Unit of Study: ICT5351 Cyber Defence

Overview

In this unit students explore cyber threats from a personal, corporate and national security perspective. Students study the principal motivations behind cyberattacks, which may be political, ideological, revenge, or profit-based. These attacks are examined with a focus on analysing the system vulnerabilities that 'hackers' exploit. The unit also covers how to defend against cyberattacks through the use of policy, procedure and technical controls. Finally, 'ethical hacking' is also considered as a strategy to strengthen cyber defence.

Course	Master of Information Technology
Credit Points	8 credit points
Duration	12 weeks (10 teaching weeks; 1 revision week; 1 final assessment week)
Level	Postgraduate Advanced
Student Workload	Students should expect to spend approximately 13 hours per week over 12 weeks (totalling approximately 156 hours) on learning activities for this unit.
Mode(s) of Delivery	On campus, Blended
Pre-Requisites	ICT5250 Computer Networks and Security
Unit Coordinator	As per current timetable
Contact Information	Consultation: 1 hour scheduled session

Unit Learning Outcomes

On successful completion of this unit, students will be able to:

ULO1 Analyse trends in cyberattacks.

ULO2 Defend against different techniques used by intruders to penetrate a system.

ULO3 Analyse the motivation, tactics/strategy, and impacts of cyberattacks highlighting the system vulnerabilities exploited.

ULO4 Critique security policy, procedural and technical controls and countermeasures to mitigate the threats of cyberattacks.

Weekly Schedule

Detailed information for each week's activities can be found on Unit's Weekly Modules in Canvas.

Week	Topic
Week 1	Cyberattack motivations including hacktivism, private sector, and military
Week 2	Cyber espionage, sabotage, terrorism and warfare including nation state malware
Week 3	Cyber monitoring, surveillance and intelligence
Week 4	SCADA systems and public infrastructure
Week 5	Ethical hacking part 1
Week 6	Ethical hacking part 2
Week 7	Cyberattacks and defences part 1 • Defending in-depth
Week 8	Cyberattacks and defences part 2 • Defending networks
Week 9	Cyberattacks and defences part 3 • Defending data
Week 10	Cyberattacks and defences part 4 • Defending applications and Operating systems
Week 11	Revision
Week 12	Final Assessments

Assessments

1. All assessments are compulsory.
2. To pass the unit students must:
   - achieve a total of 50% or more of marks offered; and
   - pass all individual invigilated assessments; and
   - have attempted all assessments.

   Where one or more of these requirements are not met, the Board of Examiners will consider a student's overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision.
3. The Board of Examiners may grant a supplementary assessment where a student:
   - achieves a total of 45% or more; and
   - has passed all individual invigilated assessments in the unit; and
   - has attempted all assessments; and
   - has a recommendation for supplementary assessment by the Unit Coordinator and the Head of Discipline.

   Where one or more of these requirements are not met, the Board of Examiners will consider a student's overall progress towards meeting the unit learning outcomes and any special circumstances before reaching a decision. Attendance and engagement in class will be considered.
4. APIC awards common result grades as set out in the Award of Grade Policy.
5. Detailed information for each assessment can be found on the Unit's Home Page and in the Assessment Brief.

Assessment Task	Type	Weighting	Due	Length	ULOs
Assessment 1: Weekly Workshop Activity Students will complete in class workshop assessments including on-line quizzes, situation analyses and practical application of skills.	Individual Invigilated	25%	Weeks 2, 3, 6, 7, 8	(equiv. 1200 words)	ULO1 ULO2 ULO3 ULO4
Assessment 2: Quiz Students will complete in class on-line quizzes,	Individual	10%	Week 5	15 minutes (equiv. 300 words)	ULO1 ULO3
Assessment 3: Case Study Report Analysis specific cyber events to understand the actors' motivations, strategies adopted, their impacts, and potential defensive strategies.	Individual	35%	Week 8	3000 words	ULO3 ULO4

Assessment 4a: Case Studies For a given set of cyberattacks mechanisms, investigate where these have occurred, what system vulnerabilities were exploited, and their impact. Propose potential mitigation strategies that could prevent or reduce the incidence of such incidents as well as their impact. **Assessment 4b: Oral Defence** The group will defend their findings in Assessment 3a and justify the mitigation strategies proposed.	Group	Part A 20% Part B 10%	Part A Week 11 Part B Weeks 11, 12	Part A 3000 words Part B 15 minutes (equiv. 1500 words)	ULO1 ULO2 ULO4

equiv. – equivalent word count based on the Assessment Load Equivalence Guide.

Prescribed text(s):

Whyte C. and Mazanec B., 2018, Understanding Cyber Warfare: Politics, Policy and Strategy, Routledge.

Recommended Readings:

Walker, M., 2019. CEH certified ethical hacker exam guide (Fourth edition. ed.). New York: McGraw-Hill Education.

Charles P, P. and Shari Lawrence, P., 2015. Security in Computing FIFTH EDITION.
Manjikian, M., 2019. Introduction to cyber politics and policy. CQ Press.
Seker, E. and Ozbenli, H.H., 2018, June. The concept of cyber defence exercises (cdx): Planning, execution, evaluation. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-9). IEEE.

Lee, S. and Kim, S., 2021. Blockchain as a cyber defense: opportunities, applications, and challenges. *IEEE Access*, *10*, pp.2602-2618.

Şenol, M., 2022, December. Cyber Security and Defense: Proactive Defense and Deterrence. In *2022 3rd International Informatics and Software Engineering Conference (IISEC)* (pp. 1-6). IEEE.

Paffenroth, R.C. and Zhou, C., 2019. Modern machine learning for cyber-defense and distributed denial-of-service attacks. *IEEE Engineering Management Review*, *47*(4), pp.80-85.

Academic integrity

Ethical conduct and academic integrity and honesty are fundamental to the mission of APIC and academic misconduct will not be tolerated by the College. It is the responsibility of every student to make sure that they understand what constitutes academic misconduct and to refrain from engaging in it. Please refer to APIC's Academic Integrity Policy for further details.

Other Important Information and Links

Special consideration If your academic work is impacted by significant documented illness, hardship, or other adverse circumstances beyond your control, you may make an application for Special Consideration. Please refer to the Assessment Policy for further details.	**Late submission** Penalties apply when work is submitted after the due date without approval. Please refer to the Assessment Policy for information about late submission.
Assessment appeals If you are concerned about a mark you have received for an assessment or final grade, you may apply to formally appeal the grade. Please see the Assessment Policy for further details.	**Award of grades** APIC awards common result grades, set out in the Award of Grade Policy.
Expectations of student conduct Students are expected to conduct themselves in a manner that is consistent with a safe and respectful study environment. More information can be found in the Student Code of Conduct.	**Study resources** APIC Library and Student Learning Support resources and services can be accessed via the Student Lounge or your Dashboard on the OLS (Canvas).
Student Services The Student Services team provides administrative support for students and handles enquiries about enrolment, timetables, important dates and submitting forms. More information can be found on the Student Services page on the OLS (Canvas).	**Key dates** Key dates through the academic year, including teaching periods, census, payment deadlines and exams can be found on the Academic Calendar section of the APIC website.

Changes and Updates to the Unit of Study Guide

This Unit of Study Guide may be updated and amended from time to time. Students will be notified of any changes to the unit via the Online Learning System (Canvas) space for the unit.

This Unit of study Guide was last modified on 20th of May 2024.