UNIVERSITY OF WESTMINSTER

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

Module Title:	**Security and Forensics**
Module Code:	**6COSC002W / 6COSC008C**
Module Leader:	Ayman El Hajjar
Exam Period:	May 2019
Time Allowed:	**90 Minutes**

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.

Attempt all questions.

Each answer is awarded 25 mark for being correct.

This exam is worth 50% of your marks for this module.

THIS PAPER MUST 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 difference between a passive and active attack **(6 marks)**

(b) Explain what IP spoofing is and why it is carried out **(7 marks).**

(c) Describe how a system can be protected against known exploit attacks **(2 marks)**

(d) Describe how a system can be protected against known man-in-the-middle **(2 marks)**

(e) Describe how a system can be protected against known Trojan horse **(2 marks)**

(f) Define the terms below. **(6 marks)**

1. Interception
2. Fabrication
3. Vulnerability
4. Threat

Question 2

(a) Define what “pretexting” is and explain how it can be used by hackers for information gathering **(5 marks)**

(b) To protect your organization from a cyber-attack, it’s important to understand how an attacker goes about stealing sensitive information. What are the typical stages that an attack goes through? **(8 marks)**

(c) UDP and TCP are two transport layer protocols mostly used in our Internet communication. Evaluate how suitable TCP and UDP are for the two different services listed below and justify your answers **(4 marks).**

- Online Gaming
- Secure shell connection

(d) TCP is a connection-oriented protocol. Explain how TCP ensure reliability of its connection and how it can guarantee delivery of data. **(8 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 on the different types DoS:

1. Explain what the meaning of DoS is and how damaging it is for companies. **(4 marks)**
2. What is the difference between DoS and DDoS? **(2 marks)**
3. Give an example of a recent DDoS attack. **(3 marks)**
4. What was the disruptive technology that made DDoS more damaging than ever before? **(3 marks)**

(b) Session hijacking is a serious threat for end devices and servers likewise.

1. Explain what blind hijack attack is **(4 marks)**
2. Describe how you can identify how vulnerable your network is to session hijacking **(4 marks)**

(c) HTTP and HTTPS are two of the most used application layer protocols.

1. Explain what the difference between them is. **(2marks)**
2. Show the process that HTTPS uses with SSL and TLS to encrypt messages. **(3 marks)**

Question 4

(a) 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.

1. Discuss “Central log servers” evidence and how much forensics value they hold. **(5 marks)**
2. Discuss ‘routers” evidence and how much forensics value they hold. **(4 marks)**

(b) Network-based evidence poses special challenges in several areas including acquisition, content, storage, privacy, seizure and admissibility.

1. Explain why acquisition is a challenge in network-based evidence **(4 marks)**
2. Explain why privacy is a challenge in network-based evidence **(4 marks)**

(c) For a successful investigation, it is extremely important to know how to handle the evidence. A set of fundamental rules should be followed.

1. List those rules and explain them briefly **(3 marks)**
2. What are the characteristics for getting to satisfactory completion of a digital forensics case? **(5 marks)**

END OF THE EXAM PAPER