UNIVERSITY OF BOLTON

CREATIVE TECHNOLOGIES

BSC COMPUTER NETWORKS & SECURITY

SEMESTER ONE EXAMINATION 2019/2020

ETHICAL HACKING AND DIGITAL FORENSICS

MODULE NO: SEC6102

Date: Wednesday 15th January 2020   Time: 10:00 – 12:00

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

Answer **FOUR** questions.

All questions carry equal marks.

Individual marks are shown within the question.

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2019-2020
Ethical Hacking and Digital Forensics
Module No. SEC6102

QUESTION 1

a)   Social networking sites are becoming ever more popular, and many other sites now let users add each other as friends. Discuss the impact social context has on
(i)   Phishing;
(ii)   Reconnaissance;
(iii)   Confidentiality;
(iv)   Integrity.

(7 marks)

b)   Explain the difference between Risk, Threat and Vulnerability, highlighting the difference between risk and residual risk and the secondary risk.

(8 marks)

c)   In the Quantitative Risk Assessment, if the Asset value=£950,000 and the exposure factor=30%, 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=£100.000.
Calculate the ROSI (**R**eturn **O**n **S**ecurity **I**nvestment).

(10 marks)

PLEASE TURN THE PAGE….

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2019-2020
Ethical Hacking and Digital Forensics
Module No. SEC6102

QUESTION 2

a)   Examine the risk management concept in term of qualitative and semi-
quantitative and quantitative impact and risks.

(8 marks)

b)   The Children Act 2004 empowers the Government to establish child
protection databases for England and Wales, which will, it is hoped, identify
cases of child abuse at an early stage. These databases will be fed with
medical and school records, police intelligence data, and social work
assessments. Social workers, doctors, nurses, teachers and police officers
will be able to query them. Sketch possible database security threats and
how to mitigate them.

(10 marks)

c)   Using the ISO-27002 standard, discuss the CIA, DAD concepts needed for
information security.

(7 marks)

QUESTION 3

a)   Critically assess the Network scanning standard techniques, in particular
sweeping and port scan?
Support your answer with examples using hping3, fping, nmap, and zenmap.
(9 marks)

b)   Evaluate the vulnerabilities scanning techniques, discuss the Nessus scanner
and web-site vulnerabilities scanners, support your answer with examples and
diagrams. **(8 marks)**

c)   Assess DOS and DDOS in terms of Bandwidth/throughput, protocols and
software vulnerabilities attacks. **(8 marks)**

PLEASE TURN THE PAGE….

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2019-2020
Ethical Hacking and Digital Forensics
Module No. SEC6102

QUESTION 4

a) Explain with details and examples the following terms: LAND, TEARDROP, SYN flood and SMURF attacks.

(10 marks)

b) Discuss the Enumerations concept, methods and tools.
    State the steps and techniques to perform the enumerations.

(5 marks)

c) ABC Company has established Business Continuity (BC) & Disaster Recovery (DR) plan; an Incident happened on Monday at 9.00 am.
    The MTD =5 hours.
    The RTO took precisely 3.30 hours, and the RPO needs 3 Hour.
    Evaluate the following terms MTD, RTO, RPO, SDO?
    Do you think the company met the MDT in their Business Continuity & Disaster Recovery plan? **(10 marks)**

QUESTION 5

a) Critically evaluate the digital forensic memory analyses in term of the processes, connections, connscan, atom, clipboard and crashinfo.

(10 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 that will assist this recovery before disaster strikes.

(5 marks)

c) What is ment by multi-factor authentication? Evaluate different types of multi-factor authentication and explain biometrics, graphical passwords, captchas and one-time passwords.

(10 marks)

PLEASE TURN THE PAGE….

Creative Technologies
BSc Computer Networks & Security
Semester Two Examination 2019-2020
Ethical Hacking and Digital Forensics
Module No. SEC6102

QUESTION 6

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

(10 marks)

b)   Discuss Session Hijacking concepts and tools using examples and diagrams in terms of a typical session; discuss attack methods, session sniffing, and man in the middle attack.
How do you mitigate Session Hijacking?   **(15 marks)**

END OF QUESTIONS