COMP6320

Offensive Security

Session 2, In person-scheduled-weekday, North Ryde 2024

School of Computing

Contents

Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

General Information

Unit convenor and teaching staff
Lecturer and Convenor
Natasha Fernandes
natasha.fernandes@mq.edu.au

Lecturer
Damian Jurd
damian.jurd@mq.edu.au

Credit points
10

Prerequisites
Admission to MInfoTechCyberSec or GradCertInfoTech

Corequisites

Co-badged status
COMP2320

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 and demonstrate 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, privilege escalation, etc.

ULO4: Effectively communicate results, both verbally and in-writing, to technical and non-technical audiences.

General Assessment Information

Requirements to Pass this Unit

To pass this unit you must:

1. Attempt all assessments, and

2. Achieve a total mark equal to or greater than 50%.

There are no hurdle requirements for the unit.

Late Assessment Submission

Late assessments are not accepted in this unit unless a Special Consideration has been submitted and approved.

Special Consideration

The Special Consideration Policy aims to support students who have been impacted by short-term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment.

Practical Exams and Group Presentations: If you experience circumstances or events that affect your ability to participate at the scheduled time in either the group presentation or any of the practical exams you must inform the convenor as soon as is possible, and submit a Special Consideration request through ask.mq.edu.au. Given the group nature of these assessments your entire group *may* be given an alternative time and date for the assessment.

Practical Exam Reports: If you experience circumstances or events that affect your ability to complete the written exam reports in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

Weekly practice-based tasks: Your mark for this components is calculated by summing the best 6 out of 9 of the marks for the weekly in-class exercises. As such you should only apply for special consideration if you miss more than three of these practical classes.

Assessment Tasks

Name	Weighting	Hurdle	Due
In-Class Exercises	30%	No	Weeks 1, 2, 3, 4, 6, 7, 8, 10 and 11
Practical exams	60%	No	Weeks 5, 9 and 12

Name	Weighting	Hurdle	Due
Research and Presentation	10%	No	Week 13

In-Class Exercises

Assessment Type [1]: Practice-based task
Indicative Time on Task [2]: 15 hours
Due: **Weeks 1, 2, 3, 4, 6, 7, 8, 10 and 11**
Weighting: **30%**

During workshops, you will be set an in-class exercise related to that week's lecture topic to complete during the class. No late submissions are accepted.

On successful completion you will be able to:

- Explain the importance of and demonstrate 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.

Practical exams

Assessment Type [1]: Practice-based task
Indicative Time on Task [2]: 30 hours
Due: **Weeks 5, 9 and 12**
Weighting: **60%**

Practical exams will be conducted during the semester as group exercises. Students will be required to submit a report following each exam for individual assessment. Formative feedback will be given with students being able to improve their marks as the semester progresses.

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, both 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.

On successful completion you will be able to:

- Explain the importance of and demonstrate ethics and ethical behaviour in relation to offensive security and penetration testing.
- Effectively communicate results, both 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

Week 1

Each week you should participate in your scheduled two hour practical workshop. For details of scheduled classes consult the timetables webpage.

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

Also note that you must only attend the practical that you are enrolled in.

Textbook and Reading Materials

COMP6320 is a practice-oriented unit and as such the practical exercises and lecture notes make up the bulk of the learning material. Additional reading materials will be provided on iLearn as required.

Unit Websites

COMP6320 is administered via iLearn (http://ilearn.mq.edu.au/).

This unit outline can be found in the university's unit guides

Lecture Recordings

Digital recordings of lectures may be available. They will be linked from iLearn.

Technologies Used and Required

COMP6320 is a BYOD (Bring Your Own Device) unit. You will be expected to bring your own laptop computer (Windows, Mac, or Linux) to the workshop, install and configure the required software, and incorporate secure practices into your daily work (and play!) routines. The laptop must be capable of running a Kali Linux virtual machine. At a minimum your laptop should have 120GB of free disk space, 8GB of memory, and 4 CPU cores.

General Notes

In this unit, you should do the following:

- Review recorded lecture materials.
- Participate your weekly Practical session.
- Work on any assignments that have been released.

Note that Workshops commence in week 1. Please note that you will be required to submit work every week.

Communication Methods in COMP6320

All announcements about unit-related matters will be communicated through iLearn. It is the student's responsibility to ensure they check iLearn announcements, forums and FAQ sections regularly.

Students are encouraged to use the iLearn forums for asking questions about unit content and concepts. Where questions are about specific details in an assessment submission, this may need to be sent via a private forum post in the first instance (details are provided in iLearn about how this is set up) so as not to be at risk of breaching the university academic integrity policy.

Students should use the appropriate iLearn forms for contacting staff. There may be occasions where unit staff will email a student directly to their @students.mq.edu.au email address. It is the student's responsibility to ensure they check their official university email regularly for communications from the university staff.

COVID Information

For the latest information on the University's response to COVID-19, please refer to the Coronavirus infection page on the Macquarie website: https://www.mq.edu.au/about/coronavirus-faqs. Remember to check this page regularly in case the information and requirements change during semester. If there are any changes to this unit in relation to COVID, these will be communicated via iLearn.

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 connect.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 an d 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 Advocacy provides independent advice on MQ policies, procedures, and processes

Student Enquiries

Got a question? Ask us via the Service Connect Portal, 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.

Changes from Previous Offering

We value student feedback to be able to continually improve the way we offer our units. As such we encourage students to provide constructive feedback via student surveys, to the teaching staff directly, or via the FSE Student Experience & Feedback link in the iLearn page.

Student feedback from the previous offering of this unit was very positive overall, with students pleased with the clarity around assessment requirements and the level of support from teaching staff. As such, no change to the delivery of the unit is planned, however we will continue to strive to improve the level of support and the level of student engagement.

Unit information based on version 2024.02 of the Handbook