






Level 5 Diploma in PC Engineering & Structured Cabling (108)
133 Credits



Unit: Computer Security	Total Qualification Time: 220
Exam Paper No.: 5	Number of Credits: 22
Prerequisites: Knowledge in Windows Operating System.	Corequisites: A pass or better in Certificate in Networking or equivalence.
<p>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 unit incorporates theory and practice of designing and building secure computer systems that protects information and resists attacks. It aims to equip learners with all the required theoretical and practical knowledge to enter a career in development of security systems, or information security consultancy. The unit provide learners 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 unit will be of great use to numerous fields including network security, forensics, audit, security leadership, and application security.</p>	
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.	
<p>Major Learning Outcomes:</p> <ol style="list-style-type: none"> How throughout the world organisations are increasingly targeted by overlapping surges of cyber attacks. Computer and information security terminology concepts and administering security features. Organisational security systems; the role of people in security and data breaches caused by people rather than technical failure. The avenues for exploiting and compromising web servers using brute force password guessing attacks and web application attacks. How Public Key Infrastructure (PKI) enable users unsecure public network such as the Internet to securely and privately exchange data and money. How Encrypting folders and files as a way of protecting them from unwanted access and firewalls offers security. 	<p>Assessment Criteria:</p> <ol style="list-style-type: none"> Describe security problems Analyse and narrate security incidents Analysing and identify security threats Identify LAN, cloud computing and eCommerce security issues Define security terminology Analyse access control Define authentication Describe security models Describe organisational security policies, procedures, standards and guidelines Identify physical security aspects Describe electromagnetic eavesdropping Identify poor security practices Describe application vulnerabilities Describe encryption algorithms Describe hashing methods/formulas Distinguish symmetric and asymmetric encryption Identify and analyse the purpose of encryption Analyse the public key framework Describe certificate technology and verification techniques Identify certificate classes and architectural models Identify PKI standards and protocols Analyse interoperability issues with PKI standards Describe Encrypting File System (EFS) Describe how physical security affects network security Explain steps to mitigate security risks Describe network architecture and components Describe network security concerns

<p>7. Connection and authentication issues in remote access and how users cannot reach locations beyond the remote access server.</p> <p>8. The concepts of Intrusion Detection Systems (IDS), how they work, what sorts of things they monitor for, what the results mean.</p> <p>9. Understand how to establish a well defined security configuration baseline hardware and applications that run on computer devices.</p> <p>10. How organisations prevent computer and network attacks using routers and firewalls to help control access to a home computer.</p>	<p>6.6 Describe network security design topologies</p> <p>7.1 Describe remote access protocols and procedures</p> <p>7.2 Describe wireless security implications</p> <p>7.3 Define Virtual Private Network (VPN)</p> <p>7.4 Define Internet Protocol Security (IPSec)</p> <p>8.1 Describe the origins of intrusion detection system</p> <p>8.2 Identify the purpose of IDS</p> <p>8.3 Analyse incident response plan steps</p> <p>9.1 Be able to create a password policy</p> <p>9.2 Describe operating system and network hardening</p> <p>9.3 Develop an organisational security baseline</p> <p>9.4 Produce a security baseline checklist</p> <p>9.5 Create a corporate security baseline for Windows Operating System</p> <p>10.1 Analyse the different categories of attacks</p> <p>10.2 Describe malicious software</p> <p>10.3 Define auditing</p> <p>10.4 Analyse email security issues</p> <p>10.5 Discuss email security practices</p> <p>10.6 Examine web components and services</p> <p>10.7 Describe web security protocols</p> <p>10.8 Describe the difference between network intrusion prevention and network detection systems</p>
<p>Methods of Evaluation: A 2½-hour written examination paper with five essay questions, each carrying 20 marks. Candidates are required to answer all questions. Candidates also undertake project/coursework in Computer Security with a weighting of 100%.</p>	

Recommended Learning Resources: Computer Security

<p>Text Books</p>	<ul style="list-style-type: none"> • 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
<p>Study Manuals</p> 	<p>BCE produced study packs</p>
<p>CD ROM</p> 	<p>Power-point slides</p>
<p>Software</p> 	<p>Windows Server</p>