UNSW Course Outline

ZZCA9205 Cyber Operations - 2024

Published on the 04 Jan 2024

General Course Information

Course Code : ZZCA9205
Year : 2024
Term : Hexamester 1
Teaching Period : KB
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : Canberra School of Professional Studies
Delivery Mode : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : Canberra City
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course provides students with theoretical framework and technical skills for securing modern networks against attack. The course provides an overview of modern attacks and modern defensive measures and tools, including strengths and limitations. The course has a practical focus and will equip students with technical skills needed to design and secure modern

networks.

Course Aims

This course equips students for handling data in secure ways, understanding the nature and principles of privacy, and how to securely identify manage and respond to privacy risks across large datasets and current best practice in a changing global environment.

Relationship to Other Courses

ZZEN9201 is an enrolment requirement for this course.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Explain the fundamentals of defensive network security mechanisms and how to effetely deploy, operate, and assure them.
CLO2 : Design network and host based defensive systems for large and small organisations in order to detect malicious actors, in accordance with best-practice.
CLO3 : Explain the role of the human in defending networks, systems, and cyber assets.
CLO4 : Apply current security frameworks and and best-practice to assure the security of legacy and emerging technologies.
CLO5 : Provide advice and briefings on defensive technologies, processes, and cyber-threats to both technical and non-technical stakeholders.

Course Learning Outcomes	Assessment Item
CLO1 : Explain the fundamentals of defensive network security mechanisms and how to effetely deploy, operate, and assure them.	• Laboratory Exercises • Reflective Portfolio
CLO2 : Design network and host based defensive systems for large and small organisations in order to detect malicious actors, in accordance with best-practice.	• Laboratory Exercises • Reflective Portfolio
CLO3 : Explain the role of the human in defending networks, systems, and cyber assets.	• Report and presentation • Laboratory Exercises • Reflective Portfolio
CLO4 : Apply current security frameworks and and best-practice to assure the security of legacy and emerging technologies.	• Laboratory Exercises • Reflective Portfolio
CLO5 : Provide advice and briefings on defensive technologies, processes, and cyber-threats to both technical and non-technical stakeholders.	• Report and presentation • Laboratory Exercises • Reflective Portfolio

Learning and Teaching Technologies

Moodle - Learning Management System | Blackboard Collaborate | Skillable

Learning and Teaching in this course

The course contains a variety of resources and activities that are carefully designed to enhance your learning.
Some activities require you to work and think alone, by reading some text, listening to a recording or watching
a video. You might be asked to engage with the material and explore interactive elements by clicking to reveal
content, to help you better absorb and process the concepts. Some activities require you to produce work of
your own. You might be answering a question, writing code to solve a problem, or posting to a forum, for
example. Some activities are assessment tasks, which have been carefully designed to measure how well
you have achieved the learning outcomes of the course. Typically, you will get feedback on your work, either
from yourself (by checking your work with models that are provided), or from an automatic marking process,
or from your peers, or from your teacher.

You also have access to a variety of ways to communicate with your peers and with the teaching staff. The
general discussion forums are a place for you to ask and answer questions, to interact with your peers, and
to be challenged by your teachers. Getting involved in these forums will enhance your learning experience
and make it more enjoyable. Your course may include Webinars, which provide an opportunity to hear directly
from your Online Lecturers and ask questions in real time. All webinars are recorded so you can access them
at any time. Online Lecturers are available for consultations and will post information about how to access

consultations on the course website. You can also contact your Online Lecturer by email using the email
address in the teaching staff section of this outline.

It is up to you how much work you do. The more time and effort that you can dedicate to the course, the
better will be your learning and your results.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Laboratory Exercises Assessment Format: Individual	35%	Start Date: Not Applicable Due Date: Monday Week 3 (Lab 1); Tuesday Week 6 (Lab 2), 12:00pm Sydney time
Reflective Portfolio Assessment Format: Individual	30%	Start Date: Not Applicable Due Date: Week 2 (Portfolio 1) and Week 5 (Portfolio 2), Monday 12:00pm Sydney time
Report and presentation Assessment Format: Individual	35%	Start Date: Not Applicable Due Date: Week 7, Monday 12:00pm Sydney time

Assessment Details

Laboratory Exercises

Assessment Overview

Labs are designed to give you hands-on, practical experience. It's one thing to hear about the process, and another to try it. We are aiming to provide a safe zone for experimentation. Each activity will respond to topics covered in that week and will be helpful in consolidating the ideas explored.

Course Learning Outcomes

- CLO1 : Explain the fundamentals of defensive network security mechanisms and how to effetely deploy, operate, and assure them.
- CLO2 : Design network and host based defensive systems for large and small organisations in order to detect malicious actors, in accordance with best-practice.
- CLO3 : Explain the role of the human in defending networks, systems, and cyber assets.
- CLO4 : Apply current security frameworks and and best-practice to assure the security of legacy and emerging technologies.
- CLO5 : Provide advice and briefings on defensive technologies, processes, and cyber-threats

to both technical and non-technical stakeholders.

Detailed Assessment Description

- This assessment is submitted in two parts.
- Lab 1 is due in Week 3.
- Lab 2 is due in Week 6.
- See Moodle for more detail.

Reflective Portfolio

Assessment Overview

Portfolios represent an exploration of areas related to this course, that are personal or will require to take a professional stance as a cyber security professional.

Course Learning Outcomes

- CLO1 : Explain the fundamentals of defensive network security mechanisms and how to effetely deploy, operate, and assure them.
- CLO2 : Design network and host based defensive systems for large and small organisations in order to detect malicious actors, in accordance with best-practice.
- CLO3 : Explain the role of the human in defending networks, systems, and cyber assets.
- CLO4 : Apply current security frameworks and and best-practice to assure the security of legacy and emerging technologies.
- CLO5 : Provide advice and briefings on defensive technologies, processes, and cyber-threats to both technical and non-technical stakeholders.

Detailed Assessment Description

- This assessment is submitted in two parts.
- Portfolio 1 is due in Week 2.
- Portfolio 2 is due in Week 5.
- See Moodle for more detail.

Assessment Length

Portfolio 1: 600, Portfolio 2: 900

Report and presentation

Assessment Overview

This assessment has two options. Firstly, a report relating to the course topic and a video presentation. Secondly, a smaller report and associated code, again with an associated video presentation.

Course Learning Outcomes

- CLO3 : Explain the role of the human in defending networks, systems, and cyber assets.
- CLO5 : Provide advice and briefings on defensive technologies, processes, and cyber-threats

to both technical and non-technical stakeholders.

Assessment Length

2,500 words + 5 minute presentation or code + 1000 words + 5 minute presentation

General Assessment Information

Generative AI Statement:

UNSW accepts the potential of these tools and is excited to explore ways to use Generative AI (GenAI) to enrich your learning experience while maintaining the integrity of our programs and, therefore, of your degrees. We expect that, as we learn about how best to do this, our policies will adapt. For advice and guidance on how to use GenAI please see the Generative AI Statement in Moodle, or refer to the Universities resources: Chat GPT & Generative AI at UNSW | UNSW Current Students.

There are three key principles across the university:

1. Always do what you are asked to do in the assessment; if you don't follow the instructions, you can't get marks.
2. If you are asked to do your own work, then that is what you should do, as we want to see that *you* have undertaken that learning rather than someone or something else.
3. When you incorporate ideas that are not your own, you should always acknowledge them. That applies in the world of AI, just as it did before.

In ***this course,*** the permitted level of GenAI use is '***Drafting Assistance***'.

What is Drafting Assistance?

As this course's assessment tasks involve some planning or creative processes, you are permitted to use software to generate initial drafts, ideas, structures, etc. However, you must develop or edit those ideas to such a significant extent that what is submitted is your own work, i.e., what is generated by the software should not be a part of your final submission. It is a good idea to keep copies of your initial drafts to show your lecturer if there is any uncertainty about the originality of your work.

Please note that your submission will be passed through an AI-text detection tool. If your marker has concerns that your answer contains passages of AI-generated text that have not been sufficiently modified, you may be asked to explain your work, but we recognise that you are permitted to use AI-generated text as a starting point, and some traces may remain. If you are

unable to satisfactorily demonstrate your understanding of your submission, you may be referred to the UNSW Conduct & Integrity Office for investigation for academic misconduct and possible penalties.

Assessment Tolerances:

Assessment submissions have a tolerance of +/- 10% for length, meaning your submission length can go over or under the word or time limit by 10%. For example:

- A written assessment that has a 1,000-word limit can be between 900 and 1,100 words without penalty.
- An audio or video assessment that has a 10-minute time limit can be between 9 and 11 minutes without penalty.

Grading Basis

Standard

Requirements to pass course

In order to pass the course you must achieve an overall mark of at least 50%.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 January - 21 January	Online Activity	Cyber defence foundations
Week 2 : 22 January - 28 January	Online Activity	Risk assessment and threat modelling
Week 3 : 29 January - 4 February	Online Activity	Defense technologies
Week 4 : 5 February - 11 February	Online Activity	Security operations centres and SecOps
Week 5 : 12 February - 18 February	Online Activity	Incident response
Week 6 : 19 February - 25 February	Online Activity	Machine learning and future technologies in cyber defense

Attendance Requirements

Not Applicable - as no class attendance is required

Course Resources

Prescribed Resources

All resources required to complete this course are available via Moodle.

Recommended Resources

Students have access to a number of additional support resources.

Please check your Moodle page for additional readings and advice relevant to the course.

Course Evaluation and Development

Evaluation and Development

Toward the end of the hexamester you will be asked to give feedback about the course, via UNSW's MyExperience survey. Your feedback will be used, along with feedback from other stakeholders, to help improve the course. You can also contact your Course Convenor any time you have suggestions or other feedback.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct Policy: https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Quality Assurance

UNSW actively monitors student learning and quality of the student experience in its programs. A random selection of completed assessment tasks may be used for quality assurance, such as determining the extent to which program learning goals are being achieved. The information is required for accreditation purposes, and aggregated findings will be used to inform changes aimed at improving the quality of programs. All material used for such processes will be treated as confidential.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Travis Quinn					No	Yes
Postgraduate coordinator	Tom Townsend					No	No

Other Useful Information

School-specific Information

ACADEMIC INFORMATION

Course Policies and Support

The Canberra School of Professional Studies expects students to be familiar with the contents of course outlines and UNSW's learning expectations, rules, policies and support services as listed

below.

- Academic Integrity and Plagiarism
- Student Responsibilities and Conduct
- Special Consideration
- Cyber Security - Policies and Standards
- Cyber Security Policy
- Acceptable use of Information Resources Policy
- Use of AI for Assessments

Student Learning Outcomes

Course Learning Outcomes (CLOs) are competencies you should be able to demonstrate by the end of this course, if you participate fully in learning activities and successfully complete all assessment items.

CLOs contribute to the achievement of the Program Learning Outcomes (PLOs), which are developed across the duration of a program. PLOs are, in turn, directly linked to the UNSW graduate capabilities.

ACADEMIC HONESTY AND PLAGIARISM

As a student of UNSW you are expected to display academic integrity in your work interactions. Where a student breaches the UNSW Student Code with respect to academic integrity, the University may take disciplinary action under the Student Misconduct procedure. To assure academic integrity, you may be required to demonstrate reasoning, research and the process of constructing work submitted for assessment.

To assist you in understanding what academic integrity means, and how to ensure that you do comply with the UNSW Student Code, it is strongly recommended that you enrol in and complete the Working with Academic Integrity module before submitting your first assessment task. It is a free, online, self-paced Moodle module that should take no more than one hour to complete.

SUBMISSION OF ASSESSMENT TASKS

Special Consideration

Students can apply for special consideration when illness or other circumstances beyond your control interfere with your performance in a specific assessment task or tasks, including online exams.

Special consideration is primarily intended to provide you with an extra opportunity to demonstrate the level of performance of which you are capable. To apply, and for further information, see Special Consideration on the UNSW Current Students page.

Special considerations will be assessed centrally by the Case Review Team, who will update the online application with the outcome and add any relevant comments. The change to the status of the application immediately sends an email to the student and to the assessor with the outcome of the application.

Please note the following:

1. Applications can only be made through Online Services in myUNSW (see the UNSW Current Students page). Applications will not be accepted by teaching staff. The course convenor will be automatically notified when your application is processed.
2. Applying for special consideration does not automatically mean that you will be granted a supplementary exam or other concession.
3. If you experience illness or misadventure in the lead up to an exam or assessment, you must submit an application for special consideration, either prior to the examination taking place or prior to the assessment submission deadline, except where illness or misadventure prevent you from doing so.
4. If your circumstances stop you from applying before your exam or assessment due date, you must apply within 3 working days of the assessment, or the period covered by your supporting documentation.
5. Under the UNSW Fit to Sit/Submit rule, if you sit the exam/submit an assignment, you are declaring yourself well enough to do so and cannot subsequently apply for special consideration.
6. If you become unwell on the day of - or during - an exam, you must stop working on your exam, advise your course convenor or tutor and provide a medical certificate dated within 24 hours of the exam, with your special consideration application. For online exams, you must contact your course convenor or tutor immediately via email, Moodle and advise them you are unwell and submit screenshots of your conversation along with your medical certificate and application.
7. Special consideration requests do not allow the awarding of additional marks to students.

Late Submission Penalties

For assessments other than examinations. late submission will normally incur a penalty of 5% per day or part thereof (including weekends) from the due date and time. An assessment will not be accepted after 5 days (120 hours) of the original deadline unless special consideration has been approved. An assignment is considered late if the requested format, such as hard copy or

electronic copy, has not been submitted on time or where the 'wrong' assignment has been submitted.

For assessments which account for 10% or less of the overall course grade, and where answers are immediately discussed or debriefed, course convenor may stipulate a different penalty. Details of such late penalties will be available on the course Moodle page.

Feedback on Your Assessment Task Performance

Feedback on student performance from formative and summative assesment tasks will be provided to students in a timely manner. Assessment tasks completed within the teaching period of a course, other than the final assessment, will be assesed and students provided with feedback, with or without a provisional result, within 10 working days of submission, under normal circumstances. Feedback on continuous assessment tasks e.g., laboratory and studio-based, workplace-based, weekly quizzes etc. will be provided prior to the mid-point of the course.

School Contact Information

Academic enquiries

Email : canberrasps@canberra.unsw.edu.au

Phone: 02 5114 5369