COURSE OUTLINE

SEC303 Device & Network Security

School: School of Science, Technology and Engineering

2026 | Trimester 2

UniSC Sunshine Coast UniSC Moreton Bay 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

Devices and networks form the backbone to modern internet communications and secure personal data and activities. You will be introduced to fundamental competencies and skills to effectively secure computer devices and networks and develop and test their competency. You will also develop an understanding of ethical hacking and vulnerability/penetration testing. You will work 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 online learning materials	2hrs	Week 1	12 times
Tutorial/Workshop 1 – On campus theory and practical workshops	2hrs	Week 1	12 times
ONLINE			
Learning materials – Asynchronous learning material	2hrs	Week 1	12 times
Tutorial/Workshop 1 – Online workshop	2hrs	Week 1	12 times

1.3. Course Topics

- Introduction to device and network security
- Network security and vulnerabilities
- Ethical Hacking
- Defensive strategies and tools
- Protecting your data and resources
- Diagnose device and network security – case studies

2. What level is this course?

300 Level (Graduate)

Demonstrating coherence and breadth or depth of knowledge and skills. Independent application of knowledge and skills in unfamiliar contexts. Meeting professional requirements and AQF descriptors for the degree. May require pre-requisites where discipline specific introductory or developing knowledge or skills is necessary. Normally undertaken in the third or fourth full-time study year of an undergraduate program.

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	Identify and describe device and network security vulnerabilities.	Knowledgeable
2	Identify data points and device/network behaviours that reveal vulnerabilities in the computer network.	Knowledgeable
3	Explain the role of data access restrictions, white-listing, administrative privileges, and related controls from a multi-actor perspective in an organisational context.	Knowledgeable
4	Diagnose device and network security vulnerabilities using online resources.	Empowered
5	Work as part of a team to effectively undertake and communicate security activities.	Engaged
6	Demonstrate effective written and oral communication skills to present research and findings 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

ICT211 or SEC301 or (SEC100 and ICT120)

5.2. Co-requisites

Not applicable

5.3. Anti-requisites

Not applicable

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

Not applicable

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

Weekly exercises will provide students with formative feedback weekly. Additionally, the group assessment in Task 2 will be designed to have regular formative feedback.

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 5	Online Assignment Submission with plagiarism check
All	2	Artefact - Professional, and Written Piece	Individual and Group	50%	3000 words (total)	Week 11	Online Assignment Submission with plagiarism check
All	3	Examination - Centrally Scheduled	Individual	40%	2 hours	Exam Period	Online Assignment Submission with plagiarism check

All - Assessment Task 1: Mid Trimester Exam

GOAL:	You will become competent across a range of device and network security tools, security tradecrafts, and practices.
PRODUCT:	Examination - not Centrally Scheduled
AUTHORSHIP STATEMENT:	
FORMAT:	Short answer questions on device and network security
CRITERIA:	

No.		Learning Outcome assessed
1	Identification and description of device and network security, cryptographic methodologies, security frameworks, threats, vulnerabilities and controls, network security, alerts, incident response management, Cybersecurity careers	1 2 3 4

GENERIC SKILLS:	Communication, Problem solving, Applying technologies, Information literacy

All - Assessment Task 2: Group scenario project

GOAL:	You will work through a network security case study. You will review, investigate and action appropriate network security controls.
PRODUCT:	Artefact - Professional, and Written Piece
AUTHORSHIP STATEMENT:	
FORMAT:	This is a collaborative project. More details will be provided on Canvas.
CRITERIA:	

No.		Learning Outcome assessed
1	Identification of compromise	1 2 3 4
2	Explanation of methodologies to exploit identified vulnerabilities	1 2 4
3	Identification of security remedies and strategies and justify their implementation	3
4	Professional communication	6
5	Digital collaboration	5

GENERIC SKILLS:	Communication, Collaboration, Problem solving, Organisation, Applying technologies

All - Assessment Task 3: Final Exam

GOAL:	You will demonstrate discipline knowledge and skills through a number of short/long exams questions.
PRODUCT:	Examination - Centrally Scheduled
AUTHORSHIP STATEMENT:	
FORMAT:	Individual exam covering security skills gained throughout course.
CRITERIA:	

No.		Learning Outcome assessed
1	Identification of the key elements of a cyber breach	1 2 4
2	Identification and articulation of consequences of cyber breach	1 2 3
3	Compare various vulnerabilities in computer networks	1 2

GENERIC SKILLS:	Communication, Problem solving, Applying technologies

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 P. Pfleeger,Shari Lawrence Pfleeger,Jonathan Margulies	2015	Security in Computing	5th	Pearson College Division

8.2. Specific requirements

This course requires access to computers and specialist software which is provided at USC campuses for student use. If you elect to do this course online, you
may either; attend a campus at which it is available, discuss alternative solutions with your course coordinator that would enable you to demonstrate the learning outcomes, or if you prefer you may acquire this software (if necessary at your own expense). Some software providers
may offer discounted or free academic licensing.

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