University of the West of Scotland
Module Descriptor

Session: 2024/25

Last modified: 19/07/24

Title of Module: CCNA: CyberOps

Code: COMP09116	**SCQF Level: 9** **(Scottish Credit and Qualifications Framework)**	**Credit Points: 20**	**ECTS: 10** **(European Credit Transfer Scheme)**
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Sean Sturley		

Summary of Module

Cybersecurity operations play a key part in securing information systems through monitoring, detecting, investigating, analysing, and responding to security events, thus protecting systems from cybersecurity risks, threats, and vulnerabilities. Cybersecurity operations jobs are also among the fastest-growing roles in IT, as organizations set up Security Operations Centre's (SOCs), and establish teams to monitor and respond to security incidents.

The module makes use of Cisco Networking Academy teaching materials and is designed to give students the opportunity to progress towards Cisco certification.

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

Module Delivery Method

Face-To-Face	Blended	Fully Online
	✓	

Face-To-Face
Term used to describe the traditional classroom environment where the students and the lecturer meet synchronously in the same room for the whole provision.

Fully Online
Instruction that is solely delivered by web-based or internet-based technologies. This term is used to describe the previously used terms distance learning and e learning.

Blended
A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered “blended” if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations

Campus(es) for Module Delivery

The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit)

Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online Learning:	Other:
			✓			D&G and NCL

Learning Outcomes: (maximum of 5 statements)

On successful completion of this module the student will be able to:

L1. Critically evaluate cyber security policies, standards, processes, and guidelines for the security management and monitoring of critical enterprise infrastructure.

L2. Demonstrate a detailed knowledge of potential security threats, the securing of host and network devices, and the integration of security and cryptographic systems.

L3. Install, configure and test network security technologies according to industry standards using commercial equipment.

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 Level 9. Students will develop a critical understanding of fundamental security layers and processes involved in cyber operations. They will obtain critical knowledge and understanding of the commercial and economic context of running cyber operations.
Practice: Applied Knowledge and Understanding	SCQF Level 9. Students will gain in-depth knowledge about cyber operations by identifying the key attributes to an attack by investigating cyber attacks.
Generic Cognitive skills	SCQF Level 9. To complete their group reports, students will first build skills to critically understand key issues in managing cyber operations. They will develop learning awareness of comprehensive security architectures based upon multiple layers of protection.

Communication, ICT and Numeracy Skills	SCQF Level 9. In the labs, students will be able to work in groups to discuss various cyber security protections to develop technical communication skills with peers and lecturer. They will also develop the ability to write formal technical reports and documentation in the group report. The labs will develop ICT skills by configuring computers and network devices to allow/disallow attacks on these devices.
Autonomy, Accountability and Working with others	SCQF Level 9. Students will demonstrate an ability to work independently on their own laboratory task and acquire the autonomy and accountability through these tasks. In the lab sessions, they will autonomously plan and manage the work progress and finish the writing of the lab note and report in a timely and professional manner. They will also gain accountability and teamwork skills by finishing the group report which require cooperation from the team members and thus develop the teamwork spirit and cooperation skills.

Pre-requisites:	Before undertaking this module the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

* Indicates that module descriptor is not published.

Learning and Teaching	
Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	12
Tutorial/Synchronous Support Activity	12
Laboratory/Practical Demonstration/Workshop	24
Independent Study	152
	200 Hours Total

****Indicative Resources: (eg. Core text, journals, internet access)**

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

Cisco Net Academy

McNab, C. (2016). Network Security Assessment: Know Your Network (3rd Edition), O'Reilly. ISBN-10: 149191095X, ISBN-13: 978-1491910955

Nathans, D. (2014). Designing and Building a Security Operations Center, Syngress. ISBN-10: 128008997, ISBN-13: 978-0128008997

Santos, O and Muniz, J (2017), CCNA Cyber Ops (SECFND #210-250 and SECOPS #210-255) Official Cert Guide Library (1st Edition), Cisco Press. ISBN-10: 1587145006, ISBN-13: 978-1587145001

Chu, A (2019), CCNA Cyber Ops SECOPS – Certification Guide 210-255: Learn the skills to pass the 210-255 certification exam and become a competent SECOPS associate, Packt Publishing. ISBN-10: 1838559868
ISBN-13: 978-1838559861

(**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 Requirements

In line with the Academic Engagement and Attendance Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on Moodle, and complete assessments and submit these on time. Please refer to the Academic Engagement and Attendance Procedure at the following link: Academic engagement and attendance procedure

Supplemental Information

Programme Board	Computing
Assessment Results (Pass/Fail)	No
Subject Panel	Applied Computing
Moderator	Steve Eager

External Examiner	
Accreditation Details	
Version Number	1.02

Assessment: (also refer to Assessment Outcomes Grids below)
Online Exam (50%) and Ongoing Assessments (10%)
Practical Skills Test(40%)
(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 Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Unseen open book	✓	✓		10	0
Class test (written)	✓	✓		50	0

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Class test (practical)		✓	✓	40	0
			Combined Total For All Components	100%	0 hours

Footnotes
A. Referred to within Assessment Section above
B. Identified in the Learning Outcome Section above

Note(s):

1. More than one assessment method can be used to assess individual learning outcomes.
2. Schools are responsible for determining student contact hours. Please refer to University Policy on contact hours (extract contained within section 10 of the Module Descriptor guidance note).
   This will normally be variable across Schools, dependent on Programmes &/or Professional requirements.

Equality and Diversity
UWS Equality and Diversity Policy

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)