Azurtem

Dernière modification le 06 avril 2019

*Déclaration d'activité enregistrée sous le numéro **93060803406** du préfet de région de Provence Alpes Côte d'Azur*

Mikrotik Certified Security Engineer (MTCSE)

Stage de formation

Durée: 2 jours (9h-12h30 et 13h30-17h)

Objectif: A la fin de cette session de formation, le participant sera en mesure de planifier et de mettre en œuvre des mesures de sécurité appropriées et adaptées au réseau concerné.

Public visé: Les ingénieurs et techniciens réseaux désireux de déployer et maintenir des réseaux sécurisés basés sur les appareils MikroTik.

Intervenant : Yann Shukor, formateur et gérant de la société Azurtem, certifié MTCNA, MTCRE, MTCWE, MTCINE, MTCSE, MTCIPv6E, TRAINER

Prérequis: Certificat MTCNA.

Equipement nécessaire : Un ordinateur portable équipé d'interfaces Ethernet et Wifi capable d'exécuter un applicatif Windows

Titre	Objectif
Module 1 Introduction	• Attaques, mécanismes et services • Les menaces les plus courantes • Déploiement de la sécurité RouterOS • **Module 1 labo**
Module 2 Parefeu	• Flux de paquets, chaînes de pare-feu • Pare-feu dynamique • Table RAW • Atténuation des inondations SYN à l'aide de la table RAW • Configuration par défaut de RouterOS • Meilleures pratiques pour l'accès de gestion • Détection d'attaques contre des services réseaux critiques • Filtres du pont • Options avancées des filtres du pare-feu • Filtrage ICMP • **Module 2 labo**
Module 3 Attaques des couches OSI	• Attaques MNDP et prévention • DHCP : serveurs 'rogue', attaques d'épuisement et prévention • Attaques TCP SYN et prévention • Attaques UDP et prévention • Attaques "Smurf ICMP" et prévention • Attaques FTP, Telnet et brute-force SSH et prévention • Détection et prévention du balayage des ports • **Module 3 labo**

Module 4
Chiffrement
	• Introduction au chiffrement et à la terminologie
	• Méthodes de chiffrement
	• Algorithmes - symétrique, asymétrique
	• Infrastructure à clé publique (PKI)
	• Certificats
	  • Certificats auto-signés
	  • Certificats valides et gratuits
	  • Utilisation des certificats dans RouterOS
	• **Module 4 labo**

Module 5 Sécurisation du Routeur	• Port knocking • Connexions sécurisées (HTTPS, SSH, WinBox) • Ports par défaut des services • Construction d'un tunnel au travers de SSH • **Module 5 labo**

Module 6 Tunnels Sécurisés	• Introduction à IPsec • L2TP + IPsec • SSTP avec certificats • **Module 6 labo**

-=oOo=-