CRT02

UNIVERSITY OF BOLTON

SCHOOL OF CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER 2 EXAMINATION 2023/2024

ETHICAL HACKING AND DIGITAL FORENSICS

NO: SEC6202

Date: Tuesday 14th May 2024 **Time: 2:00 – 4:00pm**

INSTRUCTIONS TO CANDIDATES: **There are FIVE questions.**

Answer ANY FOUR questions.

All questions carry equal marks.

Individual marks are shown within the question.

School of Creative Technologies
BSc Computer Networks & Security
Semester 2 Examination 2023-2024
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 1

A) Critically evaluate the distinctions between risk, threat, and vulnerability, emphasising the nuanced differentiation between residual risks and secondary risks.

(10 marks)

B) Star Company has established a Disaster Recovery (DR) plan, and a significant incident took place on Wednesday at 10:00 am. The (MTD) was found to be 5 hours. The Recovery Time Objective (RTO) was precisely set at 3.30 hours, while the Recovery Point Objective (RPO) required 2 hours.
Assess the concepts of MTD, RTO, RPO, and SDO.
Do you believe the company effectively achieved the MTD as specified in its Business Continuity & Disaster Recovery plan? Provide a justification for your answer.

(15 marks)

Total 25 marks

PLEASE TURN THE PAGE

School of Creative Technologies
BSc Computer Networks & Security
Semester 2 Examination 2023-2024
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 2

a) Evaluate the concept of risk management in relation to its impact. Discuss the methodologies of qualitative, semi-quantitative, and quantitative risk analyses.

(10 marks)

b) Within the framework of Quantitative Risk Assessment, given an Asset value of £50,000 and an exposure factor of 34%, calculate both the single and annual loss expectancy. Additionally, assume that post the implementation of a safeguard, the annual rate of occurrence has reduced from 4 times to 2. With the solution cost amounting to £30,000, determine the Return On Security Investment (ROSI).

(15 marks)

Total 25 marks

QUESTION 3

Within the domain of software security testing, Fuzzing is employed as a method involving the intentional transmission of malformed data to a program to provoke failures. Critically analyse the effectiveness of the SPIKE fuzzer in identifying vulnerabilities.

(25 marks)

Total 25 marks

PLEASE TURN THE PAGE

School of Creative Technologies
BSc Computer Networks & Security
Semester 2 Examination 2023-2024
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 4

a) In the context of digital forensic memory analysis, conduct a critical assessment of the methodologies used for examining processes, connections, connscan, atom, clipboard, and crashinfo.

(10 marks)

b) Examine and evaluate various digital forensic techniques used in modern investigative practices. Provide a comprehensive analysis of their effectiveness, limitations, and ethical considerations in uncovering evidence and identifying digital crimes.

(15 marks)

Total 25 marks

QUESTION 5

a) In the realm of cybersecurity, critically assess the Metasploit Framework (MSF), focusing on its strengths, weaknesses, and overall effectiveness as a penetration testing tool in identifying vulnerabilities and testing network defences.

(15 marks)

b) In the context of cybersecurity, critically analyse the distinctions between a SYN flooding attack and a SYN spoofing attack, emphasizing their methodologies, potential impacts, and countermeasures. Furthermore, examine the objectives and tactics employed in an HTTP flood attack, and discuss its significance in the realm of cyber threats and network security.

(10 marks)

Total 25 marks

END OF QUESTIONS
END OF PAPER