Murdoch
UNIVERSITY

Unit Overview

ICT287 Computer Security

ACKNOWLEDGEMENT OF COUNTRY

I would like to acknowledge that Murdoch University is situated on the lands of the Whadjuk Nyungar people.

I pay respect to their enduring and dynamic culture and the leadership of Nyungar elders both past and present.

The boodjar (country) on which Murdoch University is located has, for thousands of years, been a place of learning. We at Murdoch University are proud to continue this long tradition.

Reconciliation ACTION PLAN INNOVATE RAP

Murdoch UNIVERSITY

Is a disability/medical condition part of your life?

Get appropriate support for exams/coursework from

Access and Inclusion

Call: 9360 6084

Email: access@murdoch.edu.au

Murdoch UNIVERSITY

Student Assist

Got a problem? Your Guild can help.

WELFARE ASSISTANCE

- Book Subsidy Scheme (for all students)
- Tenancy Issues
- Tax Help
- Accommodation Database
- Welfare services referral
- Food Bank (non-perishable food)
- Advice on individual welfare cases.

EDUCATION ASSISTANCE

- Policy & Procedure Advice
- Academic Appeals
- Re-marking
- Retrospective Withdrawals
- Deferring Examinations
- Academic Misconduct Appeals
- Supplementary Assessment
- Advice on individual academic cases
- Murdoch Guild Peer Tutoring Program.

GET IN TOUCH:

studentassist@murdochguild.com.au / 9360-2999

www.facebook.com/MurdochStudentAssist

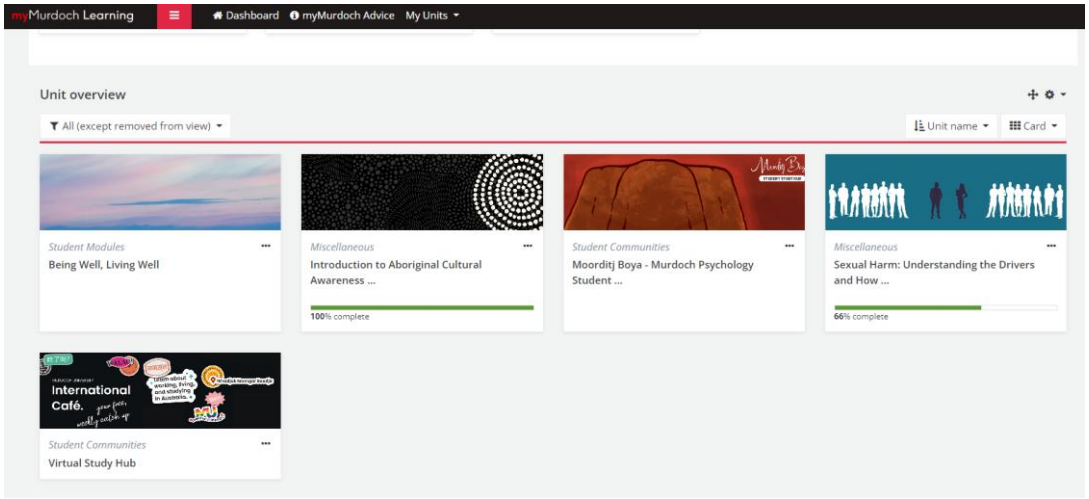
Murdoch International Café

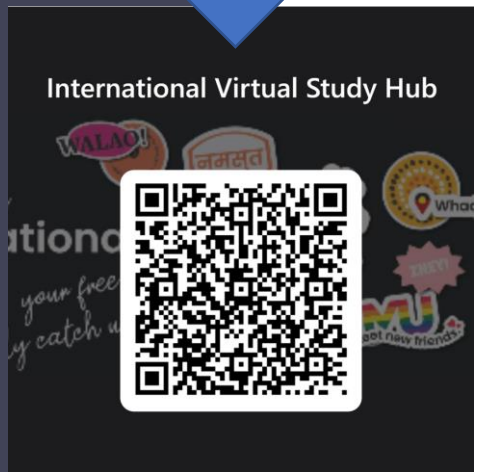
The Base/ Winter Garden

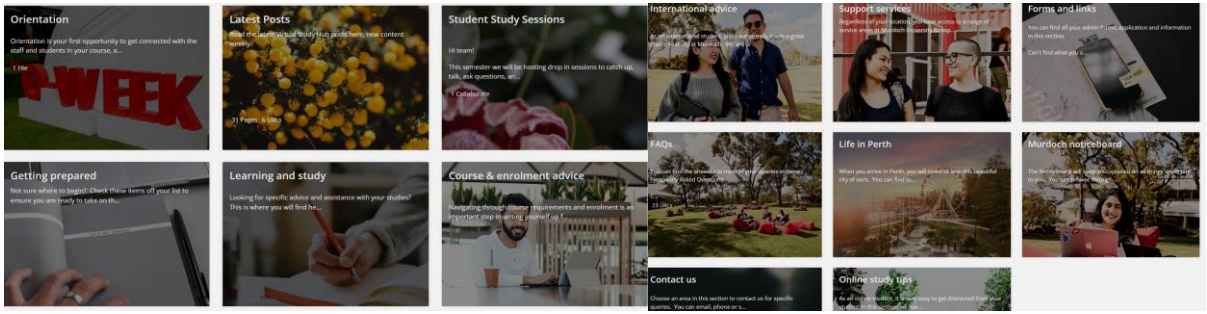
Every Wednesday, 11 am – 1 pm

- Build new friendships and contacts
- **FREE** snacks, drinks and activities
- Connects students to sources of information
- An excellent way to learn about events/opportunities
- Meet internal and external support services (Allianz, StudyPerth, Guild, MISA, student Specialist, PASS/PAC, counselling, medical centre etc.)
- Celebration of cultural days or significant dates

Join the International Virtual Study Hub







Welcome

- In this unit you will learn about **various weaknesses** in computer systems, **how they can be exploited** and how they can be prevented or mitigated
- Focus more on weaknesses and how they can be exploited (red team) – ICT379 will cover prevention and mitigation in more detail (blue team)
- Lots of hands-on labs, practical assignments and learning through doing, which includes using various tools and some coding
- Think of it as **Applied Computer Security**
- With some Ethical Hacking / Pen Testing

Welcome

- Content in this unit builds on each other, so you need to stay current with topics
- If you don’t keep up to date you will struggle to catch up later - this is the case in all units, but more so here

Disclaimer

- This unit will cover tools and techniques for security analysis – if used without permission, these can be entirely illegal
- It is essential that you use this information responsibly and follow the direction of your teacher as you are accountable for your actions

Prerequisites

- ICT171 Introduction to Server Environments and Architectures
- ICT159 Foundations of Programming

- Assumed you are familiar with basic Linux commands (command line), virtualization and networking, and you are also familiar with basic C programming
- These are all covered in ICT171 and ICT159, so it may be wise to review these concepts at start of this unit so that they are fresh in your mind

Teaching Staff

- **Unit Coordinator**: Sebastian Zander

  Email: s.zander@murdoch.edu.au

  Room: Science & Computing 1.007

  Phone: +618 9360 2296

- **For non-urgent communication email is the preferred method**
  - Will answer everything within few hours, but not if you send me email on Sat evening

- **If your question is non-urgent and of general interest use the discussion forum on learning management system (LMS)**

Teaching Staff

- **Tutors**
  - Thu 10:30 and Fri 10:30 labs:
    Paul Redman (paul.redman@murdoch.edu.au)
  - Thu 8:30 lab and Externals:
    Sebastian Zander (s.zander@murdoch.edu.au)

- Please check with your tutor what their preferred communication method is

Who Do I Contact?

- **Technical Questions**
  - Ask your tutor
    - If you're not happy with answer, ask me
  - Ask me during and after lecture
  - Post on LMS discussion forum

- **Admin questions**
  - Ask your tutor if related to lab
    - If you want to swap labs in one week talk to both tutors
  - If of general interest, post on LMS forum
  - Otherwise contact me via email etc.

Teaching

- 2 hour lecture
- 2 hour lab (**labs start in week 1**)
- Attendance is not compulsory, but there is a strong correlation between non-attendance and poor performance
- If you miss a class, all handouts will be available for download from LMS
- 3pt unit, so approx. 10h per week of work (including the 4h lecture & lab)

Teaching

- **Everything is online**: Readings, videos, electronic lab handouts that can be completed at home on your own computer
- Use this resource when necessary, but always try to attend lectures and labs/workshops in person
- It is very easy to say: “Its all conveniently online so I will do it later”. Not a good approach!
- Make sure you keep up and ask lots of questions
- There is not one book that covers unit, but some book recommendations are in unit guide

Unit Guide

Unit Guide on LMS explains study schedule and assessments

You must read unit guide before coming to first lecture/lab

Study Schedule

Session	Lecture Topic	Labs	Assessment
1.	Unit Introduction Introduction to Computer Security	Kali Linux, Basic Information Gathering	
2.	Network Security Attack Surface Analysis	Network Security Attack Surface Analysis	
3.	Software Security	C Memory Management, Buffer Overflow Basics	
4.	Malware	Metasploit	
5.	Security Models	Buffer Overflow Advanced	**Project Registration**
6.	Cryptography	Codes and Ciphers	
7.	Authentication	Password Attacks	
8.	Web Security	Setup BadStore, Web Security 1	**Project Vulnerability Description**
9.	Malware Commoditization (Crimeware), Cyber Laws	Web Security 2	
10.	Covert Channels	Covert Channels	
11.	Human Factors Emerging Trends	Man in the middle attacks Hacking Challenge	
12.	Unit Review	Demonstration of Group Project by Students	**Project Demo and Final Report**
Exam week			**Final Exam**

Assessments

Assessment	Description	Aligned Learning Outcomes	Value	Due
Participation	Participation in lab activities	1,2,4,5	10%	Throughout all sessions
Project	Individual assignment, develop and demonstrate practical skills with a real world problem	1,2,3,5,6	40%	See schedule
Final Exam	120 minute final exam	1,3,4,6	50%	Exam Period TBA

Participation

- Weekly activities, mainly LMS quizzes
  - Questions related to lab work → **important to do labs**
  - Questions on important theoretical concepts
- Due generally **end of following week, check LSM for the actual due dates**
- There will be 11 quizzes, each contributing 1 mark, but overall 10 marks, so worst quiz does not count
- As in any assessment **no plagiarism**, collusion, but feel free to discuss the questions with other students (or even your tutor)

Participation (cont.)

- These quizzes are not marked on correctness, but to get marks:
  - Response must be at least 50 words (~3 sentences)
  - Response must be clear attempt to answer the question (and not other questions not asked)
  - Response must address all parts of question (partial marks if it doesn't)
  - For questions related to practical tasks there must be clear evidence that task was attempted
  - **Copying of answers from Internet or other sources is not permitted**

Project

- Real world assessment to be done individually or as group of **exactly** 2 students
- Research and learn about security vulnerability, you choose and then develop test environment to demonstrate this vulnerability
- **Choose vulnerability until due date in session 5**
- Submit written vulnerability description report in session 8
- Demonstrate vulnerability and submit written report about demo setup and exploitation in session 12

Final Exam

- Online open book, 120 minutes
  - Multiple choice
  - Short answer
  - Long answer
- Comprehensive final exam covering topics from lectures, labs and readings
- Conducted during University exam period

Challenge Leaderboard

- Some labs have challenge questions
- First two students of each lab who complete challenge will be entered in leader board on LMS
- Sorry no prizes, only bragging rights
- When it comes to selecting teams for Cyber Sec competitions we will also look at leader board

Plagiarism

- We will check for plagiarism in all assessments including participation quizzes
- **Any substantial plagiarism found will trigger academic misconduct investigation**
    - Result could be assessment fail or even unit fail as well as entry on student record
- Make sure you don’t copy text from other sources unless it is properly referenced (text in “” plus proper citation)
- Note that larger amounts of quoting are not misconduct but will lead to low marks, as we treat this as text you haven’t written it yourself

Academic Misconduct

- We will also check for other forms of misconduct such as collusion
- Do the MAP module to understand the various forms of misconduct and how to avoid them
- **You must complete MAP:** http://our.murdoch.edu.au/Student-life/Study-Successfully-Advice/Murdoch-Academic-Passport/

How to Pass Unit

- Achieve total for all assessments of 50% or better
- Achieve at least 40% in final exam

- If you achieve less than 50% you may be given supplementary assessment in line with University policy
- **Less likely that you will get supp if you showed poor participation during teaching period, i.e. low participation mark, low attendance in lectures and tutes**

How to Succeed

- Keep up to date with weekly tasks (lectures, lab quizzes)
- **Do all participation quizzes and challenges**
- Submit participation quizzes in first week (2nd week really is build-in extension if you are sick etc. in first week)
- Get organised and start working on project early
- Prepare well for final exam (see Unit Review)

Extra Curricular Activities

- Get involved in extra (legal) curricular activities, such as CTFs

- Some Capture The Flag (CTF) challenges
  - picoCTF (easy, for school kids)
  - Vulnhub (relatively easy to advanced)
  - Hack The Box (advanced)

- Australian Defence Force Cyber Gap Program

Cyber Security Competitions

- Several nation-wide or international competitions with prizes for high scoring teams
- Variety of challenges in different topics, e.g. cryptography, web security, binary exploits
- If interested, contact me but we will only select students that have practical experience, e.g. hacking group, ICT287 lab challenges
- Possible comps for 2023
    - WACTF 2023
    - DownUnderCTF 2023

Questions?