COMP8310

Security Technologies and Forensic Analysis

Session 1, In person-scheduled-weekday, North Ryde 2024

School of Computing

Contents

General Information

Unit convenor and teaching staff
Milton Baar
milton.baar@mq.edu.au

Credit points
10

Prerequisites
ITEC647 or COMP6250

Corequisites

Co-badged status

Unit description
This unit covers the fundamental technologies and processes that form the foundation of effective systems security management within modern organisations. We consider the underlying mechanics of information and communications technology security infrastructures, risk management, attack modelling, software security, firewalls, intrusion detection and forensics.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

ULO1: Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

ULO2: Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.

ULO3: Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.

ULO4: Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.

ULO5: Present and discuss concepts related to software and network security at an advanced level.

General Assessment Information

General Faculty Policy on assessment submission deadlines and late submissions:

To pass this unit you must achieve a total mark of at least 50%.

Online quizzes, in-class activities, or scheduled tests and exam must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure, students may apply for Special Consideration.

All other assessments must be submitted by 2355 on their due date.

Should these assessments be missed due to illness or misadventure, students should apply for Special Consideration.

Assessments not submitted by the due date will receive a mark of zero **unless** late submissions are specifically allowed as indicated in the unit guide or on iLearn.

Late submissions are **NOT** permitted.

Quiz 1

Assessment Type [1]: Quiz/Test Indicative Time on Task [2]: 2 hours Due: **Week 4** Weighting: **5%**

This quiz will be based on your previously covered lecture material for weeks 1-3. The quiz questions will be online multiple choice. Quiz will serve as a feedback mechanism to monitor your progress in the unit and there will be a discussion on the solutions when all students have completed the quiz. The allowed time for completion is intentionally short so that you must answer with your own retained information; your answers must be your own original information and not copied from somewhere else.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

Quiz 2

Assessment Type [1]: Quiz/Test Indicative Time on Task [2]: 3 hours Due: **Week 9** Weighting: **5%**

This quiz will be based on your previously covered lecture material for weeks 4-8. The quiz questions will be short answer. Quiz will serve as a feedback mechanism to monitor your progress in the unit and there will be a discussion on the solutions when all students have completed the quiz. The allowed time for completion is intentionally short so that you must answer with your own retained information; your answers must be your own original information and not copied from somewhere else.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

Group Project

Assessment Type [1]: Project Indicative Time on Task [2]: 15 hours Due: **Week 11 & Week 12** Weighting: **30%**

Presentations are held in weeks 11 & 12 but content due by mid semester. Group project with up to 6 students per group. Projects will be related to security and forensics issues with emerging technologies such as smart grid and cloud. Each group will be allocated a time slot for presenting their work during Week 11 OR Week 12. Each student in the group is expected to present their work which will be followed by QA session. The QA session will be conducted by the panel (which includes convener and/or other staff members and/or PhD students within the computing department). The presentation and QA session will help the panel to evaluate the individual contribution of each student. The Project will account to 30% (Report-10%, Presentation-10% and QA-10%) of the unit marks.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.
- Present and discuss concepts related to software and network security at an advanced level.

Practical activities report

Assessment Type [1]: Report Indicative Time on Task [2]: 10 hours Due: **Week 07 (initial review and award of up to 10%) and Week 13 (final review and award of up to 10%)** Weighting: **20%** During the unit, there will be practical activities relating to security technologies and forensics.

On successful completion you will be able to:

- Analyse techniques for exploiting software and networks. Investigate operating system

and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.

Final Examination

Assessment Type [1]: Examination Indicative Time on Task [2]: 20 hours Due: **Exam period S1** Weighting: **40%** The exam will be a written exam with questions from topics covered in the lectures. It will be held in the usual examination period of the semester.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Present and discuss concepts related to software and network security at an advanced level.

Methods of Communication

Our primary means of communication will be through your university email and announcements on iLearn. It is crucial to consistently check your university email for important updates and information related to the course. Additionally, significant announcements will be posted on iLearn, a centralized platform for accessing vital details about the course. Should you have any queries or require assistance from the teaching staff, including the unit convenor, you have two communication channels. Firstly, you can post your queries on the iLearn discussion board, providing an interactive space for instructors and peers to engage in discussions. Alternatively, you may send emails to the corresponding addresses of the teaching staff using your university email address for official communication. Through these communication methods, we aim to ensure effective and timely dissemination of information and provide the necessary support throughout the course.

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment

task and is subject to individual variation

Assessment Tasks

Name	Weighting	Hurdle	Due
Quizzes	10%	No	Weeks 4 & 9
Practical activities report	30%	No	Weeks 7 & 12
Final Examination	40%	Yes	During the Exam Period
Group Project	20%	No	Weeks 11 & 12

Quizzes

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 5 hours
Due: **Weeks 4 & 9**
Weighting: **10%**

Quizzes will be based on your previously covered lecture material.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.

Practical activities report

Assessment Type [1]: Report
Indicative Time on Task [2]: 10 hours
Due: **Weeks 7 & 12**
Weighting: **30%**

During the unit, there will be practical activities relating to security technologies and forensics.

On successful completion you will be able to:

- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.

- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.

Final Examination

Assessment Type [1]: Examination
Indicative Time on Task [2]: 20 hours
Due: **During the Exam Period**
Weighting: **40%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

The exam will be a written exam with questions from topics covered in the lectures. It will be held in the usual examination period of the semester.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Present and discuss concepts related to software and network security at an advanced level.

Group Project

Assessment Type [1]: Project
Indicative Time on Task [2]: 15 hours
Due: **Weeks 11 & 12**
Weighting: **20%**

Group project with 3-4 students per group. Projects will be related to security and forensics issues with emerging technologies such as smart grid and cloud.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- Analyse techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Design and/or apply security techniques to mitigate software and network attacks. Identification of tools and recovery mechanisms, including forensic analysis and process.
- Evaluate security techniques used to deal with the attacks and the limitations of forensic tools.
- Present and discuss concepts related to software and network security at an advanced level.

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

- Lectures are held weekly and are two-hours long; a video of the lecture is automatically captured and will be available on iLearn/Echo360. Lecture slides will be published on iLearn **after** the completion of the lecture.
- Immediately following the lecture, there is a one-hour general consultation period where discussions and questions will be covered in an informal setting, such as an open lounge area near the lecture theatre or in a small Active Learning area.
- All reading and viewing material for both background and to support learning outcomes is provided on iLearn and external information is listed in the lecture material.
- Practical activities are designed to be undertaken off-campus at a time and location suitable to the indivudual student.
- Students must use their own computer equipment to undertake the practical activities, a PC or Mac or Linux system is required as the practical activities cannot be undertaken on a phone or tablet.

- Students **MUST** purchase and use a specific type of workbook that will be described in Week 1; **ONLY** an appropriate workbook will satisfy the requirements of the Week 13 workbook deliverable.

Unit Schedule

Week	Topic	Practical activity
1	Introduction	No week 1 practical activity
2	Risk management frameworks	Practical activity systems setup
3	Operating System vulnerabilities	Forensic tools part 1
4	Practice and Procedure	Quiz 1
5	Introduction to Digital Evidence and Computer Crime	Forensic tools part 2
6	Introduction to file systems/Windows file systems	Forensic management tools
7	Linux file systems	Forensic tools part 3
8	“Big End of Town” file systems	Quiz 2
9	Introduction to Steganography	Forensic tools part 3 and disk/data identification
10	Introduction to Cryptography	Practical report writing
11	Group project presentation	
12	Group project presentation	
13	Review	

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure

- Assessment Procedure
- Complaints Resolution Procedure for Students and Members of the Public
- Special Consideration Policy

Students seeking more policy resources can visit Student Policies (https://students.mq.edu.au/support/study/policies). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au or if you are a Global MBA student contact globalmba.support@mq.edu.au

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

The Writing Centre

The Writing Centre provides resources to develop your English language proficiency, academic writing, and communication skills.

- Workshops
- Chat with a WriteWISE peer writing leader
- Access StudyWISE
- Upload an assignment to Studiosity
- Complete the Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and processes

Student Enquiries

Got a question? Ask us via AskMQ, or contact Service Connect.

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Unit information based on version 2024.03 of the Handbook