UNSW Course Outline

ZEIT8020 Cyber Offence: Threats and Opportunities - 2024

Published on the 11 Feb 2024

General Course Information

Course Code : ZEIT8020
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 : Online
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Postgraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

Every person, business, organisation and government around the world is investing in cyber security. Information is increasing in value, the growth of devices online is exponential, and the complexity of systems is driving increasing opportunity for their subversion. Both software and security vendors strive to design, build and distribute technologies to protect information, plug software holes, and detect malicious activity.

The Cyber domain is an active arms-race where the attacking side has the inherent advantage: attackers need only discover a single vulnerability within a target's wilderness of code, architecture or configuration to successfully breach security. At the same time, defenders race to discover vulnerabilities and implement counter measures.

Combatting attacker tools using technical mitigation and detection measures is an incomplete strategy. New thinking in the realm of cyber security focusses more and more on defeating cyber threat actor behaviour rather than just their technology. Hack-back, active-defence, and infiltration of cyber threat actor networks, are examples of targeting the people behind the keyboard.

Essential to combating cyber threat actor behaviour is understanding it. The tactics, techniques and procedures (TTPs) employed by a cyber threat actor are also known as 'tradecraft'. It is this tradecraft, which is the focus of this course.

Students will be walked through the various stages of the Cyber Kill Chain. The Cyber Kill Chain is an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organisation.

Course Aims

The aim of this course is to provide the theoretical foundation for offensive cyber operations, to develop knowledge and skills of various tools, techniques and procedures involved with offensive cyber operations, and to develop competence in addressing strategic, operational and tactical issues of offensive cyber operations.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.
CLO2 : On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft and acting upon them.
CLO3 : On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.
CLO4 : On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.

Course Learning Outcomes	Assessment Item
CLO1 : On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.	• Practical Exercise • Practical Project
CLO2 : On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft and acting upon them.	• Theoretical Presentation & Participation • Practical Project
CLO3 : On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.	• Practical Exercise • Practical Project
CLO4 : On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.	• Theoretical Presentation & Participation • Practical Project

Learning and Teaching Technologies

Moodle - Learning Management System

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Practical Exercise Assessment Format: Individual	25%	Due Date: 15/03/2024 11:59 PM
Theoretical Presentation & Participation Assessment Format: Individual	35%	Due Date: 26/04/2024 11:59 PM
Practical Project Assessment Format: Individual	40%	Due Date: 07/06/2024 12:00 AM

Assessment Details

Practical Exercise

Assessment Overview

Students will undertake practical laboratory exercises under supervision of the lecturers. Lab reports will be marked on 1) completeness, 2) quality of analysis, and 3) quality of documentation.

Course Learning Outcomes

- CLO1 : On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.
- CLO3 : On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.

Detailed Assessment Description

- On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.
- On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.

Theoretical Presentation & Participation

Assessment Overview

Students will deliver a 5 minute presentation on a cyber offense topic of their choice, and will provide feedback to other students' presentations. The marketing criteria are 1) depth and breadth of research, 2) structure and coherence, and 3) discussion participation.

Course Learning Outcomes

- CLO2 : On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft

and acting upon them.
- CLO4 : On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.

Detailed Assessment Description

- On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft and acting upon them.
- On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.

Practical Project

Assessment Overview

The Practical Project comprises a cyber offense scenario walkthrough. The marking criteria for the Practical Project are 1) complexity and diversity (targets, techniques, tools), 2) creativity and originality, and 3) suitability and feasibility.

Course Learning Outcomes

- CLO1 : On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.
- CLO2 : On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft and acting upon them.
- CLO3 : On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.
- CLO4 : On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.

Detailed Assessment Description

- On successful completion of this course, students will be able to: Conduct simple cyber offensive operations by applying the cyber kill chain to a variety of use cases.
- On successful completion of this course, students will be able to: Improve an organisation's security by identifying opportunities in defeating cyber threat actor tradecraft and acting upon them.
- On successful completion of this course, students will be able to: design executive active defence strategies against cyber threat actors.
- On successful completion of this course, students will be able to: evaluate complex cyber offense concepts, capabilities, and doctrines, and provide advice to non-expert executives and policy makers.

General Assessment Information

Grading Basis

Standard

Course Schedule

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Shabnam Kasra		Building 15, Room 217	0251145356		No	Yes
	Bevan Jones					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)