Stormshield Network - Troubleshooting and support

4 jours (28h00) | ★★★★½ 4,6/5 | STO-CSNTS | Certification CSNTS (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Offre éditeurs

À l'issue de ce stage vous serez capable de :

- Reconnaître l'organisation du système de fichiers ainsi que les démons et processus d'une appliance Stormshield Network
- Localiser, explorer et manipuler les différents fichiers de configuration et de journalisation des activités (logs)
- Distinguer des particularités et anomalies dans une configuration réseau et routage
- Réaliser et étudier des captures de trafic réseau
- Etudier une politique de sécurité et en identifier les directives générales et les paramètres particuliers
- Identifier les traitements appliqués aux connexions en cours
- Produire un relevé d'informations adapté, complet et exploitable pour l'établissement d'un diagnostic
- Configurer des politiques de tunnels VPN IPSec, identifier les mécanismes activés et en diagnostiquer les dysfonctionnements
- Analyser et diagnostiquer une configuration en haute disponibilité.

Niveau requis

Avoir suivi la formation STO-CSNE "Stormshield Network - Expert". Avoir une certification CSNE en cours de validité. Avoir des connaissances approfondies en TCP/IP et shell UNIX.

Public concerné

Responsables informatique, administrateurs réseaux, ou tout technicien informatique.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Introduction

Système d'exploitation et commandes UNIX liées

- Méthodes d'accès au shell et paramètres
- SSH : fonctionnalités
- Système de fichier et commandes associées
- Répertoires et commandes associées
- Environnement système et utilisateur
- Fichiers et commandes associées

Logs

- Logs locaux
  - Localisation
  - Caractéristiques
  - Syntaxe
  - Catégories
- Commandes associées
- Fichiers de configuration
- Logd, logctl, journalisation des messages noyau

Fichiers de configuration

- Répertoires, structure et syntaxe générale
- Sauvegarde (*.na), deckbackup, tar
- Configuration usine

Objets

- Syntaxe des objets
- Objets dynamiques et FQDN

Réseau et routage

- Paramètres des interfaces réseau
- Le bridge et les commandes associées
- Routage : fonctions de routage et leur priorité
- Routes par défaut et routes statiques
- Gatemon et les objets routeurs
- Routage dynamique
- Commandes relatives, affichage des routes
- Mode verbose

Capture et analyse de trafic

- Introduction et conseils
- Syntaxe générale et arguments
- Filtres usuels
- Exemples commentés et préparation pour faire de bonnes captures
- Analyse de trafic par tcpdump (flux TCP, UDP / icmp)

ASQ : les étapes d'analyse

- Analyse pas à pas des couches réseau
- Commandes associées
- Paramètres globaux

- Profils et paramètres particuliers
- ASQ asynchrone : différents cas et watermarking
- ASQ verbose mode

ASQ : politique de sécurité

- Répertoires et fichiers de configuration, syntaxe des règles
- Filtre : commandes associées
- Filtre : exemple de règles chargées
  - Action
  - Niveau d'inspection
  - Plug-in
  - PBR
  - QoS
  - Interfaces
  - Proxy
- Filtre : traduction des groupes et des listes
- NAT : rappels
  - NAT Dynamique
  - NAT Statique par port
  - NAT Statique / Bimap
  - Non NAT
- NAT : commandes associées
- NAT : syntaxe des règles chargées

ASQ : stateful et tables d'états

- Table d'adresses protégées
- Table des hôtes
- Table des connexions
  - Exemples d'états de connexion (NAT, vconn, FTP plug-in, async, Lite...)

Démons et processus

- Liste et rôle
- Démon superviseur
- Commandes relatives

Eventd : le gestionnaire d'évènements

VPN IPSec

- Implémentation IKE / IPSec Stormshield Network
- Fichiers de configuration
- Politique de sécurité (SPD, SA)
- Les négociations IKE
- Négociations : mode Main et mode Aggressive
- ISAKMP et IPSec SA
- Propositions IKE
- Particularités : NAT-T, DPD, Keepalive, SharedSA, Politique None, SPD Cache
- Commandes associées
- Analyse d'une IPSec SA
- Logs
- Notifications de "delete SA"
- Capture et analyse du trafic ISAKMP
- Particularités des correspondants dynamiques
- Mode Verbose, erreurs courantes

PKI et certificats

- Rappels et directives globales
- Répertoire de CA
- Astuces de configuration
- Vérification des certificats

Haute disponibilité

- Généralités
- Fichiers de configuration
- Commandes relatives
- Etapes d'activation, gestion des interfaces réseau
- Processus et trafics impliqués
- Réplications / synchronisation
- Evènements et logs HA

Passage de la certification

- Cette formation comprend le voucher nécessaire à l'inscription et au passage (ultérieur) de l'examen
- Il devra être passé dans un délai de 3 semaines (maximum) à partir du dernier jour de la session de formation
- L'examen (en français) s'effectue en ligne (sur la plateforme https://institute.stormshield.eu) et durera en moyenne 3h00
- Ce dernier sera composé de 60 questions (70% de bonnes réponses sont nécessaires pour l'obtention de la certification) dont des QCM et des questions ouvertes sur les fonctionnalités, paramétrages et méthodes de dépannage avancées à mettre en oeuvre pour répondre exhaustivement à des rapports d'incidents issus de nos clients
- En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième (et dernier) passage est ouvert automatiquement pour une durée d'une semaine supplémentaire

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Le support de cours et les labs sont également disponibles en français et en anglais.