Certified Advanced Security Engineer (MTCASE)

Training outline

Duration:	2 days
Outcomes:	By the end of this training session, the participant will be able to plan and implement appropriate advanced security measures suitable for the network at hand.
Target audience:	Network engineers and technicians wanting to deploy and maintain secure MikroTik device based networks.
Course prerequisites:	MTCSE certificate

Title	Objective
Module 1 Introduction	• Threats, mechanisms, attacks and services • The most common threats • RouterOS security deployment • **Module 1 laboratory**
Module 2 IPv6 Attacks	• IPv6 review • Threat types • Duplicate address detection DoS • Neighbor discovery spoofing • Router advertisment spoofing • Router advertisment flooding • IPv6 attack prevention • **Module 2 laboratory**

Module 3
Securing the Routing
	• OSPF attack types
	  • Resource starvation attacks
	  • Misdirecting the traffic
	  • Eavesdropping (man-in-the middle)
	  • Protecting OSPF network
	• Attacking OSPF network (simulation)
	• Preventing OSPF attacks
	• BGP attack types
	• BGP security
	  • MD5 and maximum prefix limit
	  • Prefix filtering
	  • AS-path filtering
	  • Traffic filtering
	• **Module 3 laboratory**

Module 4
Cryptography
	• Introduction to cryptography and terminology
	• Encryption methods
	• Algorithms - symmetric, asymmetric
	• Public key infrastructure (PKI)
	• Certificates
	  • Self-signed certificates
	  • Free of charge valid certificates
	  • Using the certificates in RouterOS
	• **Module 4 laboratory**

Module 5 High Availability	• Interface bonding • VRRP • VRRP + interface bonding • **Module 5 laboratory**