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



**End Semester Examination – Nov / Dec – 2019**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **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. | Draw the incident Management lifecycle and explain. | CO1 | 15 |
| b. | Discuss the general computer security incidents and its impact to an organization. | CO1 | 5 |
| **(OR)** | | | | |
| 2. | a. | Outline the Information system disaster incidents and Natural disaster incidents. Compare Manmade disaster and Natural disaster in the information system environment. Analyze the ways in which both Manmade and Natural disaster can be managed efficiently and effectively. | CO1 | 20 |
|  |  |  |  |  |
| 3. | a. | Explain windows system initial incident response process, tasks and steps to prepare tool kit. | CO2 | 10 |
| b. | Design the goals of an internal data centre. Explain the process involved in monitoring/tracking the progress and achievement of the goals. | CO2 | 10 |
| **(OR)** | | | | |
| 4. | a. | As an incident management expert, draw general CSIRT Organization resources structure with roles and responsibilities for an IT organization. | CO2 | 10 |
| b. | Educate your classmate about the following tools and process diagram with an example   1. NETCAT 2. CRYPTCAT | CO2 | 5  5 |
|  |  |  |  |  |
| 5. | a. | Explain the following in detail:   1. Admissible evidences with an example. 2. Hardware device (Compact Disc - CD, Hard Disk - HD, Universal Serial Bus - USB) restoring with an example. 3. Forensic Duplication tool requirements and ways of duplication. 4. Mirroring with an example. | CO3 | 5  5  5  5 |
| **(OR)** | | | | |
| 6. | a. | Describe Restoring image, legal issue in handling forensic duplicate, creating qualified Forensic duplicate with Safe Back and EnCase tool. | CO4 | 20 |
|  |  |  |  |  |
| 7. | a. | Describe your understanding of Windows File Systems ( FAT and NTFS) and file System layout. Justify the usage of file system and its benefits. | CO4 | 10 |
| b. | Explain Integrated Drive Electronics(IDE), Small Computer and System Interface(SCSI) Standards, Drive cabling, where it is used and what is the significance of these devices? | CO4 | 10 |
| **(OR)** | | | | |
| 8. | a. | Explain the file system Layers in detail. | CO4 | 10 |
| b. | Explain the the various process in a file system from forensic analyst perceptive. | CO4 | 10 |
|  | | **Compulsory**: |  |  |
| 9. | a. | Identify where the evidence resides on the windows system and procedures to conduct windows system investigation for an incident. | CO6 | 10 |
| b. | Explain in a professional way “Audit Logs” and “Log Analysis” with an example. | CO6 | 10 |