UNIVERSITY OF WESTMINSTER
FACULTY OF SCIENCE & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

Module Title:	**SECURITY AND FORENSICS**
Module Code:	**6COSC002W / 6COSC008C**
Module Leader:	AYMAN EL HAJJAR
Date:	**03 MAY 2018**
Start:	**10:00**
Time Allowed:	**1.5 Hours**

INSTRUCTIONS FOR CANDIDATES

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.

Answer all questions.

Each question carries 25 marks.

THIS PAPER SHOULD NOT BE TAKEN OUT OF THE EXAMINATION ROOM

DO NOT TURN OVER THIS PAGE
UNTIL THE INVIGILATOR INSTRUCTS YOU TO DO SO

Question 1-

a. Briefly explain the differences between OSI layers and TCP/IP layers. (6 marks)
b. In term of cyber security, explain what each of the term below mean:
   - Threat (1 mark)
   - Vulnerability (1 mark)
   - Control (1 mark)
c. Attacks are usually grouped into four different types: Interception, interruption, modification and fabrication.
   - Explain what each of those types' means in term of the assets for a company. (8 marks)
   - Give an example of each of those attack types. (4 marks)

Question 2-

a. Define what elicitation is and explain how it can be used by hackers for information gathering. (6 marks)
b. Define the different attack stages listed below:
   - Reconnaissance (2 mark)
   - Scanning (2 mark)
   - Escalation (2 mark)
c. UDP and TCP are the two most used transport layer protocols.
   - State and briefly explain four features of UDP. (4 marks)
   - State and briefly explain four features of TCP. (4 marks)
   - Evaluate TCP and UDP in terms of security and speed of transmission. (5 marks)

Question 3-

a. A denial of service (DoS) attack is about one thing: making a service unavailable to a user. Answer the following questions the different types of DoS attacks:
   - Explain what the meaning of DoS is and how damaging it is for companies? (4 marks)
   - What is the difference between DoS and DDoS? (2 marks)
     - Give an example of a recent DDoS attack. (2 marks)
     - What is the disruptive technology that led to many DDoS attacks occurring in the last few years? Give an example of a recent attack. (4 marks)

b. Session hijacking is a method in which attackers are able to intercept and modify communications as well as provide some tricks and techniques attackers use.
   - State the three categories that session hijacking attacks fall in. (3 marks)
   - How is network level session hijacking achieved with TCP? (5 marks)
   - Identify a method that network security undertakes to determine if their network is susceptive to network level session hijacking attacks. (2 marks)
   - Explain what countermeasures can be taken to defeat and stop network level session hijacking attacks. (3 marks)

Question 4-

a. For any successful digital forensics investigation, it is extremely important to successfully collect, collate, preserve, and analyse the evidence. To begin with, we need to identify the sources of evidence for any investigation.
   - Briefly discuss evidence obtainable from within the network (8 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 “On the Wire” evidence and how much forensics value they hold. (6 marks)
   - Discuss “Authentication Servers” evidence and how much forensics value they hold. (6 marks)

c. There are many methods to investigate network forensics. One of those methodologies is TAARA investigation methodology
   - Explain TAARA methodology and all its stages (5 marks)

END OF EXAM