School of Science, Computing and Engineering Technologies

SWINBURNE UNIVERSITY OF TECHNOLOGY

Unit Outline

COS30015
IT Security

Semester 2 2022

Please read this Unit Outline carefully. It includes:

PART A Unit summary

PART B Your Unit in more detail

PART C Further information

PART A: Unit Summary

Unit Code(s)		COS30015
Unit Title		IT Security
Duration		2022 Semester 2
Total Contact Hours		4 hours per week
Requisites:		
	Pre-requisites	COS10009 Introduction to Programming or SWE20004 Technical Software Development and one of COS10005 Web Development or COS10011 Creating Web Applications or COS10026 Computing Technology Inquiry Project and one of TNE10005 Network Administration or TNE10006 Networks and Switching
	Co-requisites	
	Concurrent pre-requisites	
	Anti-requisites	
	Assumed knowledge	Database/web scripting and fundamentals of programming and networking.
Credit Points		12.5
Campus/Location		Hawthorn
Mode of Delivery		Face-to-face
Assessment Summary		1. Research project Individual 40% 2. Online Quiz Individual 20% 3. Practical project Individual 40%

Aims

Students who complete this unit of study:

- Will understand the nature of security threats to IT systems.
- Will be familiar with the tools used by hackers and crackers and be aware of ways ofidentifying and rectifying security breaches.
- Will understand how to assess the vulnerability of computing systems.

Unit Learning Outcomes

Students who successfully complete this Unit should be able to:

1. **Evaluate security of client and server computer.**

   Students will be able to describe and discover network services using a variety of tools and evaluate the security vulnerabilities of those services. Students will be able

to change default settings in Windows and common web browsers to minimise vulnerabilities.

Students will be able to describe and discover common vulnerabilities in Internet-based servers running Unix or Linux including web servers, scripting languages, database servers and permissions.

2. **Plan security audits.**

   Students will be able to develop a specific methodology for an audit for a particular server or system.

3. **Critically analyse the concepts of social engineering and physical security.**

   Students will be able to evaluate system risks based on human behaviour (for example password management), motivations of potential attackers and the degree of risk to a specific system or service.

   Students will be able to identify risks associated with access to computers, servers and network devices (e.g. keyloggers, boot disks, alternate operating systems, data recovery).

4. **Use a variety of security-related tools to identify attacks and mitigate attacks.**

   Students will be able to use DNS, network status and other system monitoring tools and draw conclusions from the output of such tools.

   Students will be able to identify Denial of Service attacks and other unwanted network-borne traffic (spam, messaging) and describe options for minimising the effects of such activities.

5. **Evaluate authentication and encryption systems.**

   Students will be able to describe authentication schemes (e.g. multi-factor) and encryption schemes (e.g. PGP, shared key, Certificates, SSH, IPSec) and describe their effectiveness.

6. **Research issues in IT Security systems.**

   Independently research and present a topic on IT security, including identifying technologies, issues, vulnerabilities and mitigation strategies.

Graduate Attributes

This unit may contribute to the development of the following Swinburne Graduate Attributes:

- Communication skills
- Teamwork skills
- Digital literacies

Content

- Overview of Internet Crime and computer security threats.
- Operating System Flaws.
- Security Tools
- System logs.
- Firewalls, security: theory, practice, design.
- Ports scanning, packet sniffing and intrusion detection.
- Understanding and responding to security alerts.
- Server technologies, risks and policies.
- Vulnerability analysis and Audit.
- Secure programming practices.
- Script injection and input sanitizing

- Security Models.
- Physical Security.
- Authentication (identity, biometrics and digital signatures).

PART B: Your Unit in more detail

Unit Improvements

Feedback provided by previous students through the Student Survey has resulted in improvements that have been made to this unit. Recent improvements include:

- Replace the final exam with a practical project in a move toward authentic assessment tasks, Merge two online tests into one and remove the hurdle as it is no longer required. ULOs amended as part of continuous improvement. Assessment ranges added.

Unit Teaching Staff

Name	Role	Room	Phone	Email	Consultation Times
Prof. JunZhang	Convenor	Hawthorn EN511b	392143823	junzhang@swin.edu.au	by appointment
Dr. Rory Coulter	Lecturer			rjcoulter@swin.edu.au	
Lin Li	Lecturer			linli@swin.edu.au	
JAMIE OOI	Tutor			jooi@swin.edu.au	
Daniel Hood	Tutor			dhood@swin.edu.au	
Andrew Plapp	Tutor			aplapp@swin.edu.au	
Yasas AkuruddaLiyanage Don	Tutor			yakuruddaliyanagedon@swin.edu.a	

Learning and Teaching Structure

Activity	Total Hours	Hours per Week	Teaching Period Weeks
Lectures	24 hours	2 hours	Weeks 1 to 12
Laboratory Work	24 hours	2 hours	Weeks 1 to 12

2 hour lectures every week, for one hour video-streaming lecture and one hour live-streaming lecture.

2 hour laboratory class every week including week 1.

In a Semester, you should normally expect to spend, on average, twelve and a half hours of total time (formal contact time plus independent study time) a week on a 12.5 credit point unit of study.

Week by Week Schedule

Week	Week Beginning	Teaching and Learning Activity	Laboratory	Podcast/ Reading	Student Task or Assessment
1	Aug 1	Overview: Security concepts and models, usability issues, types of threats, Security Terminology, What's Legal Security Resources.	Linux Lab. Listen to *Security Now* episodes 50, 53, 57.	*Security Now* 1, 47, 65. *Risky Business* 217. *Goodrich* Chapter 1	
2	Aug 8	Physical and Converged Security: Authentication, Forensics,Physical access attacks. Recent threats	Network lab	*Security Now* 211, 213, 137, 90, 94, 291 *Risky Business* 240, 163. 159, 129, 73, 70, 52,51 *Goodrich* Chapter 2	Release Assignment 1
3	Aug 15	Operating System security:Access control, buffer overflows, virtualisation, DEP, ASLR, sandboxing.	Buffer overflows	Security Now 39, 53, 54, 55, 78, 172, 174, Risky Business 152, 120 Goodrich Chapter 3	
4	Aug 22	Malware: Types, attacks, examples, countermeasures. GhostRAT, WannaCry, Stuxnet Flame, BEAST, Zeus, CRIME	Malware RATs and remote access Buffer Overflows	Security Now 8, 9, 21, 22, 191, 193, 321, 353 Risky Business 67, 170, 169, 160, 17 Goodrich Chapter 4	
5	Aug 29	Network Security 1: Revision, hardware, protocols, layers. MITM, DDOS attacks	Denial of Service	Security Now 25, 26, 27, 29, 195, 313, 319. Risky Business 11, 187, 188, 189 Goodrich Chapter 5	
6	Sept 5	Network Security 2: DNS, SSH, IPSec, VPNs,	Firewalls, nmap, Wireshark,	Security Now 11, 13, 155,	Research projectdue

		Intrusions, WiFi	netstat, ifconfig	170, 260, 335, 337, 355. Risky Business 87. Goodrich Chapter 6	Thursday 23:59
	Sept 12	Non-teaching week			
7	Sept 19	Web Security: cookies, session hijacks,XSS, defences	Online quiz in the lab.	Security Now 85, 86, 87, 166, 168, 217, 219, 221, 225, 285. Risky Business 174 Goodrich Chapter 7	Online quiz *taken in this labclass.*
8	Sept 26	Cryptography: pre-shared key symmetric key asymmetric key PGP / GPG SSH / SSL brute force attack authentication digital certificates	XSS, cookies	*Security Now* 125, 151, 179, 181, 183, 185, 195, 243. *Risky Business* 187, 197, 212 *Goodrich* Chapter 8	
9	Oct 3	Security Models: Trust, Access control models, standards, patching, Vulnerability, Disclosure, Encryption, TPM, code signing.	Crypto	Security Now 99, .307, 319 Risky Business 141, 217, 230 Goodrich Chapter 9	
10	Oct 10	Web Application Security: Transaction processing, e-mail, Credit card security, DRM, social networking, SQL injection, Spam.	SQL Injection	*Security Now Risky Business 102* *Goodrich* Chapter 10	
11	Oct 17	Cloud security and law: Virtualisation security, PIE,TNO, Risk, Jurisdictional issues	Metasploit	Cloud-security-guidance	
12	Oct 24	Revision Lecture and guest talk	TBA	TBA	Practical projectdue Sunday 23:59

Assessment

a) Assessment Overview

Tasks and Details	Individual or Group	Weighting	Unit Learning Outcomes that this assessment task relates to	Assessment Due Date
Online quiz	Individual	20%	1, 2, 4	Week 7 starting 21th Sept
Research project	Individual	40%	1,2,4,6	8th Sept
Practical project	Individual	40%	1,2,3,4,5	30th Oct

b) Minimum requirements to pass this Unit

To pass this unit, you must:

- achieve an overall mark for the unit of 50% or more

c) Examinations

If the unit you are enrolled in has an official examination, you will be expected to be available for the entire examination period including any Special Exam period.

No exam for this unit.

d) Submission Requirements

Assignments and other assessments are generally submitted online through the Canvas assessment submission system which integrates with the Turnitin plagiarism checking service.

Please ensure you keep a copy of all assessments that are submitted.

In cases where a hard copy submission is required an Assessment Cover Sheet must be submitted with your assignment. The standard Assessment Cover Sheet is available from the Current Students web site (see Part C).

e) Extensions and Late Submission

Late Submissions - Unless an extension has been approved, late submissions will result in a penalty. You will be penalised 10% of your achieved mark for each working day the task is late, up to a maximum of 5 working days. After 5 working days, a zero result will be recorded.

Extensions will only be granted in exceptional circumstances, on medical or compassionate grounds. Extensions must be applied for in advance of the due date (except in emergencies). Students should contact the convener by phone or in person to apply for an extension. Medical or other certificates will be required. The convener must sign the bottom of the assignment cover sheet when approving the extension.

f) Referencing

To avoid plagiarism, you are required to provide a reference whenever you include information from other sources in your work. Further details regarding plagiarism are available in Section C of this document.

Referencing conventions required for this unit are: Vancouver (as used by IEEE).

Helpful information on referencing can be found at https://www.swinburne.edu.au/library/referencing/

https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf

Helpful information on referencing can be found at http://www.swinburne.edu.au/library/referencing/

g) Groupwork Guidelines

A group project is the collective responsibility of the entire group, and if one member is temporarily unable to contribute, the group should be able to reallocate responsibilities to keep to schedule. In the event of longer-term illness or other serious problems involving a member of a project group, it is the responsibility of the other members to make the project supervisor aware of the situation straight away.

Group project reports must be submitted with the project cover sheet, signed by all members of the group.

All group members must be satisfied that the work has been correctly submitted. Any penalties for late submission will apply to all group members, not just the person who submitted.

Required Textbook(s)

The required textbook(s) are available from Swinburne Bookshop: http://bookshop.swin.edu.au

Reference books may available as electronic resources (use the links listed) or in print from the Swinburne library (Hawthorn branch).

• Introduction to Computer Security, M T Goodrich and R Tamassia, Addison Wesley (Pearson), any edition.

Recommended Reading Materials

The Library has a large collection of resource materials, both texts and current journals. Listed below are some references that will provide valuable supplementary information to this unit. It is also recommended that you explore other sources to broaden your understanding.

• Gray Hat Hacking, The ethical hacker's handbook 3rd. ed, A Harper [et al.], McGraw-Hill 2011

• Hands-on Ethical Hacking and Network Defense, Michael T Simpson, Thomson 2006

• Computer Security Fundamentals, Chuck Easttom, Pearson/Prentice Hall NJ, 2006.

• Advanced Guide to Linux Networking and Security, Ed Sawicki, Nicholas Wells, Thomson/Course Technology Australia, 2006.

• Please check updated unit website in Canvas for more

References:

- *Podcasts* can be obtained from http://risky.biz, http://www.grc.com/SecurityNow.html

andhttp://www.twit.tv
- *Buffer overflow attacks- detect, exploit, prevent.* James C. Foster ... [et al.], http://ezproxy.lib.swin.edu.au/login?url=http://library.books24x7.com/library.asp?^B&bookid=94 03
- *Aggressive network self-defense,* Neil Archibald ... [et al.], http://ezproxy.lib.swin.edu.au/login?url=http://library.books24x7.com/library.asp?^B&isbn=1931 836205
- *Network Defence and Countermeasures Principles and Practice*, Chuck Easttom,Pearson/Prentice Hall, NJ, USA, 2005.

PART C: FURTHER INFORMATION

For further information on any of these topics, refer to Swinburne's Current Students web page http://www.swinburne.edu.au/student/.

Student behaviour and wellbeing

All students are expected to: act with integrity, honesty and fairness; be inclusive, ethical and respectful of others; and appropriately use University resources, information, equipment and facilities. All students are expected to contribute to creating a work and study environment that is safe and free from bullying, violence, discrimination, sexual harassment, vilification and other forms of unacceptable behaviour.

The Student Charter describes what students can reasonably expect from Swinburne in order to enjoy a quality learning experience. The Charter also sets out what is expected of students with regards to your studies and the way you conduct yourself towards other people and property.

You are expected to familiarise yourself with University regulations and policies and are obliged to abide by these, including the Student Academic Misconduct Regulations, Student General Misconduct Regulations and the People, Culture and Integrity Policy. Any student found to be in breach of these may be subject to disciplinary processes.

Examples of expected behaviours are:

- conducting yourself in teaching areas in a manner that is professional and not disruptive to others
- following specific safety procedures in Swinburne laboratories, such as wearing appropriate footwear and safety equipment, not acting in a manner which is dangerous or disruptive (e.g. playing computer games), and not bringing in food or drink
- following emergency and evacuation procedures and following instructions given by staff/wardens in an emergency response

Canvas

You should regularly access the Swinburne learning management system, Canvas, which is available via the Current Students webpage or https://swinburne.instructure.com/ Canvas is updated regularly with important unit information and communications.

Communication

All communication will be via your Swinburne email address. If you access your email through a provider other than Swinburne, then it is your responsibility to ensure that your Swinburne email is redirected to your private email address.

Academic Integrity

Academic integrity is about taking responsibility for your learning and submitting work that is honestly your own. It means acknowledging the ideas, contributions and work of others; referencing your sources; contributing fairly to group work; and completing tasks, tests and exams without cheating.

Swinburne University uses the Turnitin system, which helps to identify inadequate citations, poor paraphrasing and unoriginal work in assignments that are submitted via Canvas. Your Unit Convenor will provide further details.

Plagiarising, cheating and seeking an unfair advantage with regards to an exam or assessment are all breaches of academic integrity and treated as academic misconduct.

Plagiarism is submitting or presenting someone else's work as though it is your own without full and appropriate acknowledgement of their ideas and work. Examples include:

- using the whole or part of computer program written by another person as your own
- using the whole or part of somebody else's written work in an essay or other assessable work, including material from a book, journal, newspaper article, a website or database, a set of lecture notes, current or past student's work, or any other person's work
- poorly paraphrasing somebody else's work
- using a musical composition or audio, visual, graphic and photographic work created by another
- using realia created by another person, such as objects, artefacts, costumes, models
- submitting assessments that have been developed by another person or service (paid or unpaid), often referred to as contract cheating
- presenting or submitting assignments or other work in conjunction with another person or group of people when that work should be your own independent work. This is regardless of whether or not it is with the knowledge or consent of the other person(s). Swinburne encourages students to talk to staff, fellow students and other people who may be able to contribute to a student's academic work but where an independent assignment is required, the work must be the student's own
- enabling others to plagiarise or cheat, including letting another student copy your work or by giving access to a draft or completed assignment

The penalties for academic misconduct can be severe, ranging from a zero grade for an assessment task through to expulsion from the unit and, in the extreme, exclusion from Swinburne.

Student support

Swinburne offers a range of services and resources to help you complete your studies successfully. Your Unit Convenor or studentHQ can provide information about the study support and other services available for Swinburne students.

Special consideration

If your studies have been adversely affected due to serious and unavoidable circumstances outside of your control (e.g. severe illness or unavoidable obligation), you may be able to apply for special consideration (SPC).

Applications for Special Consideration will be submitted via the SPC online tool normally no later than 5.00pm on the third working day after the submission/sitting date for the relevant assessment component.

Accessibility needs

Sometimes students with a disability, a mental health or medical condition or significant carer responsibilities require reasonable adjustments to enable full access to and participation in education. Your needs can be addressed by Swinburne's AccessAbility Services by negotiating and distributing an 'Education Access Plan'. The plan makes recommendations to University teaching and examination staff. You must notify AccessAbility Services of your disability or condition within one week after the commencement of your unit to allow the University to make reasonable adjustments.

Review of marks

An independent marker reviews all fail grades for major assessment tasks. In addition, a review of assessment is undertaken if your final result is between 45 and 49 or within 2 marks of any grade threshold.

If you are not satisfied with the result of an assessment, you can ask the Unit Convenor to review the result. Your request must be made in writing within 10 working days of receiving the result. The Unit Convenor will review your result to determine if your result is appropriate.

If you are dissatisfied with the outcomes of the review, you can lodge a formal complaint.

Feedback, complaints and suggestions

In the first instance, discuss any issues with your Unit Convenor. If you are dissatisfied with the outcome of the discussion or would prefer not to deal with your Unit Convenor, then you can complete a feedback form. See https://www.swinburne.edu.au/corporate/feedback/

Advocacy

Should you require assistance with any academic issues, University statutes, regulations, policies and procedures, you are advised to seek advice from an Independent Advocacy Officer at Swinburne Student Life.

For an appointment, please call 03 9214 5445 or email advocacy@swin.edu.au For more information, please see https://www.swinburne.edu.au/current-students/student-services-support/advocacy/