

4rd edition:

MikroTik

Certified Security
Engineer (MTCSE)

hotelinking

Certificación

MikroTik MTCSE

Duration

2 days (12 hours)

Price

€ 500 - Subsidized training for companies is available (more information on request: admin@hotelinking.com)

Next date

October 2024

Course schedule:

Thursday: 9 am to 6 pm (includes 1 hour for lunch).

Friday: 9 am to 6 pm (includes 1 hour for lunch).

Location

HOTECMA - Former ASIMA Fire Station

Son Castelló Polygon

Gremi Picapedrers, 1

07009 - Palma

Outcomes:

By the end of this training session, the participant will be able to plan and implement appropriate 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:

MTCNA certificate

Title	Objective
Module 1 Introduction	<ul style="list-style-type: none"> ■ Attacks, mechanisms and services ■ The most common threats ■ RouterOS security deployment ■ Module 1 laboratory

Title	Objective
Module 2 Firewall	<ul style="list-style-type: none"> ■ Packet flow, firewall chains ■ Stateful firewall ■ RAW table ■ SYN flood mitigation using RAW table ■ RouterOS default configuration ■ Best practices for management access ■ Detecting an attack to critical infrastructure services ■ Bridge filter ■ Advanced options in firewall filter ■ ICMP filtering ■ Module 2 laboratory

Title	Objective
Module 3 OSI Layer Attacks	<ul style="list-style-type: none"> ■ MNDP attacks and prevention ■ DHCP: rogue servers, starvation attacks and prevention ■ TCP SYN attacks and prevention ■ UDP attacks and prevention ■ ICMP Smurf attacks and prevention ■ FTP, telnet and SSH brute-force attacks and prevention ■ Port scan detection and prevention ■ Module 3 laboratory

Title	Objective
<p>Module 4 Cryptography</p>	<ul style="list-style-type: none"> ■ Introduction to cryptography and terminology ■ Encryption methods ■ Algorithms - symmetric, asymmetric ■ Public key infrastructure (PKI) ■ Certificates <ul style="list-style-type: none"> ■ Self-signed certificates ■ Free of charge valid certificates ■ Using the certificates in RouterOS ■ Module 4 laboratory

Title	Objective
<p>Module 5 Securing the Router</p>	<ul style="list-style-type: none"> ■ Port knocking ■ Secure connections (HTTPS, SSH, WinBox) ■ Default ports for the services ■ Tunneling through SSH ■ Module 5 laboratory

Title	Objective
<p>Module 6 Secure Tunnels</p>	<ul style="list-style-type: none"> ■ Introduction to IPsec ■ L2TP + IPsec ■ SSTP with certificates ■ Module 6 laboratory

hotelinking

CONTACTLESS TECH TO CONNECT WITH YOUR GUESTS

Carretera de Valldemossa, Km. 7,4 Parc Bit. Edifici Disset 3ª Planta Puerta D7, 07120

www.hotelinking.com | help@hotelinking.com

