Digital Security and Forensics

AICT006-4-2-DSF Version 1

Introduction and Overview

Lecturer Information (Lecture)

Lecturer Name: Reshiwaran Jegatheswaran

Email: reshiwaran@staffemail.apu.edu.my

Pre-requisites for this module

- None

Synopsis

- This module is an introduction to a range of technologies associated with computer security and digital forensics.
- It will expose students to tools and mechanisms in achieving an ideal information security environment.
- Some of the content is mapped to CompTIA Security+ certification to provide knowledge on industry-relevant technologies and practices.
- Students will also be guided to perform digital forensics investigations following the correct methodology and process.

Course Learning outcomes, CLOs

At the end of this course, YOU should be able to:

1. Discuss security and forensic techniques and technologies in different scenarios.
2. Identify the existence of vulnerabilities in the given virtual machine using appropriate tools.
3. Propose appropriate solutions to patch the vulnerabilities.
4. Prepare forensic image file of Random Access Memory (RAM) and Hard Disk Drive (HDD) of the given virtual machine.

CLO - Course Learning Outcomes
PLO - Programme Learning Outcomes

Mapping of CLOs with MOEs Domain

8	Mapping of the Course Learning Outcomes to the Programme Learning Outcomes, Teaching Methods and Assessment : Please select the learning outcome Domain(LOD) for each PLO in the cells above it. E.g PLO1- Knowledge and Understanding, PLO2- Cognitive Skills, PLO3-Practical Skills													
	Course Learning Outcomes (CLO)	**Programme Learning Outcomes (PLO)**												**Teaching Methods**	**Assessment**
		Knowledge and Understanding,	Cognitive Skills,	Practical Skills,	Interpersonal Skill,	Communication skill,	Digital Skills,	Numeracy Skills,	Personal Skills,	Entrepreneurial Skills,	Ethics and professionalism			
		PLO1	**PLO2**	**PLO3**	**PLO4**	**PLO5**	**PLO6**	**PLO7**	**PLO8**	**PLO9**	**PLO10**	**PLO11**	**PLO12**		
	CLO 1	✓												Lecture, Tutorial	Final Exam
	CLO 2						✓							Tutorial	Group Assignment - Individual component
	CLO 3					✓								Tutorial, Case Study	Group Assignment - Individual component
	CLO4				✓									Tutorial, Case Study	Group Assignment - Group component

PLO1 - Knowledge and Understanding
PLO4 - Interpersonal Skill
PLO5 - Communication skill
PLO6 - Digital Skills

Teaching Strategies

- Lecture
- Tutorial
- Case Study (Individual and Group)

Assessment Methods

- Final Exam **(40%)**: CLO1
- Group Assignment & Individual, Presentation **(60%)**
  - Appraise Security issues
  - Propose solutions
  - Presentation

Student Learning Time (SLT)

- **Course Credit Value: 4**
- **Total Learning Hours:**
  - Lecture: 28 hours per semester
  - Tutorial / Case Study : 28 hours per semester

Course Content Outline

Lecture	Tutorial / Assignment
Security Concepts	Malicious Code
Cybersecurity Threats Landscape	Social Engineering, Physical and Password Attacks
Cryptography & PKI	Vulnerability Assessment and Testing
Identity and Access Management	Incidents Respond
Security Policies, Standards, and Compliance	Data Acquisition and Data Recovery
Risk Management and Privacy	Data Hiding and Obfuscation
Digital Forensics	Forensic Tools and Techniques

Achievement requirements

Undergraduate:

Marks	Alphabetical Grade	Grading Point	Classification
80-100	A+	4.0	Distinction
75-79	A	3.7	
70-74	B+	3.3	Credit
65-69	B	3.0	
60-64	C+	2.7	Pass
55-59	C	2.3	
50-54	C-	2.0	
40-49	D	1.7	Fail (marginal)
30-39	F+	1.3	Fail
20-29	F	1.0	Fail
0-19	F-	0	Fail

What is expected of you

- You should abide by all the rules & regulations of APU
  - Proper attire
  - No speaking of dialects
  - Attendance is compulsory and valid medical certificates or letters from parents /guardians must support any absence from class.
  - Three lateness will be equal to one absence
  - All pagers and handphones should be turned off during lectures.

What is expected of you

- **Additional do and don'ts due during Online Digital Learning (ODL) Session:**
  - **Join the session on time (Meeting list will be downloaded at any time after 15mins session start if join after 15mins without any reason attendance mark as late).**
  - **Attendance – automatically / manually.**
  - **Mute your mic – when not in use.**
  - **Q & A session please use your mic instead of meeting chat.**
  - **Participate / engage in the teaching and learning session.**

What support is available for you

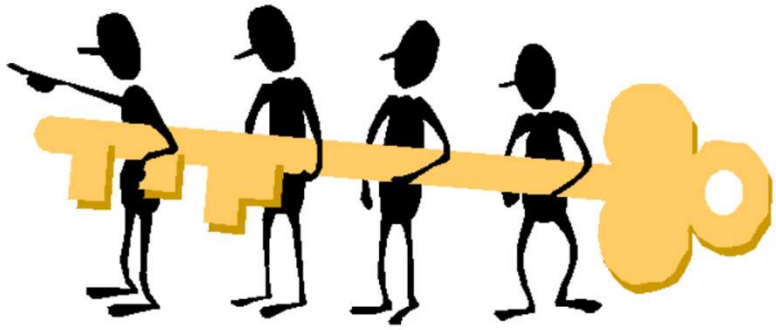
1. Consultation hours (Refer to the i-consult system)

2. Resources
   a. Tutorials Materials
      - MS Teams announcement
      - Moodle
   b. Reference material
   c. Essential Reading
      - Chapple, M., Seidl, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. 8th ed. John Wiley & Sons. USA. ISBN: 978-1119736257
      - Nelson, B., Philips, A. and Steuart, C. (2019) Guide To Computer Forensics and Investigations - Standalone Book. 6th ed. Cengage. USA. ISBN: 978-1337568944
      - Introduction to security and network forensics Technologies, William J. Buchanan 2011, CRC Press ISBN 9780849335686
   d. Internet resources

And when you need a shoulder to cry on
When you need a friend to rely on
When the whole world is gone
You won't be alone, cause I'll be here

I'll be your shoulder to cry on
I'll be here
I'll be a friend to rely on
When the whole world is gone
You won't be alone, cause I'll be here

from the album *Tommy Page* (1988)



Question and answer session

A · P · U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Q & A

What we will cover next

- Week 1