UNSW Course Outline

ZEIT8026 Cyber Defence: Network Security Operations - 2024

Published on the 27 Jun 2024

General Course Information

Course Code : ZEIT8026
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 : 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

The modern corporate computer network is broad and varied. It is no simple task to defend against known and emerging threats. This course provides in-depth understanding of the technical and policy used in computer and network defence. Numerous cyber defence technologies and their effectiveness against modern threats are discussed. This course is a combination of theoretical underpinnings and practical skills, with lectures reinforced with practical laboratories.

Course Aims

This course is designed to provide students with advanced knowledge on communications network security, both theoretical and practical.

Thus, this directly addresses the mechanisms necessary to circumvent or defend against attacks as well as studying the security protocols and standards in common use.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Demonstrate threat modelling against computers and network systems to understand how attacks occur and develop cyber defence techniques and tools.
CLO2 : Discuss malicious indicators of compromise, vulnerabilities, and their correlations to build threat intelligence and cyber defence.
CLO3 : Explain existing firewalls, IDS, and machine learning-based intrusion detection to identify known and unknown cyber-attacks from computers and network systems.
CLO4 : Give insights about SIEM and SOC, including models, processes, procedures, and machine learning-enabled innovative defensive techniques.

Course Learning Outcomes	Assessment Item
CLO1 : Demonstrate threat modelling against computers and network systems to understand how attacks occur and develop cyber defence techniques and tools.	• Technical Report • Discussion Essay • Practical Defence Project
CLO2 : Discuss malicious indicators of compromise, vulnerabilities, and their correlations to build threat intelligence and cyber defence.	• Technical Report • Discussion Essay • Practical Defence Project
CLO3 : Explain existing firewalls, IDS, and machine learning-based intrusion detection to identify known and unknown cyber-attacks from computers and network systems.	• Discussion Essay • Practical Defence Project
CLO4 : Give insights about SIEM and SOC, including models, processes, procedures, and machine learning-enabled innovative defensive techniques.	• Practical Defence Project

Learning and Teaching Technologies

Moodle - Learning Management System

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Technical Report Assessment Format: Individual Short Extension: Yes (2 days)	15%	Due Date: 29/07/2024 03:00 PM
Discussion Essay Assessment Format: Individual Short Extension: Yes (7 days)	40%	Start Date: Not Applicable Due Date: 25/09/2024 03:00 PM
Practical Defence Project Assessment Format: Group Short Extension: Yes (7 days)	45%	Due Date: Week 13: 21 October - 25 October

Assessment Details

Technical Report

Assessment Overview

The Technical Report/Essay must reflect practical exercises and theoretical analysis for cyber defences. The marking criteria for the Technical Report/Essay will be 1) completeness, 2) quality of analysis, and 3) quality of documentation.

Course Learning Outcomes

- CLO1 : Demonstrate threat modelling against computers and network systems to understand how attacks occur and develop cyber defence techniques and tools.
- CLO2 : Discuss malicious indicators of compromise, vulnerabilities, and their correlations to build threat intelligence and cyber defence.

Assessment information

For this assessment task, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work

or not. Please note that your submission will be passed through an AI-generated text detection tool. If your marker has concerns that your answer contains passages of AI-generated

text you may be asked to explain your work. If you are unable to satisfactorily demonstrate your understanding of your submission you may be referred to UNSW

Conduct & Integrity Office for investigation for academic misconduct and possible

penalties.

Discussion Essay

Course Learning Outcomes

- CLO1 : Demonstrate threat modelling against computers and network systems to understand how attacks occur and develop cyber defence techniques and tools.
- CLO2 : Discuss malicious indicators of compromise, vulnerabilities, and their correlations to build threat intelligence and cyber defence.
- CLO3 : Explain existing firewalls, IDS, and machine learning-based intrusion detection to identify known and unknown cyber-attacks from computers and network systems.

Assessment information

For this assessment task, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work

or not. Please note that your submission will be passed through an AI-generated text detection tool. If your marker has concerns that your answer contains passages of AI-generated

text you may be asked to explain your work. If you are unable to satisfactorily

demonstrate your understanding of your submission you may be referred to UNSW

Conduct & Integrity Office for investigation for academic misconduct and possible

penalties.

Practical Defence Project

Assessment Overview

The Practical Project comprises cyber defence scenarios covering various attacks, IDS, SOC, SIEM and IR. The project's submission includes a recorded video for the presentation and a technical report. The marketing criteria for the recorded presentation will be 1) depth and breadth of research, 2) structure and coherence, and 3) sustainability and feasibility. The marking criteria for the technical report of the project are 1) complexity and diversity (targets, techniques, tools), 2) creativity and originality, and 3) suitability and feasibility.

Course Learning Outcomes

- CLO1 : Demonstrate threat modelling against computers and network systems to understand how attacks occur and develop cyber defence techniques and tools.

- CLO2 : Discuss malicious indicators of compromise, vulnerabilities, and their correlations to build threat intelligence and cyber defence.
- CLO3 : Explain existing firewalls, IDS, and machine learning-based intrusion detection to identify known and unknown cyber-attacks from computers and network systems.
- CLO4 : Give insights about SIEM and SOC, including models, processes, procedures, and machine learning-enabled innovative defensive techniques.

Assessment information

For this assessment task, you are permitted to use standard editing and referencing functions in word processing software. You must not use any functions that generate or paraphrase [or translate] passages of text, whether based on your own work

or not. Please note that your submission will be passed through an AI-generated text detection tool. If your marker has concerns that your answer contains passages of AI-generated

text you may be asked to explain your work. If you are unable to satisfactorily

demonstrate your understanding of your submission you may be referred to UNSW

Conduct & Integrity Office for investigation for academic misconduct and possible

penalties.

General Assessment Information

Grading Basis

Standard

Requirements to pass course

An overall mark of 50% is required

Course Schedule

Attendance Requirements

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

Course Resources

Prescribed Resources

No prescribed texts

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Convenor	Tim Lynar					Yes	No
Lecturer	Edward Farrel l					No	Yes

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)