CYBER SECURITY SHORT COURSE

Short 1 Week Course (40 Hours)

Organisational Learning Centre

HE College of Excellence

COURSE SUMMARY

Our **Cyber Security Short Course** equips learners with both the theoretical foundation and practical skills needed to **secure networks** and ensure the **safe transmission of data**, including protection of commonly used Internet services.

The course explores the core technologies used in network security and introduces the key principles and techniques involved in protecting information systems. Learners will develop the ability to **assess security risks** within computer networks and explore the tools and methods available to **mitigate these risks.**

It includes an in-depth look at cryptographic algorithms from a mathematical **perspective**, with hands-on examples of **code-breaking** to enhance understanding. Building on this knowledge, learners will be introduced to **cryptographic protocols** used for a range of purposes such as **authentication, secure communication**, and **digital signatures.**

The course also covers additional aspects of network security, including the use of access control systems, firewalls, virtual private networks (VPNs), network address translation (NAT), malware, vulnerability assessments, and Intrusion Detection Systems (IDS).

OUR APPROACH TO TRAINING AND CONSULTANCY

OLC (Europe) Ltd provide International Bespoke Business Training & Learning and Development Consultancy from nearly 30 years of experience driven from the expertise of leaders and educators from the United Kingdom.

The experience of training and consulting is not only worldwide but has been delivered across all sectors of service, industrial, engineering, and commercial including banking, insurance, manufacturing, oil and gas, mining, hospitality and education.

REQUIRED ASSETS

Hardware	Software
Access to a number of networked computers with peripheral devices e.g. printers and scanners	Network/server software and relevant security software.
Internet access, routers, and firewalls.	Manipulation Software e.g. Adobe Photoshop
Wireless devices that can either connect to the main network or be used to set up a separate wireless network.	VPN server and client software, and a remote desktop application (e.g. www.logmein.com).
	Suitable open source software may also be used.

LEARNING OUTCOMES

01

Get to know the main types of cryptographic algorithms.

1.1 Describe the main types of cryptographic algorithms, such as block ciphers, public-key ciphers, and hash functions.
1.2 Choose a suitable cryptographic algorithm for a specific use case and explain why it's the best option.

02

Public-key Infrastructure

2.1 Public-key Infrastructure Definition
2.2 The purpose of Certification Authorities

03

How data is kept safe on networks using security protocols

3.1 Explain how Transport Layer Security (TLS) is used to keep websites and online data secure.
3.2 Describe the methods used to protect email communication.
3.3 Outline how disk encryption works to safeguard stored data.
3.4 Apply file encryption techniques to protect individual files.

04

Digital Signatures for Emails and Files

4.1 Describe what digital signatures are and how they help verify authenticity.
4.2 Show how to request and install a digital certificate.
4.3 Use a digital signature to sign an email securely.

05

Understanding Vulnerability Assessments and the Limitations of Password-Based Authentication

5.1 Discuss the importance and purpose of conducting vulnerability assessments.
5.2 Analyse and interpret the contents of a vulnerability assessment report.
5.3 Outline various authentication methods and how they function.
5.4 Define multifactor authentication and explain its significance in enhancing security.
5.5 Describe biometric authentication methods and discuss the challenges associated with them.

LEARNING OUTCOMES CONT.

06 Ability to Conduct Basic Vulnerability Assessments and Password Audits

6.1 Utilise port scanning tools to identify and analyse open ports on a system.
6.2 Execute password auditing techniques using dictionary attacks and brute-force methods.

07 Competence in Configuring Basic Firewall Architectures

7.1 Configure access control mechanisms
7.2 Describe the components of a firewall
7.3 Configure a DMZ firewall
7.4 Evaluate the limitations of firewalls
7.5 Apply and manage port forwarding rules

08 Understanding Virtual Private Networks (VPNs)

8.1 Describe the purpose, function, and benefits of Virtual Private Networks.
8.2 Identify and choose suitable remote access solutions based on specific requirements.

09 Ability to Implement Wireless Security Measures

9.1 Identify and explain common vulnerabilities found in wireless networks.
9.2 Design and deploy a secure architecture for wireless network access.
9.3 Set up and manage Access Control Lists (ACLs) to control network access.
9.4 Implement encryption techniques to secure wireless communications.