Unit outline

Name of unit
Network and System Security

Unit description
This subject covers modern network and system security concepts, strategies and techniques. Students develop practical and working tactics to achieve the understanding of digital security in networks, operation systems, databases and servers. Students apply security measures and principles into the design, implementation, and configurations crossing the networks. The framework of network and system security, safety principles and guidelines, are to be explored and students will utilize various security tools in the context. This subject cover mechanisms and prominent techniques of system hardening. Students learns the use of network and system hacking tools & approaches in practical sessions.

SECTION 1 – GENERAL INFORMATION

1.1 Administrative details

Associated higher education awards (for example, Bachelor, Diploma)	Duration (for example, one semester, full year)	Level (for example, introductory, intermediate, advanced level, 1st year, 2nd year, 3rd year)	Unit coordinator
Bachelor of ICT	One semester	1st year, 2nd semester	

1.2 Core or elective unit

Indicate if the unit is a:

☒ core unit

☐ elective unit

☐ other (please specify below):

1.3 Unit weighting

Using the table below, indicate the credit point weighting of this unit and the credit point total for the course of study (for example, 10 credit points for the unit and 320 credit points for the course of study).

Unit credit points Example: 10 credit points	Total course credit points Example: 320 credit points
12.5	300

1.4 Student workload

Using the table below, indicate the expected student workload per week for this unit.

No. timetabled hours per week (1)	No. personal study hours per week (2)	Total workload hours per week (3)
4	6	10

(1) Total time spent per week at lectures, tutorials, clinical and other placements, etc.
(2) Total time students are expected to spend per week in studying, completing assignments, etc.
(3) Sum of (1) and (2) equals workload hours.

For those students requiring additional English language support, how many additional hours per week is it expected that they will undertake?

Additional English language support: ____ hours per week

1.5 Delivery mode

Tick all applicable delivery modes for the unit and provide details in the following text box: If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

- ☒ Face to face on site
- ☐ E-learning (online)
- ☐ Intensive/block mode (where the unit or a face to face component is delivered in a block)
- ☐ Mixed/blended
- ☐ Distance/independent learning (untimetabled)
- ☒ Full-time
- ☒ Part-time
- ☐ External
- ☐ Fast track

☐ Other (please specify)

1.6 Work-integrated learning activity

If the unit includes a work-integrated learning component (where completion of the unit requires students to undertake learning in a workplace outside of their higher education provider), provide details including the rationale, the specification and methods for assessing the learning outcomes, monitoring arrangements and whether the work integrated learning is required for professional accreditation. If necessary or preferred, you may provide this information in a separate document, using the 'Attach evidence here' function of the online form.

Also if available, upload copies or templates of the formal agreements with third parties for the work-integrated learning activity, using the 'Attach evidence here' function of the online form.

Refer to the TEQSA Guidance Note on Work-Integrated Learning as required (available on the TEQSA website).

N/A

1.7 Prerequisites and co-requisites

Are students required to have undertaken a prerequisite or co-requisite unit for this unit?

☒ Yes ☐ No

If YES, provide details of the prerequisite or co-requisite requirements below.

1.8 Other resource requirements

Do students require access to specialist facilities and/or equipment for this unit (for example, special computer access, physical education equipment)?

☒ Yes ☐ No

If YES, provide details of specialist facilities and/or equipment below.

SECTION 2 – ACADEMIC DETAILS

Learning outcomes for the unit **On successful completion of this unit students will be able to:**
1. Review the different types of security systems, their functionalities, their architectures, and their configurations. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
2. Understand computer security systems, and generate and present a proposal to address security problems Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
3. Identify and analyse security vulnerabilities and propose justifiable technical solutions and potential remedy actions based on findings. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Final exam
4. Apply problem solving, design and decision-making methodologies to develop components, systems and processes to meet specified requirements. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Mid-term test, final exam
5. Explore abstraction, mathematics and discipline fundamentals, software, tools and techniques to evaluate, implement and operate systems. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Assignment I, final exam
6. Work as an effective member or leader of diverse teams, communicating effectively and operating within cross-disciplinary and cross-cultural contexts in the workplace. ● Suggested teaching methods: Lecture, tutorial ● Assessment strategies: Final exam
7. Identify, engage, interpret and analyse stakeholder needs and cultural perspectives, establish priorities and goals, and identify constraints, uncertainties and risks (social, ethical, cultural, legislative, environmental, economics etc.) to define the system requirements.

- Suggested teaching methods: Lecture, tutorial
- Assessment strategies: Assignment II, final exam

Topics included in the unit
1. Introduction of Network and System Security
2. Basics of Network Security and System Security Tools And Plattforms
3. User Authentication
4. Network Access Control
5. Database Security
6. Denial-of-Service Attacks
7. Firewalls and Intrusion Prevention Systems
8. Software Security
9. Operating System Security
10. Trusted Computing and Multilevel Security
11. Management Issues
12. Review Lecture

Assessment tasks			
Type	**When assessed – year, session and week (for example, year 1, semester 1, week 1)**	**Weighting (% of total marks for unit)**	**Cross reference to learning outcomes**
Mid-term Test (Individual) - A 2-hour written test based on contents from weeks 1-6.	7	15	1, 2, 4
Assignment I This assessment is for students to conduct independent research on one of the latest	9	15	5

networks and system security topics. Students will be required to follow the standard procedure to investigate research papers in the area of network and system security. Students must generate a proposal to address the current network and system security issues in the literature and present a proposal to their peers in a 5-minute presentation			
Assignment II (Group) This assessment task is for students to identify security vulnerabilities by various attacks to hardened system. The students will be grouped in defensive team and offensive team. The offensive team has to choose on a subset of the top ten vulnerabilities listed on OWASP project website, identify these vulnerabilities in systems nominated by the defensive team and document their findings. Defensive team Students will be tested on their ability to harden the system. Both teams are required to verify experimental outcomes and to propose solutions to remedy the identified vulnerabilities.	11	10	7

Final Exam (Individual) - A 3-hour written exam covering contents from weeks 1-12.	Exam Period	60	1, 2, 3, 4, 5, 6, 7, 8

2.1 Prescribed and recommended reading

Provide below, in formal reference format, a list of the prescribed and recommended reading for the unit.

Recommended Book:

Matt Bishop (2018) *Computer Security Art and Science, 2nd Edition*

William Stallings (2012), *Computer Security Principles and Practice*. Pearson.

William Stallings (2016), *Network Security Essentials: Applications and Standards*, 6th Edition

Pieprzyk, Josef, Thomas Hardjono, and Jennifer Sebberry, (2013) *Fundamentals of computer security*.