Module Descriptor

Title	Network Security Issues		
Session	2025/26	**Status**	Published
Code	COMP11118	**SCQF Level**	11
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Shahriar Al-Ahmed		

Summary of Module

The security of computer networks has been a major concern for the management of information systems used by businesses of all kinds, from start-ups to enterprises. Computer networks are frequently compromised as a result of insufficient security and management measures to detect malicious access privilege escalation, monitor network traffic and services, ensure network confidentiality and privacy, prevent network attacks, and build resilience to modern-day cyber-attacks.

This module discusses network security fundamentals within the context of network and data management for trustworthy and untrusted computer networks.

It is intended to cover key network security approaches, algorithms, and tools, as well as provide hands-on experience in creating and operating secure, privacy-aware, and resilient computer networks.

This module will work to develop a number of the key 'I am UWS' Graduate Attributes to make those who complete this module. Universal: Critical Thinker; Ethically-minded; and Research-minded. Work Ready: Problem-Solver; Effective Communicator; and Ambitious. Successful: Autonomous; Resilient; and Driven.

Module Delivery Method	**On-Campus[1]**	**Hybrid[2]**	**Online[3]**	**Work -Based Learning[4]**
	☒	☐	☐	☐

[1] Where contact hours are synchronous/ live and take place fully on campus. Campus-based learning is focused on providing an interactive learning experience supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus contact hours will be clearly articulated to students.

[2] The module includes a combination of synchronous/ live on-campus and online learning events. These will be supported by a range of digitally-enabled asynchronous learning opportunities including learning materials, resources, and opportunities provided via the virtual learning environment. On-campus and online contact hours will be clearly articulated to students.

[3] Where all learning is solely delivered by web-based or internet-based technologies and the participants can engage in all learning activities through these means. All required contact hours will be clearly articulated to students.

[4] Learning activities where the main location for the learning experience is in the workplace. All required contact hours, whether online or on campus, will be clearly articulated to students

Campuses for Module Delivery	☐ Ayr ☐ Dumfries		☐ Lanarkshire ☒ London ☒ Paisley		☐ Online / Distance Learning ☐ Other (specify)	
Terms for Module Delivery	Term 1	☒	Term 2	☒	Term 3	☒
Long-thin Delivery over more than one Term	Term 1 – Term 2	☐	Term 2 – Term 3	☐	Term 3 – Term 1	☐

Learning Outcomes	
L1	Demonstrate extensive knowledge of the core theories, concepts and principles of secure network design, attacks, and mitigation techniques
L2	Demonstrate a comprehensive understanding of network security frameworks and best practices
L3	Develop skills to analyse and critically evaluate security of networked systems and recommend relevant technical and management improvements or solutions
L4	N/A
L5	N/A

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	**During completion of this module, there will be an opportunity to achieve core skills in:**
Knowledge and Understanding (K and U)	**SCQF 11** Students will learn comprehensive knowledge of network security. Students are expected to be familiar with the key technologies and techniques and their application in practice
Practice: Applied Knowledge and Understanding	**SCQF 11** Students will gain in-depth understanding and critical awareness of knowledge of network security, and apply this in planning, implementing, configuration and testing of the security state of the test environment. They will also develop capability to apply a range of specialised research skills and relevant tools and software for their written assignment and lab tasks
Generic Cognitive skills	**SCQF 11** To complete their written reports and laboratory tasks, students will first build skills to integrate information and apply knowledge from various sources including technology advances informed by research and industry
Communication, ICT and Numeracy Skills	**SCQF 11** Working in interacting groups, students will develop communication skills as well as the ability to write technical reports and documentation
Autonomy, Accountability and Working with Others	**SCQF 11** Each student will generate a comprehensive technical report summarizing the finding for a given relevant topic on computer networks

Prerequisites	Module Code	Module Title
	Other	
Co-requisites	Module Code	Module Title

Learning and Teaching

In line with current learning and teaching principles, a 20-credit module includes 200 learning hours, normally including a minimum of 36 contact hours and maximum of 48 contact hours.

This module includes interactive lectures and lab sessions, as well as problem-based learning exercises and corresponding practical workshops. Beyond lectures, the rationale is to impart information linked to computer network administration, data transfer, and network security. Students will study various algorithms, protocols, and strategies for securing computer networks of various sizes and configurations through lectures.

Furthermore, students will be taught to specific cybersecurity issues to help them comprehend vulnerabilities in the network generation of computer networks. The lab sessions will aid in the development of an in-depth comprehension of the knowledge presented in the lectures, as well as the critical evaluation of algorithms and approaches when applied to a specific situation.

This module's material will be given in accordance with the following list of possible topics:

- Common networked system risks and weaknesses
- Network perimeter methods.
- Techniques for network monitoring.
- Cryptographic techniques.
- Protocols and techniques for network authentication.
- Data transfer across a secure network.
- Secure network architecture

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture / Core Content Delivery	20
Tutorial / Synchronous Support Activity	4
Laboratory / Practical Demonstration / Workshop	18
Independent Study	158
Please select	
Please select	
TOTAL	200

Indicative Resources

The following materials form essential underpinning for the module content and ultimately for the learning outcomes: Leirvik, R. (2021) Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program, Apress Diogenes, Y and Ozkaya, E. (2018) Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics. Packt Publishing*
(N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance and Engagement Requirements
In line with the Student Attendance and Engagement Procedure, Students are academically engaged if they are regularly attending and participating in timetabled on-campus and online teaching sessions, asynchronous online learning activities, course-related learning resources, and complete assessments and submit these on time. **For the purposes of this module, academic engagement equates to the following:** The School of Computing, Engineering and Physical Sciences considers attendance and engagement to mean a commitment to attending, and engaging in, timetabled sessions. You will scan your attendance via the scanners each time you are on-campus and you will login to the VLE several times per week. Where you are unable to attend a timetabled learning session due to illness or other circumstance, you should notify the Programme Leader that you cannot attend. Across the School an 80% attendance threshold is set. If you fall below this, you will be referred to the Student Success Team to see how we can best support your studies.

Equality and Diversity
The University's Equality, Diversity and Human Rights Procedure can be accessed at the following link: UWS Equality, Diversity and Human Rights Code. Aligned with the University's commitment to equality and diversity, this module supports equality of opportunity for students from all backgrounds and learning needs. Using the VLE, material will be presented electronically in formats that allow flexible access and manipulation of content. This module complies with University regulations and guidance on inclusive learning and teaching practice. This module has lab-based teaching and as such you are advised to speak to the Module Co-ordinator to ensure that specialist assistive equipment, support provision and adjustment to assessment practice can be put in place, in accordance with the University's policies and regulations.
(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)

Supplemental Information

Divisional Programme Board	**Computing**
Overall Assessment Results	☐ **Pass / Fail** ☒ **Graded**
Module Eligible for Compensation	☐ **Yes** ☒ **No** **If this module is eligible for compensation, there may be cases where compensation is not permitted due to programme accreditation requirements. Please check the associated programme specification for details.**

School Assessment Board	Business & Applied Computing
Moderator	Raja Majid Ujjan
External Examiner	A Esfahani
Accreditation Details	
Module Appears in CPD catalogue	☐ **Yes** ☒ **No**
Changes / Version Number	1.1

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
During the laboratory sessions, each student will be required to successfully complete the task(s) mentioned in the lab manual (weighted 40%), consequently assessing the achievement of L1.
Assessment 2
A formal written report (weighted 60%) will be required from each student summarizing their finding of a given topic and demonstrate their skills to secure network and network services – agreed by the module coordinator, to evaluate L2, L3. This assignment will require the students to do some literature review, identify possible solutions, demonstrate efficacy of proposed solutions, and justify / critics them accordingly.
Assessment 3
(N.B. (i) Assessment Outcomes Grids for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed. (ii) An indicative schedule listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Module Handbook.)

Component 1							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Laboratory/ Clinical/ Field notebook	☒	☐	☐	☐	☐	40	0

Component 2							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
Report of practical/ field/ clinical work	☐	☒	☒	☐	☐	60	0

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**

	☐	☐	☐	☐	☐		
Combined total for all components						100%	hours

Change Control

What	**When**	**Who**
Attendance, EDI and External Examiner updated	22/01/2025	A Adamson