**This Version is No Longer Current**
The latest version of this module is available here

## MODULE DESCRIPTOR

### Module Title

Security Testing

| | | | |
|---|---|---|---|
| Reference | CMM518 | Version | 2 |
| Created | April 2018 | SCQF Level | SCQF 11 |
| Approved | August 2017 | SCQF Points | 15 |
| Amended | June 2018 | ECTS Points | 7.5 |

### Aims of Module

To enable students to apply strategies for identifying security vulnerabilities in systems and networks.

### Learning Outcomes for Module

On completion of this module, students are expected to be able to:

| | |
|---|---|
| 1 | Analyse, evaluate and discuss the threats to computer systems. |
| 2 | Explore and analyse the technical as well as non-technical vulnerabilities of computer systems. |
| 3 | Apply relevant penetration testing tools and methods to exploit, document and report on the vulnerabilities. |
| 4 | Evaluate and discuss the standards and the ethical issues pertaining to performing security testing. |

### Indicative Module Content

Ethics and hacking. Methodologies and Frameworks (e.g. 27000 series and Common Criteria, Ethical hacking framework and offensive security). Information gathering, Vulnerability identification and exploitation. System and network penetration testing with Kali Linux Python programming for penetration testing. Reporting results. Audit methodologies (e.g., Certified Information Systems Auditor - CISA). Audit processes and techniques (e.g. HMG IA Maturity Model).

### Module Delivery

Key concepts are introduced and illustrated through lectures and directed reading. The understanding of students is tested and further enhanced through lab sessions.

| Indicative Student Workload | Full Time | Part Time |
|---|---|---|
| Contact Hours | 44 | 44 |
| Non-Contact Hours | 106 | 106 |
| Placement/Work-Based Learning Experience [Notional] Hours | N/A | N/A |
| TOTAL | 150 | 150 |
| *Actual Placement hours for professional, statutory or regulatory body* | | |

| Module Ref: | CMM518 v2 |
|---|---|

## ASSESSMENT PLAN

*If a major/minor model is used and box is ticked, % weightings below are indicative only.*

### Component 1

| Type: | Coursework | Weighting: | 50% | Outcomes Assessed: | 2, 3 |
|---|---|---|---|---|---|
| Description: | This will be an assessed lab where students will be applying pentration testing methods to a given scenario. | | | | |

### Component 2

| Type: | Practical Exam | Weighting: | 50% | Outcomes Assessed: | 1, 4 |
|---|---|---|---|---|---|
| Description: | This is a coursework where students will be preparing a pentrating testing report. | | | | |

## MODULE PERFORMANCE DESCRIPTOR

### Explanatory Text

The calculation of the overall grade for this module is based on 50% weighting of C1 and 50% weighting of C2 components. An overall minimum grade D is required to pass the module.

| | | Practical Exam: | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **A** | **B** | **C** | **D** | **E** | **F** | **NS** |
| Coursework: | **A** | A | A | B | B | C | E | |
| | **B** | A | B | B | C | C | E | |
| | **C** | B | B | C | C | D | E | |
| | **D** | B | C | C | D | D | E | |
| | **E** | C | C | D | D | E | E | |
| | **F** | E | E | E | E | E | F | |
| | **NS** | Non-submission of work by published deadline or non-attendance for examination | | | | | | |

## Module Requirements

| | |
|---|---|
| Prerequisites for Module | None. |
| Corequisites for module | None. |
| Precluded Modules | None. |

## INDICATIVE BIBLIOGRAPHY


| | |
|---|---|
| 1 | Allsopp, W. (2017). Advanced Penetration Testing: Hacking the World's Most Secure Networks. John Wiley & Sons. |
| 2 | Nastase, R. (2018). Hacking with Kali Linux: A step by step guide for you to learn the basics of cybersecurity and hacking. Elsevier. |
| 3 | Peter, K. (2018). The Hacker Playbook 3: Practical Guide To Penetration Testing. Security planet LLC. |
| 4 | Anderson, R. (2020). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons. |
| 5 | Messier, R. (2021). CEH v11 Certified Ethical Hacker Study Guide. John Wiley & Sons. |