COMP2320

Offensive Security

Session 1, Weekday attendance, North Ryde 2020

Dept of Computing

Contents

General Information

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

Alireza Jolfaei
alireza.jolfaei@mq.edu.au

Credit points
10

Prerequisites

Corequisites
(COMP2110 or COMP249) and (COMP2250 or COMP247) and (COMP2300 or COMP343)

Co-badged status
COMP6320

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

Learning Outcomes

ULO1: Explain the importance of ethics and ethical behaviour in relation to offensive security and penetration testing.

ULO2: Perform scoping, vulnerability scanning and reconnaissance on a range of devices, platforms, protocols, systems and organisations.

ULO3: Exploit vulnerabilities for a range of purposes, including access control, payload delivery and privilege escalation.

ULO4: Effectively communicate results verbally and in-writing to technical and non-

technical audiences.

General Assessment Information

General Assessment Information

Assignments

Assignment work must be written clearly, with good grammar, correct word usage, correct punctuation,and lack of spelling errors. Poor or bad expression will be penalized, Wherever required, all written work must be properly referenced and conform to standard stylistic conventions.

Late Submissions

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
In-class exercises	8%	No	Weekly
CTF #1	14%	No	Week 4
CTF #2	14%	No	Week 8
CTF #3	14%	No	Week 12
Research and Presentation	10%	No	Week 13
Final Examination	40%	No	Formal exam period

In-class exercises

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 4 hours
Due: **Weekly**
Weighting: **8%**

During workshops, you will be set an in-class exercise related to that week's lecture topic to complete during the 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 and privilege escalation.

CTF #1

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 4**
Weighting: **14%**

This capture-the-flag exercise will be completed at a fixed time but outside of scheduled class time. Teams will compete against each other and students will be assessed individually via a report to be submitted one week after the CTF.

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

CTF #2

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 8**
Weighting: **14%**

This capture-the-flag exercise will be completed at a fixed time but outside of scheduled class time. Teams will compete against each other and students will be assessed individually via a report to be submitted one week after the CTF.

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 and privilege escalation.
- Effectively communicate results verbally and in-writing to technical and non-technical

audiences.

CTF #3

Assessment Type [1]: Project
Indicative Time on Task [2]: 7 hours
Due: **Week 12**
Weighting: **14%**

This capture-the-flag exercise will be completed at a fixed time but outside of scheduled class time. Teams will compete against each other and students will be assessed individually via a report to be submitted one week after the CTF.

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

Research and Presentation

Assessment Type [1]: Presentation
Indicative Time on Task [2]: 5 hours
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 implications 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.

Final Examination

Assessment Type [1]: Examination
Indicative Time on Task [2]: 20 hours
Due: **Formal exam period**

Weighting: **40%**

A three-hour closed book examination during the examination period.

On successful completion 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 and privilege escalation.
- Effectively communicate results verbally and in-writing to technical and non-technical audiences.

---

[1] If you need guidance or support to understand or complete this type of assessment, please contact the Learning Skills Team

[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

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

COMP2320 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 participate in the CTF exercises.
- 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	Submission
1	Systems	Introduction, ethics, group selection Virtual machines, kali linux, windows, file systems, process models, vulnerabilities	No pracs week 1	
2			Diagnostic Test In-class exercise	
3			In-class exercise	
4			Capture The Flag (CTF)	
5	Web	Web infrastructure, injections, cross-site scripting, cookies, headers, fuzzing, vulnerabilities	In-class exercise	CTF Report
6			In-class exercise	
7			In-class exercise	
Mid Semester Break				
8			Capture The Flag (CTF)	

9	Networking	Network stack, scanning, services, authentication protocols, services, vulnerabilities	In-class exercise	CTF Report
10			In-class exercise	
11			In-class exercise	
12			Capture The Flag (CTF)	Presentation Report
13	Presentations		Group presentations	CTF Report
14-16	Formal Exam			

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.)*

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.

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.

Changes since First Published

Date	Description
17/02/2020	Correction of a typographic error. Re-ordered assesments chronologically.
14/02/2020	Added co-badged status