**MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**P.O. Box 972-60200 – Meru-Kenya**

**Tel: 020-2069349, 061-2309217. 064-30320 Cell phone: +254 712524293, +254 789151411**

**Fax: 064-30321**

**Website:** [**www.must.ac.ke**](http://www.must.ac.ke) **Email:** **info@must.ac.ke**

**University Examinations 2016/2017**

THIRD YEAR FIRST SEMESTER EXAMINATION

FOR THE DEGREE OF

BACHELOR OF SCIENCE IN COMPUTER SCIENCE AND FORENSICS

**CCF 3301: INCIDENT RESPONSE IN IT SECURITY**

**DATE: DECEMBER 2016 TIME: 2 HOURS**

**INSTRUCTIONS:** *Answer question* ***one*** *and any other* ***two***questions.

**QUESTION ONE (30 MARKS)**

1. With examples, differentiate between incident response and computer forensics (5 marks)
2. Discuss 5 types of incidences which a CSIRT would respond to (5 marks)
3. Explain some of the benefits of having an organized incident response program (5 marks)
4. What factors should be considered when deciding whether to include law enforcement in your incident response (5 marks)
5. You arrive at work a few minutes early one day. As you walk past a few of the open employee cubicles, you notice several of the IT staff viewing in appropriate images on their monitors. You also notice that an employee seems offended and upset about it.
6. Could this scenario lead to the formation of a computer security incident response team and why (5 marks)
7. Which of the organizations departments would need to be involved in the response and why. (5 marks)

**QUESTION TWO (20 MARKS)**

1. In the event of a security incident, outline the types of volatile information you would retrieve from a computer system before powering it off (5 marks)
2. Identify and explain three factors that are used to determine risk (6 marks)
3. Discuss how network topology affect incident response (4 marks)
4. Your boss asks you to monitor a co-worker’s email. What are factors which will influence your answer (5 marks)

**QUESTION THREE (20 MARKS)**

1. When interviewing a source of information (witness) for an incident;
2. Should you listen to his whole story first before taking any notes, or should you scribble down every remark when you first hear it? (5 marks)
3. How does you interview of a manager differ from discussing incidents with a system administrator (5 marks)
4. List and explain the qualities that an indecent response team leader should possess (5 marks)
5. Discuss the criteria you would want to consider when determining what resources you need to respond to a computer security incident (5 marks)

**QUESTION FOUR (20 MARKS)**

1. What considerations would you make when choosing a storage device for your forensic tools (5 marks)
2. In order to determine if executable files are associated with listening ports, what solution would you apply (5 marks)
3. Why is it unnecessary to obtain application logs during live response (5 marks)
4. Outline reasons why remotely viewing event logs not considered a sound practice (5 marks)

**QUESTION FIVE (20 MARKS)**

1. Discuss the steps necessary for a live data collection process (4 marks)
2. Distinguish between a netcat and a cryptcat (4 marks)
3. When probing an incident on a Unix or a Linux system why is it necessary to perform a live response on a rather than just shut down the system and perform a hard drive duplication? (4 marks)
4. During initial response lsof and netstat are important tools which are very similar. In which cases would one apply each of these tools exclusively (4 marks)
5. Explain the techniques for risk-related modeling and calculation (4 marks)