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

# PRESIDENCY UNIVERSITY

## BENGALURU

**End - Term Examinations – MAY 2025**

**Date:** 29-05-2025 **Time:** 09:30 am – 12:30 pm

| | | |
|---|---|---|
| **School:** SOCSE | **Program:** B.Tech-Cyber Security | |
| **Course Code:** CSE3145 | **Course Name: :** Intrusion Detection & Prevention System | |
| **Semester**: VI | **Max Marks**: 100 | **Weightage**: 50% |

| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** | **CO5** |
|---|---|---|---|---|---|
| **Marks** | **24** | **24** | **26** | **26** | **--** |

**Instructions:**

*(i) Read all questions carefully and answer accordingly.*

*(ii) Do not write anything on the question paper other than roll number.*

## Part A

**Answer ALL the Questions. Each question carries 2marks.** **10Q x 2M=20M**

| | | | | |
|---|---|---|---|---|
| **1** | List phases of intrusion analysis process | **2 Marks** | **L1** | **CO1** |
| **2** | List cons of IPS. | **2 Marks** | **L1** | **CO1** |
| **3** | List threat detection methods used by IPS. | **2 Marks** | **L1** | **CO2** |
| **4** | Describe components of IDPS | **2 Marks** | **L1** | **CO2** |
| **5** | Mention features of IDPS tool. | **2 Marks** | **L1** | **CO3** |
| **6** | List features of Azure Firewall Premium | **2 Marks** | **L1** | **CO3** |
| **7** | List features of Snort. | **2 Marks** | **L1** | **CO3** |
| **8** | Mention objectives of ISO 27039. | **2 Marks** | **L1** | **CO4** |
| **9** | Describe ISO/IEC 18043:2006 standard. | **2 Marks** | **L1** | **CO4** |
| **10** | Describe weaknesses of IDPS tools. | **2 Marks** | **L1** | **CO4** |

## Part

**Answer the Questions** **Total 80 Marks.**

| | | | | | |
|---|---|---|---|---|---|
| **11.** | **a** | Explain the Internal threat and How to protect company from threats? | **10 Marks** | **L2** | **CO1** |
| | **b** | You are the security operations manager at a large AVC financial institution. Your company handles sensitive customer data, including personal information and financial transactions. but has faced challenges in identifying insider threats and advanced persistent threats (APTs). These types of attacks often involve malicious actors who may initially appear as legitimate users but then start to exhibit suspicious behavior, traffic and protocol . which analysis process will suitable ? explain the analysis process | **10 Marks** | **L3** | **CO1** |

**Or**

| | | | | | |
|---|---|---|---|---|---|
| **12.** | **a** | Explain the Management of IDPS and list the CONS of IDS | **10 Marks** | **L2** | **CO1** |
| | **b** | YKC cyber security company, a leading financial institution, has been experiencing a series of increasingly sophisticated cyber-attacks targeting its network infrastructure. The attacks are primarily aimed at exploiting known vulnerabilities in the network protocols, with attackers trying to infiltrate the system by sending malicious payloads in regular traffic. The company has decided to use intrusion-analysis process for enhance the security to detect known attack patterns in real-time.assume that your working in this company , which analysis process will be suitable ? explain the analysis process. | **10 Marks** | **L3** | **CO1** |

| | | | | | |
|---|---|---|---|---|---|
| **13.** | **a** | SSS organization decides to deploy a honeypot system. A honeypot will be used to attract, trap, and observe malicious actors by mimicking vulnerable systems, while ensuring that the rest of the network remains secure. You are tasked with designing and implementing a honeypot strategy that provides valuable insight into the attackers' behavior, tools, and tactics, while also minimizing the risk of the attackers gaining unauthorized access to critical systems., SSS organization have four networks one router, one firewall , five switches and it is connected with two servers , Draw the diagram for the scenario and explain the honeypot ,in this network how the honeypot will be connected and secure the network | **10 Marks** | **L3** | **CO2** |
| | **b** | Explain the types of Honeypot | **10 Marks** | **L2** | **CO2** |

**or**

| | | | | | |
|---|---|---|---|---|---|
| **14.** | **a** | ACC company has decided to implement an Intrusion Detection and Prevention System (IDPS) based on the Diamond Model of Intrusion Analysis. The Diamond Model focuses on identifying and analyzing the four key elements of an attack. The model's goal is to provide insight into the relationships between these elements to improve threat detection, attribution, and response. Your task is to design and implement an IDPS using the Diamond Model that can detect and respond to sophisticated cyber threats while providing actionable intelligence for your security team. | **10 Marks** | **L3** | **CO2** |
| | **b** | Discuss the various relationships between components of Diamond Model | **10 Marks** | **L2** | **CO2** |

| | | | | | |
|---|---|---|---|---|---|
| **15.** | **a** | You are the Network Security Administrator at a large hospital. The hospital relies heavily on wireless networks for medical devices, staff communication, patient monitoring systems, and administrative functions. Given the sensitive nature of the data being transmitted, including patient health records and financial information, the hospital is subject to strict regulations such as HIPAA (Health Insurance Portability and Accountability Act). which tool will be suitable for this scenario ? explain the tool | **10 Marks** | **L3** | **CO3** |
| | **b** | Compare SNORT with Azure Firewall Premium IDPS | **10 Marks** | **L2** | **CO3** |

**Or**

| | | | | | |
|---|---|---|---|---|---|
| **16.** | **a** | DataCorp Solutions, a leading provider of cloud-based data analytics, has recently expanded its operations to include a wide range of sensitive customer data. DataCorp's network has become increasingly complex, with a mixture of on-premises systems, cloud services (Azure, AWS), and remote work environments , this company wants self-learning security tool. Assume that your working in this company , which tool will be suitable ? explain the tool | **10 Marks** | **L3** | **CO3** |
| | **b** | Compare Meraki MX Advanced Security Edition with Cisco Secure IPS | **10 Marks** | **L2** | **CO3** |
| **17.** | **a** | Assume that You are working in VCT company , as a Digital Forensics Investigator for a large e-commerce company that has recently experienced a data breach. The breach was detected after customers reported suspicious activity involving unauthorized transactions on their accounts.The company is concerned about the potential theft of sensitive customer data, including personal information and payment details. Your primary task is to collect, preserve, and analyze digital evidence from various sources, such as workstations, servers, cloud storage, and network devices. Explain the digital evidence for the scenario | **10 Marks** | **L3** | **CO4** |
| | **b** | Explain the Intrusion Investigation and Legal Consideration for the analyzing computer evidence . | **10 Marks** | **L2** | **CO4** |

| | | | | | |
|---|---|---|---|---|---|
| | | **Or** | | | |
| **18.** | **a** | Assume that your working in APS company , as a Cybersecurity Forensics Analyst at a large healthcare organization that stores and processes sensitive patient data. Recently, the organization discovered signs of a potential data breach that may have involved unauthorized access to patient health records. To conduct a thorough forensic investigation, your team has decided to rely on log files from various systems across the network, including web servers, database servers, firewalls, and endpoint security tools. Explain the log files as forensic evidence for the scenario | **10 Marks** | **L3** | **CO4** |
| | **b** | Explain the Post Intrusion Computer Forensic | **10 Marks** | **L2** | **CO4** |

******* BEST WISHES *******