

Network & Security Fundamentals

Course Overview

This professional training program is designed to build strong foundations in networking and cybersecurity. The course combines theory with hands-on labs focused on real enterprise environments.

Target Audience

- 1 • IT & Networking beginners
- 2 • Cybersecurity entry-level learners
- 3 • Junior Network / System Administrators
- 4 • Students preparing for DevOps & Security tracks

Course Index

Module 1 – Network Fundamentals

Module 2 – Cybersecurity Basics

Module 3 – Firewall Configuration

Module 4 – MikroTik Configuration & Security

Module 5 – Final Project & Practical Labs

Module 1 – Network Fundamentals

- 1 • Networking concepts and architectures
- 2 • LAN, WAN, WLAN models
- 3 • OSI & TCP/IP models
- 4 • IPv4 addressing & subnetting
- 5 • Network devices & protocols

Module 2 – Cybersecurity Basics

- 1 • Introduction to cybersecurity
- 2 • CIA Triad principles
- 3 • Common cyber attacks
- 4 • Network security fundamentals
- 5 • Security best practices



Module 3 – Firewall Configuration

- 1 • Firewall concepts & types
- 2 • Security zones & policies
- 3 • NAT & port forwarding
- 4 • Traffic filtering & logging

Module 4 – MikroTik Configuration

- 1 • RouterOS overview
- 2 • IP addressing & routing
- 3 • Firewall rules on MikroTik
- 4 • Bandwidth control & queues
- 5 • Router hardening & security

Module 5 – Final Project

- 1 • Secure network topology design
- 2 • Firewall & router deployment
- 3 • Cybersecurity implementation
- 4 • Troubleshooting & documentation

Learning Outcomes

- 1 • Strong understanding of networking fundamentals
- 2 • Ability to identify and mitigate security threats
- 3 • Firewall configuration skills
- 4 • MikroTik deployment & security skills

