|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No |  |  |  |  |  |  |  |  |  |  |  |  |

****

**Presidency University**

**Bengaluru**

**School Of Computer Science and Engineering & Information Science**

**Summer term End-Term Examinations, August 2024**

**Odd Semester**: 2023 - 24

**Course Code**: CSE3145

**Course Name**: INTRUSION DETECTION & PREVENTION SYSTEM

**Department:** CSE

**Date**: 05.08.2024

**Time**: 01:00PM – 04:00PM

**Max Marks**: 100

**Weightage**: 50%

**Instructions:**

1. *Read the all questions carefully and answer accordingly.*
2. *Do not write any matter on the question paper other than roll number.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Q. No** | **Questions** | **Marks** | | **CO** | **RBT** |
| 1 | 1. Explain the CISCO secure IPS. | 4 | | CO1 | L1 |
| 1. State the importance of regularly updating the signatures in signature-based IDS? | 6 | | CO1 | L2 |
| 1. Elaborate the steps taken by system administrator to support investigation and prosecution. | 10 | | CO1 | L3 |
| OR | | | | | |
| 2 | 1. Describe the key techniques used for intrusion detection in a network environment? | | 4 | CO1 | L1 |
| 1. Explain in brief importance of Incidence Response Plan. | | 6 | CO1 | L2 |
| 1. Explain in detail Post Intrusion Computer Forensic. | | 10 | CO1 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | 1. Explain how credential based vulnerability assessment is performed. | 4 | CO2 | L1 |
| 1. Compare Amazon Web Services (AWS) Guard Duty with Azure Firewall Premium IDPS. | 6 | CO2 | L2 |
| 1. Examine the concept of anomaly detection in IDS. How does this method detect deviations from normal behavior, and what techniques are commonly used? | 10 | CO2 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 | 1. Describe the conditions which need to be satisfied to make evidences applicable for legal requirements. | 4 | CO2 | L1 |
| 1. Distinguish between network-based IDS and host-based IDS in terms of visibility? | 6 | CO2 | L2 |
| 1. Discuss a comprehensive model for intrusion analysis. Include the stages of detection, analysis, and response, and explain how each stage contributes to the overall effectiveness of an intrusion detection/prevention strategy. | 10 | CO2 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5 | 1. Discuss the different relationship between the components of analysis model. | 4 | CO3 | L1 |
| 1. Explain the Host-Based IDS with diagram. | 6 | CO3 | L2 |
| 1. Discuss the significance of legal standards in the implementation of Intrusion Detection and Prevention Systems (IDPS). How do these standards influence the effectiveness, compliance, and overall security posture of organizations? | 10 | CO3 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | 1. Explain honeypot in the context of intrusion detection. | 4 | CO3 | L1 |
| 1. Explain primary purpose of network traffic filtering. | 6 | CO3 | L2 |
| 1. Explain the importance of logging and monitoring for detecting and preventing intrusions. Support your answer with example. | 10 | CO3 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | 1. Identify the factors that should be considered in the tool selection and acquisition process for an Intrusion Detection System (IDS)? | 4 | CO4 | L1 |
| 1. Elaborate some advantages and disadvantages of IPS. | 6 | CO4 | L2 |
| 1. Describe the main types of attacks that an Intrusion Detection System (IDS) can detect. Provide examples of at least two specific attack types and explain how IDS detects them | 10 | CO4 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8 | 1. Elaborate the working of WIPS. | 4 | CO4 | L1 |
| 1. Explain the External Threat with examples and how you can protect company from external threats. | 6 | CO4 | L2 |
| 1. Differentiate between Internal and External threat. | 10 | CO4 | L3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 9 | 1. Elaborate the different modes of snort tool. | 4 | CO1 | L1 |
| 1. Describe the architecture models typically used for Intrusion Prevention Systems. | 6 | CO1 | L2 |
| 1. Define some practices to understand that your IDPS is safeguarding the network. | 10 | CO1 | L3 |

OR

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10 | 1. Explain Prelude IDPS. | 4 | CO2 | L1 |
| 1. Explain Non-Credential based Vulnerability Assessment. | 6 | CO2 | L2 |
| 1. Explain in detail BRO IDPS with proper diagram. | 10 | CO2 | L3 |