Oct/Nov - 2025

Total No. of Questions :5]

SEAT No. :

PE4212

[Total No. of Pages : 3

Dr. D.Y. Patil Institute of Management & Entrepreneurship Development LIBRARY

[6554]-3004

S.Y.M.C.A. (Management)

EPS613 MJ : END-POINT SECURITY

(2024 Pattern) (Semester-III)

Time : 2½ Hours] *[Max. Marks : 50*

Instructions to the candidates:

1) *All questions are compulsory.*
2) *Figures to the right indicate full marks.*

Q1) Solve any two

a) Define endpoint security and list three types of endpoints, explaining their importance in organizational data protection. **[5]**

b) Describe how data loss prevention (DLP) Functions as endpoints protection technology and why it is crucial for compliance in organizations. **[5]**

c) Evaluate the effectiveness of antivirus/antimalware software for endpoint protection, using criteria like threat detection rates **[5]**

Q2) a) Define the three main types of network security controls and provide an example of each, explaining their role in endpoint protection. **[5]**

b) Compare SSL/TLS and IPsec protocols analyzing their use cases, strengths, and limitations for secure endpoint communications. **[5]**

OR

c) CASE Study **[10]**

A medium-sized IT company, Technova solutions, suffered a data breach when a junior software developer accessed confidential client data from the internal CRM database. The company had granted all developers administrative access to the database for convenience. No role based access controls (RBAC) were implemented.

P.T.O.

SPPUQuestionPapers.com

Discuss the following Questions.

i) Which access control principle was violated

ii) How could Role-Based Access control (RBAC) have prevented this breach?

iii) What administrative measures should the company adopt?

iv) How can logging and monitoring help in such cases?

Q3) Solve any Two

a) What is multi-factor authentication (MFA)? List its components and deseribe its importance in addressing password weaknesses **[5]**

b) Evaluate the effectiveness of file-level encryption for protecting sensitive data on endpoints, using criteria like performance and granularity **[5]**

c) Explain the Break down role of VPNs in encrypted communications, identifying how they integrate with endpoint authentication. **[5]**

Q4) Solve any two

a) Recall the importance of patch management and list three tools for automated patching, with examples of their configuration. **[5]**

b) Compare CIS Controls and ISO/IEC 27001 standards, analysing their applications and differences in endpoint security for hybrid environment **[5]**

c) Analyse challenges in minimizing attack surfaces on IoT devices, using hardening techniques and patch management as examples. **[5]**

Q5) a) Evaluate the effectiveness of VPNs for securing remote endpoints, using criteria like encryption strength and ease of use. **[5]**

b) Analyse the role of IoT in emerging endpoint security trends, including challenges, AI/ML applications, and integration with NGEP. **[5]**

OR

c) CASE STUDY **[10]**

Sunrise Institute of technology introduce a BYOD policy allowing students and faculty to use their personal devices to access online learning platforms, internal portals, and digital libraries. After a few months, the IT department noticed increased malware infections unauthorized File sharing, and network slowdowns, some students even accesses restricted administrative data due to weak access control.

i) Identify the major security challenges faced by the Institute after implement BYOD

ii) Explain how Access control models (RBAC, MAC, or DAC) could help prevent unauthorized access.

iii) Suggest technical and administrative controls that the institution can apply to secure its BYOD environment.

SPPUQuestionPapers.com
CMMP020351 103.68.11.123 08/12/2025 09:38:51 103