Reg.No. \_\_\_\_\_\_\_\_\_\_\_\_

G:\logo and QP Template\logo 3 Feb 2018 final.tif

**End Semester Examination – Nov/Dec – 2018**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA3017** | **Duration :** | **3hrs** |
| **Sub. Name :** | **INCIDENT RESPONSE AND COMPUTER FORENSICS** | **Max. marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Define Computer Security incident. | CO1 | 3 |
| b. | List the factors that affect the way an incident is handled. | CO1 | 4 |
| c. | Discuss the goals of Incident response. | CO2 | 5 |
| d. | Illustrate briefly the pre incident preparation | CO1 | 8 |
| (OR) | | | | |
| 2. | a. | Elaborate the seven major components of incident response. | CO1 | 10 |
| b. | Tabulate the common situations with response strategies and potential outcomes in incident response. | CO1 | 10 |
|  |  |  |  |  |
| 3. | a. | On what media do you store and use the forensic toolkit? Why? | CO3 | 5 |
| b. | How do you determine which executables are associated with listening ports? | CO3 | 5 |
| c. | Why is it unnecessary to obtain application logs during live response? | CO3 | 5 |
| d. | Why is remotely viewing event logs not considered a sound practice? | CO3 | 5 |
| (OR) | | | | |
| 4. | a. | What step is repeated twice in the live data collection process? Why is this important? | CO3 | 5 |
| b. | What is the difference between netcat and cryptcat? Why is this important during initial data collection? | CO3 | 5 |
| c. | Why is it important to record time/date stamps as one of the first steps in the live response? | CO2 | 5 |
| d. | Why perform a live response on a Unix system rather than just shut down the system and perform a hard drive duplication? | CO2 | 5 |
|  |  |  |  |  |
| 5. | a. | What is a Forensic duplicate? Explain. | CO4 | 5 |
| b. | Differentiate between a restored image and a mirror image. | CO4 | 5 |
| c. | Discuss the legal issues to be encountered when a forensic duplication tool is used. | CO4 | 5 |
| d. | Brief about any 2 tools to create forensic duplicate of hard drive. | CO4 | 5 |
| (OR) | | | | |
| 6. | a. | What are the primary differences between a forensic duplicate and a qualified forensic duplicate? | CO4 | 5 |
| b. | What is ODD? Discuss the portions of ODD package. | CO4 | 5 |
| c. | How do you create a Qualified Forensic Duplicate with EnCase? | CO4 | 10 |
|  |  |  |  |  |
| 7. | a. | Discuss in detail the types of storage media to recover digital evidences. | CO3 | 10 |
| b. | Write a detailed note on the two interface standards that most computer forensic analysts will encounter. | CO6 | 10 |
| (OR) | | | | |
| 8. | a. | Identify and explain the six layers of the file system. | CO4 | 10 |
| b. | Name five methods for hiding data on a hard drive, using the layers below the information classification layer only. How would you, as an examiner, detect these conditions? | CO4 | 10 |
|  | |  |  |  |
|  | | **Compulsory**: |  |  |
| 9. | a. | What are some tasks you need to perform on a forensic duplicate before you run string searches on the entire contents of the data set? | CO4 | 5 |
| b. | In your opinion, is it easier to perform forensic analysis of a Windows system or a Unix system? State three specific reasons why you made your selection. | CO4 | 5 |
| c. | How is static analysis of a hacker tool done? | CO6 | 5 |
| d. | Discuss the mitigation strategies for cybercrime. | CO5 | 5 |