[CRT01]

UNIVERSITY OF BOLTON

SCHOOL OF ART & CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER TWO EXAMINATION 2022/2023

ETHICAL HACKING AND DIGITAL FORENSICS

MODULE NO.: SEC6202

Date: Tuesday 9th May 2023 **Time: 14:00 – 16:00**

INSTRUCTIONS TO CANDIDATES:

There are FIVE questions.

Answer FOUR questions.

All questions carry equal marks.

Individual marks are shown within the question.

QUESTION 1

a) Objectively assess the differences between risk, threat and vulnerability, and focus accurately on the discrepancy between residual risks and secondary risks

(10 marks)

b) ABC Company has established Business Continuity (BC) & Disaster Recovery (DR) plan; an Incident happened on Monday at 11.00 am.
The MTD =11 hours.
The RTO took precisely 3.30 hours, and the RPO needs 3 Hours.
Evaluate the following terms MTD, RTO, RPO, and SDO.
Do you think the company met the MDT in their Business Continuity & Disaster Recovery plan?

(15 marks)

QUESTION 2

a) Critically assess the concept of risk management in terms of impact, Discuss the qualitative, semi-quantitative and quantitative risk analyses.

(10 marks)

b) Objectively assesses security compliance standards and explains the Information Security Management System (ISMS) and ISO27001, and ISO27002.
Support your answer with examples and sacrificial schemes.

(15 marks)

PLEASE TURN THE PAGE….

QUESTION 3

a) In the Quantitative Risk Assessment, if the Asset value=£1880 and the exposure factor=40%, calculate the single and annual loss expectancy.
If you know that, after implementing the safeguard, the annual rate of occurrence was reduced from 6 times to 3,
And the cost of the solutions=£1890
Calculate the ROSI (Return On Security Investment).

(15 marks)

b) Fuzzing is a process of sending deliberately malformed data to a program in order to generate failures; Critically evaluates fuzzers (SPIKE) to find vulnerabilities.

(10 marks)

QUESTION 4

a) Critically evaluate the digital forensic memory analyses regarding the processes, connections, connscan, atom, clipboard, crashinfo.

(10 marks)

b) Accurately evaluate digital forensic techniques (e.g. imaging, digital investigations, and evidence analysis tools), and explain in detail how these tools can be used to collect and provide forensic evidence under the law.

(15 marks)

PLEASE TURN THE PAGE….

QUESTION 5

a) Critically evaluate the MSF framework, Why we need to use msfvenom, and PostgreSQL. Support your answer with examples.

(15 marks)

b) Critically analyse the difference between an SYN flooding attack and an SYN spoofing attack, and the goal of an HTTP flood attack.

(10 marks)

END OF PAPER