UNIVERSITY OF WESTMINSTER

School of Computer Science and Engineering
TIMED ASSESSMENT SEMESTER 2 2020/21

Module Code:	**6COSC002W/6COSC008C**
Module Title:	**Security and Forensics**
Module Leader:	**Saman Hettiarachchi**
Exam Start Time:	**06/05/2021 at 14:30 LKT**
Recommended Exam End Time:	**06/05/2021 at 16:00 LKT**
Submission Window:	**1hr and 10 minutes**
Submission Deadline:	**06/05/2021 at 17:10 LKT**

Instructions to Candidates:

Please read the instructions below before starting the paper

- Module specific information is provided below by the Module Leader
- The Module Leader will be available during the exam release time to respond to any queries via the Discussion Board in the Assessment area of the module's Blackboard site
- As you will have access to resources to complete your assessment any content you use from external source materials will need to be referenced correctly. Whenever you directly quote, paraphrase, summarise, or utilise someone else's ideas or work, you have a responsibility to give due credit to that person. Support can be found at:

  https://www.westminster.ac.uk/current-students/studies/study-skills-and-training/researchskills/referencing-your-work
- This is an individual piece of work so do not collude with others on your answers as this is an academic offence
- Plagiarism detection software will be in use
- Where the University believes that academic misconduct has taken place the University will investigate the case and apply academic penalties as published in Section 10 Academic Misconduct regulations.
- ***Once completed please submit your paper via the Assignment content. In case of problems with submission, you will have TWO opportunities to upload your answers and the last uploaded attempt will be marked. Note that instructions on how to compile and submit your handwritten and/or typed solutions will have been sent to you separately.***
- ***Work submitted after the deadline will not be marked and will automatically be given a mark of zero***

Module Specific Information

- Attempt all questions.
- This paper has 4 questions.
- All questions carry 25 marks each.
- This exam is worth 50% of your marks for this module.

Please read the instructions below before starting the paper

- Throughout the Exam duration you must remain connected to this Zoom Meeting room using the IIT gmail accounts

- You must keep your video on, microphone off and audio level up in the Zoom meeting throughout the exam duration unless you have been asked to turn your mic on by an invigilator.

- You cannot leave the virtual exam hall (zoom meeting) during the first 30 minutes and during the last 30 minutes of the exam. You can only leave during 3.00pm – 4.40pm time window. If you want to leave during this period, you must type in 'Submitted' after submitting your answers and then leave the Zoom meeting.

- If you have any query, please raise your hand and wait for the invigilator to contact you.

- If you have any Exam questions related doubts, Please post your question in the discussion board available in assessment section in the Blackboard module page.

Question 1

a. A company that deals with sensitive data regularly recruits new employees as they keep on expanding rapidly and they are always in need of new staff. Identify which security principle you think is most appropriate for this type of organizations when giving access to new staff. Justify your answer.

(9 marks)

b. Companies and individuals are continuously subject to different types of threats whether internally, externally, intentionally or by mistake. Briefly explain each of the threat type categories and identify which CIA tenet it violates. Give an attack example for each threat type.

(10 marks)

c. When malicious hackers are planning an attack on a network environment they usually follow a structured process that is very similar to what penetration testers will do when assessing the strength of the environment they are testing. List at least three differences between the processes.

(6 marks)

Question 2

a. Explain why in a typical IT infrastructure the threats differ from one domain to another. Give an example to show the difference.

(10 marks)

b. SSL/TLS is a protocol suite that protects the application layer protocol HTTPS by encrypting data while in transit while keeping the header of the packet not encrypted. Explain why the head of the packet is not encrypted and a client and the server need to negotiate the cipher suite before the authentication can happen between them.

(8 marks)

c. Injection flaws in applications have been in top ten owasp vulnerabilities for a long period. Give a general overview of how injection flaws can be exploited and identify what are the measures that should be done to protect against them.

(7 marks)

Question 3

a. An intrusion detection system (IDS) is usually an effective method to detect different types of threats. List the different types of threats that an IDS can detect and explain what base rate fallacy is when it comes to the effectiveness of IDS.

(10 marks)

b. Rule based access control (RBAC) is an access control model that is widely used. Explain how Rule based access control works and why it requires administrators to be heavily involved. Identify a scenario where this access control model should be used.

(8 marks)

c. Explain what SSH is and briefly discuss the key exchange handshakes for connection establishment. Explain how SSH differs from VPN.

(7 marks)

Question 4

a. Security controls limit activities that might pose a risk to organizations. However regular reviewing of those controls is essential to make sure controls are effective and current. Identify activities that security reviews include and briefly explain each. Give an example of a tool or process that is used for each security control review identified.

(8 marks)

b. Digital forensics process is a rapid pace changing environment. This is due to the nature of attacks that are also changing and adapting to new technologies. Which digital forensics activity changed and why? Identify an example of attack that the change of the process is mainly recommended for.

(10 marks)

c. Suppose you are analysing a network attack event and you were asked to identify what vulnerability allowed such attack to happen.

1- Which of the TAARA methodology steps do you need to complete to be able to answer this question?

(4 marks)

2- Identify some of the challenges that a cyber incident investigator might face when attempting to investigate the source of the attack.

(3 marks)

END OF EXAM