COMP2320

Offensive Security

Session 2, Special circumstance 2020

Department of Computing

Contents

Notice

As part of Phase 3 of our return to campus plan, most units will now run tutorials, seminars and ot her small group learning activities on campus for the second half-year, while keeping an online ver sion available for those students unable to return or those who choose to continue their studies onli ne.

To check the availability of face-to-face and onlin e activities for your unit, please go to timetable vi ewer. To check detailed information on unit asses sments visit your unit's iLearn space or consult yo ur unit convenor.

General Information

Unit convenor and teaching staff
Unit Convenor, Lecturer
Alireza Jolfaei
alireza.jolfaei@mq.edu.au

Lecturer
Mehdi Baratipour
mehdi_baratipour@msn.com

Mehdi Baratipour
mehdi.baratipour@mq.edu.au

Credit points
10

Prerequisites

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

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:

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.

Assessment Tasks

Name	Weighting	Hurdle	Due
CTF #1	24%	No	Week 5
CTF #3	24%	No	Week 13
In-class exercises	18%	No	Weekly
Research and Presentation	10%	No	Weeks 12 (Report and Slides). Week 13 (Presentation)
CTF #2	24%	No	Week 9

CTF #1

Assessment Type [1]: Project
Indicative Time on Task [2]: 12 hours
Due: **Week 5**
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 13**
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.

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:

- 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.

Research and Presentation

Assessment Type [1]: Presentation
Indicative Time on Task [2]: 5 hours
Due: **Weeks 12 (Report and Slides). Week 13 (Presentation)**
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.

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.

[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

COMPUTING FACILITIES

COMP2320 is a BYOD (Bring Your Own Device). 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.

CLASSES

Each week you should complete any assigned readings and review the lecture slides in order to prepare for the lecture. There are two hours of lectures and a two-hour workshop every week.

The hands-on exercises in workshops help to reinforce concepts introduced during the lectures. You should have chosen a practical on enrollment. You will find it helpful to read the workshop instructions before attending - that way, you can get to work quickly! For details of days, times, and rooms consult the timetables webpage.

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

RECOMMENDED TEXTS

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.

DISCUSSION BOARDS

This unit makes use of discussion boards hosted within iLearn. Please post questions there; they are monitored by the staff on the unit.

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	Weight	Submit
1	Systems	Introduction, ethics, group selection, Virtual machines, Kali Linux, Windows, file systems, process models, vulnerabilities	In-class exercise Diagnostic Test	2%	
2			In-class exercise	2%	
3			In-class exercise	2%	
4			Capture The Flag (CTF) #1	24%	
5	Web	Web infrastructure, injections, cross-site scripting, cookies, headers, fuzzing, vulnerabilities	In-class exercise	2%	CTF #1 Report

6			In-class exercise	2%	
7			In-class exercise	2%	
Mid Semester Break - Recess					
8			Capture The Flag (CTF) #2	24%	
9	Networking	Network stack, scanning, services, authentication protocols, services, vulnerabilities	In-class exercise	2%	CTF #2 Report
10			In-class exercise	2%	
11			In-class exercise	2%	
12			Capture The Flag (CTF) #3	24%	Presentation Slides
13	Presentations		Group presentations	10%	CTF #3 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.)*

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 help you improve your marks and take control of your study.

- Getting help with your assignment
- Workshops
- StudyWise
- 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

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.