COURSE OUTLINE

# SEC603 Introduction to Device & Network Security

**Course Coordinator:** Fida HASAN (khasan@usc.edu.au) **School:** School of Science, Technology and Engineering

2021 | Semester 2

Online ONLINE You can do this course without coming onto campus.

*Please go to the USC website 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 |
|---|---|---|---|
| **ONLINE** | | | |
| **Online** – The online course will take 10-12 hours per week and may include a combination of webinar, peer to peer collaboration, asynchronous online materials, and synchronous lecturer and peer to peer zoom meetings. | 12hrs | Not applicable | 13 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<br>On successful completion of this course, you should be able to... | | GRADUATE QUALITIES<br>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 | Demonstrate leadership in a virtual team environment. | Engaged |
| 6 | Communicate research and findings to specialist and non-specialist audiences. | Engaged |

## 5. Am I eligible to enrol in this course?

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

### 5.1. Pre-requisites

SEC601 and enrolled in Program SC509, SC517 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.

## 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

Using marking rubrics, students will participate in continuous peer and self-assessment tasks.

## 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 | Portfolio | Individual | 15% | Weekly entries | Throughout teaching period (refer to Format) | Online ePortfolio Submission |
| All | 2 | Report | Group | 40% | 3,000 Words | Week 7 | Online Assignment Submission with plagiarism check |
| All | 3 | Oral and Written Piece | Individual | 45% | 15 min Executive Briefing (recorded presentation) | Exam Period | To Supervisor |

**All - Assessment Task 1:** Competency portfolio

| | |
|---|---|
| **GOAL:** | You will become competent across a range of device and network security tools, security tradecrafts, and practices. Vulnerability assessments will be part of this portfolio. |
| **PRODUCT:** | Portfolio |
| **FORMAT:** | Submit: Weekly from 2 to 11.<br><br>This online portfolio will include descriptions, research and supported documentation related to weekly learnings. You will be given a format to use and will be given support and feedback to ensure you are meeting this competency based assessment. This portfolio is graded and makes up 15% of total marks for the course. |
| **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 |
| 2 | Justification of selections of tools | 4 |
| 3 | Professional communication | 6 |

**All - Assessment Task 2:** Group threat scenario project

| | |
|---|---|
| **GOAL:** | You will work through a set case study of a security incident case study in a virtual group environment. You will review, investigate and outline the issues, vulnerabilities and apply appropriate methodologies. |
| **PRODUCT:** | Report |
| **FORMAT:** | This is a digital collaboration project.The product to be presented is a 3,000-word report on the analysis of a case study. |
| **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 |

**All - Assessment Task 3:** Case Study on a Security Breach – written report and oral presentation to Senior Management

| | |
|---|---|
| **GOAL:** | You will demonstrate an ability to prepare and provide an oral presentation to senior management reporting on a cyber security breach. Emphasis on this report will be a concise, accurate and informative presentation to identify and present the most valuable information the senior executives require including recommendations. |
| **PRODUCT:** | Oral and Written Piece |
| **FORMAT:** | There are two products to be submitted:<br><br>1. A presented is a video recorded presentation to senior management detailing the circumstances and consequences of a cyber security breach from the provided case study.<br><br>You will also provide recommendations on how to prevent further breaches using a variety of controls and technical measures.<br><br>2. Written report on the analysis of the case study, detailing the circumstances and consequences of a cyber security breach. You will also provide recommendations on how to prevent further breaches using a variety of controls and technical measures. |

**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 | 3 |
| 3 | Technical briefing using language suitable for senior management who may lack in-depth technical skills | 1 2 3 |
| 4 | Identification of key messages to be delivered to senior management for further security consideration | 3 |
| 5 | Provide security recommendations | 1 2 3 |
| 6 | Professional communication | 6 |

## 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. Directed study hours may vary by location. 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 Blackboard site– Please log in as soon as possible.

### 8.1. Prescribed text(s) or course reader

Please note that you need to have regular access to the resource(s) listed below. Resources may be required or recommended.

| REQUIRED? | AUTHOR | YEAR | TITLE | PUBLISHER |
|---|---|---|---|---|
| Required | Pfleeger, Pfleeger and Margulies | 2015 | Security in Computing | Pearson Australia |

### 8.2. Specific requirements

This is an online course and will require access to a computer and the internet for at least 10 hours per 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 Blackboard, are electronically checked through SafeAssign. This software allows for text comparisons to be made between your submitted assessment item and all other work that SafeAssign has access to.

## 10.2. Assessment: Additional Requirements

Your eligibility for supplementary assessment in a course is dependent of the following conditions applying:

The final mark is in the percentage range 47% to 49.4%
The course is graded using the Standard Grading scale
You have not failed an assessment task in the course due to academic misconduct.

## 10.3. Assessment: Submission penalties

Late submission of assessment tasks may be penalised at the following maximum rate:
- 5% (of the assessment task's identified value) per day for the first two days from the date identified as the due date for the assessment task.
- 10% (of the assessment task's identified value) for the third day - 20% (of the assessment task's identified value) for the fourth day and subsequent days up to and including seven days from the date identified as the due date for the assessment task.
- A result of zero is awarded for an assessment task submitted after seven days from the date identified as the due date for the assessment task. Weekdays and weekends are included in the calculation of days late. To request an extension you must contact your course coordinator to negotiate an outcome.

## 10.4. Study help

For help with course-specific advice, for example what information to include in your assessment, you should first contact your tutor, then your course coordinator, if needed.

If you require additional assistance, the Learning Advisers are trained professionals who are ready to help you develop a wide range of academic skills. Visit the Learning Advisers web page for more information, or contact Student Central for further assistance: +61 7 5430 2890 or studentcentral@usc.edu.au.

## 10.5. Wellbeing Services

Student Wellbeing provide free and confidential counselling on a wide range of personal, academic, social and psychological matters, to foster positive mental health and wellbeing for your academic success.

To book a confidential appointment go to Student Hub, email studentwellbeing@usc.edu.au or call 07 5430 1226.

## 10.6. AccessAbility Services

Ability Advisers ensure equal access to all aspects of university life. If your studies are affected by a disability, learning disorder mental health issue, , injury or illness, or you are a primary carer for someone with a disability or who is considered frail and aged, AccessAbility Services can provide access to appropriate reasonable adjustments and practical advice about the support and facilities available to you throughout the University.

To book a confidential appointment go to Student Hub, email AccessAbility@usc.edu.au or call 07 5430 2890.

## 10.7. 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
- Administration of Central Examinations
- Deferred Examinations
- Student Academic Misconduct
- Students with a Disability

Visit the USC website: http://www.usc.edu.au/explore/policies-and-procedures#academic-learning-and-teaching

## 10.8. General Enquiries

**In person:**

- **USC Sunshine Coast** - Student Central, Ground Floor, Building C, 90 Sippy Downs Drive, Sippy Downs
- **USC Moreton Bay** - Service Centre, Ground Floor, Foundation Building, Gympie Road, Petrie
- **USC SouthBank** - Student Central, Building A4 (SW1), 52 Merivale Street, South Brisbane
- **USC Gympie** - Student Central, 71 Cartwright Road, Gympie
- **USC Fraser Coast** - Student Central, Student Central, Building A, 161 Old Maryborough Rd, Hervey Bay
- **USC Caboolture** - Student Central, Level 1 Building J, Cnr Manley and Tallon Street, Caboolture

**Tel:** +61 7 5430 2890

**Email:** studentcentral@usc.edu.au