In Progress

Please note that this Unit Profile is still in progress. The content below is subject to change.

COIT11241 *Cyber Security Technologies*

Term 2 - 2024

Profile information current as at 17/05/2024 04:47 pm

All details in this unit profile for COIT11241 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

Cyber security professionals need to create, analyse and test computer systems and networks to assure they will operate in the presence of attacks. In this unit, you will learn the types of attacks that may be encountered and the tools and techniques to prevent, detect and respond to those attacks. You will build your skills in virtualisation, cloud services and scripting to solve cyber security challenges. You will also learn special cyber security tools for detecting vulnerabilities, monitoring network traffic and responding to attacks.

Details

Career Level: *Undergraduate*
Unit Level: *Level 1*
Credit Points: *6*
Student Contribution Band: *8*
Fraction of Full-Time Student Load: *0.125*

Pre-requisites or Co-requisites

Pre-Requisites: COIT11238 Networked Infrastructure Foundations AND COIT11222 Programming Fundamentals.
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 - 2024

- Brisbane
- Cairns
- Melbourne
- Online
- 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 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

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 Evaluations and Teaching Team Reflections

Feedback
The unit requirements are unclear.

Recommendation
More detailed steps will be included in the assessments and tutorial exercises will be created to help students understand the assessment requirements.

Feedback from Teaching Team Reflections

Feedback
The unit covers too many topics.

Recommendation
The topics covered by the unit will be reduced. For example, advanced topics such as Metasploit will be removed.

Feedback from Teaching Team Reflections

Feedback
Windows virtual machines and Wazuh are difficult to use on computers with less than 16Gbytes of RAM and 30Gbytes of free hard drive space.

Recommendation
Additional information about the hardware requirements for a machine that can handle simultaneous virtual machines will be added to the eUnit profile and unit materials. Troubleshooting support will also be added to the tutorials.

Feedback from Student Evaluations and Teaching Team Reflections

Feedback
Students appreciate learning real world skills.

Recommendation
Continue to cover tools such as Kali, Wazuh, and Windows controls and attacks.

Unit Learning Outcomes

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

1. Explain cyber security challenges and the technologies available to address those challenges
2. Apply cyber security tools to identify vulnerabilities and protect computer systems
3. Apply cloud services tools to automate common IT processes and task.

The Australian Computer Society (ACS) recognises the Skills Framework for the Information Age (SFIA). SFIA is adopted by organisations, governments and individuals in many 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.
This unit contributes to the following workplace skills as defined by SFIA 7 (the SFIA code is included)

- Information security (SCTY)
- Programming/software development (PROG)
- Security administration (SCAD)
- Penetration testing (PENT)

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:

- K0003 Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
- K0004 Knowledge of cybersecurity and privacy principles.
- K0005 Knowledge of cyber threats and vulnerabilities.
- K0006 Knowledge of specific operational impacts of cybersecurity lapses.
- K0040 Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
- K0044 Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- K0071 Knowledge of remote access technology concepts.
- K0075 Knowledge of security system design tools, methods, and techniques.
- K0130 Knowledge of virtualization technologies and virtual machine development and maintenance.
- K0135 Knowledge of web filtering technologies.
- K0160 Knowledge of the common attack vectors on the network layer.
- 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.
- K0290 Knowledge of systems security testing and evaluation methods.
- K0297 Knowledge of countermeasure design for identified security risks.
- K0318 Knowledge of operating system command-line tools.
- K0339 Knowledge of how to use network analysis tools to identify vulnerabilities.
- S0031 Skill in developing and applying security system access controls.
- S0060 Skill in writing code in a currently supported programming language (e.g., Java, C++).
- S0073 Skill in using virtual machines. (e.g., Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.).
- S0154 Skill in installing system and component upgrades. (i.e., servers, appliances, network devices).
- S0167 Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).

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
1 - Online Quiz(zes) - 30%		•	•
2 - Portfolio - 50%		•	•
3 - Presentation - 20%	•		

Alignment of Graduate Attributes to Learning Outcomes

Graduate Attributes	Learning Outcomes		
	1	2	3
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

Information for Textbooks and Resources has not been released yet.

This information will be available on Monday 17 June 2024

Academic Integrity Statement

Information for Academic Integrity Statement has not been released yet.

This unit profile has not yet been finalised.