Level 5 Diploma in Internet Security (615) 177 Credits

Unit: Ethical Hacker **Exam Paper No.:** 5	**Guided Learning Hours:** 200 **Number of Credits:** 20
Prerequisites: Basic networking concepts, social media and computer technology security issues	**Corequisites:** Internet technology.
Aim: Knowledge of implications caused by hackers; including skills in conducting investigations and analysing target systems to identify security vulnerabilities. The ethical hacking course leads to a variety of job roles such as defending network, testing, risk management and quality assurance testing. Major threats in today's world to organisation network security is being hacked. Having knowledge in how hackers operate helps identify, prioritise potential threats and how best to provide remedy. This course provide knowledge in: • identifying loopholes in network security • setting up better defence systems	
Required Materials: Recommended Learning Resources.	**Supplementary Materials:** Lecture notes and tutor extra reading recommendations.
Special Requirements: This is a hands-on unit, hence practical use of computers is essential. Requires intensive lab work outside of class time.	
Intended Learning Outcomes:	**Assessment Criteria:**
1. Understand programming and networking skills required in order for one to master the hacking tools, techniques and strategies.	1.1 What is ethical hacking? 1.2 Describe LAN/WAN technologies 1.3 Describe functions of routers and switches Explain TCP/IP 1.4 Define black hat hackers 1.5 Define white hat hackers 1.6 Describe symptoms of virus-infected computer system 1.7 Outline ethical hacking tools
2. Understand network framework tools and debugging capabilities in order to analyse IP packets, routing and how packets are filtered.	2.1 Define data packets 2.2 Demonstrate diagnosing a network system using NMAP 2.3 Describe network protocols 2.4 Demonstrate scanning a network 2.5 Define malware and different types of malware 2.6 Identify malware removal tools.
3. Understand reverse engineering; from recovering design to restoring structure, functionality, features and functions.	3.1 Define reserve engineering 3.2 Describe uses of reverse engineering 3.3 Describe reasons for reverse engineering 3.4 Identify reverse engineering tools 3.5 Describe SQL/LDAP injections Describe Intrusion Detection System (IDS) and its tools
4. Understand the different threats to e-commerce platforms and the effect it poses to businesses and consumers.	4.1 Describe regions, zones and data centres.

	4.2 Describe electronic payment system 4.3 Analyse threats to different e-commerce platforms 4.4 Define threat hunting and the different associated tools 4.5 Analyse threats to business intellectual property and the tools used. 4.6 Discuss Advanced Persistent Threats (APT) 4.7 Describe data recovery techniques 4.8 Be able to perform cyber security risk assessment
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 coursework/projects in Ethical Hacker.	

Recommended Learning Resources: Ethical Hacker

Text Books	• What Is Hacking? by Kasandra Tanguay. ISBN-13 : 979-8536547373 • Computer Hacking Beginners Guide by Alan T. Norman. ISBN-13 : 978-1980390978 • Cyber Security Basics Cyber Security Basics. ISBN-13 : 978-1522952190
Study Manuals	BCE produced study packs
CD ROM	Power-point slides
Software	N/A