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



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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA3020** | **Duration :** | **3hrs** |
| **Sub. Name :** | **INTRUSION DETECTION AND PREVENTION SYSTEM** | **Max. Marks :** | **100** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** |  | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. |  | Define and differentiate IDS and IPS. Discuss briefly on the analysis schemes of IDS and IPS. | CO1 | 20 |
| **(OR)** | | | | |
| 2. |  | Discuss misuse detection and explain the use of misuse detection in modern IDS and IPS systems. | CO1 | 20 |
|  |  |  |  |  |
| 3. |  | Explain the advantage and disadvantage of fuzzy logic and Bayes theory. | CO2 | 20 |
| **(OR)** | | | | |
| 4. |  | Define Artificial Neural networks and discuss briefly about Artificial Neural networks components and its functions. | CO2 | 20 |
|  |  |  |  |  |
| 5. |  | State the use of centralized IDS and IPS systems. Illustrate the implementation challenges in centralized IDS and IPS. | CO3 | 20 |
| **(OR)** | | | | |
| 6. |  | Discuss distributed IDS and IPS systems and explain briefly on implementation methods and advantages over centralized system. | CO4 | 20 |
|  |  |  |  |  |
| 7. |  | Define and illustrate functions of:   1. Detection insecurity 2. Threat Briefing 3. Quantifying risk 4. Return on Investment (ROI) | CO4 | 5  5  5  5 |
| **(OR)** | | | | |
| 8. |  | Deduce forensic tool selection and acquisition methods with respect to IDS and IPS. Illustrate the challenges in IDS and IPS data acquisition. | CO5 | 20 |
|  | | **Compulsory**: |  |  |
| 9. |  | Discuss briefly on criminal prosecutions with respect to IDS and IPS crimes. List the different sections in Indian law enforcement that are associated to Network crime. | CO6 | 20 |