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

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

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

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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Compare Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). | CO1 | 10 |
| b. | Illustrate various Attacks on Critical Infrastructure. | CO3 | 10 |
| (OR) | | | | |
| 2. |  | Explain in detail misuse detection, anomaly detection and hybrid detection methods. | CO4 | 20 |
|  |  |  |  |
| 3. | a. | Illustrate fuzzy logic with examples. | CO2 | 10 |
| b. | Illustrate Bayes theory with examples. | CO2 | 10 |
| (OR) | | | | |
| 4. | a. | Discuss Evolutionary Computing with examples. | CO3 | 10 |
| b. | Examine Association Rules with examples. | CO3 | 10 |
|  |  |  |  |  |
| 5. | a. | Debate Centralised Intrusion Detection System. | CO4 | 10 |
| b. | Illustrate Distributed Intrusion Detection System. | CO4 | 10 |
| (OR) | | | | |
| 6. | a. | Explain Tiered Architeture. | CO4 | 10 |
| b. | Describe Hybrid Intrusion Detection System. | CO1 | 10 |
|  |  |  |  |  |
| 7. | a. | Illustrate an example for Quantifying Risk and calculate Return of Investment (ROI) for deploying safeguards. | CO3 | 20 |
| (OR) | | | | |
| 8. | a. | Explain Tools selection and Acquisition. | CO5 | 10 |
| b. | Describe the rule syntaxes of Snort Intrusion Detection System. | CO5 | 10 |
|  | |  |  |  |
|  | | **Compulsory**: |  |  |
| 9. | a. | Explain Due care and Due diligence. | CO6 | 10 |
| b. | Illustrate the role of Law Enforcement on Intrusion into organisations critical assets. | CO6 | 10 |