[CRT02]

UNIVERSITY OF BOLTON

CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER 1 EXAMINATION 2021/2022

ETHICAL HACKING AND DIGITAL FORENSICS

MODULE NO: SEC6202

Date: Wednesday 12th January 2022 Time: 10:00 – 12:00

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

Answer FOUR questions.

All questions carry equal marks.

Individual marks are shown within the question.

BSc Computer Networks & Security
Semester One Examination 2021-2022
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 1

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

b) List some of the keys of ISO 13335- IT security risk assessment-that guide IT security management.
(9 marks)

c) In detail and examples, what are for means of authenticating user identity? Finally, list and briefly describe the principal threats to the security of passwords.
(8 marks)

BSc Computer Networks & Security
Semester One Examination 2021-2022
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 2

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

(7 marks)

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

(10 marks)

c) Critically analysis the difference between a SYN flooding attack and SYN spoofing attack, and the goal of an HTTP flood attack?

(8 marks)

PLEASE TURN THE PAGE….

BSc Computer Networks & Security
Semester One Examination 2021-2022
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 3

a) List and describe the classification of Intrusion detection systems based on the source and type of data analysis.

(8 marks)

b) In the Quantitative Risk Assessment, if the Asset value=£950,000 and the exposure factor=20%, calculate the single and annual loss expectancy.
If you know that, after implementing the safeguard, the annual rate of occurrence reduced from 3 times to 1,
And the cost of the solutions=£300.000.
Calculate the ROSI (Return On Security Investment).

(9 marks)

c) the process of fuzzing an application to find exploitable bugs. Vulnserver, critically evaluate fuzzers (SPIKE) to find vulnerabilities.

(8 marks)

QUESTION 4

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

(8 marks)

b) Companies often use forensics techniques in disaster recovery to retrieve the information they have lost. Give 2 (two) things that companies should do or put in place to assist this recovery before disaster strikes.

(7 marks)

c) 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?

(10 marks)

PLEASE TURN THE PAGE….

BSc Computer Networks & Security
Semester One Examination 2021-2022
Ethical Hacking and Digital Forensics
Module No. SEC6202

QUESTION 5

a) Critically evaluate the MSF and Armitage, what are the main differences between them. Support your answer with examples.

(15 marks)

b) What are the main differences in testing the hardware and software within the Security Assessment and Testing framework? Explain in detail the differences between Real User Monitoring (RUM): and Synthetic Performance Monitoring (SPM)

(10 marks)

END OF QUESTIONS