LONDON CAPITAL COMPUTER COLLEGE

Certificate in Networking (107) – Network Security

Prerequisites: Basic knowledge in the use of Microsoft Windows Applications.	**Corequisites:** A pass or higher in Diploma in Information Technology or equivalence
Aim: Network security is a major issue for enterprises, with breaches of security possibly being punished by legal sanctions, financial loss, or loss of customer confidence. Topics covered include security appliances such as firewalls, proxies, and Intrusion Detection Systems; security services such as confidentiality, integrity and authentication; and technologies such as IPSec, SSL, etc. The course conveys an in-depth exploration of the issues that apply to network security. On completion learners will be well placed to contribute to the security solution of a modern organisation. This course provides the student with and introduction to the key concepts and fundamentals of Network Security. The Network Security course provide critical foundational information concerning firewall technology, security risks and remediation, as well as network security design and implementation considerations. Additionally, candidates will learn how to configure and implement firewall appliances, and extend firewall capabilities using rules, security applications and other network specific functions, and troubleshooting techniques. The course covers: IPSec overview; VPN; Metwork Address Translation; Configuring the Firewall; Working with Zones, Groups, and Objects;Security Services; DMZ, FW Services, Routing and Policies, Proxy Relay, load Balancing and Failover, Probe and Monitor.	
Required Materials: Recommended Learning Resources.	**Supplementary Materials:** Lecture notes and tutor extra reading recommendations.
Special Requirements: The course requires a combination of lectures, demonstrations, discussions, and hands-on labs.	
Intended Learning Outcomes:	**Assessment Criteria:**
1. Describe the security terminology and Information security legal issues.	1.1 Explore security terminology 1.2 Steps in safeguarding data and information 1.3 Describe security attacks 1.4 Analyse hacker technologies 1.5 Define confidentiality, integrity and accountability
2. Analyse management security decisions and identify administrative and technical security	2.1 Describe risk analysis stages 2.2 Describe network standards and architecture 2.3 Describe organisational security policies 2.4 Be able to conduct an information security assessment
3. Analyse the elements of cryptography	3.1 Define cryptography 3.2 Explain encryption concept and the type of encryption
4. Analyse the popular cryptographic standards and demonstrate issues with viruses, trojan horses and worms.	4.1 Define VPN 4.2 Define SSL/TLS 4.3 Describe wireless LAN security 4.4 Describe the different types of intrusion detection system
5. Describe central authentication and analyse how central authentication servers receive data	5.1 Describe access control systems 5.2 Explain access cards and tokens 5.3 Describe biometric authentication 5.4 Identify Public key infrastructure

	5.5 Describe RADIUS authentication
6. Analyse the importance of firewalls and demonstrate the implementation of a firewall.	6.1 Describe firewall operation 6.2 Explain the firewall architecture concepts 6.3 Describe the type of firewalls
7. Explore the elements of host data and important computer security threats and technologies.	7.1 Describe host threats 7.2 Describe server operating systems 7.3 Analyse Unix security issues 7.4 Describe Windows security issues
8. Analyse the steps in securing network applications in both client-side and server side security.	8.1 Describe application security threats 8.2 Explore web and ecommerce services 8.3 Identify browser security issues and protections available 8.4 Describe email security issues 8.5 Describe VOIP security threats 8.6 Describe Skype security concerns 8.7 Describe TCP/IP supervisory protocols 8.8 Describe the internet architecture 8.9 Be able to explain database server security issues 8.10 Describe wireless security issues
9. Identify different ways of responding to incidents and disasters and the recovery plans.	9.1 Describe the process of responding to an intrusion 9.2 Analyse cybercrime laws 9.3 Describe backup processes 9.4 Define risk 9.5 Describe the components of risk

Recommended Learning Resources:
Network Security

Text Books	• Network Security: Private Communication in a Public World (2nd Edition) by Charlie Kaufman, Radia Perlman, and Mike Speciner ISBN-10: 0130460192 • Network Security Essentials: Applications and Standards by William Stallings ISBN-10: 0136108059
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	Server Operating System (Optional)