



COMP6320

Offensive Security

Session 2, In person-scheduled-weekday, North Ryde 2026

School of Computing

Contents

<u>General Information</u>	2
<u>Learning Outcomes</u>	2
<u>General Assessment Information</u>	3
<u>Assessment Tasks</u>	4
<u>Delivery and Resources</u>	6
<u>Policies and Procedures</u>	7
<u>Changes from Previous Offering</u>	9

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

Convenor and Lecturer

Natasha Fernandes

natasha.fernandes@mq.edu.au

Lecturer

Rohitranjan Vasantkumar Gupta

rohitranjanvasantkumar.gupta@mq.edu.au

Credit points

10

Prerequisites

Admission to MInfoTechCyberSec

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.

Learning in this unit enhances student understanding of global challenges identified by the United Nations Sustainable Development Goals ([UNSDGs](#)) Industry, Innovation and Infrastructure; Peace, Justice and Strong Institutions.

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 to technical and non-technical audiences.

General Assessment Information

Release Dates

- Proficiency Assessment: information and sample questions are to be released no later than week 4
- Professional Report - Preliminary Engagement: to be released no later than week 6
- Professional Report - Supplementary Engagement: to be released no later than week 10

Requirements to Pass this Unit

To pass this unit, you must:

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

Late Submission Policy

- **5% penalty per day:** If you submit your assessment late, **5% of the total possible marks** will be deducted for each day (including weekends), up to 7 days.
 - *Example 1 (out of 100):* If you score 85/100 but submit 20 hours late, you will lose 5 marks and receive **80/100**.
 - *Example 2 (out of 30):* If you score 27/30 but submit 1 day late, you will lose 1.5 marks and receive **25.5/30**.
- **After 7 days:** Submissions more than 7 days late will receive a **mark of 0**.

Assessments where Late Submissions will be accepted

- Proficiency Assessment - NO, this is an invigilated in-class assessment.
- Professional Report - Preliminary Engagement - YES, Standard Late Penalty applies.
- Professional Report - Supplementary Engagement - YES, Standard Late Penalty applies.

Short extensions

Short Extensions are not available for any assessments in this unit.

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. If you experience circumstances or events that affect your ability to complete the assessments in this unit on time, please inform the convenor and submit a Special Consideration request through <http://connect.mq.edu.au/>.

Generative AI Usage

The university has taken a 'two lane' approach with GenAI: assessments can be AI Open (meaning students complete the assessment in their own time and may use GenAI) and Observed (students complete assessments in supervised environments, where use of AI is controlled or not permitted). More information on the use of GenAI in Assessment can be found [here](#).

In this unit the assessments fall into the two lanes as follows:

- Proficiency Assessment - AI Observed (this is an invigilated in-class assessment).
- Professional Report, Preliminary - AI Open.
- Professional Report, Supplementary - AI Open.

Assessment Tasks

Name	Weighting	Hurdle	Due	Groupwork/Individual	Short Extension	AI Approach
Proficiency Assessment	30%	No	Week 6 Workshops	Individual	No	Observed
Professional Report - Preliminary Engagement	30%	No	25/09/2026	Individual	No	Open
Professional Report - Supplementary Engagement	40%	No	13/11/2026	Individual	No	Open

Proficiency Assessment

Assessment Type ¹: Examination

Indicative Time on Task ²: 6 hours

Due: **Week 6 Workshops**

Weighting: **30%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Observed

You will be assessed on your knowledge of penetration testing tasks from a technical, methodological, and ethical perspective.

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.

Professional Report - Preliminary Engagement

Assessment Type ¹: Professional task

Indicative Time on Task ²: 28 hours

Due: **25/09/2026**

Weighting: **30%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Open

You will complete various activities, recording your results in a journal. Drawing upon your journal as evidence, you will produce a professional report written in a form that is suitable for submission to a client for review by both executive and technical audiences.

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.
- Effectively communicate results to technical and non-technical audiences.

Professional Report - Supplementary Engagement

Assessment Type ¹: Professional task

Indicative Time on Task ²: 38 hours

Due: **13/11/2026**

Weighting: **40%**

Groupwork/Individual: Individual

Short extension ³: No

AI Approach: Open

You will complete various activities, recording your results in a journal. Drawing upon your journal as evidence, you will produce a professional report written in a form that is suitable for submission to a client for review by both executive and technical audiences.

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.
- Effectively communicate results 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
- [Academic Success](#) 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.

³ An automatic short extension is available for some assessments. Apply through the [Service Connect Portal](#).

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 \(http://ilearn.mq.edu.au/\)](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 or Mac) 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 CommandoVM 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 the dedicated unit email address 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.

Policies and Procedures

Macquarie University policies and procedures are accessible from [Policy Central \(https://policies.mq.edu.au\)](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) (<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) (<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 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/>

Academic Success

[Academic Success](#) provides resources to develop your English language proficiency, academic writing, and communication skills.

- [Ask a Study Coach](#)
- [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 <https://students.mq.edu.au/support/technology/service-desk>.

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 2026.04 of the **Handbook**