Course Outline

Contents

- Course Details
- Course Summary
- Assumed Knowledge
- Student Learning Outcomes
- Teaching Strategies
- Student Conduct
- Assessment
- Course Schedule
- Resources for Students
- Course Evaluation and Development

Course Details

Course Code	COMP6447
Course Title	System and Software Security Assessment
LiC	Richard Buckland
Lecturer	Brendan Hopper
Teaching Staff	Sean Yeoh
Course Admin	Tek Huynh
Course Email	cs6447@cse.unsw.edu.au
Units of Credit	6
Course Website	https://webcms3.cse.unsw.edu.au/COMP6447/18s2/ (https://webcms3.cse.unsw.edu.au/COMP6447/18s2/)
Handbook Entry	http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP6447.html (http://www.handbook.unsw.edu.au/undergraduate/courses/current/COMP6447.html)

Course Summary

This course looks at cyber attack and defence. Students learn how to assess and identify vulnerabilities and how vulnerabilities are exploited. Students learn the principles and theory of exploitation, the common security models, and how approaches to exploitation and defence have evolved over time.

Students from this course will engage in war games competitions, analyse real world case studies of vulnerabilities in complex software used on widespread systems, and gain an understanding of the technical process of finding and fixing low-level software vulnerabilities and also of the economics and causal factors involved with their real world use.

The course covers techniques and skills including vulnerability classes, source code auditing, fuzzing, security bugs, software security assurance, taint analysis, memory corruption, overflows and return oriented programming . The c ourse coverage will be constantly updated over time to reflect emerging attack and defence methods.

There are numerous formative assessments and activities throughout the course to provide feedback and learning opportunities. These do not directly contribute to your final grade but are expected to be used to provide evidence of your capabilities in your portfolio.

Students need a keen, devious and analytical mind. To get the most from this course students will need to engage in independent study and research and be able to act as independent self directed learners.

Binary exploits = hardcore.

BEWARE

To get the most from these courses you will need to engage in independent study and act as a self directed learner. Attending lectures alone will not be sufficient to pass the course. You will need to devote considerable practice to all the techniques we cover and read further on topics which interest you or which you do not fully understand. For a credit level result we expect you will spend 11 hours per week in total on this course, including over the mid semester break.

Seek feedback from your friendly lecturers and class peers constantly over the semester and closely monitor yourself to make sure you are not falling behind. We treat you like adults and do not force you to do the self directed work and practice - but experience has shown that students who do not work hard in the course do not do well, and often express disappointment later on at the missed opportunity. (Since we have awesome tutors and speakers here for you during the course - make sure you make full use of them and your time.)

Assumed Knowledge

You need to have taken and passed COMP6441 or COMP6841 or COMP3441 or COMP9321.

Prior to commencing the course, students should have an understanding of how computers work, including the following:

1. Virtual Memory
2. C
3. Linux

If you have any knowledge gaps, you will need to take responsibility for covering those topics in your own time with private practice and study.

Student Learning Outcomes

After completing this course, you will:

- Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, fuzzing, security bugs, software security assurance and testing, taint analysis, memory corruption, numeric overflows, return oriented programming)
- Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures
- Given a system being able to identify and analyse its key vulnerabilities and design and implement reliable exploits to make use of this
- Given a system being able to identify and analyse its key vulnerabilities and design and implement reliable remedies and countermeasures to prevent successful exploitation
- Have an understanding of the key legal, ethical, and professional issues of offensive-defence; and to be able to apply this understanding to design and conduct professional offensive-defence operations.

This course contributes to the development of the following graduate capabilities:

Graduate Capability	**Acquired in**
Scholars capable of independent and collaborative enquiry, rigorous in their analysis, critique and reflection, and able to innovate by applying their knowledge and skills to the solution of novel as well as routine problems	Tutorials, Assignments, Wargames
Entrepreneurial leaders capable of initiating and embracing innovation and change, as well as engaging and enabling others to contribute to change	Tutorials, Assignments, Wargames
Professionals capable of ethical, self- directed practice and independent lifelong learning	Lectures, Assignments, Wargames
Global citizens who are culturally adept and capable of respecting diversity and acting in a socially just and responsible way	Lectures, Tutorials

Teaching Strategies

Lectures will be used to introduce students to theoretical and practical concepts and will include live demonstrations. There will be guest lecturers coming in from industry to share practical specialised experience with the students. A detailed list of lecture topics and the slides used for the lectures will be posted on the course website as session progresses.

Assignments : Students are expected to apply the knowledge gained in practical environments known as **war games** .

Assignments will be subject to a late penalty. Due to their diversity, the late penalty will be tailored for each individual assignment.

The **Final Exam** will be a theoretical and practical exam where students apply their knowledge and skills learnt over the entire course.

Supplementary exams will only be awarded in well justified cases, in accordance with School policy for *Special Consideration* , **not** as a second chance for poorly performing students. In particular, it is unlikely that a supplementary will be awarded to students who have actually sat the proper exam. **Make up your mind whether or not you are sick before attempting the exam.**

Student Conduct

The **Student Code of Conduct** (Information (https://student.unsw.edu.au/conduct) , Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)) sets out what the University expects from students as members of the UNSW community. As well as the learning, teaching and research environment, the University aims to provide an environment that enables students to achieve their full potential and to provide an experience consistent with the University's values and guiding principles. A condition of enrolment is that students *inform themselves* of the University's rules and policies affecting them, and conduct themselves accordingly.

In particular, students have the responsibility to observe standards of equity and respect in dealing with every member of the University community. This applies to all activities on UNSW premises and all external activities related to study and research. This includes behaviour in person as well as behaviour on social media, for example Facebook groups set up for the purpose of discussing UNSW courses or course work. Behaviour that is considered in breach of the Student Code Policy as discriminatory, sexually inappropriate, bullying, harassing, invading another's privacy or causing any person to fear for their personal safety is serious misconduct and can lead to severe penalties, including suspension or exclusion from UNSW.

If you have any concerns, you may raise them with your lecturer, or approach the School Ethics Officer (mailto:ethics-officer@cse.unsw.edu.au) , Grievance Officer (mailto:grievance-officer@cse.unsw.edu.au) , or one of the student representatives.

Plagiarism is defined as (https://student.unsw.edu.au/plagiarism) using the words or ideas of others and presenting them as your own. UNSW and CSE treat plagiarism as academic misconduct, which means that it carries penalties as severe as being excluded from further study at UNSW. There are several on-line sources to help you understand what plagiarism is and how it is dealt with at UNSW:

- Plagiarism and Academic Integrity (https://student.unsw.edu.au/plagiarism)
- UNSW Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

Make sure that you read and understand these. Ignorance is not accepted as an excuse for plagiarism. In particular, you are also responsible that your assignment files are not accessible by anyone but you by setting the correct permissions in your CSE directory and code repository, if using. Note also that plagiarism includes paying or asking another person to do a piece of work for you and then submitting it as your own work.

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. Plagiarism undermines academic integrity and is not tolerated at UNSW. Plagiarism at UNSW is defined as using the words or ideas of others and passing them off as your own.

If you haven't done so yet, please take the time to read the full text of

- UNSW's policy regarding academic honesty and plagiarism (https://student.unsw.edu.au/plagiarism)

The pages below describe the policies and procedures in more detail:

- Student Code Policy (https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf)
- Student Misconduct Procedure (https://www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf)
- Plagiarism Policy Statement (https://www.gs.unsw.edu.au/policy/documents/plagiarismpolicy.pdf)
- Plagiarism Procedure (https://www.gs.unsw.edu.au/policy/documents/plagiarismprocedure.pdf)

You should also read the following page which describes your rights and responsibilities in the CSE context:

- Essential Advice for CSE Students (https://www.engineering.unsw.edu.au/computer-science-engineering/about-us/organisational-structure/student-services/policies/essential-advice-for-cse-students)

Good Faith Policy

This course has a "Good Faith Policy". This means we expect you to act in good faith at all times. We expect you to be a good citizen. To not invade, alter or damage the property of others including the university, invade the privacy of others, break any laws or regulations, annoy other people, deprive others of access to resources, breach or weaken the security of any system, or do or omit to do anything else which you know or suspect we would not be happy about. Furthermore you are not to do anything which appears OK by a loophole or a strict interpretation of "the letter of the law" but which is not consistent with the spirit. Basically you must not act in any way so as to bring disrepute to the reputation of the course, the course staff, fellow students, the school, the university, or the ICT profession. Also, don't be a dick.

If you are unsure, ask!

If, in our sole discretion, we feel you have violated the Good Faith Policy you will be awarded 0 Fail for the course. Further penalties may apply also depending on the nature and severity of the violation. Students who have violated the Good Faith Policy may not be permitted to re-enrol in future offerings of the course.

Students who are found (or who have previously been found and have not disclosed this) guilty of academic or computer related misconduct or any other activity in a way which which casts doubt on their ability or willingness to comply with the Good Faith Policy will be dis-enrolled and will be not permitted to re-enroll in future offerings of the course. If you have ever been found guilty of such an activity you must disclose it to the lecturer in writing immediately.

Assessment

Item	Topics	Due	Marks
Mini Exam	Weeks 1 to 4	Week 5	10%
Wargames - Practical homework assignments	Various	Week 13	20%
Assignment	Kernel/Rootkits	Week 11	30%
Final Exam	See notes	Exam period	40%

Exam and overall course marks may be scaled to ensure a consistent standard from session to session.

If you do not pass the invigilated final exam your final mark for the course will be capped at your exam mark.

All in-semester marks must be finalised by the end of stuvac. If you think there is a problem with any of your marks then you need to advise us by emailing the course administrator within two weeks of the mark being released, and, in all cases before the end of stuvac. No in-semester marks will be changed after the end of stuvac.

Supplementary Exam

A supplementary examination will be held soon after the results have been released. If you think that you may be eligible for the Supplementary Examination, make sure you are available around that time. Be careful not to plan any overseas travel at that time. If you can't attend the sup exam you will not be offered a second chance. WE CAN ONLY RUN ONE SUP EXAM.

It is your responsibility to check your email, the CSE website, and to contact the CSE student office for details of Supplementary Examinations. If you think there is any chance you might be eligible for a Supplementary Exam then you should prepare for it. Requests such as "I didn't find out until the day before the sup exam that I could sit the sup exam, so I need more time to study" or "I have to go overseas at that time and I have already purchased the tickets so can you write and administer a special sup exam just for me" will not be granted.

Course Schedule

Week	Lectures	Assignments	Wargames	Notes
1	How computers work History of Hacking	-	-	-
2	Unix/Priv Esc	-	-	-
3	Reversing Intro to exploitations	-	Wargame 1	-
4	Reversing continued	-	-	-
5	Midsem Exam	-	Wargame 2	-
6	Source Code Auditing	-	-	-
7	Kernel/Rootkit	Assignment Released	Wargame 3	-
8	Fuzzing	-	Wargame 4	Not examinable
9	Malware	Assignment Check In 1		Not examinable
Midsem Break	Possible revision	-	-	-
10	Windows	Assignment Check In 2	-	Not examinable
11	Google Guest Speaker	-	-	Not examinable
12	Wireless/Mobile	Assignment Check In 3	-	Not examinable
13	TBA	-	-	-

Resources for Students

Textbook

- Designing BSD Rootkits

Reference Books

- The Art of Software Security Assessment Vol 1 and 2
- Shellcoder's Handbook
- Hacking- The Art of Exploitation

Course Evaluation and Development

This course is still relatively new, and we strongly encourage students to actively provide feedback about the course's progress.

This course will be evaluated by UNSW's myExperience program. You'll receive an email to your student email address with instructions on completing this; we'll also (endeavour to) send out a notification.

This course will also be evaluated by the CSE Student Representatives' mid-session Course Survey.

Resource created 3 years ago (Monday 16 July 2018, 04:16:54 PM), last modified 3 years ago (Wednesday 08 August 2018, 04:53:15 PM).