UNIVERSITY OF WESTMINSTER

COLLEGE OF DESIGN, CREATIVE AND DIGITAL INDUSTRIES
School of Computer Science and Engineering
ONLINE EXAMINATION SEMESTER 2 2019/20

Module Code:	**6COSC002W/ 6COSC008C**
Module Title:	**Security and Forensics**
Module Leader:	**Ayman El Hajjar**
Release Time:	**06 May 2020 BST Time 10:00 AM**
Submission Deadline:	**06 May 2020 BST Time 13:00 PM**

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 Timed 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/research-skills/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 submission. 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

Here copy the original *Instructions to Candidate* from the first page of your exam.

You are advised (but not required) to spend the first ten minutes of the examination reading the questions and planning how you will answer those you have selected.

- Attempt all questions.
- Each answer is awarded 25 mark for being correct.
- This script must be handed in after the exam.
- This exam is worth 50% of your marks for this module
- This script must not be made available to students after the exam.

Question 1

a. A company wants to implement a centralized access control administration method for their staff. One of their main essential requirements is for the staff to be able to access the system remotely and while mobile. Which one you would recommend for them. Justify your answer.

(8 marks)

b. Explain how SSH key exchange works and discuss what it can potentially reveal if someone is sniffing this communication exchange.

(10 marks)

c. What is the difference between intrusion detection system (IDS) and intrusion prevention system (IPS). Give an example where each should be used.

(7 marks)

Question 2

a. Network level session hijacking attacks allow attackers to remotely take over sessions, usually undetected. Explain how this attacks happens over a TCP connection and recommend a solution to protect your network against it.

(12 marks)

b. Identify for each attack below whether it is an active attack or a passive attack. Justify your answer and briefly recommend a countermeasure for these attacks.
   1- Packet sniffing
   2- Dictionary attack

(8 marks)

c. There are three different type of viruses, they are system infector, file infector and Data infector. Explain how system infector works and briefly evaluate its threat level in comparison with the others.

(5 marks)

Question 3

a. It is essential for network administrators to know what is happening in their network. Different security monitoring exist for networks and computer systems.

1- List the various security monitoring types and explain each of them briefly.

(6 marks)

2- What are the different log information you can capture. Identify which of those logs information is essential to ensure accountability and which is essential to track application use.

(3 marks)

b. A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. State the different type of firewalls, explaining each briefly.

(9 marks)

c. Security principles tends to follow one of the ten security principles widely used. Explain the Least privilege and the Separation of privilege principles and give an example where each should be used.

(7 marks)

Question 4

a. Digital evidence is fragile. It can easily be destroyed or tampered with. It is essential for digital forensics analysts and investigators to handle evidence carefully. Identify what are the fundamental rules on how to handle evidence.

(6 marks)

b. When it comes to network forensics, forensic analysts need to look within the sources of Network-Based Evidence. There are many sources of network-based evidence in any environment. Discuss "Evidence in the air" evidence and how much forensics value they hold.

(8 marks)

c. Physical analysis is looking for things that may have been overlooked or are invisible to the user.

1- Identify the important steps a forensics analyst must undertake to retrieve or access the hidden and deleted files.

(4 marks)

2- Two important physical locations that should not be overlooked, swap file and unallocated space. Explain each of those two and identify how they can be used.

(7 marks)

END OF EXAM