COIT11241 *Cyber Security Technologies*
Term 2 - 2024

Profile information current as at 29/07/2024 05:47 pm

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

1. **Online Quiz(zes)**
Weighting: 30%
2. **Portfolio**
Weighting: 50%
3. **Presentation**
Weighting: 20%

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

Textbooks

There are no required textbooks.

IT Resources

You will need access to the following IT resources:

- CQUniversity Student Email
- Internet
- Unit Website (Moodle)
- VirtualBox image (provided on Moodle)
- Suitable storage media, such as a removable USB 3.0 stick (≥128GB) for oncampus students without a laptop or as a fallback if you do not have enough harddrive space free
- Virtualbox (Version 7 or later)
- A computer with hardware resources suitable to run multiple virtual machines simultaneously, e.g. 12GB RAM, 128GB HDD free, Intel core i5 or above, Windows 7 or later.

Referencing Style

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

Teaching Contacts

Jamie Shield Unit Coordinator
j.shield@cqu.edu.au

Schedule

Week 1 - 08 Jul 2024

Module/Topic	Chapter	Events and Submissions/Topic
1 Systems approach to Cybersecurity	Refer to the unit website for the readings. Chapter 6 of Hassell, J 2017, *Learning PowerShell,* Boston, DeG Press.	You must make at least four weekly contributions to a private Git repository prior to the due date for A2 Portfolio: Attacks (50%)

Week 2 - 15 Jul 2024

Module/Topic	Chapter	Events and Submissions/Topic
2 Prioritising Controls	CIS Controls	You must attend the Week 2 tutorial: refer to Assignment 3 for details

Week 3 - 22 Jul 2024

Module/Topic	Chapter	Events and Submissions/Topic
3 Cyber Threat Intelligence	Chapter 3 of Thompson, E 2020, *Designing a HIPAA-Compliant Security Operations Center*, Apress L. P, Berkeley, CA.	• A1 Quiz 1 (6%) due Week 3 • A3 Presentation: Group demo (5%) You must attend the Week 3 tutorial.

Week 4 - 29 Jul 2024

Module/Topic	Chapter	Events and Submissions/Topic
4 Prioritising Vulnerabilities	Chapter 4 of (Thompson 2020)	

Week 5 - 05 Aug 2024

Module/Topic	Chapter	Events and Submissions/Topic
5 Monitoring for attacks	Chapter 5 of (Thompson 2020)	

Vacation Week - 12 Aug 2024

Module/Topic	Chapter	Events and Submissions/Topic
No classes		

Week 6 - 19 Aug 2024

Module/Topic	Chapter	Events and Submissions/Topic
6 Cybersecurity Attacks	Chapter 1 of Bijalwan, A 2021, *Network Forensics*, CRC Press.	Commit to private A2 Git repository.

Week 7 - 26 Aug 2024

Module/Topic	Chapter	Events and Submissions/Topic
7 Linux and Bash Scripting	Chapters 6, 9, 10, 16, 17, 19, 20, 26-29 and 33 of Shotts 2019, *The Linux Command Line*.	• A1 Quiz 2 Networking (9%) • Commit to private A2 Git repository.

Week 8 - 02 Sep 2024

Module/Topic	Chapter	Events and Submissions/Topic
8 Cybersecurity Architectures	Chapter 3 of Garbis, J & Chapman, J 2021. *Zero Trust Security*, Apress.	Commit to private A2 Git repository.

Week 9 - 09 Sep 2024

Module/Topic	Chapter	Events and Submissions/Topic
9 Cloud Foundations	Chapter 1 of Collier, M & Shahan, R 2016, *Foundations of Azure*, 2nd edn, Microsoft.	**Portfolio** Due: Week 9 Friday (13 Sept 2024) 11:59 pm AEST

Week 10 - 16 Sep 2024

Module/Topic	Chapter	Events and Submissions/Topic
10 Python Scripting	Chapters 2-11 of Severance, C 2016, *Python for Everybody*.	

Week 11 - 23 Sep 2024

Module/Topic	Chapter	Events and Submissions/Topic
11 Presentations (tutorial only)		A3 Presentation: Final (15%). You must present live in class for full marks. A recording is permitted but you will not be able to achieve full marks.

Week 12 - 30 Sep 2024

Module/Topic	Chapter	Events and Submissions/Topic
No classes		A1 Quiz 3: Review (15%)

Term Specific Information

Unit Coordinator: Jamie Shield, j.shield@cqu.edu.au, Cairns
You must make contributions to a private Git repository prior to the due date for A2 Portfolio: Attacks (50%).
You must attend the Week 2 and 3 tutorials or, on your own initiative, work in a group outside of the tutorials to complete the A3 Presentation: Group Demo which is due in the Week 3 tutorial.
You must present live in class during your Week 11 tutorial to be eligible for full marks for Assignment 3.

Assessment Tasks

1 Quizzes

Assessment Type
Online Quiz(zes)

Task Description
There are three quizzes. You will be assessed on background concepts in cybersecurity, networking, ICT and computer security technologies, offensive types of cybersecurity technologies, and applying defensive cybersecurity technologies. The quizzes will involve short answer questions and activities such as writing shell commands and using cybersecurity tools. You may attempt the quizzes as many times as you like until the due date.

Number of Quizzes
3

Frequency of Quizzes
Other

Assessment Due Date

Weeks 3, 7 and 12.

Return Date to Students

Immediate feedback

Weighting
30%

Assessment Criteria
This assessment consists of short answer questions and small activities such as the use of PowerShell, Bash and Python commands for scripting, network defense, monitoring and attacks. Each question will be marked according to the correctness of the answer, for example, successful use of commands to start a SYN flood attack.

- Quiz 1: PowerShell and Virtualisation (6%)
- Quiz 2: Networking (9%)
- Quiz 3: Review (15%)

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Complete the quizzes on the unit website.

Learning Outcomes Assessed

- Apply cyber security tools to identify vulnerabilities and protect computer systems
- Apply cloud services tools to automate common IT processes and task.

2 Portfolio

Assessment Type
Portfolio

Task Description
You will create a portfolio to demonstrate that you can apply malicious and defensive cybersecurity technologies such as file integrity monitors and network scanners. You will be provided with an information system such as a small organisation's network. To prepare the organisation's information system to survive an imminent attack from a known Threat Actor (TA), you will:

- Search the information system for vulnerabilities
- Analyse Cyber Threat Intelligence (CTI) and prioritise vulnerabilities
- Implement defenses
- Develop and run attacks like those used by the TA
- Detect the attacks

Groupwork
You may work alone or in groups of 2 or 3 people for this assignment and for your final Assignment 3 presentation. All group members must be identified in the groupwork artefacts. Evidence must be provided that all group members contributed adequately to the final submissions. All group members must submit via the unit website. The moderation process might allocate group members different marks. Sharing of artefacts, for example, code or virtual machines, between groups is not permitted.
Repository
Create a private code repository and invite your tutor and the unit coordinator. One code repository is to be used by all group members. You must make at least four weekly contributions to a private Git repository prior to the due date for A2 Portfolio: Attacks (50%).

Assessment Due Date
Week 9 Friday (13 Sept 2024) 11:59 pm AEST

Return Date to Students

Feedback will be provided within 2 weeks of the due date.

Weighting
50%

Assessment Criteria
The following is a summary of the assessment criteria. The criteria have equal weighting. Refer to the unit website for more details.

Vulnerability search	Excellent use of tools. Excellent search scope. Teamwork, e.g. excellent individual contributions, communication & team management. Process, e.g. 4 weekly Git commits.
CTI	Excellent lifecycle summary. Excellent prioritisation of threats & vulns including ATT&CK TTPs, CAPECs, CWEs & CVEs. Excellent references, e.g. trustworthy. Teamwork. Process, e.g. 4 weekly Git commits.
Defences	Installation and testing of defences are scripted. Pre- and Post-tests demonstrate effect of safeguards. Teamwork. Process, e.g. 4 weekly Git commits.
Attacks	Resembles actual attack code. Attacks are scripted. Correct categorisation of ATT&CK codes for attacks. Code consistent, reasonable layout. Functions documented appropriately. Git commits showing script & function development. Teamwork. Process, e.g. 4 weekly Git commits.
Detections	Excellent detections or preventions, e.g. not too specific yet not noisy. Excellent testing of detections showing alerts & preventions showing difference in attack behaviour. Code consistent, reasonable layout. Functions documented appropriately. Git commits showing script & function development. Teamwork. Process, e.g. 4 weekly Git commits.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
Submit artefacts to both a private code repository and to the unit website. Submit a link to your private repository to the unit website. All group members must submit.

Learning Outcomes Assessed

- Apply cyber security tools to identify vulnerabilities and protect computer systems
- Apply cloud services tools to automate common IT processes and task.

3 Presentations

Assessment Type
Presentation

Task Description
In this assignment you will provide two demonstrations:

- Group demonstration: you will be assigned a cybersecurity technology which, in a small group, you will need to investigate and demonstrate. You must attend the Week 2 and 3 tutorials and/or, on your own initiative, work in a group outside of the tutorials to complete this task.
- Final presentation: You will demonstrate, live, the Information System (IS) you prepared in Assignment 2. You will

run live tests to demonstrate the defensive cybersecurity technologies have been successfully implemented on the system. You will run live attacks on the system and demonstrate the detection, mitigation or protections in action. You will demonstrate that the system is now more resilient against the adversary. You may complete this task alone or in a small group. You must present live in class during your Week 11 tutorial to be eligible for full marks for this task.

Groupwork
You must complete the Group demonstration task in groups of 2 or 3 people. Groups will be formed in the Week 2 tutorial. If you do not attend the Weeks 2 and 3 tutorials, you must form your own group, for example, using the forums on the unit website. You may work alone or in groups of 2 or 3 people for the rest of this assignment, that is, for your Final Presentation. All group members must be identified in the groupwork artefacts. All group members must submit via the unit website. Group members are marked individually on presentation criteria.

Assessment Due Date

The Group demonstration task is due in Week 3. Your Final Presentations are due in your Week 11 tutorial. PowerPoint slideshow (and video if you do not present in class) are due at the end of Week 11.

Return Date to Students

Feedback for the Group Demonstration will be returned within two weeks of the due date. Feedback for the Final Presentation will be returned on the Certification of Grades day.

Weighting
20%

Assessment Criteria
The following is a summary of the assessment criteria. The criteria have equal weighting. Refer to the unit website for more details.

Group demonstration	Excellent use of tools. Excellent explanation. Introduces themselves; well prepared, e.g. does not read; clear voice; good eye contact; appropriate timing & pace; includes gestures that support the message; engages audience.
Final demonstration	
Demonstrations of, e.g. controls, attacks & detections	Presents in-class. Excellent evidence controls have been implemented well. Excellent use of tools.
Stage presence	Presents in-class. Introduces themselves; well prepared, e.g. does not read; clear voice; good eye contact; appropriate timing & pace; includes gestures that support the message; engages audience.
Slideshow framing	Includes title, summary & reference slides; uses point form; slide numbers & footers; efficient transitions; large fonts; consistent, excellent theme, e.g. good contrast; only relevant images; free from mechanical, grammatical & spelling errors.

Referencing Style

- Harvard (author-date)

Submission
Online

Submission Instructions
For the group demonstration: you can either present live in your Week 3 tutorial or you can submit a video to the unit website. For your final presentation: submit your PowerPoint slideshow to the unit website. If you do not present in class, you should also submit a video of your presentation. You will not receive full marks if you do not present in-class. Submissions need to be less than 100Mb.

Learning Outcomes Assessed

- Explain cyber security challenges and the technologies available to address those challenges

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