1. **Title of the module**

COMP8920 (CO892) - Advanced Network Security

1. **School or partner institution which will be responsible for management of the module**

School of Computing

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 7

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Spring

1. **Prerequisite and co-requisite modules**

Pre-requisite: COMP8710 Advanced Java for Programmers

or (COMP8810 Object-Oriented Programming

and COMP8820 Advanced Object-Oriented Programming)

1. **The programmes of study to which the module contributes**

Portfolio of taught postgraduate programmes in Computing

1. **The intended subject specific learning outcomes.  
   On successfully completing the module students will be able to:**

8.1 Have a knowledge of the threats faced by computer operating systems, applications and networks that originate from network-based attacks, intrusion and misuse;

8.2 Have a knowledge of the types of countermeasures that can be put in place in computer systems, networks, and network infrastructures to identify, reduce or prevent problems caused by network attacks or misuse;

8.3 Be capable of making informed choices of the appropriate countermeasures that should be put in place to protect systems from network attacks or misuse and to maintain network security;

8.4 Have a deeper and integrated understanding of selected key topics at the forefront of this field, including recent developments and outstanding issues;

8.5 Have the skills to keep abreast of future developments in network security;

8.6 Be able to undertake an investigation into areas covered by this module and report on their findings.

1. **The intended generic learning outcomes.  
   On successfully completing the module students will be able to:**

9.1 Time management and organisation;

9.2 Communication skills;

9.3 Be able to undertake an independent investigation into areas covered by this module and report on their findings;

9.4 Problem solving;

9.5 Independent study and appropriate use of relevant resources.

1. **A synopsis of the curriculum**

* Network security and cybercrime.
* Analysis of real world network security incident (IoT botnet).
* Email security issues (spam and phishing attacks; spam filtering systems).
* Spyware (system vulnerabilities; stealth techniques; detection and removal).
* Network-related data security (data breaches; data loss prevention; remote sniffer detection).
* Security of WiFi networks.
* Network forensics and incident response.
* Emerging network protocols
* IPv6 security.
* Honeypots and honeynets.
* Software-defined networking.

Penetration testing.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Christos Douligeris & Dimitrios Nikolaou Serpanos, “Network security: current status and future directions”, John Wiley and Sons (2007).

Joseph Migga Kizza, “Guide to Computer network security”, 4th ed., Springer (2017).

NIST SP800-61 r2, “Computer Security Incident Handling Guide” (2012), <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

Sherri Davidoff and Jonathan Ham, “Network Forensics: Tracking Hackers Through Cyberspace”, Prentice Hall (2012).

Michael Bazzell, “Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information”, 7th ed (2019).

Enisa, “Introduction to Network Forensics” (2019), <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf>

William Stallings, “Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud”, Addison Wesley (2016).

1. **Learning and teaching methods**

Total contact hours: 20

Private study hours: 130

Total study hours: 150

1. **Assessment methods**
   1. Main assessment methods

Two sets of coursework (25% total)

Examination, 2-hour (75%)

13.2 Reassessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | *8.1* | *8.2* | *8.3* | *8.4* | *8.5* | *8.6* | *9.1* | *9.2* | *9.3* | *9.4* | *9.5* |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |  |  |
| Private Study |  |  |  | X | X | X | X | X | X | X | X |
| Lectures | X | X | X | X |  |  |  |  |  |  |  |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |  |
| Reports | X |  |  | X | X | X | X | X | X | X | X |
| Examination | X | X | X | X |  |  |  |  |  | X |  |

1. **Inclusive module design**

The School recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

The topics addressed by this module relate to a field which is of international importance, given the global role of computers in today's technological innovation. The topics covered by this module are international in nature, being identical worldwide and independent of traditional spoken language.

**FACULTIES SUPPORT OFFICE USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of the delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
| 03/08/20 | Minor | January 2021 | 10,11,13 | No |
|  |  |  |  |  |

Revised FSO Jan 2018