COIT12202 *Network Security Concepts*

Term 2 - 2023

Profile information current as at 06/05/2024 06:24 am

All details in this unit profile for COIT12202 have been officially approved by CQUniversity and represent a learning partnership between the University and you (our student). The information will not be changed unless absolutely necessary and any change will be clearly indicated by an approved correction included in the profile.

General Information

Overview

As the Internet becomes more pervasive, so do the threats to the security of our computer systems and communications. This unit provides you with grounding in security technology. You will study common network security attacks, then the technologies to defend against those attacks. These technologies include cryptography, access control, authentication, firewalls, and wireless network protocols. This unit provides security knowledge that is required for industry standard certification exams, such as CompTIA.

Details

Career Level: *Undergraduate*
Unit Level: *Level 2*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites

Prerequisite: COIT12206 OR COIT13147
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 2 - 2023

- Brisbane
- Cairns
- Melbourne
- Online
- Rockhampton
- Sydney
- Townsville

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 6-credit Undergraduate unit at CQUniversity requires an overall time commitment of an average of 12.5 hours of study per week, making a total of 150 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. **Online Quiz(zes)**
Weighting: 30%
2. **Written Assessment**
Weighting: 25%
3. **Written Assessment**
Weighting: 45%

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 Teaching staff and discipline team feedback

Feedback

Advanced security practices or exercises can be included as emerging topics in this unit, such as wireless, IoT applications, and cloud cybersecurity.

Recommendation

Update the teaching materials with advanced cybersecurity practices and exercises, such as wireless, IoT applications, and cloud cybersecurity.

Feedback from Students and teaching team feedback

Feedback

Python/(Power)Shell scripting can be introduced for cybersecurity practices/exercises.

Recommendation

Design some practices or lab exercises based on the Python/(Power)Shell scripting to enhance students' understanding of how to use the scripting technologies to perform cybersecurity practices.

Unit Learning Outcomes

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

1. Describe key security concepts and principles
2. Discuss how common security attacks and defences work
3. Explain the role of cryptographic mechanisms in providing computer and network security
4. Apply access control technologies, including firewalls and authentication, to secure computer networks
5. Explain threats and defences that are specific to wireless networks.

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:

- Information Security (SCTY)
- Penetration Testing (PENT)
- Network Support (NTAS)
- Security Administration (SCAD)
- Problem Management (PBMG)
- Data Analysis (DTAN)
- System Design (DESN)
- Incident Management (USUP)

The National Initiative for Cybersecurity Education (NICE) Framework defines knowledge, skills and tasks needed to perform various cyber security roles. Developed by the National Institute of Standards and Technology (NIST), the NICE Framework is used by organisations to plan their workforce, including recruit into cyber security positions.
This unit helps prepare you for roles such as Systems Security Analyst, Network Operations Specialist and Systems Administrator, contributing to the following knowledge and skills:

- K0002 Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
- K0003 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004 Knowledge of cybersecurity and privacy principles.
- K0019 Knowledge of cryptography and cryptographic key management concepts
- K0038 Knowledge of cybersecurity and privacy principles used to manage risks related to the use, processing, storage, and transmission of information or data.
- K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized

zones, encryption).

- K0056 Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
- K0075 Knowledge of security system design tools, methods, and techniques.
- K0104 Knowledge of Virtual Private Network (VPN) security.
- K0158 Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).
- K0160 Knowledge of the common attack vectors on the network layer.
- K0179 Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- K0203 Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
- K0260 Knowledge of Personally Identifiable Information (PII) data security standards.
- K0261 Knowledge of Payment Card Industry (PCI) data security standards.
- K0262 Knowledge of Personal Health Information (PHI) data security standards.
- K0263 Knowledge of information technology (IT) risk management policies, requirements, and procedures.
- K0274 Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.
- K0276 Knowledge of security management.
- K0284 Knowledge of developing and applying user credential management system.
- K0297 Knowledge of countermeasure design for identified security risks.
- K0333 Knowledge of network design processes, to include understanding of security objectives, operational objectives, and trade-offs.
- S0027 Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
- S0031 Skill in developing and applying security system access controls.
- S0036 Skill in evaluating the adequacy of security designs.
- S0040 Skill in implementing, maintaining, and improving established network security practices.
- S0076 Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, antivirus software, anti-spyware).
- S0077 Skill in securing network communications.
- S0079 Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters).
- S0084 Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).
- S0141 Skill in assessing security systems designs.
- S0147 Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
- S0167 Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
- S0170 Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).
- S0367 Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

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
1 - Written Assessment - 25%	•	•	•		
2 - Written Assessment - 45%				•	•
3 - Online Quiz(zes) - 30%	•	•	•	•	•

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes				
	1	2	3	4	5
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					

Textbooks and Resources

Textbooks

COIT12202

Prescribed

CompTIA security+ guide to network security fundamentals
Edition: 7th (2022)
Authors: Ciampa, Mark
Cengage
Boston , Massachusetts , USA
ISBN: 978-0-357-42437-9
Binding: Paperback

View textbooks at the CQUniversity Bookshop

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- Cisco Packet Tracer
- Python 3.7 or higher
- ACS virtual machine

Referencing Style

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

Teaching Contacts

Zhenglin Wang Unit Coordinator
z.wang@cqu.edu.au

Schedule

Week 1 - 10 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Introduction to Security	Module 1: Introduction to Security	

Week 2 - 17 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Threats and Attacks	Module 3: Threats and Attacks on Endpoints	

Week 3 - 24 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Basic Cryptography	Module 6: Basic Cryptography	

Week 4 - 31 Jul 2023

Module/Topic	Chapter	Events and Submissions/Topic
Public Key Infrastructure and Cryptographic Protocols	Module 7: Public Key Infrastructure and Cryptographic Protocols	

Week 5 - 07 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Networking Threats, Assessments, and Defenses	Module 8: Networking Threats, Assessments, and Defenses	**Assessment 1 Quiz One and Two** Due: Week 5 Friday (11 Aug 2023) 11:45 pm AEST

Vacation Week - 14 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic

Week 6 - 21 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Network Security Appliances and Technology	Module 9: Network Security Appliances and Technologies	**Assessment 2 - Written Assessment** Due: Week 6 Friday (25 Aug 2023) 11:55 pm AEST

Week 7 - 28 Aug 2023

Module/Topic	Chapter	Events and Submissions/Topic
Secure Network Management and Development	Module 2: Threat Management and Cybersecurity Resources Module 4: Endpoint and Application Development	

Week 8 - 04 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Cloud and Virtualization Security	Module 10: Cloud and Virtualization Security	

Week 9 - 11 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Authentication	Module 12: Authentication	

Week 10 - 18 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Wireless Network Security	Module 11: Wireless Network Security	

Week 11 - 25 Sep 2023

Module/Topic	Chapter	Events and Submissions/Topic
Mobile and Embedded Device Security	Module 5: Mobile, Embedded, and Specialized Device Security	

Week 12 - 02 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
Summary of the Unit and Case Study	N/A	

Review/Exam Week - 09 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic
		Assessment 3 - Case Study Due: Review/Exam Week Monday (9 Oct 2023) 11:45 pm AEST

Exam Week - 16 Oct 2023

Module/Topic	Chapter	Events and Submissions/Topic

Term Specific Information

Unit coordinator is Dr. Zhenglin Wang (z.wang@cqu.edu.au). Contact best by email or in Microsoft Teams (see link in Moodle under "Microsoft").

Assessment Tasks

1 Assessment 1 Quiz One and Two

Assessment Type
Online Quiz(zes)

Task Description
There will be two online quizzes, Quiz 1 and Quiz 2, each consisting of a series of True/False, Multiple Choice, and Analytical questions. The questions will be randomly selected from a pool of topics covered in weeks 1 to 4 for Quiz 1 and weeks 5 to 10 for Quiz 2. Please note that the questions asked will differ from those given to other students and in subsequent attempts at the quiz. You will have a 1-hour time limit for each attempt. Please submit your attempt before the due date, as the quiz will automatically close and a zero mark will be recorded for incomplete submissions. You can attempt each quiz up to two times, with the higher score being recorded as your final score. We encourage you to utilize the opportunity to take the quiz twice to achieve your best possible scores.

Number of Quizzes
2

Frequency of Quizzes

Assessment Due Date
Week 5 Friday (11 Aug 2023) 11:45 pm AEST

Return Date to Students
Week 7 Friday (1 Sept 2023)

Weighting
30%

Assessment Criteria
Quiz questions will be graded automatically.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Describe key security concepts and principles
- Discuss how common security attacks and defences work
- Explain the role of cryptographic mechanisms in providing computer and network security
- Apply access control technologies, including firewalls and authentication, to secure computer networks
- Explain threats and defences that are specific to wireless networks.

2 Assessment 2 - Written Assessment

Assessment Type
Written Assessment

Task Description
The written assignment consists of five questions and is designed to assess students' understanding of the material covered from Week 1 to Week 5. To successfully complete the assignment, students are expected to refer to the teaching materials and utilize online resources independently.

Assessment Due Date
Week 6 Friday (25 Aug 2023) 11:55 pm AEST

Return Date to Students
Week 8 Friday (8 Sept 2023)

Weighting
25%

Assessment Criteria
Reference solutions are available for the written assignment. Students' answers should convey similar ideas and include key words to demonstrate their understanding.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Describe key security concepts and principles
- Discuss how common security attacks and defences work
- Explain the role of cryptographic mechanisms in providing computer and network security

3 Assessment 3 - Case Study

Assessment Type
Written Assessment

Task Description
This is an individual assessment. In this assessment task, you will analyse a scenario given in this assessment item, and develop and produce a written report on the given tasks. You are required to present a topic about network security in the provided scenario. This assessment includes two parts as follows:
Part A: You will draft a report for the provided scenario with the given tasks. The written report is due on Monday, week 13.
Part B: There will be a presentation on a topic about network security you are interested in. Presentation slides and a recorded video of the presentation are due on Monday, week 13.

Assessment Due Date
Review/Exam Week Monday (9 Oct 2023) 11:45 pm AEST

Return Date to Students
Exam Week Friday (20 Oct 2023)

Weighting
45%

Assessment Criteria
The assessment criteria have been provided in the assignment specification.

Referencing Style

- Harvard (author-date)

Submission
Online

Learning Outcomes Assessed

- Apply access control technologies, including firewalls and authentication, to secure computer networks
- Explain threats and defences that are specific to wireless networks.

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