ICT348 Information Security Offence Defence and Incident Management

Level: 3

Credit Units: 5 Credit Units

Language: ENGLISH

Presentation Pattern: EVERY REGULAR SEMESTER

Synopsis:

ICT348 Information Security Offence Defence and Incident Management enables students to not only understand how cyber attacks are carried out, but also learn the security measures that organisations can implement to ensure protection against cyber attacks. Students will learn how to gather information and identify vulnerabilities of targeted computing systems that may be potentially exploited by cyber attackers. Penetration testing will be introduced so that students can determine information security weaknesses. In addition, students will be able to explain how various types of security appliances can be utilized to improve the cyber defence of organisations. Students will also know how to investigate information security incidents through incident response using log analysis and forensics tools.

Topics:

- Stages of Cyber Attacks
- Pentest Planning and Scoping
- Reconnaissance Techniques
- Exploiting Vulnerabilities
- Vulnerability Management
- Secure Software Development
- Security Appliances
- Logging and Analysis
- Incident Response
- Forensic Tools
- Incident Analysis and Recovery
- Security Architecture

Learning Outcome:

- Use information gathering and vulnerability identification
- Apply ethical hacking
- Improve defence strategy
- Implement incident investigation
- Demonstrate penetration testing
- Assess vulnerabilities and threats
- Design incident response

Assessment Strategies - Regular Semester (Daytime Class):

Components	Description	Weightage Allocation (%)

Overall Continuous Assessment	PRE-CLASS QUIZ 1	2
	PRE-CLASS QUIZ 2	2
	PRE-CLASS QUIZ 3	2
	QUIZ 1	6
	TUTOR-MARKED ASSIGNMENT 1	18
Overall Examinable Components	Written Exam 2	70
Total		**100**

*The information listed is subject to review and change.