ITEC653

Offensive Security

S2 Day 2019

Dept of Computing

Contents

General Information

Unit convenor and teaching staff
Convenor
Damian Jurd
damian.jurd@mq.edu.au

Lecturer
Alireza Jolfaei
alireza.jolfaei@mq.edu.au

Credit points
4

Prerequisites
Admission to MInfoTech(Cyber Sec)

Corequisites

Co-badged status

Unit description
This unit provides an introduction to ethical hacking and offensive security. Strong emphasis is given to ethics and ethical behaviour as students are exposed to penetration techniques and methods. In other words, students are taught how to systematically look for and exploit vulnerabilities in software, protocols and systems in order to report those vulnerabilities and improve the safety of those software, protocols and systems. Communication, in speaking and writing plays a critical role in this unit. The most proficient students in this unit may be selected to represent the University at various national pentesting competitions and challenges.

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:

Explain the importance of ethics and ethical behaviour in relation to offensive security and penetration testing

Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations

Exploit vulnerabilities for a range of purposes, including access control, payload delivery,

privilege escalation, etc

Effectively communicate results verbally and in-writing to technical and non-technical audiences

General Assessment Information

Late Submission

No extensions will be granted without an approved application for Special Consideration. There will be a deduction of 20% 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 – 40% penalty or 2 marks deducted from the total. No submission will be accepted after solutions have been posted.

Supplementary Exam

If you receive Special Consideration for the final exam, a supplementary exam will be scheduled after the normal exam period, following the release of marks. 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. Approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

Assessment Tasks

Name	Weighting	Hurdle	Due
In-class exercises	12%	No	Weeks 2, 4, 6, 8, 10, 12
CTF - Capture The Flag	18%	No	Weeks 3, 7, 11
Module Exams	60%	No	Weeks 5, 9, Exam Period
Research Topic	10%	No	Week 13

In-class exercises

Due: **Weeks 2, 4, 6, 8, 10, 12**
Weighting: **12%**

During even numbered weeks you will be set an in-class exercise related to that week's lecture topic to complete during your workshop class. Your work will be checked and marked in the workshop class in which it is completed. No late submissions are accepted.

On successful completion you will be able to:

- Perform scoping, vulnerability scanning and reconnaissance on a range of devices,

platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc

CTF - Capture The Flag

Due: **Weeks 3, 7, 11**
Weighting: **18%**

For each of the three modules you will compete in a group based capture-the-flag exercise. Students will have the opportunity to apply the principles, tools, and techniques that they have learnt against live systems in order to find various vulnerabilities. The CTF will be conducted during your practical class. Students will complete the CTF as members of a group in class and individually submit a report describing what vulnerabilities were found and their attack methodology. CTF reports will be due before the following week's practical class.

On successful completion you will be able to:
- Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc
- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Module Exams

Due: **Weeks 5, 9, Exam Period**
Weighting: **60%**

Module exams will be conducted as capture-the-flag exercises and will follow the structure of the CTF exercise conducted two weeks prior to the module exam. Unlike the CTF exercise students will complete the module exams individually, not in groups. As for the CTF a report will be submitted before the following week's practical class.

On successful completion you will be able to:
- Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc
- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Research Topic

Due: **Week 13**
Weighting: **10%**

Student groups will research a well known vulnerability (chosen by the teaching staff) and provide a presentation and demonstration of the vulnerability. Each presentation will be followed by a brief question-and-answer session. Group members will submit a report individually with a focus on the ethical implicatoins of the use and misuse of the vulnerability.

On successful completion you will be able to:

- Explain the importance of ethics and ethical behaviour in relation to offensive security and penetration testing
- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Delivery and Resources

Classes

Each week you should attend three hours of lectures, and a three hour practical workshop. For details of days, times and rooms consult the timetables webpage.

Note that practicals workshops (lab sessions) commence in **week 1**. The week-by-week details of the practical (lab) classes will be available from iLearn.

You must attend the practicals that you are enrolled in.

Textbook and Reading Materials

The following two textbooks contain the bulk of the weekly readings.

1. Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman (available online from the library).
2. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard and Marcus Pinto (available online from the library).

Web Resources

Unit Websites

ITEC653 is administered via iLearn (http://ilearn.mq.edu.au/).

Lecture recordings

Digital recordings of lectures *may* be available. When available they will be linked from iLearn.

General Notes

In this unit, you should do the following:

- Attend lectures, take notes, ask questions.
- Attend your weekly Practical session.
- Ensure that you attend the CTFs
- Ensure that you attend moule exams.
- Read appropriate sections of the text, add to your notes and prepare questions for your lecturer/tutor.
- Work on any assignments that have been released.

Lecture notes will be made available each week but these notes are intended as an outline of the lecture only and are not a substitute for your own notes or the recommended reading list.

Unit Schedule

Tentative teaching schedule, subject to change:

Week	Module	Lecture Topics	Assessment	Mode	Weight	Submit
1	Systems	Introduction, ethics, group selection Virtual machines, kali linux, windows, file systems, process models, vulnerabilities	Diagnostic Test	Individual	0%	
2			In-class exercise	Individual	2%	
3			Capture The Flag (CTF)	Group	6%	
4			In-class exercise	Individual	2%	CTF Report
5	Web	Web infrastructure, injections, cross-site scripting, cookies, headers, fuzzing, vulnerabilities	Module Exam	Individual	20%	
6			In-class exercise	Individual	2%	Module Report
7			CTF	Group	6%	
8			In-class exercise	Individual	2%	CTF Report
9	Networking	Network stack, scanning, services, authentication protocols, services, vulnerabilities	Module Exam	Individual	20%	
10			In-class exercise	Individual	2%	Module Report

11			CTF	Group	6%	
12			In-class exercise	Individual	2%	CTF Report
13			Group presentations	Group	10%	Reflective Report
Formal Exam Period			Module Exam	Individual	20%	Module Report

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 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.

Graduate Capabilities

Creative and Innovative

Our graduates will also be capable of creative thinking and of creating knowledge. They will be imaginative and open to experience and capable of innovation at work and in the community. We want them to be engaged in applying their critical, creative thinking.

This graduate capability is supported by:

Learning outcome

- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc

Assessment tasks

- In-class exercises
- CTF - Capture The Flag
- Module Exams

Capable of Professional and Personal Judgement and Initiative

We want our graduates to have emotional intelligence and sound interpersonal skills and to demonstrate discernment and common sense in their professional and personal judgement. They will exercise initiative as needed. They will be capable of risk assessment, and be able to handle ambiguity and complexity, enabling them to be adaptable in diverse and changing environments.

This graduate capability is supported by:

Learning outcomes

- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc
- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Assessment tasks

- In-class exercises
- CTF - Capture The Flag
- Module Exams
- Research Topic

Discipline Specific Knowledge and Skills

Our graduates will take with them the intellectual development, depth and breadth of knowledge, scholarly understanding, and specific subject content in their chosen fields to make them competent and confident in their subject or profession. They will be able to demonstrate, where relevant, professional technical competence and meet professional standards. They will be able to articulate the structure of knowledge of their discipline, be able to adapt discipline-specific knowledge to novel situations, and be able to contribute from their discipline to inter-disciplinary solutions to problems.

This graduate capability is supported by:

Learning outcomes

- Explain the importance of ethics and ethical behaviour in relation to offensive security and penetration testing
- Perform scoping, vulnerability scanning and reconnaissance on a range of devices,

platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc
- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Assessment tasks

- In-class exercises
- CTF - Capture The Flag
- Module Exams
- Research Topic

Critical, Analytical and Integrative Thinking

We want our graduates to be capable of reasoning, questioning and analysing, and to integrate and synthesise learning and knowledge from a range of sources and environments; to be able to critique constraints, assumptions and limitations; to be able to think independently and systemically in relation to scholarly activity, in the workplace, and in the world. We want them to have a level of scientific and information technology literacy.

This graduate capability is supported by:

Learning outcomes

- Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc

Assessment tasks

- In-class exercises
- CTF - Capture The Flag
- Module Exams

Problem Solving and Research Capability

Our graduates should be capable of researching; of analysing, and interpreting and assessing data and information in various forms; of drawing connections across fields of knowledge; and they should be able to relate their knowledge to complex situations at work or in the world, in order to diagnose and solve problems. We want them to have the confidence to take the initiative in doing so, within an awareness of their own limitations.

This graduate capability is supported by:

Learning outcomes

- Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations
- Exploit vulnerabilities for a range of purposes, including access control, payload delivery, privilege escalation, etc

Assessment tasks

- In-class exercises
- CTF - Capture The Flag
- Module Exams

Effective Communication

We want to develop in our students the ability to communicate and convey their views in forms effective with different audiences. We want our graduates to take with them the capability to read, listen, question, gather and evaluate information resources in a variety of formats, assess, write clearly, speak effectively, and to use visual communication and communication technologies as appropriate.

This graduate capability is supported by:

Learning outcome

- Effectively communicate results verbally and in-writing to technical and non-technical audiences

Assessment tasks

- CTF - Capture The Flag
- Module Exams
- Research Topic

Engaged and Ethical Local and Global citizens

As local citizens our graduates will be aware of indigenous perspectives and of the nation's historical context. They will be engaged with the challenges of contemporary society and with knowledge and ideas. We want our graduates to have respect for diversity, to be open-minded, sensitive to others and inclusive, and to be open to other cultures and perspectives: they should have a level of cultural literacy. Our graduates should be aware of disadvantage and social justice, and be willing to participate to help create a wiser and better society.

This graduate capability is supported by:

Learning outcome

- Explain the importance of ethics and ethical behaviour in relation to offensive security

and penetration testing

Assessment task

- Research Topic

Socially and Environmentally Active and Responsible

We want our graduates to be aware of and have respect for self and others; to be able to work with others as a leader and a team player; to have a sense of connectedness with others and country; and to have a sense of mutual obligation. Our graduates should be informed and active participants in moving society towards sustainability.

This graduate capability is supported by:

Learning outcome

- Explain the importance of ethics and ethical behaviour in relation to offensive security and penetration testing

Assessment task

- Research Topic

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, the final mark will be calculated by combining the marks for all assessment tasks according to the percentage weightings shown in the assessment summary. The practical classes are classified as a hurdle assessment, this means that you will be required to perform to a satisfactory standard in at least nine of the practical classes to pass the unit.

Concretely, **in order to pass the unit**, you must obtain an overall total mark of 50% or higher, and satisfactorily complete at least 9 out of the 12 practical exercises.

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 to obtain High Distinction;
  - have a total mark of 75% or higher to obtain Distinction;
  - have a total mark of 65% or higher to obtain Credit.