COIT13236 *Network Security Project*
Term 1 - 2017

Profile information current as at 26/04/2024 03:23 pm

General Information

Overview

This unit is a capstone to the network security specialisation of the undergraduate BIT course and is designed so that final year students can demonstrate their learning across their whole course of study before making the transition to the next stage of his/her career. Students are required to apply, synthesise and demonstrate the skills that they have developed in earlier network security specialisation units. This will be demonstrated through a group project where students are required to develop an integrated solution to real-world security problems and threats. The group project will have a designated client (or acting client). Students will be required to design and implement a security plan by meeting the real or simulated client requirements. Deliverables will include the formal security plan and configured secure infrastructure (including servers and networks), forming part of an overall portfolio of planning and design documentation, scripts and rules. In order to deliver a robust solution, students will need to choose and employ an appropriate project management methodology. The delivered infrastructure will undergo stress testing and simulated security attack scenarios.

Details

Career Level: *Undergraduate*
Unit Level: *Level 3*
Credit Points: *12*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.25*

Pre-requisites or Co-requisites

Prerequisites: (COIS13064 or COIT12208) and COIT12202 Corequisites: COIT13146 and COIT13229
Important note: Students enrolled in a subsequent unit who failed their pre-requisite unit, should drop the subsequent unit before the census date or within 10 working days of Fail grade notification. Students who do not drop the unit in this timeframe cannot later drop the unit without academic and financial liability. See details in the Assessment Policy and Procedure (Higher Education Coursework).

Offerings For Term 1 - 2017

- Brisbane
- Distance
- Melbourne
- Rockhampton
- Sydney

Attendance Requirements

All on-campus students are expected to attend scheduled classes – in some units, these classes are identified as a mandatory (pass/fail) component and attendance is compulsory. International students, on a student visa, must maintain a full time study load and meet both attendance and academic progress requirements in each study period (satisfactory attendance for International students is defined as maintaining at least an 80% attendance record).

Website

This unit has a website, within the Moodle system, which is available two weeks before the start of term. It is important that you visit your Moodle site throughout the term. Please visit Moodle for more information.

Class and Assessment Overview

Recommended Student Time Commitment

Each 12-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 25 hours of study per week, making a total of 300 hours for the unit.

Class Timetable

Regional Campuses
Bundaberg, Cairns, Emerald, Gladstone, Mackay, Rockhampton, Townsville

Metropolitan Campuses
Adelaide, Brisbane, Melbourne, Perth, Sydney

Assessment Overview

1. **Written Assessment**
Weighting: 20%
2. **Group Work**
Weighting: 80%

Assessment Grading

This is a graded unit: your overall grade will be calculated from the marks or grades for each assessment task, based on the relative weightings shown in the table above. You must obtain an overall mark for the unit of at least 50%, or an overall grade of 'pass' in order to pass the unit. If any 'pass/fail' tasks are shown in the table above they must also be completed successfully ('pass' grade). You must also meet any minimum mark requirements specified for a particular assessment task, as detailed in the 'assessment task' section (note that in some instances, the minimum mark for a task may be greater than 50%). Consult the University's Grades and Results Policy for more details of interim results and final grades.

CQUniversity Policies

All University policies are available on the CQUniversity Policy site.
You may wish to view these policies:

- Grades and Results Policy
- Assessment Policy and Procedure (Higher Education Coursework)
- Review of Grade Procedure
- Student Academic Integrity Policy and Procedure
- Monitoring Academic Progress (MAP) Policy and Procedure – Domestic Students
- Monitoring Academic Progress (MAP) Policy and Procedure – International Students
- Student Refund and Credit Balance Policy and Procedure
- Student Feedback – Compliments and Complaints Policy and Procedure
- Information and Communications Technology Acceptable Use Policy and Procedure

This list is not an exhaustive list of all University policies. The full list of University policies are available on the CQUniversity Policy site.

Previous Student Feedback

Feedback, Recommendations and Responses

Every unit is reviewed for enhancement each year. At the most recent review, the following staff and student feedback items were identified and recommendations were made.

Feedback from Student feedback and unit evaluation

Feedback
Positive comments about the unit as a real world project experience

Recommendation
Continue with the project-based learning approach

Feedback from Unit evaluation

Feedback
Provide more details in marking sheet

Recommendation
Redesign the marking guidelines including more comprehensive information

Unit Learning Outcomes

On successful completion of this unit, you will be able to:

1. Develop solutions to security problems and threats.
2. Apply the concepts taught in network security specialisation units.
3. Evaluate security protections and assess their level of compliance and effectiveness.
4. Identify “client” or employer requirements and propose solutions.
5. Apply time management, prioritisation and organisational skills in order to address real world problems.
6. Demonstrate productive participation and contribution to a project team or work environment.
7. Demonstrate technical skills, communication skills, and both professional and ethical behaviour.

Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is in use in over 100 countries and provides a widely used and consistent definition of ICT skills. SFIA is increasingly being used when developing job descriptions and role profiles.
ACS members can use the tool MySFIA to build a skills profile at
https://www.acs.org.au/professionalrecognition/mysfia-b2c.html
This unit contributes to the following workplace skills as defined by SFIA. The SFIA code is included:

- Project Management (PRMG)
- IT Management (ITMG)
- Information Security (SCTY)
- Security Administration (SCAD)
- IT Governance (GOVN)
- Technical specialism (TECH)
- IT Operations (ITOP)
- Systems Installation/Decommissioning (HSIN)
- Network Support (NTAS)
- Network Planning (NTPL)
- Network Design (NTDS)
- System Design (DESN).

Alignment of Learning Outcomes, Assessment and Graduate Attributes

N/A Level | Introductory Level | Intermediate Level | Graduate Level | Professional Level | Advanced Level

Alignment of Assessment Tasks to Learning Outcomes

Assessment Tasks	Learning Outcomes						
	1	2	3	4	5	6	7
1 - Written Assessment - 20%	•	•	•		•		•
2 - Group Work - 80%	•	•	•	•	•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes						
	1	2	3	4	5	6	7
1 - Communication				•	•	•	•
2 - Problem Solving	•	•	•	•			
3 - Critical Thinking	•	•	•	•			
4 - Information Literacy	•	•	•				
5 - Team Work					•	•	
6 - Information Technology Competence	•	•	•				•
7 - Cross Cultural Competence						•	
8 - Ethical practice	•		•			•	•
9 - Social Innovation							
10 - Aboriginal and Torres Strait Islander Cultures							

Alignment of Assessment Tasks to Graduate Attributes

Assessment Tasks	Graduate Attributes									
	1	2	3	4	5	6	7	8	9	10
1 - Written Assessment - 20%	•	•	•	•		•		•		
2 - Group Work - 80%	•			•	•	•		•		

Textbooks and Resources

Textbooks

There are no required textbooks.

Additional Textbook Information
There is no requirement for a prescribed textbook.

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)

Referencing Style

All submissions for this unit must use the referencing style: Harvard (author-date)
For further information, see the Assessment Tasks.

Teaching Contacts

Edilson Arenas Unit Coordinator
e.arenas@cqu.edu.au

Schedule

Week 1 - 06 Mar 2017

Module/Topic	Chapter	Events and Submissions/Topic
Form project groups; please see Moodle unit website for introduction to project by mentor	No specific textbooks for this unit	

Week 2 - 13 Mar 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor Project Selection		

Week 3 - 20 Mar 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in Week-1, Week-2 and Week-3

Week 4 - 27 Mar 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week 2. Submit DRAFT network security plan 3. Submit Project Plan 4. Submit Group Project Progress Report-1

Week 5 - 03 Apr 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week

Vacation Week - 10 Apr 2017

Module/Topic	Chapter	Events and Submissions/Topic
		Make entries in the Portfolio covering activities performed in this week

Week 6 - 17 Apr 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week

Week 7 - 24 Apr 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week 2. Deliver Group Presentation of the implementation of proposed network security plan 3. Submit Group Project Progress Report-2

Week 8 - 01 May 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week

Week 9 - 08 May 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week 2. Submit Group Project Progress Report-3

Week 10 - 15 May 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		Make entries in the Portfolio covering activities performed in this week

Week 11 - 22 May 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week 2. Deliver presentation of DRAFT Project Report and Technical Implementation 3. Submit Group Project Progress Report-4

Week 12 - 29 May 2017

Module/Topic	Chapter	Events and Submissions/Topic
Weekly meeting with project mentor		1. Make entries in the Portfolio covering activities performed in this week 2. Submit FINAL Project Report including Project Working Documents

Review/Exam Week - 05 Jun 2017

Module/Topic	Chapter	Events and Submissions/Topic
	This unit does not have an examination	

Exam Week - 12 Jun 2017

Module/Topic	Chapter	Events and Submissions/Topic
	This unit does not have an examination	

Term Specific Information

Dr. Edilson Arenas, Ph.D.
Discipline Leader – Networks and Information Security | School of Engineering and Technology, Higher Education Division
CQUniversity Australia, 120 Spencer Street, Melbourne, Victoria, 3000, Australia
Phone +61 03 96160570 | **Email** e.arenas@cqu.edu.au

Assessment Tasks

1 Activity journals and Periodic project progress reports

Assessment Type
Written Assessment

Task Description
This assessment comprises two different parts:

1. Activity journal
2. Periodic project progress reports

Assessment Due Date

Please refer to the unit website in Moodle for more details

Return Date to Students

Within two weeks of submission

Weighting
20%

Assessment Criteria

Individual Activity Journals (8%)

Due date: Fridays, Week 3, 6, 9 and 12

This is an individual assessment.

As part of your Portfolio and during the term unit, you are required to write and submit four activity journals (in weeks 3, 6, 9 and 12) that illustrate your individual contribution to the project and lessons learnt. This should capture everything you do, including:

1. Tasks that you performed
2. Time spent
3. How that contributed to your overall project requirements
4. Challenges faced, and
5. A bibliography of researched resource materials such as technical journals, web sites, trade magazines

It is important to maintain this document throughout the term as it is the only component of the unit assessed individually.

Please use the standard template provided in the unit website in Moodle to write and submit your activity journals.

Periodic Project Progress Reports (12%)

Due: Fridays, Week 4, 7, 9 and 11

This is a group assessment.

Each group must submit four periodic project progress reports using a standard template provided in the unit website in Moodle.

On-campus students

Each member of your group MUST give in-class presentation of each periodic project progress report (4).

Distant or Flexible students

The Unit Coordinator will provide you necessary instructions to present your group's periodic progress reports.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
via Moodle.

Learning Outcomes Assessed

- Develop solutions to security problems and threats.
- Apply the concepts taught in network security specialisation units.
- Evaluate security protections and assess their level of compliance and effectiveness.
- Apply time management, prioritisation and organisational skills in order to address real world problems.
- Demonstrate technical skills, communication skills, and both professional and ethical behaviour.

Graduate Attributes

- Communication
- Problem Solving
- Critical Thinking
- Information Literacy
- Information Technology Competence
- Ethical practice

2 Group Project and Documentation

Assessment Type
Group Work

Task Description
This is the major assessment for your project and comprises five different parts:
1. DRAFT network security plan (Week 4)
2. Project plan (Week 4)
3. Group presentation of Net Sec Plan presentation (Week 7)
4. Project report and technical implementation (Week 12)
5. Project Working Documents (Week 12)

You are required to (as a group with up to four team members) work on a project.
Note: Please contact the unit coordinator if you have genuine problem and are unable to participate in a group.

Assessment Due Date

As per unit Website in Moodle.

Return Date to Students

On certification day

Weighting
80%

Assessment Criteria
The project documentation will be assessed upon the quality of content. This includes the presentation layout and the depth and breadth of project recommendations adhering to the implementation of a secured computer network. The assessment criteria for each part of the assessment, as described in Task Description is as follows:

NOTE: Please refer to the unit website in Moodle for submission due dates and detailed marking criteria.

DRAFT network security plan (5%)

Due: Friday, Week 4

You are required to submit a DRAFT network security plan that you believe will mitigate, enhance or address the network security of the organisation (project case study).

Project plan (10%)

Due: Friday, Week 4

You are required to submit a project plan that will include: Project Charter outlining project scope, objectives and constraints, statement of work, project team members, and a RACI matrix Project Work Breakdown Structure using project GANTT Chart that also shows a timeline and allocation of tasks to team members Project risks and proposed mitigation plan

Group presentation of Network Security Pan (10%)

Due: Friday, Week 7

In this group presentation you will:

- present the summary of your network security plan that you have produced
- identify and justify your selection of key threat or security challenge to the organisation
- explain what technologies will you implement to mitigate or address such threats and challenges
- describe how you will test the security technologies what types of policy and/or procedure documents that you have intended to produce

On-campus students: The date and time of this presentation will be determined by your local lecturer/tutor.

Distant students: The time of the presentation and technology employed will be determined on an individual basis.

Presentation of DRAFT Project Report (10%)

Due: Friday Week 11

Each group must present their project in plenary session in week 11 of the term.

Each member of the group must submit their group's PowerPoint slide through the appropriate link in Moodle. Please refer to the unit website in Moodle for detailed information about the presentation session and marking criteria.

On-campus students: The date and time of this presentation will be determined by your local lecturer/tutor.

Distant students: The time of the presentation and technology employed will be determined on an individual basis.

Project working documents (5%)

Due: Friday, Week 12

This submission includes the group's important project artifacts/ documents such as DRAFT security plan produced prior to building a project plan, agendas and minutes of team meetings. This document should be included in the FINAL project report as an Annex with an appropriate title page.

Project report and technical implementation (40%)

Due: Friday, Week 12

This assessment is comprised of two different parts:

1. Produce detailed network security plan
2. Identify key security threats or challenges and implement technology to mitigate or address them.

Produce detailed network security plan

The project group is required to produce a detailed security plan for an organisation in order to meet its network security threats and challenges.

Identify key security threats or challenges and implement technology to mitigate or address them

This is a practical activity that requires demonstration of the implementation of your group's network security plan. Your group must identify key threats and challenges and implement technology to mitigate or address it. The technology has to address key challenges to the organisation's network environment. You should pick an area of network, infrastructure or security that you have already touched in your studies, but you would like to explore them in-depth and implement.

Your group needs to show how that was implemented and how the tests were carried. Your group is required to submit documentation including a test plan, test results and any network security policy and/or procedures that result from your implementation test.

Referencing Style

- Harvard (author-date)

Submission
Online Group

Submission Instructions
via Moodle

Learning Outcomes Assessed

- Develop solutions to security problems and threats.
- Apply the concepts taught in network security specialisation units.
- Evaluate security protections and assess their level of compliance and effectiveness.
- Identify "client" or employer requirements and propose solutions.
- Apply time management, prioritisation and organisational skills in order to address real world problems.
- Demonstrate productive participation and contribution to a project team or work environment.
- Demonstrate technical skills, communication skills, and both professional and ethical behaviour.

Graduate Attributes

- Communication
- Information Literacy
- Team Work
- Information Technology Competence
- Ethical practice

Academic Integrity Statement

As a CQUniversity student you are expected to act honestly in all aspects of your academic work.

Any assessable work undertaken or submitted for review or assessment must be your own work. Assessable work is any type of work you do to meet the assessment requirements in the unit, including draft work submitted for review and feedback and final work to be assessed.

When you use the ideas, words or data of others in your assessment, you must thoroughly and clearly acknowledge the source of this information by using the correct referencing style for your unit. Using others' work without proper acknowledgement may be considered a form of intellectual dishonesty.

Participating honestly, respectfully, responsibly, and fairly in your university study ensures the CQUniversity qualification you earn will be valued as a true indication of your individual academic achievement and will continue to receive the respect and recognition it deserves.

As a student, you are responsible for reading and following CQUniversity's policies, including the **Student Academic Integrity Policy and Procedure**. This policy sets out CQUniversity's expectations of you to act with integrity, examples of academic integrity breaches to avoid, the processes used to address alleged breaches of academic integrity, and potential penalties.

What is a breach of academic integrity?
A breach of academic integrity includes but is not limited to plagiarism, self-plagiarism, collusion, cheating, contract cheating, and academic misconduct. The Student Academic Integrity Policy and Procedure defines what these terms mean and gives examples.

Why is academic integrity important?
A breach of academic integrity may result in one or more penalties, including suspension or even expulsion from the University. It can also have negative implications for student visas and future enrolment at CQUniversity or elsewhere. Students who engage in contract cheating also risk being blackmailed by contract cheating services.

Where can I get assistance?
For academic advice and guidance, the Academic Learning Centre (ALC) can support you in becoming confident in completing assessments with integrity and of high standard.

What can you do to act with integrity?

Be Honest
If your assessment task is done by someone else, it would be dishonest of you to claim it as your own

Seek Help
If you are not sure about how to cite or reference in essays, reports etc, then seek help from your lecturer, the library or the Academic Learning Centre (ALC)

Produce Original Work
Originality comes from your ability to read widely, think critically, and apply your gained knowledge to address a question or problem