

## Module 6: IT Infrastructure Protection & Ethical Hacking

<b>Stage</b>	1						
<b>Semester</b>	2						
<b>Module Title</b>	IT Infrastructure Protection & Ethical Hacking						
<b>Module Number</b>	6						
<b>Module Status</b>	Mandatory						
<b>Module ECTS Credits</b>	10						
<b>Module NFQ level</b>	9						
<b>Pre-Requisite Module Titles</b>	None						
<b>Co-Requisite Module Titles</b>	None						
<b>Capstone Module</b>	No						
<b>List of Module Teaching Personnel</b>	Mr Alan Hannaway						
<b>Contact Hours</b>				<b>Non-contact Hours</b>			<b>Total Effort (hours)</b>
60				140			200
<b>Lecture</b>	<b>Practical</b>	<b>Tutorial</b>	<b>Seminar</b>	<b>Assignment</b>	<b>Placement</b>	<b>Independent Work</b>	
36		24		40		100	
<b>Allocation of Marks (Within the Module)</b>							
	<b>Continuous Assessment</b>	<b>Project</b>	<b>Practical</b>	<b>Final Examination</b>	<b>Total</b>		
<b>Percentage Contribution</b>	50%			50%	100%		

### Intended Module Learning Outcomes

On successful completion of this module the learner will be able to:

1. Discuss the foundational concepts of fault tolerance and resilience in IT infrastructure security
2. Design and implement assessment and audit strategies to ensure IT infrastructure security awareness
3. Contrast ethical hacking methodologies and their application on various IT architectures
4. Compare ethical hacking tools and their suitability and applicability in informing protection strategies for IT infrastructures.
5. Analyse and implement state-of-art hacking and penetration testing tools

## Module Objectives

This module introduces the learner to the latest strategies and measures for protecting IT infrastructure against faults and security risks. The learner will understand what the latest threats are, and how the threat environment is evolving. This module studies the frameworks, standards, guidelines and best practises that organisations face in legal & regulatory requirements with respect to IT infrastructure security.

With a sound foundation in the principles of Infrastructure Security, the learner will focus on Ethical Hacking, and its role in the protection of IT Infrastructure. The role of ethical hacking is extensively studied, providing the necessary understanding to develop a skillset and competence with hacking concepts like footprinting, scanning, enumeration and penetration testing.

## Module Curriculum

- **Fault Tolerance and Resilience**
  - Basic concepts on fault tolerance
  - Fault models and challenges with IT infrastructure in the cloud
  - Different levels of fault tolerance in cloud computing
  - Fault tolerance against Byzantine failures in cloud computing
- **Physical Security Essentials**
  - Overview, physical security threats
  - Physical security prevention and mitigation measures
  - Recovery from physical security breaches, threat assessment, planning, and plan implementation,
  - Case study: A Corporate Physical Security Policy
  - Integration of Physical and Logical Security
  - Physical Security Checklist
- **Assessments and Audits**
  - Assessing vulnerabilities and risk
  - Penetration testing & vulnerability assessments.
  - Risk management: quantitative risk measurements
- **Ethical Hacking**
  - Introduction to ethical hacking
  - The role of security and penetration testers
- **Footprinting**
  - The importance of footprinting
  - The role of reconnaissance
  - Unearthing initial information
  - Foot printing tools
- **Scanning**
  - Scanning in Hacking defined
  - Scanning Methodologies

Tools for scanning

- **Enumeration**

Key concepts in enumeration

Enumeration procedures

Tools for enumeration

- **System Hacking for Protection**

Key concepts in system hacking

Password hacking

Password guessing

Hacking web servers: tools for web attackers and security testers

Hacking wireless networks: Tools for hackers and countermeasures for wireless attacks

## **Reading Lists and other learning materials**

### **Recommended Reading**

Vacca J R, 2013, *Cyber Security and IT Infrastructure Protection*, Syngress / Elsevier

Simpson M T, Backman K, Corley J, 2013, *Hands-on Ethical Hacking and Network Defence, 2<sup>nd</sup> Edition*, Course Technology

### **Secondary Reading**

Harper A, Harris S, Ness J, 2011, *Gray Hat Hacking, 3<sup>rd</sup> Edition*, McGraw-Hill

Stallings W, Case T, 2012, *Business Data Communications – Infrastructure, Networking and Security*, Pearson Education

Additional reading as recommended by lecturer, appropriate to topic.

## **Module Learning Environment**

### **Accommodation**

Lectures are carried out in class rooms / lecture halls in the College. Computer Labs throughout the Campus are accessible for the purpose of completing assignments. There is no specific software required to deliver the programme.

## Library

All learners have access to an extensive range of physical and electronic (remotely accessible) library resources. The library monitors and updates its resources on an on-going basis, in line with the College's Library Acquisition Policy. Lecturers update reading lists for this course on an annual basis as is the norm with all courses run by Griffith College.

## Module Teaching and Learning Strategy

Each week, is one lecture and one tutorial / workshop / lab:

Classes are used to explain the concepts, exemplify the techniques, and solve (in workshop style) a series of exercises and problems. Some classes involve the discussion and demonstration of the latest methodologies and tools in protecting IT infrastructure. Learners are expected to read the material prior to class.

In addition to classes, the learners need to put in at least four hours of study and homework each week.

## Module Assessment Strategy

Element No.	Weighting	Type	Description	Learning Outcomes Assessed
1.	10%	Assignment	Learners are required to complete a study on the challenges of assessment and audit methodologies in ensuring good IT infrastructure security. This assignment will further challenge the learner to present a clear understanding on the threat environment to IT infrastructures.	1, 3,4
2.	40%	Weekly Exercises	For this assignment, learners are required to complete weekly exercises that demonstrate an understanding of the suitability and selection of ethical hacking methodologies in various case studies. The exercises will challenge learners to carefully implement and use a combination of tools that support the design and intent of hacking strategies.	2,3, 4, 5
3.	50%	Examination	The examination will test the learners understanding of the theoretical aspects of the coursework.	1,3,4