1a. Introduction

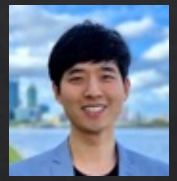
Jin Hong

jin.hong@uwa.edu.au

0. Introduction: outline

- Team
- Location
- Schedule
- Assessments
- Remember

Team



Jin Hong
Unit coordinator
Room CS1.10
jin.hong@uwa.edu.au

Weiyan Xu
Lab facilitator
Room MATH
weiyan.xu@research.uwa.edu.au

Larry Huynh
Lab facilitator
Room EZONE
larry.huynh@.uwa.edu.au

Teaching Operations (team)
Admin team
Room Main reception
teachingops-team2@uwa.edu.au

Emergency

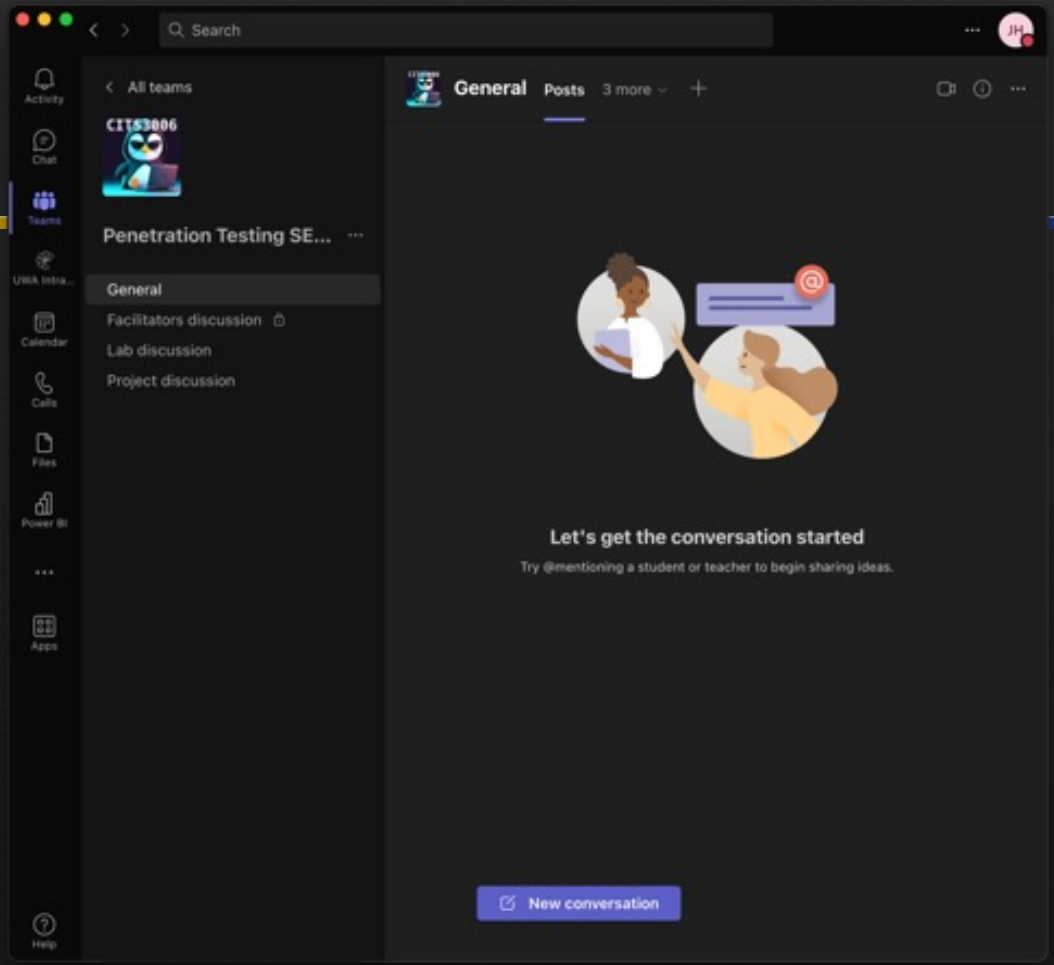
- General emergency: call campus security at 6488 2222
- In super emergency: call emergency at 000
- In all buildings, we have an emergency procedure such as this picture ->
  - Please take a time and read it.
- For more details, please have a read through our emergency procedure for various potential incidents
  - http://www.safety.uwa.edu.au/incidents-injuries-emergency/procedures

Location

- Lecture
  - Venue: MATH G18
  - Time: Mondays 1pm - 3pm
- Labs
  - Lab 1: EZONE CENT 210
  - Time: Mondays 3pm – 5pm
  - Lab 2: EZONE CENT 209
  - Time: Tue 1pm – 3pm
- Consultation
  - Office at Computer Science building room 1.10

Changes will be announced (if any)

Location


Search
Activity
Chat
Teams
UWA Intra...
Calendar
Calls
Files
Power BI
Apps
Help
All teams
CITS3006
Penetration Testing SE...
General
Facilitators discussion
Lab discussion
Project discussion
General
Posts
3 more
Let's get the conversation started
Try @mentioning a student or teacher to begin sharing ideas.
New conversation

Labs – Help server

Labs – Help server

- For labs, we will be using the help server, which allow students to queue to get help
  - This means no fighting over who put their hands up first
  - Online people can get noticed better – but we shouldn't have any in this unit
  - Please note, You won't get help **outside** the scheduled lab hours!

- How it works:
  1. Login to the help server at: https://help.jinhong.org/
     - by default, you use your student ID with temporary password “helloworld” (unless you used this server before, then it will be whatever you set the password to)
     - You can change your password once you login (you have to re-login after)
     - Any issues logging in, contact any of the facilitators or the UC (either of us can reset it for you)
  2. Fill out the form and wait until a facilitator comes to you!
     1. Note: for the location, write the desk number for F2F students, and "online" for online students.
  3. If you are doing labs via online, then the facilitator will contact you via Teams!

Course overview: Term 3

Labs start first week!

Week	Lecture	Lab	Assessments
1	Ethics + Reconnaissance	Lab 0: Setup and Linux	
2	Network Exploits + Malware	Lab 1: Network Exploits	
3	More Malware	Lab 2: Malware	
4	Software Security		Lab Quiz 1
5	Reverse Engineering	Lab 3: Reverse Engineering	
6	Privilege Escalation	Lab 4: Privilege Escalation	

Course overview: Term 4

Week	Lecture	Lab	Assessments
7	Web Security		Lab Quiz 2
8	More Web Security	Lab 5: Web Security	Project out
9	Defence Techniques	Lab 6: Active Directory	
10	Active Directory		Lab Quiz 3
11	Special Topic		Project due/demo
12	Guest Lectures and/or Revision		Project demo

Assessments

Assessment Item	When	Covers	Worth (total)
Lab Quizzes	Weeks 4, 7, A	The two labs before	60% (20% each)
Project			
Stream 1: Group Project	Week 8	Various	40%
Stream 2: Study Tour*	Project progresses through the semester. Study tour in Nov.	Various	40%

*Please note, the study tour is a failed component (i.e., if you fail this, you fail the unit).

Please note, all dates are tentative and subject to change!

How does the lab quiz work?

- During your scheduled lab time, you will be supervised by a lab facilitator to complete a timed lab quiz (~60 mins but can vary).
- You cannot receive mark if your attendance is not confirmed by the lab facilitator.
  - i.e., you must be supervised/invigilated by the lab facilitator to receive marks.
  - Attendance is required for all F2F students (unless a reasonable excuse is provided).
- You may be given a few slots during the labs, which you can sign up before the lab quiz starts (tbc).

How does the lab quiz work?

- We will be using a peer-marking system, where you will be formed into a group of 4 (or thereabout), and each person will have 15 mins to do the demo.
- Marking keys will be provided for peer markers to use and submit the report.
- The peer markers will also provide feedback to the demonstrator including the mark range.
- Facilitators will be available for any moderations and review of the peer marking process.
- All submitted peer marks will be reviewed, and finalised marks will be uploaded to csmarks.

Project

- The project consists of two streams
  1. Group project handling various penetration techniques and cybersecurity concepts
  2. Cybersecurity Practices and Cultures (Study Tour)

Stream 1: Group Project

- Details to be confirmed but this year I am thinking:
  - You will be put in a group
  - Part 1 (50%) : You will configure a vulnerable VM
  - Part 2 (30%) : You will exploit another group's VMs
  - Part 3 (20%): You will harden a randomly assigned VM (and demo Part 2)
  - Part 4 (steal points): You will exploit any hardened VMs
  - You will submit accompanying reports (group and individual)
  - Each part will be 1 week long.
  - But TBC.

Stream 2: Study Tour

You must complete Project Stream 1 as well (group project).

This year's theme is research, where you will work on a research project during the semester.

Study tour to Korea between 13 November – 3 December (~3 weeks)

- Funded travel with value up to $3000
  - Up to $2000 from my project grant
  - $1000 from GLO (you must apply and get approved).
  - To cover flight, accommodation and meals, further costs are covered by students

Stream 2: Study Tour

How to apply?

- Application essay - write at most one page about:
  - Why you want to participate in this study tour
  - Why you are a good candidate for this study tour
  - How can this study tour help you advance your career
- Up to 4 slots available for interested students:

  *No citizenship requirements (but you do need to get your own visa)

  *No age requirements

  *Preferences given to future research students (e.g., BACS)
- Please note, you should have a reasonably high WAM (70+)

Submit via Email
(due this Friday noon)

Prerequisite

- Prerequisites: 12 points of programming-based units
- This unit requires the student to be knowledgeable in various aspects of CS.
- Recommendations if you haven't done already:
  - CITS1003 Introduction to Cybersecurity
  - CITS2002 Systems Programming
  - CITS3002 Computer Networks
- This unit expects students to be knowledgeable in various programming languages such as Java, Python and C (or be able to quickly catch up).
- You should also be familiar with basic discrete mathematics and number theory.
- I highly recommend taking this unit in third year after taking various CITS units (including ones listed above) for preparations.

Please note

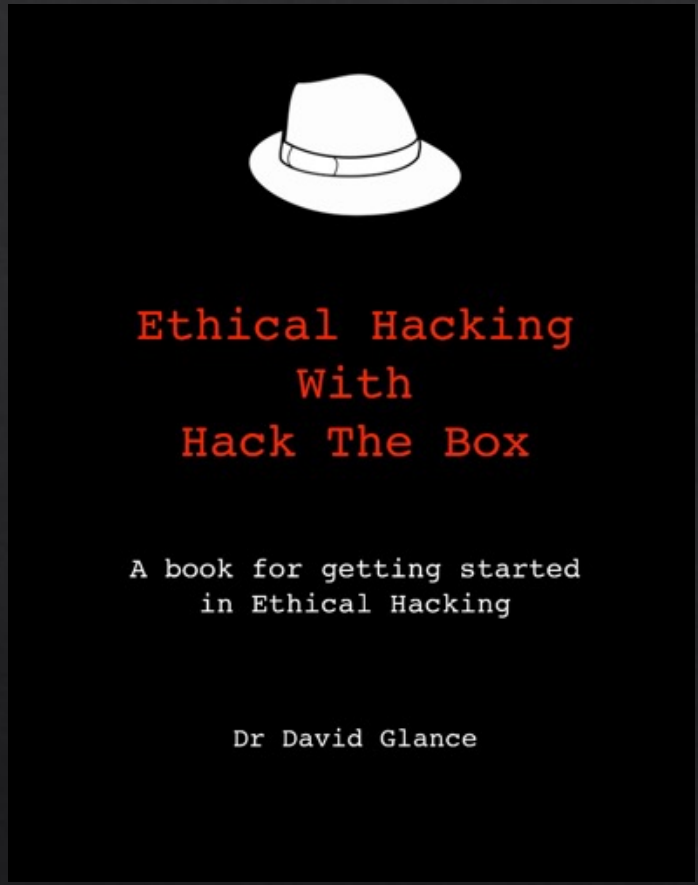
- This unit is/does NOT:
  - cover a comprehensive penetration testing techniques
    - Pentesting and cybersecurity is a broad discipline!
  - about all of the latest and greatest attacks
    - Covering selected but important fundamental themes
    - Read online sources instead to keep up to date
  - cover ethical, legal or economic issues
    - We will touch on ethical issues briefly later, but not focus on them

Please note

- Lectures provide **theoretical** and **conceptual** understandings of the topics presented
  - But we will also do some practicals in the lectures
  - So, you should bring your laptop if you want to try them in class as well
- Labs and project provide **practical skills** of the topics presented
- The contents in Lectures, labs and project will be related, but they are all **INDEPENDENT** learning materials
  - i.e., you will be learning new things in each lecture, lab and project.

Recommended reading

- Ethical hacking with Hack The Box
- A book by David Glance (former UWA academic)
- Available free online:
- https://book.ethicalhackinghtb.xyz/



Copyright notice

Commonwealth of Australia

Copyright Regulations 1969

WARNING

Materials in this unit (CITS3006 – Penetration Testing) have been reproduced and communicated to you by or on behalf of The University of Western Australia pursuant to Part VB of the *Copyright Act*1968 (**the Act**).

The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.