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



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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA2069** | **Duration :** | **3hrs** |
| **Sub. Name :** | **SECURITY THREAT MANAGEMENT** | **Max. Marks :** | **100** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. |  | Determine the Cyber security hardware threat sources, motives likely to affect hardware assets and consequences of threats. | CO1 | 20 |
| **(OR)** | | | | |
| 2. | a. | Explain how e-mail system works, threat associated with e-mail system, how to secure e-mail services and the protocols that are involved in the e-mail System. | CO1 | 10 |
| b. | From the information leakage point of view “Define intruders”, and the techniques used to intrude the system and list the counter measures. | CO1 | 10 |
|  |  |  |  |  |
| 3. |  | Evaluate (LAN, WAN) Network Vulnerabilities & Threats and technical challenges associated with network system (Electrical, data Interception, physical damage). | CO2 | 20 |
| **(OR)** | | | | |
| 4. | a. | Draw the Cloud physical and logical architecture diagram and security measures to protect data hosted on the cloud and organization reputation. | CO2 | 10 |
| b. | Referring the OWASP annual reports, write any top 5 threats / Vulnerability to web server and application security and counter measures for each threat. | CO2 | 10 |
|  |  |  |  |  |
| 5. | a. | Construct the process flow diagram of Cyber security risk analysis for a large IT Infrastructure Organization and explain each and every phases of risk analysis. | CO3 | 20 |
| **(OR)** | | | | |
| 6. |  | Describe the following activities with an example:   1. Forensic Analysis 2. Vulnerability sources 3. Vulnerability assessment 4. Top 3 Vulnerability Assessment Tool 5. Security threat correlation | CO4 | 4  4  4  4  4 |
| 7. |  | Prepare a authentication policy documents for your newly started company by covering following areas:   1. Documentation content, 2. Authentication types, 3. Authentication Techniques, 4. Authentication process followed, 5. Disciplinary action if any Non-compliance. | CO5 | 4  4  4  4  4 |
| **(OR)** | | | | |
| 8. | a. | Design the firewall audit process flow and explain the benefits to an organization. | CO5 | 10 |
| b. | Define the following topics with an example:   1. Intrusion Detection System 2. Log Files 3. Honey Pots 4. Benefits of Honey Pots | CO5 | 3  3  2  2 |
|  | | **Compulsory**: |  |  |
| 9. | a. | Explain the lifecycle of Physical access control System and types with an example namely : Access Cards, Bio-metrics. | CO6 | 10 |
| b. | Explain the types of Authorization System with an example:   1. Centralized, 2. Decentralized, 3. Implicit and 4. Explicit | CO6 | 3  3  2  2 |