Module Descriptor

Title	Network Security		
Session	2025/26	**Status**	Published
Code	COMP10014	**SCQF Level**	10
Credit Points	20	**ECTS (European Credit Transfer Scheme)**	10
School	**Computing, Engineering and Physical Sciences**		
Module Co-ordinator	Steve Eager		

Summary of Module

This module introduces the student to the fundamental concepts related to Network Security. The following network security concepts are analyzed in detail: security in ethernet network infrastructures, firewalling, proxies, network encapsulation, network authentication and network authorization. The module covers as well concepts related to symetric and asymetric cryptography, PKI protocols, key exchange and digital signature. Typical vulnerabilities are studied from the hackers' point of view and then from the Administrators perspective so that these vulnerabilities can be either stopped or prevented.

The module is complemented with labs where the concepts explained in lectures can be put in practices in order to get deeper understanding on the fundamentals of how security in IP networks is implemented.

Additionaly, 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
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient
- Driven

The scope of the module includes the following topics:

- Security of the Network Infrastructure
- Firewalls

- Cryptography
- Intrusion Detection and Prevention
- PKI Protocols, Key Exchange and Digital Signature
- Network Encapsulation
- Network Authentication and Authorization

Module Delivery Method	**On-Campus**[1] ☒	**Hybrid**[2] ☐	**Online**[3] ☐	**Work -Based Learning**[4] ☐
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 a critical understanding of security concepts
L2	Demonstrate detailed knowledge of Network Security Techniques and Technologies
L3	Evaluate the security threats to specific network
L4	Configure security measures to meet a given policy
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 10** The aim of the module is to enable the student to acquire the knowledge and understanding of Network Security through lectures, group practicals and guided self study.

[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

Practice: Applied Knowledge and Understanding	**SCQF 10** Knowledge gained will be demonstrated through successful completion of coursework, laboratories and exams.
Generic Cognitive skills	**SCQF 10** Through the development of strategies to secure a network as the student works through the lab work they will be able to apply these methodologies to other aspect of their work.
Communication, ICT and Numeracy Skills	**SCQF 10** Throughout the lab program students will have to work together in the detection and implementation of security. Students will then have to write their own evaluation of the lab work so will have to use word processing, capturing and formatting of images and other computing skills.
Autonomy, Accountability and Working with Others	**SCQF 10** Various deadlines are imposed for the handing in of course work which requires the student to manage their time. The lab work has a large component of group working so the student will learn how to work within a group yet also fulfill their own personal work schedule.

Prerequisites	**Module Code** COMP09024 COMP09089	**Module Title** Unix System Administration Windows Server Administration
	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. Lecturers are used to introduce the material, allowing the students to gain an appreciation of the topics. Tutorial discussions and practical work in a laboratory setting are there to deepen the students learning. Web-based materials are also provided to provide additional support to students.	
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	12
Laboratory / Practical Demonstration / Workshop	36
Independent Study	152
Please select	
Please select	
Please select	

TOTAL	200

Indicative Resources

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

“Hacking Exposed” 5e by S. McClure et al, McGraw-Hill Osborne, 2005, ISBN 0072260815

“Applied Cryptography” 2e by B. Schneier, John Wiley, 1996, ISBN 0471117099

“Secrets and Lies” by B. Schneier, Hungry Minds Inc,U.S., 2004, ISBN 0471453803

"Introduction to Computer Networks and Cybersecurity by Cnwan-Hwa (John) Wu, J David Irwin ISBN 978-1-4665-7213-3

Students will require access to a networked computer, installed with virtualization software and extensions hosting multiple Linux systems to enable practical lab work and assignments to be completed.

Lecture notes, laboratory sheets and tutorial questions will be posted on the VLE.

(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	D Thomson
External Examiner	R Khusainov
Accreditation Details	This module is accredited by BCS as part of a number of specified programmes.
Module Appears in CPD catalogue	☒ **Yes** ☐ **No**
Changes / Version Number	4.05

Assessment (also refer to Assessment Outcomes Grids below)
Assessment 1
Class Test (60%)
Assessment 2
Coursework (40%)
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**
Portfolio of practical work	☐	☐	☒	☒	☐	40	0

Component 2

Assessment Type	LO1	LO2	LO3	LO4	LO5	Weighting of Assessment Element (%)	Timetabled Contact Hours
Class Test	☒	☒	☒	☐	☐	60	0

Component 3							
Assessment Type	**LO1**	**LO2**	**LO3**	**LO4**	**LO5**	**Weighting of Assessment Element (%)**	**Timetabled Contact Hours**
	☐	☐	☐	☐	☐		
Combined total for all components						100%	0 hours

Change Control

What	When	Who
Attendance and Engagement Procedure and Equality and Diversity	20/1/25	F.Valentine
Module Coordinator and moderator updated. Component updated.	01/05/25	A Adamson
Change to module delivery method Changes to hours in Learning Activities / Student Learning Hours	21/06/25	S Eager