LONDON CAPITAL COMPUTER COLLEGE

Diploma in PC Engineering & Structured Cabling (108) – Computer Security

Prerequisites: Knowledge of Windows operating system.	**Corequisites:** A Pass or better in Certificate in Networking or equivalence.
Aim: Ensuring the security of the vast and complex infrastructure of computers, servers and networks is an immense challenge. Whenever computing technology is used to provide new or improved services, it gives potential attackers new opportunities to cause damage by accessing or modifying sensitive information. This course incorporates theory and practice of designing and building secure computer systems that protects information and resists attacks. It aims to equip candidates with all the required theoretical knowledge to enter a career in development of security systems, or information security consultancy. The course provide candidates the advanced skills needed to learn how to protect networks, secure electronic assets, prevent attacks, ensure the customer privacy, and build secure infrastructures. The knowledge gained in this course will be of great use to numerous fields including network security, forensics, audit, security leadership, and application security.	
Required Materials: Recommended Learning Resources.	**Supplementary Materials:** Lecture notes and tutor extra reading recommendations.
Special Requirements: The course requires a combination of lectures, demonstrations and class discussions.	
Major Learning Outcomes:	**Assessment Criteria:**
1. Describe how throughout the world organisations are increasingly targeted by overlapping surges of cyber attacks.	1.1 Outline security problems 1.2 Discuss security incidents 1.3 Identify security threats
2. Outline computer and information security terminology concepts	2.1 Outline security terminology 2.2 Analyse access control 2.3 Define authentication 2.4 Discuss security models
3. Describe organisational security systems and the role of people in security	3.1 Describe organisational policies, procedures, standards and guidelines 3.2 Identify physical security aspects 3.3 Discuss electromagnetic eavesdropping 3.4 Explore poor security practices 3.5 Describe application vulnerabilities
4. Describe the avenues for exploiting and compromising web servers: brute force password guessing attacks and web application attacks.	4.1 Analyse encryption algorithms 4.2 Describe hashing methods/formulas 4.3 Distinguish symmetric and asymmetric encryption 4.4 Identify the purpose of encryption
5. Describe how Public Key Infrastructure (PKI) enable users unsecure public network such as the Internet to securely and privately exchange data and money.	5.1 Analyse the public key framework 5.2 Discuss certificate technology and verification techniques 5.3 Identify certificate classes and architectural models 5.4 Identify PKI standards and protocols 5.5 Analyse interoperability issues with PKI standards

6. Demonstrate how encryption of files and firewalls offers security.	6.1 Discuss how physical security affects network security 6.2 Outline steps to mitigate security risks 6.3 Describe network architecture and components 6.4 Describe network security concerns 6.5 Outline network security design topologies
7. Describe connection and authentication issues in remote access and how users cannot reach locations beyond the remote access server.	7.1 Describe remote access protocols and procedures 7.2 Describe wireless security implications 7.3 Define Virtual Private Network (VPN) 7.4 Define Internet Protocol Security (IPSec)
8. Describe the concepts of Intrusion Detection Systems (IDS), how they work, what sorts of things they monitor for, what the results mean.	8.1 Discuss the origins of intrusion detection system 8.2 Identify the purpose of IDS 8.3 Analyse incident response
9. Demonstrate how to establish a well defined security configuration baseline.	9.1 Be able to create a password policy 9.2 Describe operating system and network hardening
10. Demonstrate how organisations and prevent computer and network attacks.	10.1 Analyse the different categories of attacks 10.2 Describe malicious software 10.3 Define auditing 10.4 Analyse email security issues 10.5 Discuss email security practices 10.6 Explore web components and services 10.7 Describe web security protocols

Recommended Learning Resources: Computer Security

Text Books	• Computer Security by Dieter Gollmann ISBN-10: 0470741155 • Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger ISBN-10: 0132390779 • Computer Security: Principles and Practice by William Stallings and Lawrence Brown ISBN-10: 013513711X
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	Windows Server