THE UNIVERSITY OF WESTERN AUSTRALIA

DESK No. | | | |

FAMILY NAME: _____

GIVEN NAMES: _____

SIGNATURE: _____

STUDENT NUMBER: | | | | | | | | |

SEMESTER 2, 2021 EXAMINATIONS

CITS1003

Physics, Mathematics & Computing

Introduction to Cybersecurity

Department of Computer Science & Software Engineering

This paper contains: 7 Pages **(including title page)**

Time Allowed: **2:00** hours

INSTRUCTIONS:

This exam is marked out of 100 points and is worth 50% of the overall unit mark.

Question 1: 30 points
Question 2: 15 points
Question 3: 20 points
Question 4: 20 points
Question 5: 15 points

- Your name and ID number should be written on the cover page of the answer booklet.
- Please do NOT use a pencil or a red pen.
- Please use readable handwriting. What we cannot read we cannot mark.

THIS IS A CLOSED BOOK EXAMINATION

SUPPLIED STATIONERY	**ALLOWABLE ITEMS**
Answer book	

PLEASE NOTE

Examination candidates may only bring authorised materials into the examination room. If a supervisor finds, during the examination, that you have unauthorised material, in whatever form, in the vicinity of your desk or on your person, whether in the examination room or the toilets or en route to/from the toilets, the matter will be reported to the head of school and disciplinary action will normally be taken against you. This action may result in your being deprived of any credit for this examination or even, in some cases, for the whole unit. This will apply regardless of whether the material has been used at the time it is found.
Therefore, any candidate who has brought any unauthorised material whatsoever into the examination room should declare it to the supervisor immediately. Candidates who are uncertain whether any material is authorised should ask the supervisor for clarification.

Candidates must comply with the Examination Rules of the University and with the directions of supervisors.
No electronic devices are permitted during the examination.
All question papers and answer booklets are the property of the University and remain so at all times.

This page has been left intentionally blank

Question 1. (30 points) Approximately 30 mins

Scenario 1

A financial company that makes loans to people wishing to buy pet dogs has suffered a ransomware attack. The group, calling themselves the CyberCat Criminals (CCC) compromised a user's (Bob) username and password and were able to access the company's server which was the main machine that runs all the company's systems. Although Bob worked in Finance, he had administrator privileges on the server machine. The criminals exfiltrated data about the company's customers and then encrypted the disks of the server, leaving a ransom note demanding payment in Bitcoin in exchange for a decryption key. The forensic team were unable to tell when the attack was carried out because no logging was being done on that machine.

Question 1.1 (15 points)

You oversee the incident response team that has been called in to deal with the situation outlined in Scenario 1.

[1] (5 points) Describe the skills you would need for people on the team

[2] (10 points) Describe the 4 stages you would go through in handling the incident. Include at least 2 activities in each stage.

Question 1.2 (15 points)

Referring to Scenario 1, How was the company's systems and data impacted in terms of Confidentiality, Integrity and Availability, Authorization, Authentication, and Accountability.

[1] (6 points) Give a brief explanation of the term in your own words

[2] (9 points) Explain how each term relates, or does not, to the specific situations in Scenario 1.

Question 2 (15 points) Approximately 15 mins

Scenario 2

A company has asked you to undertake a risk management assessment of the laptops and mobile phones that the company's staff uses for work. A security consultant has outlined five possible threat actors as:

1) Criminals, 2) Cyber criminals, 3) Hardware failure, 4) Hard surfaces, 5) Cups of tea

Question 2.1 (5 points)

For each threat actor, list at least 1 vulnerability that if exploited, may result in an impact on the organisation

Question 2.2 (10 points)

For each risk, list possible controls that you could use to treat the risk. For each control, state the **control type and control function.**

Question 3 (20 points) Approximately 20 mins

Scenario 3

The head of sales of a company has been accused of meeting with the CEO of a competitor company. The accuser has provided a photograph of the two of them meeting in a public place (the central square in Berlin, Germany) at a specific date and time. The head of sales has claimed that the photo is a fake and you are brought in to do a forensic examination of the image. The accuser also claimed that emails were exchanged and documents with sensitive information shared with the CEO.

Question 3.1 (10 points)

What could you do to check whether the image is fake or not? Specifically, you need to verify if the image has been altered in any way and that the place, date, and time of the meeting matches that of the image.

Question 3.2 (10 points)

You have a memory capture file of the head of sales' laptop and a network log of all traffic for the past 3 months. What things could you look for in this file to see if indeed he had been negotiating some sort of deal with the competitor company?

Question 4 (20 points) Approximately 20 mins

Scenario 4

A company is concerned about the security of their new web application and brings you in as a cybersecurity consultant to advise them on how they can check the security of the application for any issues. The application allows users to log in and depending on their level of access, they can carry out different functions on the site. The CEO wants the testing to be quick.

Question 4.1 (10 points)

What type of testing would you do? What would you need to agree with the company CEO before starting the testing? What tools could you use?

Question 4.2 (10 points)

[1] (3 points) If you were to concentrate on a set of vulnerabilities, which set would that be and why?

[2] (3 points) Give 3 examples of vulnerabilities from that set.

[3] (4 points) What advice could you give the CEO about implementing controls to reduce the risk to the web application?

Question 5 (15 points) Approximately 15 mins

Scenario 5

When Edward Snowden (ES) wanted to contact journalists to share the information he had stolen from the NSA, he had a problem to overcome. He wanted to communicate via PGP (a public key encryption program) but couldn't communicate with the journalists because he didn't have their keys. To solve this problem, he used a trusted person, Micah Lee (ML) who was also a friend of the journalist Laura Poitras (LP). ES had the keys of ML.

Question 5.1 (15 points)

Using your knowledge of public key encryption, describe a sequence of messages to get ES the key he needed to communicate with LP. When answering, consider:

[1] What key did ES need to communicate with LP?
[2] How could he trust that he had the correct key from LP?

In all these communications, ES wanted all communications to be encrypted and to be sure that people could trust the sender's identity.

[3] Describe how ES, ML and EP could know with certainty that the sender of an email was the person they claimed to be?