NCC education®

Awarding
Great British
Qualifications

CYBER SECURITY SHORT COURSE

Short Course Specification

Modification History

Version	Revision Description
V1.0	For release
V1.1	Removed the assessment methodology

Published by: NCC Education Limited, The Towers, Towers Business Park, Wilmslow Road,
Didsbury, Manchester M20 2EZ UK

Tel: +44 (0) 161 438 6200 Fax: +44 (0) 161 438 6240 Email: info@nccedu.com
http://www.nccedu.com

About NCC Education

NCC Education is a UK-based awarding body, active in the UK and internationally. Originally part of the National Computing Centre, NCC Education started offering Computing qualifications in 1976 and from 1997 developed its Higher Education portfolio to include Business qualifications, IT qualifications for school children and a range of Foundation qualifications.

With Centres in over forty countries, four international offices and academic managers worldwide, NCC Education strives to employ the latest technologies for learning, assessment and support. NCC Education is regulated and quality assured by Ofqual (the Office of Qualifications and Examinations Regulation, see www.ofqual.gov.uk).

Overview and Objectives

Our Cyber Security Short Course will provide learners with the underlying theory and practical skills required to secure networks and to send data safely and securely over network communications (including securing the most common Internet services).

This course provides a look at the technologies employed to secure a network. It is designed to provide learners with knowledge of the fundamental principles and techniques employed in securing information and networks. The course will allow learners to assess the security risks inherent in computer networks and the technologies that can be employed to counter such risks. It covers cryptographic algorithms from a mathematical point of view, including practical examples of breaking codes.

Once the learners have knowledge of the different types of algorithm, cryptographic protocols are introduced for accomplishing a varied set of tasks, including authentication, secure message exchange, digital signatures, etc. Other aspects of network security are then dealt with, such as access control devices and firewalls, VPN, NAT, malware, vulnerability assessment, Intrusion Detection Systems (IDS), etc.

Hardware and Software Requirements

Hardware: Learners need access to a number of networked computers with peripheral devices, such as printers and scanners, plus Internet access, routers, and firewalls. Wireless devices are also required that that can be added to this network or used to create a standalone wireless network.

Software: Learners must have network/server software available to them plus relevant security software. Learners will also need access to image manipulation software such as Abode Photoshop, VPN server and client software, and a remote desktop application (e.g. www.logmein.com). Suitable open source software may also be used.

Cyber Security Short Course

Title:	Cyber Security Short Course

Guided Learning Hours	40 hours

Learning Outcomes; The Learner will:	**Objectives;** The Learner can:
1. Understand the most common types of cryptographic algorithm	1.1 Explain the most common types of cryptographic algorithm (i.e. block ciphers, public-key ciphers and hash algorithms) 1.2 Select and justify an appropriate algorithm for a particular purpose
2. Understand the Public-key Infrastructure	2.1 Describe the Public-key Infrastructure 2.2 Explain the role of Certification Authorities
3. Understand security protocols for protecting data on networks	3.1 Explain the concept of Web security with TLS 3.2 Describe Email security mechanisms 3.3 Describe disk encryption mechanisms 3.4 Deploy file encryption mechanisms
4. Be able to digitally sign emails and files	4.1 Explain digital signatures 4.2 Demonstrate applying for and deploying a Digital Certificate 4.3 Digitally sign an email
5. Understand Vulnerability Assessments and the weakness of using passwords for authentication	5.1 Explain the need for vulnerability assessments 5.2 Interpret a vulnerability assessment report 5.3 Explain the different authentication mechanisms 5.4 Describe multifactor authentication 5.5 Describe biometrics and their issues
6. Be able to perform simple vulnerability assessments and password audits	6.1 Use port scanners to highlight open ports 6.2 Perform password cracking using dictionary and brute-force methods
7. Be able to configure simple 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
8. Understand Virtual Private Networks	8.1 Explain Virtual Private Networks 8.2 Select an appropriate remote access solution
9. Be able to deploy wireless security	9.1 Explain the vulnerabilities inherent in wireless networks 9.2 Deploy a secure network architecture for wireless access 9.3 Configure Access Control Lists 9.4 Encrypt and protect the wireless link

Syllabus

Syllabus content		
Topic	**Course coverage**	**Learning Outcomes covered**
Cryptography Fundamentals	• Cryptographic algorithms including: – AES block cipher – RSA public-key code – SHA hash algorithm	1
PKI	• The Public-Key Infrastructure • Certification Authorities and Digital Signatures	2&4
Web Security	• Browser security and SSL/TLS for encrypted browsing	3&4
Email Security	• PGP and S/MIME for encrypted and authenticated email	3&4
Data Protection	• File, disk and portable encryption technologies	3
Vulnerability Assessment	• Vulnerability assessment terms and tools: – Port scanners – Password crackers	5&6
Authentication	• Passwords • Multi-factor authentication • Biometrics	5
Access Control	• Packet filtering • Access control lists • NAT • IDS	7
Firewalls	• Firewall architectures and their limitations • The DMZ firewall and its limitations	7
VPN	• Virtual Private Network technologies and issues	7&8
Remote Access	• Alternative remote access technologies: – Remote desktops – Web applications	7&8
Wireless Security	• Wireless security (WEP, WPA, WPA2) • Secure network architectures for wireless deployments	9

Related National Occupational Standards (NOS)
Sector Subject Area: 6.1 ICT Professionals **Related NOS:** 6.2.A.1 - Contribute to IT/technology security management activities; 6.2.A.2 - Document IT/technology security management processes; 6.2.A.3 - Assist the management with IT/technology security systems; 6.2.P.1 - Manage the IT/technology security requirements; 6.2.P.2 - Carry out IT/technology security management activities