Dublin Business School

QQI

MSc in Information Systems with Computing

SUMMER 2020 EXAMINATIONS

Module Code: **B9IS103**

Module Description: **Computer Systems Security**

Examiner: **Mr. Gordon Reynolds**

Internal Moderator: **Mr. David Williams**

External Examiner: **Mr. Sean Russell**

Date: *Wednesday, 29th April 2020*
Time: *09:30-11:30*

INSTRUCTIONS TO CANDIDATES

Time allowed is 2 hours
Question 1 is COMPULSORY for ALL students
Answer any 2 Questions out of the remaining 3 Questions
Question 1 carries 40 marks
All other questions carry 30 marks

QUESTION ONE (COMPULSORY)

a) In relation to ***Encryption***, explain the following terms: **(4 Marks)**
   a. Plain Text
   b. Cipher Text

b) In relation to ***Firewalls***, briefly explain what is meant by ***SPI***. **(4 Marks)**

c) In relation to **Information Security**, distinguish between a ***Virus*** and a ***Worm***. **(4 Marks)**

d) Explain ***AAA*** and how it is used in a network environment. **(4 Marks)**

e) Briefly explain the term ***Confusion*** in relation to ***Encryption***. **(4 Marks)**
Give an example of a Cipher type that adds confusion.

f) Explain what an ***ACL*** is in relation to network security. **(4 Marks)**

g) In relation to ***Cyber-Security,*** define the following terms: **(4 Marks)**
   i. Vulnerability
   ii. Malware

h) Explain what ***RADIUS*** is and how it is used in a network environment. **(4 Marks)**

i) In relation to ***Encryption***, explain what is meant by ***Symmetric Encryption*** and ***Asymmetric Encryption***. **(4 Marks)**

j) In relation to configuring network equipment, briefly explain why **(4 Marks)**
   i. You should never use the default username and password.
   ii. You should use ***SSH*** over ***TELNET*** for device management

(TOTAL: 40 Marks)

QUESTION TWO

a) A core objective for an Information Security Officer (ISO), is to keep the information of a business secure. ***Explain what is meant by the term secure.*** **(4 Marks)**

b) Identify and explain the ***'Three must haves of an Attacker'***. **(6 Marks)**

c) Classify and describe the ***'Five factors of Authentication'***. **(8 Marks)**
Give examples in each case.

d) You have been recently hired by DevTech Corp. to conduct a security audit. **(12 Marks)**
Describe how you would organise and execute a basic security audit for DevTech.

(TOTAL: 30 Marks)

QUESTION THREE

a) It is generally agreed that network security commences with the design and topology of the network. Briefly discuss the previous statement by indicating security decisions commonly made during the network design process. **(4 Marks)**

b) Explain what is meant by the term ***Defence in Depth***. Illustrate your answer with a number of examples. **(6 Marks)**

c) In relation to network security, ***describe the following terms***: **(8 Marks)**
   a. IEEE 802.1X
   b. SSH
   c. IPSec
   d. DHCP Snooping

d) ***Explain the role of a DMZ in a network environment***. In your answer, refer to common DMZ topologies and how external and internal traffic accesses the DMZ. Use diagrams where appropriate. **(12 Marks)**

(TOTAL: 30 Marks)

QUESTION FOUR

a) Briefly outline the role of a VPN in a business environment. Your answer should include reference to the basic operation of VPN. **(4 Marks)**

b) In relation to VPN, discuss: **(6 Marks)**
   i. Key Exchange between VPN peers
   ii. Perfect Forward Secrecy

c) Briefly discuss the following protocols in relation to VPN: **(8 Marks)**
   i. PPTP
   ii. L2TP over IPSec

d) Compare and contrast, a ***Site-to-Site VPN*** with a ***Remote-Access VPN***. **(12 Marks)**
In your answer, distinguish between their different uses, the technology used in each type of VPN and the advantages and disadvantages of each type of VPN.

(TOTAL: 30 Marks)