UNSW Course Outline

ZEIT2104 Computers and Security - 2024

Published on the 08 Feb 2024

General Course Information

Course Code : ZEIT2104
Year : 2024
Term : Semester 1
Teaching Period : Z1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : School of Systems and Computing
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

A large part of the course deals with various details of cyber offensive and defensive principles, following the cyber kill chain methodology. In the context of these principles of cyber operations, students will learn about the legal and ethical aspects of being a cyber professional in the industry or the military, risk assessment and incident response strategies that can be taken, developments in cryptography, and the intricacies of wireless network security. Via hands-on experience in labs, students will become familiar with some of the most relevant cyber security tools and techniques.

Course Aims

This course provides basic technical and theoretical underpinnings of cyber security.

Relationship to Other Courses

It is expected that participants have completed and understood ZINT2100 (Introduction to Cyber Security) and ZEIT1110 (Computer Games) or equivalent. Technical and theoretical concepts which are treated superficially in ZINT2100 are treated in much more depth in ZEIT2104.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : On successful completion of this course, students will be able to: Comprehend, from a technical perspective, how today's computer networks work (including hardware, physical layer, link layer, wireless, and network control such as DNS), how cyber-attacks occur in such networks, and the data and information management technologies used to prevent, detect, or minimise these attacks.
CLO2 : On successful completion of this course, students will be able to: Apply basic tools, techniques, and tactics (such as network scanning) used by adversaries to attack simple insecure computer networks, to understand how they have been employed and what their limitations are.
CLO3 : On successful completion of this course, students will be able to: Comprehend fundamental theoretical cyber-security underpinnings.
CLO4 : On successful completion of this course, students will be able to: Analyse real-world problems of today, apply theoretical cyber-security knowledge to these problems, and show understanding of the role of the cyber professional in these problems, including possible ethical constraints.

Course Learning Outcomes	Assessment Item
CLO1 : On successful completion of this course, students will be able to: Comprehend, from a technical perspective, how today's computer networks work (including hardware, physical layer, link layer, wireless, and network control such as DNS), how cyber-attacks occur in such networks, and the data and information management technologies used to prevent, detect, or minimise these attacks.	• Networking Test • Lab Reports • Written Exam
CLO2 : On successful completion of this course, students will be able to: Apply basic tools, techniques, and tactics (such as network scanning) used by adversaries to attack simple insecure computer networks, to understand how they have been employed and what their limitations are.	• Lab Reports • Written Exam
CLO3 : On successful completion of this course, students will be able to: Comprehend fundamental theoretical cyber-security underpinnings.	• Lab Reports • Written Exam
CLO4 : On successful completion of this course, students will be able to: Analyse real-world problems of today, apply theoretical cyber-security knowledge to these problems, and show understanding of the role of the cyber professional in these problems, including possible ethical constraints.	• Legal and Ethical Test • Written Exam

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

The course is delivered face-to-face, as a combination of lecturing, extended and consolidated with practical laboratory exercises to be undertaken by students under the supervision of the lecturers. It employs a Constructionist learning theory and has a strong focus on reinforcing theoretical concepts with practical implementation. The theoretical components of the course support learning outcomes LO1 and LO3. The labs support LO1-3. In combining theory with practice, the student achieves LO4.

Other Professional Outcomes

Program Learning Outcomes

The student Learning Outcomes contribute to the following Program Learning Outcomes of the Bachelor of Computing and Cyber Security program. On completion of this program, graduates will be able to:

PLO3. Work in a productive, ethical, and professional manner – either independently or in teams – applying life-long learning to remain contemporary and competent in the ICT discipline. (LO4)

PLO7. Articulate the theoretical underpinnings of information confidentiality, integrity, and availability, including human aspects, organisational aspects, regulatory aspects, properties of attacks and defence, systems security, software and platform security, infrastructure security, and standards. (LO1, LO3)

PLO8. Provide comprehensive security in existing and new network architectures through the intelligent placement of multiple defensive and offensive security controls and systems, based on the different threat profiles faced and the different protections and limitations posed by each. (LO2, LO4)

PLO9. Develop software with appropriate security controls, security implementations, and testing frameworks, implement and configure cyber defensive and offensive technologies, and conduct basic network risk assessments, all in accordance with current best practices and in professional collaboration

Learning Outcomes can be found online here.

Additional Course Information

A large part of the course deals with various details of cyber offensive and defensive principles, following the cyber kill chain methodology. In the context of these principles of cyber operations, students will learn about the legal and ethical aspects of being a cyber professional in the industry or the military, risk assessment and incident response strategies that can be taken, developments in cryptography, and the intricacies of wireless network security. Via hands-on experience in labs, students will become familiar with some of the most relevant cyber security tools and techniques.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Legal and Ethical Test Assessment Format: Individual	6%	Due Date: Week 2: 04 March - 08 March
Networking Test Assessment Format: Individual	10%	Start Date: Week 4 Due Date: Week 4: 18 March - 22 March
Lab Reports Assessment Format: Individual	42%	Start Date: Not Applicable Due Date: Not Applicable
Written Exam Assessment Format: Individual	42%	Start Date: Not Applicable Due Date: Not Applicable

Assessment Details

Legal and Ethical Test

Assessment Overview

Early in the course, students have to take an online quiz on Moodle, testing their knowledge on legal and ethical aspects of conducting cyber operations. Students must pass the test before they are allowed to conduct labs on the Cyber Range.

Course Learning Outcomes

- CLO4 : On successful completion of this course, students will be able to: Analyse real-world problems of today, apply theoretical cyber-security knowledge to these problems, and show understanding of the role of the cyber professional in these problems, including possible ethical constraints.

Detailed Assessment Description

The quiz will be held in week 2. The marks will be released by the end of the week.

Assignment submission Turnitin type

Not Applicable

Networking Test

Assessment Overview

Having an adequate grasp of computer networking is crucial for comprehending both computers and security in numerous aspects. After attending a lecture and a lab session on networking, students are required to take an online quiz on Moodle to evaluate their understanding of the topic. This is a necessary step towards completing the remaining labs.

Course Learning Outcomes

- CLO1 : On successful completion of this course, students will be able to: Comprehend, from a technical perspective, how today’s computer networks work (including hardware, physical layer, link layer, wireless, and network control such as DNS), how cyber-attacks occur in such networks, and the data and information management technologies used to prevent, detect, or minimise these attacks.

Detailed Assessment Description

The quiz will be held in week 4 in the class. The details will be announced later. Marks will be ready by week 5.

Assessment information

In-class online quiz.

Assignment submission Turnitin type

Not Applicable

Lab Reports

Assessment Overview

There will be 7 labs taken during the course. Lab manuals will be provided in hardcopy and online on Moodle. The lab manuals contain questions which students need to answer in individual lab reports, to be submitted via Moodle within 5 working days after the lab dates. The lab reports are assessed on correctness of the answers and additional showing of understanding.

Course Learning Outcomes

- CLO1 : On successful completion of this course, students will be able to: Comprehend, from a technical perspective, how today’s computer networks work (including hardware, physical layer, link layer, wireless, and network control such as DNS), how cyber-attacks occur in such networks, and the data and information management technologies used to prevent, detect, or minimise these attacks.

- CLO2 : On successful completion of this course, students will be able to: Apply basic tools, techniques, and tactics (such as network scanning) used by adversaries to attack simple insecure computer networks, to understand how they have been employed and what their limitations are.
- CLO3 : On successful completion of this course, students will be able to: Comprehend fundamental theoretical cyber-security underpinnings.

Detailed Assessment Description

The submission deadline for each lab is 5 working days after the lab. Holidays and mid-semester break are not counted as working days. Labs are scheduled in advance as follows, any changes will be communicated on Moodle.

Lab 1 on Tuesday 5 March

Lab 2 on Tuesday 12 March

Lab 3 on Tuesday 19 March

Lab 4 on Tuesday 2 April

Lab 5 on Tuesday 23 April

Lab 6 (group 1) on Tuesday 7 May

Lab 6 (group 2) on Tuesday 11 May

Lab 7 on Tuesday 21 May

Assignment submission Turnitin type

This is not a Turnitin assignment

Written Exam

Assessment Overview

The written exam is a comprehensive test on knowledge and understanding of the course material. It consists of short-answer, medium-answer, and long-answer open questions. It covers the lectures (slides and notes), the additional compulsory readings, as well as what has been learned from the labs.

Course Learning Outcomes

- CLO1 : On successful completion of this course, students will be able to: Comprehend, from a

technical perspective, how today’s computer networks work (including hardware, physical layer, link layer, wireless, and network control such as DNS), how cyber-attacks occur in such networks, and the data and information management technologies used to prevent, detect, or minimise these attacks.
- CLO2 : On successful completion of this course, students will be able to: Apply basic tools, techniques, and tactics (such as network scanning) used by adversaries to attack simple insecure computer networks, to understand how they have been employed and what their limitations are.
- CLO3 : On successful completion of this course, students will be able to: Comprehend fundamental theoretical cyber-security underpinnings.
- CLO4 : On successful completion of this course, students will be able to: Analyse real-world problems of today, apply theoretical cyber-security knowledge to these problems, and show understanding of the role of the cyber professional in these problems, including possible ethical constraints.

Detailed Assessment Description

The written exam (final exam) will be scheduled in the exam period. Details will be announced later.

Assignment submission Turnitin type

Not Applicable

General Assessment Information

Assessment Requirements

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is **the only official mark.**

The course has 4 summative assessment tasks:

1) The course contains 7 Labs. Lab manuals will be provided online on Moodle. The lab manuals contain questions that students need to answer in individual lab reports, to be submitted via Moodle within 5 working days after the final lab dates. The lab reports are assessed on the correctness of the answers and additional showing of understanding.

2) The networking test which will be held in class but using Moodle after students have networking lecture and lab.

3) Students have to take an online quiz on Moodle, testing their knowledge on legal and ethical aspects of conducting cyber operations.

4) The exam is an open-book comprehensive test on knowledge and understanding of the course material. It covers the lectures (slides and notes), the additional compulsory readings, as well as what has been learned from the labs.

Grading Basis

Standard

Requirements to pass course

Students are not required to pass any one particular piece of assessment; they simply need to achieve at least 50 marks out of a total 100 marks to pass this course.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Lecture	Lecture on Friday 1 March: Introduction; Information Operations; Attack Lifecycle; Law and Ethics
Week 2 : 4 March - 8 March	Lecture	Lecture on Friday 8 March: Computer Networking, including hardware, physical layer, link layer, wireless, and network control such as DNS.
	Laboratory	Lab 1 on Tuesday 5 March: Introduction to Kali Linux
	Assessment	Legal & Ethics quiz. Details: TBA
Week 3 : 11 March - 15 March	Lecture	Lecture on Friday 15 March: Threat Modelling; Access Control; Tools, Techniques, and Procedures (TTP)
	Laboratory	Lab 2 on Tuesday 12 March: Recon: Network scanning (including Wireshark, ARP scanning, nmap, HTTP
Week 4 : 18 March - 22 March	Lecture	Lecture on Friday 22 March: Recon: Weaponisation; Delivery
	Laboratory	Lab 3 on Tuesday 19 March: Comprehensive analysis tools such as OpenVAS, and basic Recon, Weaponization, Delivery, Exploit, and Action on Objectives using Metasploit
	Assessment	The networking test will be held in this week. The details will be announced later.
Week 5 : 25 March - 29 March	Lecture	Lecture on Tuesday 26 March: Exploitation, Installation (no lab this week)
Week 6 : 1 April - 5 April	Lecture	Lecture on Friday 5 April: Command & Control; Actions on Objectives
	Laboratory	Lab 4 on Tuesday 2 April: Exploit, Action, Pivot, Obfuscate, Privilege Escalation.
Week 7 : 22 April - 26 April	Lecture	Lecture on Friday 26 April: Information flow models: risk assessment.
	Laboratory	Lab 5 on Tuesday 23 April: Advanced attacks: zero-day vulnerabilities and multiple tools in concertation.
Week 8 : 29 April - 3 May	Lecture	Lecture on Friday 3 May: Introduction to Wi-Fi; Wi-Fi security
	Tutorial	Tutorial on Tuesday 30 April (optional)
Week 9 : 6 May - 10 May	Laboratory	Lab 6 (group 1) on Tuesday 7 May: Wi-Fi Security
Week 10 : 13 May - 17 May	Lecture	Lecture on Friday 17 May: Cryptography
	Laboratory	Lab 6 (group 2) on Tuesday 11 May: Wi-Fi Security
Week 11 : 20 May - 24 May	Lecture	Lecture on Friday 24 May: Incident Response; Military Cyber
	Laboratory	Lab 7 on Tuesday 21 May: Actions on Objectives: Password cracking.
Week 12 : 27 May - 31 May	Lecture	Lecture on Friday 31 May: Data and information management technologies for cyber defence
Week 13 : 3 June - 7 June	Lecture	Lecture on Friday 7 June: Standardisation
	Tutorial	Tutorial on Tuesday 4 Jun (optional)

Attendance Requirements

Attendance is required for both lectures and labs. Students will record their attendance on Moodle.

Course Resources

Prescribed Resources

There is no compulsory text for this course. There are compulsory readings. These are available on the course Moodle page. Additional non-compulsory readings will also be available on the course Moodle page over the course period.

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of this course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the “On-going Student Feedback” link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups. Student opinions really do make a difference. Refer to the Moodle site for this course to see how the feedback from previous students has contributed to the course development.

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

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Sayed Amir Hoseini				I am usually available for consultation during normal working hours, please send me an email or Teams message to make an appointment.	No	Yes
Lecturer	Benjamin Turnbull		Room 205, Building 15 UNSW at the Australian Defence Force Academy Tobruk Road Campbell ACT 2612		by appointment	No	No
	Wendy Chen				by appointment	No	No

Other Useful Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the “On-going Student Feedback” link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

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.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning

Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

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. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: Student Code of Conduct (unsw.edu.au)

Plagiarism undermines academic integrity and is not tolerated at UNSW. **It** is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;
- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW ‘fit to sit or submit’ requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,
- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty, for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.

School-specific Information

The Leaning Management System

Moodle is the Learning Management System used at UNSW Canberra. All courses have a Moodle site which will become available to students at least one week before the start of semester. Please find all help and documentation (including Blackboard Collaborate) at the Moodle Support page.

UNSW Moodle supports the following web browsers:
• Google Chrome 50+
• Safari 10+
Internet Explorer is not recommended. Addons and Toolbars can affect any browser's performance.

Operating systems recommended are:
• Windows 10,
• Mac OSX Sierra,
• iPad IOS10

Further details:
Moodle System Requirements
Moodle Log In

If you need further assistance with Moodle:

For enrolment and login issues please contact:
IT Service Centre
Email: itservicecentre@unsw.edu.au
Phone: (02) 9385-1333
International: +61 2 9385 1333

For all other Moodle issues please contact:
External TELT Support

Email: externalteltsupport@unsw.edu.au

Phone: (02) 9385-3331

International: +61 2 938 53331

Opening hours:

Monday – Friday 7:30am – 9:30 pm

Saturday & Sunday 8:30 am – 4:30pm

Study at UNSW Canberra

Study at UNSW Canberra has lots of useful information regarding:

- Where to get help
- Administrative matters
- Getting your passwords set up
- How to log on to Moodle
- Accessing the Library and other areas.

UNSW Canberra Student Hub

For News and Notices, Student Services and Support, Campus Comminity, Quick Links, Important Dates and Upcoming Events

School Contact Information

Deputy Head of School (Education): Dr Erandi Hene Kankanamge

E: e.henekankanamge@adfa.edu.au

T: 02 5114 5157

Syscom Admin Support: syscom@unsw.edu.au

T: 02 5114 5284

Syscom Admin Office: Building 15, Level 1, Room 101 (open 10am to 3pm, Mon to Fri)