UNSW Course Outline

COMP6447 System and Software Security Assessment - 2024

Published on the 04 Sep 2024

General Course Information

Course Code : COMP6447
Year : 2024
Term : Term 3
Teaching Period : T3
Is a multi-term course? : No
Faculty : Faculty of Engineering
Academic Unit : School of Computer Science and Engineering
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : Kensington
Campus : Sydney
Study Level : Postgraduate, Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

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 wargames, 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 course 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.

Students need a keen, devious and analytical mind.

To get the most from this course 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 15 hours per week in total on this course.

Seek feedback from your friendly lecturers, tutors and class peers constantly over the term and closely monitor yourself to make sure you are not falling behind. Experience has shown that students who do not work hard at the course do not do well, and often express disappointment later on at the missed opportunity.

Course Aims

The course aims to

- introduce students to the principal concepts in offensive cyber security
- enable students to analyse vulnerabilities in existing systems
- enable students to develop remedies to prevent exploitation of vulnerabilities

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, security bugs, memory corruption, numeric overflows, heap exploitation and return oriented programming)
CLO2 : Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures
CLO3 : Given a system, be able to identify vulnerabilities and design and implement reliable exploits
CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation
CLO5 : 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

Course Learning Outcomes	Assessment Item
CLO1 : Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, security bugs, memory corruption, numeric overflows, heap exploitation and return oriented programming)	• Wargames • Assignment • Exam
CLO2 : Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures	• Wargames • Assignment • Exam
CLO3 : Given a system, be able to identify vulnerabilities and design and implement reliable exploits	• Wargames • Assignment • Exam
CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation	• Wargames • Assignment • Exam
CLO5 : 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	• Wargames • Assignment • Exam

Learning and Teaching Technologies

WebCMS | EdStem

Learning and Teaching in this course

- **Lectures** : used to introduce students to theoretical and practical concepts and will include live demonstrations. A detailed list of lecture topics and the slides used for the lectures will be posted on the course website as session progresses.

- **Laboratories** : self-guided activities with facilitators to assist your learning.
- **Wargames** : practical exercises to consolidate learning.
- **Project** : develop and apply in-depth knowledge on particular aspect of cyber security.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Wargames Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Not Applicable
Assignment Assessment Format: Group	30%	Start Date: Week 5 Due Date: Week 10: 11 November - 17 November
Exam Assessment Format: Individual	40%	Start Date: Not Applicable Due Date: Not Applicable

Assessment Details

Wargames

Assessment Overview

Weekly practical exercises. These will vary in difficulty, and the weighting of marks assigned to each challenge will reflect this.

Course Learning Outcomes

- CLO1 : Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, security bugs, memory corruption, numeric overflows, heap exploitation and return oriented programming)
- CLO2 : Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures
- CLO3 : Given a system, be able to identify vulnerabilities and design and implement reliable exploits
- CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation
- CLO5 : 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

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

Assignment

Assessment Overview

Team project to solve a security problem using technical measures and writeup and present findings.

Marked by tutor and lecturer.

Course Learning Outcomes

- CLO1 : Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, security bugs, memory corruption, numeric overflows, heap exploitation and return oriented programming)
- CLO2 : Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures
- CLO3 : Given a system, be able to identify vulnerabilities and design and implement reliable exploits
- CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation
- CLO5 : 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

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.
For more information on Generative AI and permitted use please see here.

Exam

Assessment Overview

Exam in the UNSW exam period covering all topics in the course. Practical and theoretical. Marked by the lecturer and tutors.

Course Learning Outcomes

- CLO1 : Have a knowledge of the principle elements of offensive cyber security (such as vulnerability classes, source code auditing, security bugs, memory corruption, numeric overflows, heap exploitation and return oriented programming)
- CLO2 : Recognise and explain how these elements can be exploited by attackers, their characterising features, weaknesses and countermeasures
- CLO3 : Given a system, be able to identify vulnerabilities and design and implement reliable exploits
- CLO4 : Given a system, be able to identify vulnerabilities and design and implement reliable countermeasures to prevent successful exploitation
- CLO5 : 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

Assignment submission Turnitin type

Not Applicable

Generative AI Permission Level

No Assistance

This assessment is designed for you to complete without the use of any generative AI. You are not permitted to use any generative AI tools, software or service to search for or generate information or answers.

For more information on Generative AI and permitted use please see here.

General Assessment Information

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 0 : 2 September - 8 September	Activity	Preparation
Week 1 : 9 September - 15 September	Lecture	Memory Fundamentals History of Hacking
	Tut-Lab	Tooling Environment Setup
	Homework	Learn Tooling
Week 2 : 16 September - 22 September	Lecture	Buffer overflows Stack canaries Intro to Reverse Engineering
	Tut-Lab	Buffer overflows Stack canaries Intro to Reverse Engineering
	Homework	Buffer Overflows Stack Canaries
Week 3 : 23 September - 29 September	Lecture	Shellcode Reverse Engineering
	Tut-Lab	How to write shellcode Advanced Reverse Engineering
	Homework	Shellcode
Week 4 : 30 September - 6 October	Lecture	Format Strings Countermeasures - ASLR, PIE
	Tut-Lab	Format Strings How to defeat ASLR, PIE
	Homework	Format Strings
Week 5 : 7 October - 13 October	Lecture	Source Code Auditing Fuzzers
	Tut-Lab	Source code auditing Fuzzer assignment walkthrough
	Homework	Source Code Auditing Harder Binaries
Week 6 : 14 October - 20 October	Lecture	Review of mid-term exam
Week 7 : 21 October - 27 October	Lecture	Return Oriented Programming
	Tut-Lab	Return oriented programming
	Homework	Return oriented programming
Week 8 : 28 October - 3 November	Lecture	Heap Exploitation
	Tut-Lab	Heap Exploitation
	Homework	Heap Exploitation
Week 9 : 4 November - 10 November	Lecture	Revision
	Tut-Lab	Harder return oriented programming - pivot
	Homework	Harder Challenges
Week 10 : 11 November - 17 November	Lecture	Hacking in the Real World
	Tut-Lab	Harder ROP + Revision

Attendance Requirements

CSE Attendance Guidelines :

Students are expected to be regular and punctual in attendance at all classes for the Computer Science and Engineering courses in which they are enrolled. For lab classes and tutorials, in particular, this provides the opportunity to get assistance from the demonstrator/tutor. Students who do not attend classes regularly run the risk of failing a course.

Course Resources

Recommended Resources

- The Art of Software Security Assessment Vol 1 and 2

- Shellcoder’s Handbook
- Hacking - The Art of Exploitation
- Practical Malware Analysis

Course Evaluation and Development

Every term, student feedback is requested in a survey using UNSW's myExperience online survey system where the feedback will be used to make improvements to the course.

Students are also encouraged to provide informal feedback during the session, and to let course staff know of any problems as soon as they arise. Other possible contacts including the School Grievance officer or one of the student representatives. Suggestions will be listened to openly, positively, constructively, and thankfully, and every reasonable effort will be made to address them.

Feedback from last offering indicates that students wanted more time in the beginning of the course to learn tooling, so we have allocated more time to it this term.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Lecturer	Adam Tanana					Yes	Yes
Administrator	Kristin Smith					No	No
Head tutor	Lachlan Waugh					No	No

Other Useful Information

Academic Information

I. Special consideration and supplementary assessment

If you have experienced an illness or misadventure beyond your control that will interfere with your assessment performance, you are eligible to apply for Special Consideration prior to, or within 3 working days of, submitting an assessment or sitting an exam.

Please note that UNSW has a Fit to Sit rule, which means that if you sit an exam, you are declaring yourself fit enough to do so and cannot later apply for Special Consideration.

For details of applying for Special Consideration and conditions for the award of supplementary assessment, please see the information on UNSW's Special Consideration page.

II. Administrative matters and links

All students are expected to read and be familiar with UNSW guidelines and polices. In particular, students should be familiar with the following:

- Attendance
- UNSW Email Address
- Special Consideration
- Exams
- Approved Calculators
- Academic Honesty and Plagiarism
- Equitable Learning Services

III. Equity and diversity

Those students who have a disability that requires some adjustment in their teaching or learning environment are encouraged to discuss their study needs with the course convener prior to, or at the commencement of, their course, or with the Equity Officer (Disability) in the Equitable Learning Services. Issues to be discussed may include access to materials, signers or note-takers, the provision of services and additional exam and assessment arrangements. Early notification is essential to enable any necessary adjustments to be made.

IV. Professional Outcomes and Program Design

Students are able to review the relevant professional outcomes and program designs for their streams by going to the following link: https://www.unsw.edu.au/engineering/student-life/student-resources/program-design.

Note: This course outline sets out the description of classes at the date the Course Outline is published. The nature of classes may change during the Term after the Course Outline is published. Moodle or your primary learning management system (LMS) should be consulted for the up-to-date class descriptions. If there is any inconsistency in the description of activities between the University timetable and the Course Outline/Moodle/LMS, the description in the Course Outline/Moodle/LMS applies.

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW 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.*

Plagiarism is a type of intellectual theft. It can take many forms, from deliberate cheating to accidentally copying from a source without acknowledgement. UNSW has produced a website with a wealth of resources to support students to understand and avoid plagiarism, visit: student.unsw.edu.au/plagiarism. The Learning Centre assists students with understanding academic integrity and how not to plagiarise. They also hold workshops and can help students one-on-one.

You are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting and the proper referencing of sources in preparing all assessment tasks.

Repeated plagiarism (even in first year), plagiarism after first year, or serious instances, may also be investigated under the Student Misconduct Procedures. The penalties under the procedures can include a reduction in marks, failing a course or for the most serious matters (like plagiarism in an honours thesis or contract cheating) even suspension from the university. The Student Misconduct Procedures are available here:

www.gs.unsw.edu.au/policy/documents/studentmisconductprocedures.pdf

Submission of Assessment Tasks

Work submitted late without an approved extension by the course coordinator or delegated authority is subject to a late penalty of five percent (5%) of the maximum mark possible for that assessment item, per calendar day.

The late penalty is applied per calendar day (including weekends and public holidays) that the assessment is overdue. There is no pro-rata of the late penalty for submissions made part way through a day. This is for all assessments where a penalty applies.

Work submitted after five days (120 hours) will not be accepted and a mark of zero will be awarded for that assessment item.

For some assessment items, a late penalty may not be appropriate. These will be clearly indicated in the course outline, and such assessments will receive a mark of zero if not completed by the specified date. Examples include:

- Weekly online tests or laboratory work worth a small proportion of the subject mark;
- Exams, peer feedback and team evaluation surveys;
- Online quizzes where answers are released to students on completion;
- Professional assessment tasks, where the intention is to create an authentic assessment that has an absolute submission date; and,
- Pass/Fail assessment tasks.

Faculty-specific Information

Engineering Student Support Services – The Nucleus - enrolment, progression checks, clash requests, course issues or program-related queries

Engineering Industrial Training – Industrial training questions

UNSW Study Abroad – study abroad student enquiries (for inbound students)

UNSW Exchange – student exchange enquiries (for inbound students)

UNSW Future Students – potential student enquiries e.g. admissions, fees, programs, credit transfer

Phone

(+61 2) 9385 8500 – Nucleus Student Hub

(+61 2) 9385 7661 – Engineering Industrial Training

(+61 2) 9385 3179 – UNSW Study Abroad and UNSW Exchange (for inbound students)

School Contact Information

CSE Help! - on the Ground Floor of K17

- For assistance with coursework assessments.

The Nucleus Student Hub - https://nucleus.unsw.edu.au/en/contact-us

- Course enrolment queries.

Grievance Officer - grievance-officer@cse.unsw.edu.au

- If the course convenor gives an inadequate response to a query or when the courses convenor does not respond to a query about assessment.

Student Reps - stureps@cse.unsw.edu.au

- If some aspect of a course needs urgent improvement. (e.g. Nobody responding to forum queries, cannot understand the lecturer)

You should **never** contact any of the following people directly:

- Vice Chancellor

- Pro-vice Chancellor Education (PVCE)

- Head of School

- CSE administrative staff

- CSE teaching support staff

They will simply bounce the email to one of the above, thereby creating an unnecessary level of indirection and a delay in the response.