COURSE

MikroTik

Certified Security Engineer **(MTCSE)**

hotelinking

Carlos Otín
Senior Network Engineer
de Hotelinking

Trainer

Telecommunications Technical Engineer, CCNP (Cisco Certified Network Professional), **UEWA** (Ubiquiti Enterprise Wireless Admin), **UBRSS** (Ubiquiti Broadband Router and Switching Specialist), **MTCWE** (MikroTik Certified Wireless Engineer), **MTCSE** (MikroTik Certified Security Engineer), **MikroTik Trainer**....

Certification

MikroTik MTCSE

Duration

2 days (12 hours)

Dates

April 22 and 23, 2026

Price

€500

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

Course location and schedule

The course will take place in the **Press Room of Parc Bit**, from **9:00 AM** to **6:00 PM**, with a one-hour lunch break.

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.

Course prerequisites

MTCNA certificate

Title	Objective
Module 1 Introduction	• Attacks, mechanisms and services • The most common threats • RouterOS security deployment • **Module 1 laboratory**

Title	Objective
Module 2 Firewall	• 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	• 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
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**

Title	Objective
Module 5 Securing the router	• Port knocking • Secure connections (HTTPS, SSH, WinBox) • Default ports for the services • Tunneling through SSH • **Module 5 laboratory**

Title	Objective
Module 6 Secure Tunnels	• Introduction to IPsec • L2TP + IPsec • SSTP with certificates • **Module 6 laboratory**

hotelinking

Carretera de Valldemossa, Km. 7,4 Parc Bit.
Edifici Disset 3ª Planta Puerta D9, 07120
www.hotelinking.com