ITEC855

Security Technologies and Forensic Analysis

S1 Evening 2019

Dept of Computing

Contents

General Information

Unit convenor and teaching staff
Milton Baar
milton.baar@mq.edu.au
Contact via 04 1927 9847

Credit points
4

Prerequisites
COMP343 or ITEC647 or admission to MCyberSec with a specialisation in Internetworking

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://students.mq.edu.au/important-dates

Learning Outcomes

On successful completion of this unit, 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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.
Present and discuss concepts related to software and network security at a postgraduate

level. Create a body of work for assessment that demonstrates understanding of theoretical and practical aspects of unit content.

General Assessment Information

Hurdle assessments:

- Students must achieve at least 20/40 in the final exam to be eligible to pass the unit.
- A second attempt will be provided for students that achieve a mark in the band 15/40 to 19.9/40 in the final exam.
- Students must achieve at least 15/20 in the practical lab reports to be eligible to pass the unit.
- An additional practical assessment task will be provided for students that achieve a mark in the band 10/20 to 14.9/20 in the practical lab report.

If you apply for Special Consideration for your final examination, you must make yourself available for the week after the completion of postgraduate exams. If you are not available at that time, there is no guarantee an additional examination time will be offered. Specific examination dates and times will be determined at a later date.

Second-chance hurdle examinations will also be offered in the week after the completion of postgraduate exams. You will be notified of your eligibility for a hurdle retry and you must also make yourself available during that week to take advantage of this opportunity.

Assessment Tasks

Name	Weighting	Hurdle	Due
Quiz 1	5%	No	Week 4
Quiz 2	5%	No	Week 8
Practical activities report	20%	Yes	Week 11
Group Project	30%	No	Week 11
Exam	40%	Yes	TBC

Quiz 1

Due: **Week 4**
Weighting: **5%**

Held: Week 4, Weighting: 5% Quiz (closed book) 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.

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.

Quiz 2

Due: **Week 8**
Weighting: **5%**

Held in Week 8, Weighting: 5% Quiz (closed book) 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.

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.

Practical activities report

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. Your written output from these activities, including findings, will be emailed to milton.baar@mq.edu.au in week 11.

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. Understand the legal and

practical frameworks that limit available actions. Understand limitations of forensic tools.
- Present and discuss concepts related to software and network security at a postgraduate level. Create a body of work for assessment that demonstrates understanding of theoretical and practical aspects of unit content.

Group Project

Due: **Week 11**
Weighting: **30%**

Presentations are held in weeks 11 & 12 but content due by 17-MAY-2019, Weighting: 30% 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. The project reports must be emailed to milton.baar@mq.edu.au by 17-MAY-2019 @2359.

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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.
- Present and discuss concepts related to software and network security at a postgraduate level. Create a body of work for assessment that demonstrates understanding of theoretical and practical aspects of unit content.

Exam

Due: **TBC**
Weighting: **40%**
This is a hurdle assessment task (see assessment policy for more information on hurdle

assessment tasks)

Held during Semester 1 examination period, Weighting: 40% To pass the unit, you must achieve at least 20/40 in the Exam component. To receive a "second attempt" at the exam, you must achieve a mark of at least 15/40 in the exam. 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. Students have 2 hours written time plus 10 minutes reading time for the exam.

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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.

Delivery and Resources

Technology:

- Presentations using Powerpoint
- Other computer related material

Lecture and Tutorial:

- Provided in unit schedule

All unit information will be posted on iLearn (https://ilearn.mq.edu.au/login/MQ/). We assume that students will regularly check iLearn for information regarding lecture notes and other related resources. It should be noted that no single text book completely covers the content of this unit. Below books are recommended (not compulsory) for the course.

References:

- Harlan Carvey, Windows Registry Forensics, ISBN 9780128032916, https://www.elsevier.com/books/windows-registry-forensics/carvey/978-0-12-803291-6
- Gary McGraw, Software Security: Building Security IN, https://www.oreilly.com/library/view/software-security-building/0321356705/
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, https://www.pearson.com.au/products/O-R-Pfleeger-Pfleeger/Security-in-Computing/9780134085043?R=9780134085043

- Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition, 2nd Edition, https://www.oreilly.com/library/view/hacking-exposed-malware/9780071825757/
- Building Secure Software, How to avoid security problems the right way, John Viega, Gary McGraw, https://www.pearson.com/us/higher-education/product/Viega-Building-Secure-Software-How-to-Avoid-Security-Problems-the-Right-Way/9780321624000.html
- Dafydd Stuttard, Marcus Pinto, The Web Application Hackers Handbook, Wiley, 2nd Edition, https://www.oreilly.com/library/view/the-web-application/9781118026472/chap03-sec001.html
- Howard and LeBlanc, Writing Secure Code, Microsoft Press, 2nd edition, https://www.oreilly.com/library/view/writing-secure-code/0735617228/

Unit Schedule

To successfully participate in the lab exercises and to understand the fundamentals of this unit, students should read and view the material at the following links before week 4.

Watch these:

- Binary/octal/decimal/hexadecimal number systems, https://www.youtube.com/watch?v=5sS7w-CMHkU
- Endian concepts, https://www.youtube.com/watch?v=NvlSRs_APT4
- ASCII/EBCDIC/Unicode concepts, https://www.youtube.com/watch?v=m0aOZuMhhhE
- Boot process, https://www.youtube.com/watch?v=P-zWXbPh_dg
- Operating system and kernel architecture, https://www.youtube.com/watch?v=9GDX-IyZ_C8
- Protection ring, https://www.youtube.com/watch?v=b3HlH4IubZE

Read these:

- Introduction to operating systems, https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/1_Introduction.html
- Forensic analysis of smart TV: A current issue and call to arms, http://www.sciencedirect.com/science/article/pii/S1742287614000620
- How computers measure and keep time, https://www.eecis.udel.edu/~ntp/ntpfaq/NTP-s-sw-clocks.htm

Week	Topic	Lab/ Practical activity	Recommended reading and/or viewing
1	Introduction	No week 1 lab	
2	Risk management frameworks	Lab systems setup	• Overview of Digital Forensics, https://www.youtube.com/watch?v=ZUqzcQc_syE • Digital Forensics TEDx presentation, https://www.youtube.com/watch?v=Pf-JnQfAEew
3	Operating systems vulnerabilities	Forensic tools part 1	
4	Introduction to file systems	Quiz 1	• Windows File System Structures, https://www.youtube.com/watch?v=atYQBTHnjyY • FAT file system explained, https://www.youtube.com/watch?v=HjVktRd35G8 • Windows ReFS Explained, https://www.youtube.com/watch?v=L9kNND7b9yw • ReFS in Windows Server 2012, https://www.youtube.com/watch?v=WWeZf94gXZs • Windows filesystems, https://support.microsoft.com/en-us/help/100108/overview-of-fat--hpfs--and-ntfs-file-systems • Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator, http://www.swdsi.org/swdsi2010/sw2010_preceedings/papers/pa121.pdf
5	Linux file systems	Investigating Linux	Difference Between Linux and Windows, https://www.youtube.com/watch?v=NXZoWJVOhXI
6	Introduction to Digital Evidence and Computer Crime	Forensic management tools	
7	"Big end of town" file systems	Experimentation when tools fail you	
8	Mid-course review	Quiz 2, Guest Speaker	
9	Steganography	Steganography lab	
10	Introduction to cryptography	Practical lab report writing	
11	Group project presentation		
12	Group project presentation		
13	Review		

*Lecture contents, order and schedule of lectures and practicals will vary depending on the class progress.

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). 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 *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

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

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central).

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/study/getting-started/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 improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Enquiry Service

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

Equity 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.

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.

Graduate Capabilities

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- 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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.

Assessment tasks

- Quiz 1
- Quiz 2
- Practical activities report
- Group Project
- Exam

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcomes

- 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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.
- Present and discuss concepts related to software and network security at a postgraduate level. Create a body of work for assessment that demonstrates understanding of theoretical and practical aspects of unit content.

Assessment tasks

- Quiz 1
- Quiz 2
- Practical activities report
- Group Project
- Exam

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcomes

- 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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.
- Present and discuss concepts related to software and network security at a postgraduate level. Create a body of work for assessment that demonstrates understanding of theoretical and practical aspects of unit content.

Assessment tasks

- Quiz 1
- Quiz 2
- Practical activities report
- Group Project
- Exam

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcome

- Present and discuss concepts related to software and network security at a postgraduate level. Create a body of work for assessment that demonstrates understanding of

theoretical and practical aspects of unit content.

Assessment tasks

- Practical activities report
- Group Project

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to national and global issues

This graduate capability is supported by:

Learning outcome

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

Assessment tasks

- Practical activities report
- Group Project

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcomes

- 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. Understand the legal and practical frameworks that limit available actions. Understand limitations of forensic tools.

Assessment tasks

- Practical activities report

- Group Project

Changes from Previous Offering

In 2019, the unit is including practical exercises in forensic discovery and in static forensic collection. 20% of the unit mark comes from the written report that is based on the practical activities.

Grading

At the end of the semester, you will receive a grade that reflects your achievement in the unit

- Fail (F): does not provide evidence of attainment of all learning outcomes. There is missing or partial or superficial or faulty understanding and application of the fundamental concepts in the field of study; and incomplete, confusing or lacking communication of ideas in ways that give little attention to the conventions of the discipline.
- Pass (P): provides sufficient evidence of the achievement of learning outcomes. There is demonstration of understanding and application of fundamental concepts of the field of study; and communication of information and ideas adequately in terms of the conventions of the discipline. The learning attainment is considered satisfactory or adequate or competent or capable in relation to the specified outcomes.
- Credit (Cr): provides evidence of learning that goes beyond replication of content knowledge or skills relevant to the learning outcomes. There is demonstration of substantial understanding of fundamental concepts in the field of study and the ability to apply these concepts in a variety of contexts; plus communication of ideas fluently and clearly in terms of the conventions of the discipline.
- Distinction (D): provides evidence of integration and evaluation of critical ideas, principles and theories, distinctive insight and ability in applying relevant skills and concepts in relation to learning outcomes. There is demonstration of frequent originality in defining and analysing issues or problems and providing solutions; and the use of means of communication appropriate to the discipline and the audience.
- High Distinction (HD): provides consistent evidence of deep and critical understanding in relation to the learning outcomes. There is substantial originality and insight in identifying, generating and communicating competing arguments, perspectives or problem solving approaches; critical evaluation of problems, their solutions and their implications; creativity in application.

In this unit, your final grade depends on your performance in each part of the assessment. For each task, you receive a mark that combines your standard of performance regarding each

learning outcome assessed by this task. Then the different component marks are added up to determine your total mark out of 100. Your grade then depends on this total mark and your overall standards of performance.

Concretely, in order to pass the unit, you must

- obtain a total mark of 50% or higher, and **both** obtain a mark of 20/40 or higher in the final examination and obtain a mark of 15/20 or higher in the Practical Activities Report;
- make a reasonable attempt at the exercises in the assessment tasks;
- demonstrate that you can perform at a Functional level or higher for each criterion assessed in the Quiz and Group Project/Presentation.
- reach a Functional level or higher for each criterion assessed in the final examination.

Students obtaining a higher grade than a pass in this unit will (in addition to the above)

- have a total mark of 85% or higher and perform at distinction level or higher in the final examination to obtain High Distinction;
- have a total mark of 75% or higher and perform at credit level or higher in the final examination to obtain Distinction;
- have a total mark of 65% or higher and perform at pass level but with 50% or higher in the final examination to obtain Credit.

If you receive special consideration for the final exam, a supplementary exam will be scheduled in the interval between the regular exam period and the start of the next session. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. You can check the supplementary exam information page on FSE101 in iLearn (bit.ly/FSESupp) for dates, and approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination. If you are given a second opportunity to sit the final examination as a result of failing to meet the minimum mark required, you will be offered that chance during the same supplementary examination period and will be notified of the exact day and time after the publication of final results for the unit.