classJO

PROFESSIONAL LEARNING PLATFORM

LEARN TODAY... LEAD TOMORROW

Professional Courses • Expert Instructors • Flexible Learning

PROFESSIONAL COURSES

Up-to-date content aligned with industry needs.

FLEXIBLE LEARNING

Online and in-person options that fit your schedule.

EXPERT INSTRUCTORS

Learn from professionals with real-world experience.

CERTIFICATES & SUPPORT

Earn certificates and get continuous support.

class JO

Network Security Fundamentals Training

Eng. Mansour Quzmar

class JO

Network Security Fundamentals Training

Overview

- Introduction to network security concepts, technologies, and best practices
- Understanding the fundamentals of securing enterprise networks and communication systems
- Learning common cyber threats, attack techniques, and defense mechanisms
- Understanding network architectures, protocols, and security controls
- Introduction to firewalls, intrusion detection systems, VPNs, and access control mechanisms
- Understanding secure network design and monitoring concepts
- Developing foundational cybersecurity and network protection skills
- Building practical knowledge for securing modern on-premises and cloud-connected environments

---

Training Objectives

By the end of this training, participants will be able to:

- Understand fundamental networking and network security concepts
- Identify common cyber threats, vulnerabilities, and attack methods
- Explain the principles of Confidentiality, Integrity, and Availability (CIA)
- Understand network protocols and communication mechanisms
- Implement basic network security controls and best practices
- Understand firewall technologies and access control methods
- Explain intrusion detection and prevention concepts
- Understand VPN technologies and secure remote access
- Identify common network attacks and mitigation techniques
- Understand network monitoring, logging, and security operations basics
- Apply secure network design principles

- Improve organizational network security awareness and protection capabilities

---

Training Outline

Module 1: Introduction to Network Security

- What is Network Security?
- Importance of network protection
- Security goals and objectives
- Cybersecurity fundamentals
- Confidentiality, Integrity, and Availability (CIA)
- Types of network environments

Module 2: Networking Fundamentals

- Network architecture basics
- OSI and TCP/IP models
- IP addressing and subnetting basics
- Common network protocols
    - TCP
    - UDP
    - DNS
    - HTTP/HTTPS
    - FTP
    - SSH
- Routing and switching concepts

Module 3: Common Network Threats and Attacks

- Malware and ransomware
- Phishing and social engineering
- Denial of Service (DoS/DDoS)
- Man-in-the-Middle (MITM) attacks
- Password attacks
- Spoofing and sniffing
- Insider threats
- Wireless network attacks

Module 4: Network Security Controls

- Defense-in-depth strategy
- Security policies and procedures
- Access control concepts
- Authentication and authorization
- Network segmentation
- Security hardening principles
- Least privilege concept

Module 5: Firewalls and Perimeter Security

- Firewall concepts and architecture
- Types of firewalls
    - Packet filtering
    - Stateful inspection
    - Next-Generation Firewalls (NGFW)
- Firewall rules and policies

- Demilitarized Zone (DMZ)
- Web Application Firewall (WAF) basics

Module 6: Intrusion Detection and Prevention

- IDS and IPS concepts
- Signature-based detection
- Anomaly-based detection
- Monitoring suspicious activities
- Threat detection and alerting
- Security event logging basics

Module 7: Virtual Private Networks (VPNs) and Secure Communication

- VPN concepts and benefits
- Remote access security
- Site-to-site VPNs
- Encryption fundamentals
- Secure communication protocols
    - SSL/TLS
    - IPSec
    - SSH

Module 8: Wireless Network Security

- Wireless networking basics
- Wi-Fi security risks
- WPA2 and WPA3 security
- Secure wireless configuration

- Rogue access points
- Wireless attack prevention

Module 9: Network Monitoring and Security Operations

- Network monitoring concepts
- Log management basics
- SIEM overview
- Security Operations Center (SOC) concepts
- Incident detection and response basics
- Security monitoring best practices

Module 10: Secure Network Design and Best Practices

- Secure network architecture
- Segmentation and Zero Trust concepts
- Cloud and hybrid network security basics
- Backup and recovery considerations
- Vulnerability management basics
- Security awareness and operational best practices

Module 11: Practical Scenarios and Hands-On Exercises

- Firewall configuration examples
- Network attack demonstrations
- Packet analysis basics
- Secure remote access setup
- Incident response scenarios
- Security assessment exercises

Module 12: Course Review and Next Steps

- Review of key security concepts
- Common security challenges
- Career paths in network security
- Security certifications overview
- Best practices and recommendations
- Additional learning resources