COMP2320

Offensive Security

Session 1, In person/Online-scheduled-weekday, North Ryde 2022

School of Computing

Contents

General Information	2
Learning Outcomes	2
General Assessment Information	3
Assessment Tasks	3
Delivery and Resources	6
Policies and Procedures	7

General Information

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

Credit points
10

Prerequisites

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

Co-badged status
This unit is co-badged with 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://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

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

Late submissions will not be accepted without an approved Special Consideration request. Assessments submitted after the due date will receive a mark of zero.

Assessment Tasks

Name	Weighting	Hurdle	Due
In-class exercises	18%	No	Weekly
CTF #1	24%	No	Week 4
CTF #2	24%	No	Week 9
CTF #3	24%	No	Week 12
Research and Presentation	10%	No	Week 13

In-class exercises

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 9 hours
Due: **Weekly**
Weighting: **18%**

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:

- 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.

CTF #1

Assessment Type [1]: Project
Indicative Time on Task [2]: 12 hours
Due: **Week 4**
Weighting: **24%**

This capture-the-flag exercise will be completed during 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]: 12 hours
Due: **Week 9**
Weighting: **24%**

This capture-the-flag exercise will be completed during 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]: 12 hours
Due: **Week 12**
Weighting: **24%**

This capture-the-flag exercise will be completed during 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.

---

[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

Classes

Each week you should attend two 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 practical 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.
- 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.
- Ensure that you participate in the CTF exercises (note that this will occur during the scheduled lecture period).
- Ensure that you participate in the group presentations (note that this will occur during the schedule lecture period).
- **Note that this means that lecture attendance will be compulsory during weeks 4, 9, 12, and 13.**

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.

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 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.