Module Synopses

Semester One

1. Network Security (NS)

   This module provides students with the fundamental concepts on the need for Network security. Students will be able to identify the threats and vulnerabilities of computer systems and networks and recommend the appropriate actions to be taken to counter-act such activities.

2. Firewall and Intrusion Prevention (FIP)

   This module provides the students with a guide to the most popular firewall technology implementations. In addition, with the knowledge gained from this module, students would be able to recommend and implement the necessary security solutions.

Semester Two

3. Wireless Network and Security (WNS)

   This module provides students with a complete foundation of knowledge in Wireless Networking. It covers from basic RF theory, hardware installation, configuration and management, to troubleshooting, security and site surveying. In addition, the students will be taught the concept of wireless security and how to prevent undesirable users accessing the access point.

4. Network Analysis and Forensics (NAF)

   This module teaches the use of Network Analysis and Packet Capture tools to analyse data flowing through a network. Students will learn how to use analysis tools to perform forensic test to determine the nature of any security breaches and exploits. The module will also use case studies to determine the nature of different exploits used by hackers on the Internet.

5. Project (PROJ)

   Students will be given an opportunity to plan and design a network. This project will be based on the knowledge and skills gained from their course of study. Students will learn how to integrate the knowledge from their course into a practical application in ensuring the security of the network.