

3<sup>rd</sup> 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](mailto:admin@hotelinking.com))

## Next date

11 and 12 April 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
<b>Module 1 Introduction</b>	<ul style="list-style-type: none"> <li>■ Attacks, mechanisms and services</li> <li>■ The most common threats</li> <li>■ RouterOS security deployment</li> <li>■ <b>Module 1 laboratory</b></li> </ul>

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

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

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

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

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

# hotelinking

CONTACTLESS TECH TO CONNECT WITH YOUR GUESTS

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

[www.hotelinking.com](http://www.hotelinking.com) | [help@hotelinking.com](mailto:help@hotelinking.com)

