Strathmore UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY

BACHELOR OF BUSINESS INFORMATION TECHNOLOGY

INFORMATION SYSTEMS AUDIT AND FORENSICS

END OF SEMESTER EXAMINATION

BBT4201: INFORMATION SYSTEMS AUDIT AND FORENSICS

DATE: 22nd November 2019 Time: 2 Hours

Instructions

1. This examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One

i. In establishing what evidence is admissible, many rules of evidence concentrate first on the _____ of the offered evidence.
   A. Relevancy
   B. Search and Seizure
   C. Material
   D. Admissibility

ii. _____ devices prevent altering data on drives attached to the suspect computer and also offer very fast acquisition speeds.
   A. Encryption
   B. Imaging
   C. Write Blocking
   D. Hashing

iii. If the Internet History file has been deleted, _____ may still provide information about what Web sites the user has visited.
   A. Cookies
   B. Metadata
   C. User profiles
   D. Sessions

iii. Which of the following is not a phase of major activities in the Incident Response Lifecycle?
   A. Operations
   B. Detection & Analysis
   C. Containment, Eradication & Recovery
   D. Preparation

iv. What is a "Jump Kit"?
   A. The tools needed to investigate in a remote location
   B. A written policy for a Public vendor shift
   C. A blueprint that seeks to avoid vendor lock-in
   D. A compliance catalogue for a vendor

v. Which of the following types of imaging techniques would be suitable for deriving RAM memory of an ongoing malware attack?
   A. Dead imaging
   B. Live imaging
   C. Encase imaging
   D. Raw imaging

vi. Which software tool can be used to automate playbooks?
   A. Autopsy
   B. FTK imager
   C. Fast incident Response
   D. X-ways forensics.

vii. Which of the following is a low cost tool for digital forensics?
   A. Autopsy
   B. FTK imager
   C. Fast incident Response
   D. X-ways forensics.

viii. Which of the following is not a part of the incident response plan?
   A. Expanded services catalogue
   B. Contact list
   C. Internal communication plan
   D. Network admin

ix. There is an ongoing denial of service attack. Which of the following would be an appropriate classification for the incident?
   A. High level
   B. Medium level
   C. Low level
   D. None of the above.

x. Which of the following are ways of detecting an incident?
   A. Users
   B. Third parties e.g. ISP's
   C. SIEMS
   D. All of the above.

xi. Which of the following can be audited?

   A. A business process
   B. A service
   C. A system
   D. None of the above

xii. Which of the following are not reasons why audits are carried out. Choose all that apply.

   A. Regulatory compliance
   B. To catch errant employees
   C. Ensure business objectives are met
   D. To create new policies

xiii. Which qualifications relate to IT-specific audits? Choose all that apply.

   A. CISA
   B. CPA
   C. AICPA
   D. ISO lead auditor

xiv. Which of the following is not a component of an audit?

   A. Hardware
   B. Software
   C. Operations
   D. Standards

(1 Mark each)

xv. Outline three key differences between en external and an internal audit.

(6 Marks)

Total (20 Marks)

The following scenario was taken from the website, https://www.cfreds.nist.gov/data_leakage_case/data-leakage-case.html , read it and use it to answer the questions that follow.

Scenario Overview

'Iaman Informant' was working as a manager of the technology development division at a famous international company OOO that developed state-of-the-art technologies and gadgets. One day, at a place which 'Mr. Informant' visited on business, he received an offer from 'Spy Conspirator' to leak of sensitive information related to the newest technology. Actually, 'Mr. Conspirator' was an employee of a rival company, and 'Mr. Informant' decided to accept the offer for large amounts of money, and began establishing a detailed leakage plan.

'Mr. Informant' made a deliberate effort to hide the leakage plan. He discussed it with 'Mr. Conspirator' using an e-mail service like a business relationship. He also sent samples of confidential information though personal cloud storage.

After receiving the sample data, 'Mr. Conspirator' asked for the direct delivery of storage devices that stored the remaining (large amounts of) data. Eventually, 'Mr. Informant' tried to take his storage devices away, but he and his devices were detected at the security checkpoint of the company. And he was suspected of leaking the company data.

At the security checkpoint, although his devices (a USB memory stick and a CD) were briefly checked (protected with portable write blockers), there was no evidence of any leakage. And then, they were immediately transferred to the digital forensics laboratory for further analysis.

The information security policies in the company include the following:

1. Confidential electronic files should be stored and kept in the authorized external storage devices and the secured network drives.
2. Confidential paper documents and electronic files can be accessed only within the allowed time range from 10:00 AM to 16:00 PM with the appropriate permissions.
3. Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.
4. All employees are required to pass through the 'Security Checkpoint' system.
5. All storage devices such as HDD, SSD, USB memory stick, and CD/DVD are forbidden under the 'Security Checkpoint' rules.

In addition, although the company managed separate internal and external networks and used DRM (Digital Rights Management) / DLP (Data Loss Prevention) solutions for their information security, 'Mr. Informant' had sufficient authority to bypass them. He was also very interested in IT (Information Technology), and had a slight knowledge of digital forensics.

Images were taken from the suspects Personal Computer, his flash disk and CD ROM for further investigation. You have been asked to analyse the images using the Autopsy Digital Forensics software.

i. Identify FIVE sources of evidence from the above scenario that you might use to prove that the suspect leaked the data keeping in mind Locard's exchange principle. What modules in Autopsy would you use to analyse each source of evidence?

(15 Marks).

ii. Outline FIVE key items that you would include in the final forensics report that you would create from the above scenario.

(5 Marks)

Total (20 Marks)

Question Three

i. List FOUR different types of image formats that you know of.

(4 Marks)

ii. What advantages does the AFF format have over the EnCase Format?

(2 Marks)

iii. Compare and contrast the incident response process with the digital forensics process, outlining two similarities and two differences.

(8 Marks).

iv. Name three rules of evidence and explain how digital evidence would support the rules you describe.

(6 Marks)

Total (20 Marks)

Question Four

i. Outline FOUR major types of Audits and explain their purpose.

(8 Marks)

ii. The following are controls that have been implemented in an organization. Categorize them as being: preventive, detective or corrective (by purpose), and whether they are administrative, technical or physical (by function).

a) A banner in a router warning users of consequences of unauthorized access.
b) A computer in front of a classroom kept under lock and key.
c) A policy in Strathmore University stating that students are not allowed to install software in the laboratory computers.
d) Database log files that record each and every user/ program activity including CRUD operations.
e) Biometric systems installed in the university library where students and staff scan their finger.
f) Training of users before implementation of a system so that they can know how to use the system appropriately.

Place your answer in a table like the one below. For example if you feel (a) is administrative and technical, place your answer as follows.

Number	Function	Purpose
A	Physical	Detective

(6 Marks)

iii. Explain the three basic characteristics of an audit highlighting their importance.

(6 Marks)

Total (20 Marks)

Question Five

Mr. John is an ICT manager at a large hospital. The hospital has a number of departments including core medical departments like Accident & Emergency, Maternity, Radiology etc. it also has support departments like accounting, ICT and purchasing and supplies. Mr. John feels that there is some fraud being perpetrated either in the accounts, ICT or accounts department or a collusion of all of them. He has discussed this with senior management and they have approached you as an information systems auditor to undertake a thorough audit of their information systems and report back any weaknesses in internal controls. They would like you as part of the engagement, to explain to them how you will undertake this activity.

i. Describe what steps you will take highlighting each and every activity that you will perform.

(15 Marks)

ii. Briefly state the role of IT auditing in the following:

a) IT governance
b) Risk management
c) Compliance & certification
d) IT security management
e) Quality management & quality assurance.

(5 Marks)

Total (20 Marks)