FICHE DE SYNTHESE FORMATION CSNTS

Certified Stormshield Network Troubleshooting & Support v1 (NT-CSNTS-V1)

STORMSHIELD SAS organisme de formation agréé N° 82690673169

Introduction

Cette formation a pour but de fournir des outils et méthodes pour rassembler les informations nécessaires, à l'étude et à la correction des problèmes en utilisant l'interface en ligne de commande (CLI) des produits UTM Stormshield Network.

Cette formation s'adresse aux personnels des sociétés souhaitant devenir Stormshield Network Support Center (SNSC) ou Stormshield Network Training Center (SNTC), ainsi qu'aux candidats ayant pour objectif de devenir un ingénieur support ou formateur expert sur nos produits UTM.

Public

Responsables informatique, administrateurs réseaux, tout technicien informatique.

Objectifs pédagogiques

A l'issue de la formation, et après une révision des connaissances de base, les stagiaires seront capables :

- de connaitre l'organisation du système de fichiers ainsi que les démons et processus d'une appliance Stormshield Network
- d'explorer la configuration et de diagnostiquer les anomalies à partir des logs de l'Appliance
- d'analyser et de diagnostiquer une configuration réseau et routage
- de réaliser et d'étudier des captures de trafic réseaux
- d'analyser et de diagnostiquer les flux réseaux traités par une politique de sécurité
- d'identifier les traitements appliqués aux connexions en cours
- de produire un relevé d'informations adapté, complet et exploitable
- de configurer et de diagnostiquer les politiques VPN IPSec

Lieu, durée et inscriptions

Stormshield propose des sessions de formation dans ses locaux de Paris, Lille et Lyon.

Nos formateurs peuvent également se déplacer sur site (minimum 3 participants).

La formation Troubleshooting & Support se déroule sur trois jours insécables pour une durée totale de 21 heures. Les stagiaires sont convoqués à 9h30 le premier jour de la formation et à 9h les jours suivants (sauf indication contraire de la part du formateur ou de la part de Stormshield). Toutes les demandes d'inscription doivent être envoyées au service formation Stormshield (training@stormshield.eu). Les effectifs maximum sont de 4 personnes par session. Un support de cours écrit est fourni à chaque stagiaire.

Pré requis et matériel

Le stagiaire doit avoir réussi l'examen CSNE dans les 3 ans précédent la formation CSNTS.

Connaissances approfondies en TCP/IP et shell UNIX.

Les candidats doivent avoir une certification CSNE en cours de validité.

Afin de réaliser les exercices, les stagiaires devront se munir d'un PC portable avec un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur ; et disposant des logiciels suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent Vmware (Vmware player ou Vmware workstation).

Description détaillée

Jour 1

- 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
- 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
  - Paramétrage de Gatemon
  - 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 des résultats de tcpdump (flux TCP, UDP/icmp)

Jour 2

- Démons et Processus
  - Liste et rôle
  - Superviseur présent
  - Commandes associées
- Objets
  - Syntaxe des hôtes
  - Objets dynamiques
- 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, plugin, 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 plugin, async, lite…)
- FTP : cas d'étude synthétique
  - Mécanismes des modes passif et actif
  - Règles de filtrages nécessaires

- Eventd : le gestionnaire d'événements
- 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

Examen de certification

La certification consiste en un examen effectué en ligne (2h00, 60 questions).

L'examen comporte des QCM et des questions ouvertes sur les fonctionnalités, paramétrages et méthodes de dépannage avancées à mettre en œuvre pour répondre exhaustivement à des rapports d'incidents issus de nos clients.

Le score minimum de certification est de 70%.

L'examen est ouvert automatiquement le jour suivant la fin de la formation pour une durée de six mois sur la plateforme https://institute.stormshield.eu. En cas d'échec ou d'impossibilité de passer l'examen dans ce créneau, un deuxième et dernier passage d'examen est ouvert automatiquement dans la foulée pour une durée d'une semaine.