UNSW Course Outline

ZEIT3121 Securing Networks - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT3121
Year : 2024
Term : Semester 2
Teaching Period : Z2
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

This 6UOC course aims to develop an understanding of the link between security theory and technical computer and network security. It helps students comprehend formal and technical principles underlying network security testing.

It seeks to expand on earlier courses and discuss technical and organisational controls and defences, as well as offensive techniques. Moreover, students learn to implement and test security mechanisms and technical principles in a closed laboratory environment.

Course Aims

The aim of the course is to develop an understanding of the link between security theory and technical computer and network security. It helps students comprehend formal and technical principles underlying network security testing. It seeks to expand on earlier courses and discuss technical and organisational controls and defences, as well as offensive techniques. Moreover, students learn to implement and test security mechanisms and technical principles in a closed laboratory environment.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Analyse existing cyber defence controls, their uses and limitations in deployment.
CLO2 : Develop network defense strategies based on best practices, incorporating technical and organisational controls for case studies and unique scenarios.
CLO3 : Apply the processes and mechanisms of offensive security, and the impacts of threats.
CLO4 : Assess emerging technologies and their impact on cybersecurity, including Blockchain, supply chain, and Cloud.

Course Learning Outcomes	Assessment Item
CLO1 : Analyse existing cyber defence controls, their uses and limitations in deployment.	• Reports • Portfolio
CLO2 : Develop network defense strategies based on best practices, incorporating technical and organisational controls for case studies and unique scenarios.	• Lab assessments • Reports
CLO3 : Apply the processes and mechanisms of offensive security, and the impacts of threats.	• Lab assessments • Portfolio • Reports
CLO4 : Assess emerging technologies and their impact on cybersecurity, including Blockchain, supply chain, and Cloud.	• Lab assessments • Portfolio • Reports

Learning and Teaching Technologies

Moodle - Learning Management System | Echo 360 | Skillable

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Reports Assessment Format: Individual	35%	Due Date: Week 3: 29 July - 02 August, Week 13: 21 October - 25 October
Lab assessments Assessment Format: Individual	40%	Due Date: Week 5: 12 August - 16 August, Week 12: 14 October - 18 October
Portfolio Assessment Format: Individual	25%	Due Date: Week 7: 09 September - 13 September, Week 11: 07 October - 11 October

Assessment Details

Reports

Assessment Overview

Reports: There is a major report based on a selected topic introduced in the course. Students can choose their topic from one in the list provided or negotiate their own with the course convenor.

The first report will be a preliminary report worth 5% where the topic and argument are introduced. The students will get feedback on their interpretation of the topic and argument which they should incorporate into their final report. The final report is worth 30% and will consist of a full scientific style report and a pre-recorded 5-minute presentation covering the important points of the report.

Course Learning Outcomes

- CLO1 : Analyse existing cyber defence controls, their uses and limitations in deployment.
- CLO2 : Develop network defense strategies based on best practices, incorporating technical and organisational controls for case studies and unique scenarios.
- CLO3 : Apply the processes and mechanisms of offensive security, and the impacts of threats.
- CLO4 : Assess emerging technologies and their impact on cybersecurity, including Blockchain, supply chain, and Cloud.

Lab assessments

Assessment Overview

Lab assessments: There will be two assessments based on work completed in and extending on weekly lab sessions.

Course Learning Outcomes

- CLO2 : Develop network defense strategies based on best practices, incorporating technical and organisational controls for case studies and unique scenarios.
- CLO3 : Apply the processes and mechanisms of offensive security, and the impacts of threats.
- CLO4 : Assess emerging technologies and their impact on cybersecurity, including Blockchain, supply chain, and Cloud.

Portfolio

Assessment Overview

Portfolio: Reflective portfolio tasks will have two submissions. These activities will be more theoretical and will involve higher-level analysis and synthesis of current and emerging areas of cybersecurity.

Course Learning Outcomes

- CLO1 : Analyse existing cyber defence controls, their uses and limitations in deployment.
- CLO3 : Apply the processes and mechanisms of offensive security, and the impacts of threats.
- CLO4 : Assess emerging technologies and their impact on cybersecurity, including Blockchain, supply chain, and Cloud.

General Assessment Information

It is prohibited to use any software or service to search for or generate information or answers. If its use is detected, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension and exclusion.

Grading Basis

Standard

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 15 July - 19 July	Lecture	Revision Data lifecycles Attack lifecycles and spans
Week 2 : 22 July - 26 July	Lecture	Risk Assessment Threat Intelligence
Week 3 : 29 July - 2 August	Lecture	Cryptography
Week 4 : 5 August - 9 August	Lecture	Network security
Week 5 : 12 August - 16 August	Lecture	Cyber Offence 1
Week 6 : 19 August - 23 August	Lecture	Cyber defence 1
Week 7 : 9 September - 13 September	Lecture	Cyber Offence 2
Week 8 : 16 September - 20 September	Lecture	Cyber Defence 2
Week 9 : 23 September - 27 September	Lecture	Blockchain Security
Week 10 : 30 September - 4 October	Lecture	DevSecOps
Week 11 : 7 October - 11 October	Lecture	Catch up (public holiday and training days)
Week 12 : 14 October - 18 October	Lecture	Cloud Security
Week 13 : 21 October - 25 October	Lecture	Supply chain security Future trends in cybersecurity

Attendance Requirements

Please note that lecture recordings are not available for this course. Students are strongly encouraged to attend all classes and contact the Course Authority to make alternative arrangements for classes missed.

Course Resources

Recommended Resources

- Network Security Essentials, 4/e, by William Stallings
- Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, William (Chuck) Easttom, II ©2018

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Shabnam Kasra Kermanshahi		Building 15, Room 217			Yes	Yes
Lecturer	Benjamin Turnbull		Building 15, Room 215			No	No
Demonstrator	Sayed Amir Hoseini					No	No

Other Useful Information

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 4pm, Mon to Fri)