School of Information and Physical Sciences

COMP3500: Security Attacks: Analysis and Mitigation Strategies
Callaghan
Semester 1 - 2024

OVERVIEW

Course Description	This course introduces students to techniques that are used by attackers to exploit computer systems and networks. Security attacks such as injection, rootkits and denial of service attacks will be discussed along with the detailed analysis of defending security technologies such as firewalls, host/network-based security tools and signature/anomaly-based security tools. Students who complete this course will have a good understanding of security technologies that are used for securing systems and networks. Furthermore, students should be able to perform attack detection and security anomaly analysis and manage the security aspect of a network.
Academic Progress Requirements	Nil
Assumed Knowledge	INFT2031 Systems and Network Administration or COMP2240 Operating Systems or ELEC2720 Introduction to Embedded Computing.
Contact Hours	**Callaghan** **Computer Lab** Face to Face On Campus 2 hour(s) per week(s) for 10 week(s) starting Week 3 **Lecture** Face to Face On Campus 2 hour(s) per week(s) for 13 week(s) starting Week 1
Unit Weighting	10
Workload	Students are required to spend on average 120-140 hours of effort (contact and non-contact) including assessments per 10 unit course.

CONTACTS

Course Coordinator **Callaghan**
Dr Sky Miao
Sky.Miao@newcastle.edu.au
(02) 4985 4089
Consultation:

Teaching Staff Other teaching staff will be advised on the course Canvas site.

School Office **School of Information and Physical Sciences**
SR233, Social Sciences Building
Callaghan
CESE-SIPS-Admin@newcastle.edu.au
+61 2 4921 5513
9am-5pm (Mon-Fri)

SYLLABUS

Course Content
1. Introduction to course
2. Risk Management
3. Software Security Attacks and Mitigation Techniques
4. Network Security Attacks and Mitigation Techniques
5. Wireless Network Security Attacks and Mitigation Techniques
6. Attacks in Virtual/Mobile networks
7. Penetration Testing
8. Security Technologies
9. Advanced Security Technologies
10. Best Practices for Building Secure Systems and Networks

Course Learning Outcomes

On successful completion of this course, students will be able to:
1. Identify security risks in enterprise network infrastructures

2. Analyse security threats and methods for exploiting systems and networks to generate attacks

3. Apply security mechanisms to mitigate cyber attacks

4. Investigate security technologies used to counteract the attacks

Course Materials

Recommended Reading:
- NIST publications related to the topic

- Gary McGraw, Software Security: Building Security IN, Addison-Wesley

- Charles P. Pfleeger, Shari L. Pfleeger, Security in Computing, Prentice Hall, 4th Edition

- John Viega, Gary McGraw, Building Secure Software, Addison-Wesley

- Howard and LeBlanc, Writing Secure Code, Microsoft Press, 2nd edition

COMPULSORY REQUIREMENTS

In order to pass this course, each student must complete ALL of the following compulsory requirements:

Contact Hour Requirements:
- -
Course Assessment Requirements:
- - Assessment 3 - Final Examination: Pass requirement 40% - Must obtain 40% in this assessment item to pass the course.
Compulsory Placement and WHS Requirements:
- -

SCHEDULE

ASSESSMENTS

This course has 3 assessments. Each assessment is described in more detail in the sections below.

	Assessment Name	Due Date	Involvement	Weighting	Learning Outcomes
1	Assignment 1	11:59pm, 5th April 2024, Friday of Week 6	Individual	25%	1, 2
2	Assignment 2	11:59pm, 17th May 2024, Friday of Week 10	Individual	30%	3, 4
3	Final Examination*		Individual	45%	1, 2, 3, 4

* This assessment has a compulsory requirement.

Late Submissions	The mark for an assessment item submitted after the designated time on the due date, without an approved extension of time, will be reduced by 10% of the possible maximum mark for that assessment item for each day or part day that the assessment item is late. Note: this applies equally to week and weekend days.

Assessment 1 - Assignment 1

Assessment Type	Written Assignment
Description	This assessment is related to risk management and detail analysis of attacks on systems and networks.
Weighting	25%
Due Date	11:59pm, 5th April 2024, Friday of Week 6
Submission Method	Online
Assessment Criteria	Understanding of the content, depth of review and clarity of documentation. More details are provided in Canvas.
Return Method	Online
Feedback Provided	Online - .
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 2 - Assignment 2

Assessment Type	Written Assignment
Description	This assessment is related to application of security techniques to deal with the attacks and analysis of the security mechanisms.
Weighting	30%
Due Date	11:59pm, 17th May 2024, Friday of Week 10

Submission Method	Online
Assessment Criteria	Understanding of the content, design and application of security techniques, depth of review and clarity of documentation. More details are provided in Canvas.
Return Method	Online
Feedback Provided	Online - .
Opportunity to Reattempt	Students WILL NOT be given the opportunity to reattempt this assessment.

Assessment 3 - Final Examination

Assessment Type	Formal Examination
Description	Exams are designed to test students' knowledge in the course material, understanding of the content and ability to justify their decisions. The final exam is a 2-hour open-book exam consisting of short-answer, security design and security application based questions.
Weighting	45%
Compulsory Requirements	Pass requirement 40% - Must obtain 40% in this assessment item to pass the course..
Due Date	
Submission Method	Formal Exam
Assessment Criteria	Understanding of the content, and clarity of written answers
Return Method	Not Returned
Feedback Provided	No Feedback - .
Opportunity to Reattempt	Students WILL be given the opportunity to reattempt this assessment.

ADDITIONAL INFORMATION

Grading Scheme

This course is graded as follows:

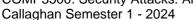| Range of Marks	Grade	Description
85-100	High Distinction (HD)	Outstanding standard indicating comprehensive knowledge and understanding of the relevant materials; demonstration of an outstanding level of academic achievement; mastery of skills*; and achievement of all assessment objectives.
75-84	Distinction (D)	Excellent standard indicating a very high level of knowledge and understanding of the relevant materials; demonstration of a very high level of academic ability; sound development of skills*; and achievement of all assessment objectives.
65-74	Credit (C)	Good standard indicating a high level of knowledge and understanding of the relevant materials; demonstration of a high level of academic achievement; reasonable development of skills*; and achievement of all learning outcomes.
50-64	Pass (P)	Satisfactory standard indicating an adequate knowledge and understanding of the relevant materials; demonstration of an adequate level of academic achievement; satisfactory development of skills*; and achievement of all learning outcomes.
0-49	Fail (FF)	Failure to satisfactorily achieve learning outcomes. If all compulsory course components are not completed the mark will be zero. A fail grade may also be awarded following disciplinary action.

*Skills are those identified for the purposes of assessment task(s).

Communication Methods	Communication methods used in this course include:
Course Evaluation	Each year feedback is sought from students and other stakeholders about the courses offered in the University for the purposes of identifying areas of excellence and potential improvement.

Oral Interviews (Vivas)	As part of the evaluation process of any assessment item in this course an oral examination (viva) may be conducted. The purpose of the oral examination is to verify the authorship of the material submitted in response to the assessment task. The oral examination will be conducted in accordance with the principles set out in the Oral Examination (viva) Procedure. In cases where the oral examination reveals the assessment item may not be the student's own work the case will be dealt with under the Student Conduct Rule.	
Academic Misconduct	All students are required to meet the academic integrity standards of the University. These standards reinforce the importance of integrity and honesty in an academic environment. Academic Integrity policies apply to all students of the University in all modes of study and in all locations. For the Student Academic Integrity Policy, refer to https://policies.newcastle.edu.au/document/view-current.php?id=35.	
Adverse Circumstances	The University acknowledges the right of students to seek consideration for the impact of allowable adverse circumstances that may affect their performance in assessment item(s). Applications for special consideration due to adverse circumstances will be made using the online Adverse Circumstances system where: 1. the assessment item is a major assessment item; or 2. the assessment item is a minor assessment item and the Course Co-ordinator has specified in the Course Outline that students may apply the online Adverse Circumstances system; 3. you are requesting a change of placement; or 4. the course has a compulsory attendance requirement. Before applying you must refer to the Adverse Circumstance Affecting Assessment Items Procedure available at: https://policies.newcastle.edu.au/document/view-current.php?id=236	
Important Policy Information	The Help button in the Canvas Navigation menu contains helpful information for using the Learning Management System. Students should familiarise themselves with the policies and procedures at https://www.newcastle.edu.au/current-students/respect-at-uni/policies-and-procedures that support a safe and respectful environment at the University.	

GRADUATE PROFILE STATEMENTS

The following table illustrates how this course contributes towards building the skills students will need to work in their profession.

Level of capability

- • Level 1 indicates an introduction to a topic at a university level
- • Levels 2 and 3 indicate progressive reinforcement of that topic
- • Level 4 indicates skills commensurate with a graduate – entry to professional practice
- • Level 5 indicates highly specialist or professional ability

Bachelor of Computer Science

	University of Newcastle Bachelor of Computer Science Graduate Profile Statement	Taught	Practised	Assessed	Level of capability
1	Knowledge of basic science and computer science fundamentals	X	X	X	3
2	In depth technical competence in the discipline of computer science	X	X	X	4
3	An ability to carry out problem analysis, requirements capture, problem formulation and integrated software development for the solution of a problem	X	X	X	4
4	Capacity to continue developing relevant knowledge, skills and expertise in computer science throughout their careers	X	X	X	3

		Taught	Practised	Assessed	Level of capability
5	An ability to communicate effectively with other Computer Scientists, Software Engineers, other professional disciplines, managers and the community generally	X	X	X	3
6	Ability to undertake and co-ordinate large computer science projects and to identify problems, their formulation and solution				
7	Ability to function effectively as an individual, a team member in multidisciplinary and multicultural teams and as leader/manager with capacity to assist and encourage those under their direction				
8	Understanding of social, cultural, global and business opportunities of the professional computer scientist; understanding the need for and principles of sustainability and adaptability				
9	Understanding of professional and ethical responsibilities and a commitment to them				
10	Understanding of entrepreneurship; need of and process of innovation, as well as the need of and capacity for lifelong learning				

Bachelor of Information Technology

	University of Newcastle Bachelor of Information Technology Graduate Profile Statement	Taught	Practised	Assessed	Level of capability
1	Demonstrate a comprehensive understanding of the discipline of information technologies with an emphasis on net-centric applications, information management, and user requirements for ethical professional practice.	X	X	X	3
2	Apply critical reasoning and systems thinking to understand and support the operation and constraints of contemporary enterprises and their dynamic environment.	X	X	X	3
3	Work independently and collaboratively to locate, manage and organise information and resources and apply evidence-based methodologies to create, modify and maintain designs and design solutions.	X	X	X	4
4	Use creativity, problem solving skills, project management skills and technical expertise to analyse, interpret, evaluate and generate solutions to complex technical and organisational problems.	X	X	X	4
5	Demonstrate professional judgement and responsibility by communicating information technology principles, practices, standards to specialist and non-specialist audience clearly and persuasively.	X	X	X	3