COMP8310

Security Technologies and Forensic Analysis

Session 1, Special circumstances 2021

School of Computing

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and other small group activities on campus, and most will keep an online version available to those students unable to return or those who choose to continue their studies online.

To check the availability of face-to-face activities for your unit, please go to timetable viewer. To check detailed information on unit assessments visit your unit's iLearn space or consult your unit convenor.

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 underpin good 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:

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

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

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

For the Group Project and Practical Activities Report (Hurdle task), no extensions will be granted without an approved application for Special Consideration. There will be a deduction of 10% of the total available marks made from the total awarded mark for each 24 hour period or part thereof that the submission is late. For example, 25 hours late in submission for an assignment worth 10 marks – 20% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Assessment Tasks

Name	Weighting	Hurdle	Due
Quiz 1	5%	No	Week 5
Quiz 2	5%	No	Week 9
Group Project	30%	No	Week 10
Practical activities report	20%	Yes	Week 11
Final Examination	40%	Yes	Exam period

Quiz 1

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

This quiz will be based on your previously covered lecture material for weeks 1-4. 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 5-8. 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 10**
Weighting: **30%**

Presentations are held in weeks 11 & 12 but content due by mid semester. 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. 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 techniques for exploiting software and networks. Investigate operating system

and file system platforms and identify attack surface.
- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- 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 11**
Weighting: **20%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

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**
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 techniques for exploiting software and networks. Investigate operating system and file system platforms and identify attack surface.
- Analyse the key security requirements and trends in software security and interconnected systems. Identify key threats and analysis tools to evaluate security deficiencies.
- 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.

---

[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

COMP8310 is a very deeply technical unit that goes into the details of operating systems and file/disk/hardware structures. If you don't have good skills in these areas, large volumes of reading and videos are provided. It is up to each student to add to their knowledge using the material available as the assumed knowledge will not be taught in the weekly lectures/practicals.

- Practical activities form an important component
- The unit design requires that you undertake all practical activities and exercises outside teaching time
- Considerable optional reading and viewing provided for each week
- You will need your own technology on which you can run a VM and download and use files from iLearn
- **The technology required is vendor neutral, you can use Windows, Linux or MacOS based devices, but you cannot successfully complete the tasks using tablet or phone devices alone**

Prerequisite knowledge includes:

- Ability to read binary, octal and hexadecimal
- Understanding file system and operating system fundamentals
- Understanding networking concepts (TCP/IP etc.)
- Programming skills

None of these will be taught, if you don't know them now, learn them quickly!

No formal texts, but the following can be useful:

- Brian Carrier, File System Forensic Analysis, ISBN: 0321268172, Addison Wesley
- Harlan Carvey, Windows Forensics and Incident Recovery, ISBN 0321200985, Addison Wesley
- D. Comer, Computer Networks and Internet, Prentice Hall.
- D. Comer, Internetworking with TCP/IP Volume One
- A.S. Tanenbaum, Computer Networks, Prentice Hall, Pearson Education
- W. Stallings, Business Data Communications, Prentice Hall

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
- Grade Appeal Policy
- Complaint Management 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

Student Support

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

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- 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

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

If you are a Global MBA student contact globalmba.support@mq.edu.au

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.