COURSE OUTLINE

SEC603 Introduction to Device & Network Security

School: School of Science, Technology and Engineering

2026 | Trimester 1

UniSC Sunshine Coast UniSC Adelaide	BLENDED LEARNING	Most of your course is on campus but you may be able to do some components of this course online.
Online	ONLINE	You can do this course without coming onto campus, unless your program has specified a mandatory onsite requirement.

Please go to unisc.edu.au for up to date information on the teaching sessions and campuses where this course is usually offered.

1. What is this course about?

1.1. Description

This online professional competency course introduces you to fundamental competencies and skills to effectively secure computer devices and networks.You will specifically develop and test your competency across device and network security vulnerabilities, behaviours and restrictions. You will also develop an understanding of ethical hacking and vulnerability/penetration testing. You will work online independently and in teams through problem based and case study activities and you will be able to diagnose and secure network devices.

1.2. How will this course be delivered?

ACTIVITY	HOURS	BEGINNING WEEK	FREQUENCY
BLENDED LEARNING			
Learning materials – Asynchronous Learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous on campus workshop	2hrs	Week 1	12 times
Seminar – On campus seminar	1hr	Week 1	2 times
ONLINE			
Learning materials – Asynchronous Learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Synchronous Zoom workshop	2hrs	Week 1	12 times
Seminar – Online seminar	1hr	Week 1	2 times

1.3. Course Topics

- Introduction to Cyber Security
- Cyber Security Roles and Frameworks
- Introduction to Threats, Vulnerabilities, Controls and Cryptography
- Incident Response
- Digital Forensics
- Network Protocols and Services
- Protecting the network and network attacks
- Principles of Network Security and Ethical Hacking
- Windows
- Linux
- Report Writing

2. What level is this course?

600 Level (Specialised)

Demonstrating a specialised body of knowledge and set of skills for professional practice or further learning. Advanced application of knowledge and skills in unfamiliar contexts.

3. What is the unit value of this course?

12 units

4. How does this course contribute to my learning?

COURSE LEARNING OUTCOMES On successful completion of this course, you should be able to...		GRADUATE QUALITIES Completing these tasks successfully will contribute to you becoming...
1	Explain device and network fundamental concepts.	Knowledgeable
2	Diagnose data points and device/network behaviours that reveal vulnerabilities in the computer network.	Empowered
3	Evaluate the role of data access restrictions, white-listing, administrative privileges, and related controls from a multi-actor perspective in an organisational context.	Creative and critical thinker
4	Communicate research and findings in systematic ways to specialist and non-specialist audiences.	Engaged

5. Am I eligible to enrol in this course?

Refer to the UniSC Glossary of terms for definitions of “pre-requisites, co-requisites and anti-requisites”.

5.1. Pre-requisites

SEC601 and Enrolled in Program SC509, SC517, SC705 or BU708

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

5.4. Specific assumed prior knowledge and skills (where applicable)

Students will be expected to have a working knowledge of computer systems and networks.

5.5. Microcredential Information

Not applicable

6. How am I going to be assessed?

6.1. Grading Scale

Standard Grading (GRD)

High Distinction (HD), Distinction (DN), Credit (CR), Pass (PS), Fail (FL).

6.2. Details of early feedback on progress

Feedback will be given to students from activities conduced in the weekly tutorials

6.3. Assessment tasks

DELIVERY MODE	TASK NO.	ASSESSMENT PRODUCT	INDIVIDUAL OR GROUP	WEIGHTING %	WHAT IS THE DURATION / LENGTH?	WHEN SHOULD I SUBMIT?	WHERE SHOULD I SUBMIT IT?
All	1	Examination - not Centrally Scheduled	Individual	10%	1 hour	Week 4	Online Test (Quiz)
All	2	Written Piece	Individual	40%	1000 words	Refer to Format	Online Assignment Submission with plagiarism check
All	3	Report	Individual	50%	1500 words	Week 12	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Security Artefact Development

GOAL:	The goal of this task is to demonstrate your understanding of foundational level knowledge of security, compliance, and identity concepts and related cloud-based solutions.
PRODUCT:	Examination - not Centrally Scheduled
AUTHORSHIP STATEMENT:	
FORMAT:	Individual 1 hour online exam. More details will be provided on Canvas.
CRITERIA:	

No.		Learning Outcome assessed
1	Describe the concepts of security, compliance, and identity.	1
2	Describe the capabilities of solutions including identity and access management, security and compliance.	2 3

GENERIC SKILLS:	

All - Assessment Task 2: Connecting theory and practice

GOAL:	The goal of this task is to apply your understanding of the weekly learning material to industry-based situations and to practice configurations and professional report writing, both skills fundamental to the work of industry professionals.
PRODUCT:	Written Piece
AUTHORSHIP STATEMENT:	
FORMAT:	3 Mini Tasks in 3 weeks (Week 3,5 and 7). Specific mini-task information will be released a minimum of one (1) week prior to each deadline. Mini tasks may include applying understandings of OS utilities, practical exercises and report writing in response to case studies.
CRITERIA:	

No.		Learning Outcome assessed
1	Generate a product or output using the task objectives	2
2	Analyse and apply research information to achieve task objectives.	1 2
3	Provide justification for decisions made to achieve task objectives.	1

GENERIC SKILLS:	

All - Assessment Task 3: Policy and Governance Report

GOAL:	The goal for this task is to apply your understanding of governance to review a fictional company's Information Technology policy and make recommendations to ensure that it represents industry best practice.
PRODUCT:	Report
AUTHORSHIP STATEMENT:	
FORMAT:	You will compile your recommendations in a written report and provide justification using relevant governance documentation. Your recommendations should be formatted as a written report and saved as a Word document. More details will be provided on Canvas.
CRITERIA:	

No.		Learning Outcome assessed
1	Identify strategies for securing networks	1 2 3
2	Identifying strategies for hardening devices	2 3
3	Provide and justify security recommendations	3
4	Identify key messages for technical and non-technical audiences	4
5	Communicate using report writing	4

GENERIC SKILLS:	

7. Directed study hours

A 12-unit course will have total of 150 learning hours which will include directed study hours (including online if required), self-directed learning and completion of assessable tasks. Student workload is calculated at 12.5 learning hours per one unit.

8. What resources do I need to undertake this course?

Please note: Course information, including specific information of recommended readings, learning activities, resources, weekly readings, etc. are available on the course Canvas site– Please log in as soon as possible.

8.1. Prescribed text(s) or course reader

You need regular access to the resource(s) below. Many texts are available as ebooks through the Library at no additional cost.

REQUIRED?	AUTHOR	YEAR	TITLE	EDITION	PUBLISHER
Recommended	Charles Pfleeger, Shari Pfleeger, Lizzie Coles-Kemp	2023	Security in Computing	6th Ed	Pearson College Division

8.2. Specific requirements

Access to a computer and the internet for activities during the week.

9. How are risks managed in this course?

Health and safety risks for this course have been assessed as low. It is your responsibility to review course material, search online, discuss with lecturers and peers and understand the health and safety risks associated with your specific course of study and to familiarise yourself with the University's general health and safety principles by reviewing the online induction training for students, and following the instructions of the University staff.

10. What administrative information is relevant to this course?

10.1. Assessment: Academic Integrity

Academic integrity is the ethical standard of university participation. It ensures that students graduate as a result of proving they are competent in their discipline. This is integral in maintaining the value of academic qualifications. Each industry has expectations and standards of the skills and knowledge within that discipline and these are reflected in assessment.

Academic integrity means that you do not engage in any activity that is considered to be academic fraud; including plagiarism, collusion or outsourcing any part of any assessment item to any other person. You are expected to be honest and ethical by completing all work yourself and indicating in your work which ideas and information were developed by you and which were taken from others. You cannot provide your assessment work to others. You are also expected to provide evidence of wide and critical reading, usually by using appropriate academic references.

In order to minimise incidents of academic fraud, this course may require that some of its assessment tasks, when submitted to Canvas, are electronically checked through Turnitin. This software allows for text comparisons to be made between your submitted assessment item and all other work to which Turnitin has access.

10.2. Assessment: Additional Requirements

Eligibility for Supplementary Assessment

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:
(a) The final mark is in the percentage range 47% to 49.4%; and
(b) The course is graded using the Standard Grading scale

10.3. Assessment: Submission penalties

Late submissions may be penalised up to and including the following maximum percentage of the assessment task's identified value, with weekdays and weekends included in the calculation of days late:
(a) One day: deduct 5%;
(b) Two days: deduct 10%;
(c) Three days: deduct 20%;
(d) Four days: deduct 40%;
(e) Five days: deduct 60%;
(f) Six days: deduct 80%;
(g) Seven days: A result of zero is awarded for the assessment task.

The following penalties will apply for a late submission for an online examination:
Less than 15 minutes: No penalty
From 15 minutes to 30 minutes: 20% penalty
More than 30 minutes: 100% penalty

10.4. Links to relevant University policy and procedures

For more information on Academic Learning & Teaching categories including:

- Assessment: Courses and Coursework Programs
- Review of Assessment and Final Grades
- Supplementary Assessment
- Central Examinations
- Deferred Examinations
- Student Conduct
- Students with a Disability

For more information, visit https://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

10.5. Student Charter

UniSC is committed to excellence in teaching, research and engagement in an environment that is inclusive, inspiring, safe and respectful. The Student Charter sets out what students can expect from the University, and what in turn is expected of students, to achieve these outcomes.

10.6. General Enquiries

For course-specific questions, contact your teaching staff or Course Coordinator.

For other enquiries or to access support, please contact Student Central:

- UniSC Student Central
- UniSC Adelaide Student Central