School of Information and Physical Sciences

COMP6500: Security Attacks: Analysis and Mitigation Strategies

Callaghan and Online

Semester 1 - 2024

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

COURSE OUTLINE

www.newcastle.edu.au

CRICOS Provider 00109J

OVERVIEW

Course Description

The course covers leading techniques currently used by attackers to exploit systems and networks. Students are introduced to various attack strategies including injection, rootkits and denial of service attacks as well as underpinning security defence techniques such as signature based analysis, anomaly-based analysis and traceback techniques for detection of attacks. Students are required to critically analyse the characteristics of various security tools such as firewalls, host/network-based security tools, and signature/anomaly-based security tools. Students who complete this course gain a practical knowledge of security attack detection and analysis, which is highly beneficial for carrying out security incident analysis in organisations.

Academic Progress Requirements

Nil

Requisites

This course has similarities to COMP3500. If you have successfully completed COMP3500 you cannot enrol in this course.

Assumed Knowledge

INFT6031 Systems and Network Administration. COMP6240 Operating Systems (in addition to INFT6031) would be preferred.

Contact Hours

Callaghan
Computer Lab
Face to Face On Campus
2 hour(s) per week(s) for 10 week(s) starting Week 3
Online students will receive equivalent instruction through online or other distance education strategies.
Lecture
Face to Face On Campus
2 hour(s) per week(s) for 12 week(s) starting Week 1
Online students will receive equivalent instruction through online or other distance education strategies.

Online
Computer Lab
Face to Face On Campus
2 hour(s) per week(s) for 10 week(s) starting Week 3
Online students will receive equivalent instruction through online or other distance education strategies.
Lecture
Face to Face On Campus
2 hour(s) per week(s) for 12 week(s) starting Week 1
Online students will receive equivalent instruction through online or other distance education strategies.

Unit Weighting Workload

10
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 and Online
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)
School of Information and Physical Sciences
SR233 Social Sciences Building
Callaghan
CESE-SIPS-Admin@newcastle.edu.au
+61 2 4921 5513

SYLLABUS

Course Content

Module 1: Risk Management Introduction
- Course overview
- Overview of security attacks in current systems and networks

Risk Management Framework
- Risk management approach
- Threat modelling and penetration testing
- Best practices for improving security

Module 2: Software Security Attacks Software security attacks and mitigation strategies
- Attacks exploiting vulnerabilities in OS and applications: buffer overflow, SQL injection
- Malware: rootkits, zero day attacks, polymorphism and metamorphism
- Attacks in virtualisation: VM escape, VM sprawl

Module 3: Network Security Attacks Network security attacks and mitigation strategies
- Attacks in wired networks: LAN attacks, insider attacks, WAN attacks, DDos
- Attacks in wireless networks: WLAN attacks, rouge access points, war driving

Module 4: Security Technologies Security technologies
- Design choices for security tools
- Analysis of border security tools: packet filter, stateful filters, DPI and application
- Analysis of host-based and network-based security tools
- Analysis of signature-based and anomaly-based security tools
- Malware analysis techniques: dynamic and static analysis techniques
- Analysis of virtualisation-based security techniques
- Analysis of network attacks traceback security techniques

Course Learning Outcomes

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

2. Analyse the methods employed by attackers to exploit vulnerabilities in networked systems.

3. Design and develop advanced security mechanisms to counteract attacks in networked systems.

4. Evaluate security technologies used to counteract security attacks in networked infrastructures.

Course Materials

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: Risk Analysis and Attack Methods	11:59pm 5th April 2024, Friday of Week 6	Individual	25%	1, 2
2	Assignment 2: Application of Security Mechanisms	11:59pm, 17 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: Risk Analysis and Attack Methods

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: Application of Security Mechanisms

Assessment Type	Written Assignment
Description	This assessment is related to application of security techniques to deal with the attacks and critical analysis of the security mechanisms.
Weighting	30%
Due Date	11:59pm, 17 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	Online Open Book Formal Examination
Description	Exams are designed to test students' knowledge in the course material, in depth 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	Online
Assessment Criteria	Understanding of the content, application of security techniques, depth of review 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

Master of Professional Engineering

	University of Newcastle Master of Professional Engineering Graduate Profile Statement	Taught	Practised	Assessed	Level of capability
1	Comprehensive, theory-based understanding of engineering fundamentals and/or the underpinning natural and physical sciences as applicable to the engineering discipline				
2	Conceptual understanding of the mathematics, numerical analysis, statistics and computer and information sciences which underpin the engineering discipline				
3	In-depth understanding of specialist bodies of knowledge within the engineering discipline	X	X	X	5
4	Discernment of knowledge development and research directions within the engineering discipline				
5	Knowledge of contextual factors impacting the engineering discipline				
6	Understanding of the scope, principles, norms, accountabilities and bounds of contemporary engineering practice in the specific discipline	X	X	X	4
7	Application of established engineering methods to complex engineering problem solving	X	X	X	5
8	Fluent application of engineering techniques, tools and resources				
9	Application of systematic engineering synthesis and design processes	X	X	X	5
10	Application of systematic approaches to the conduct and management of engineering projects	X	X	X	4
11	Ethical conduct and professional accountability	X			3
12	Effective oral and written communication in professional and lay domains				
13	Creative, innovative and pro-active demeanour				
14	Professional use and management of information				
15	Orderly management of self, and professional conduct				
16	Effective team membership and team leadership				
17	Demonstrated capacity for dealing with uncertain problems using self-direction	X	X	X	3