

**VIT**Vellore Institute of Technology
CHENNAI

Reg. Number:

21BCA1803

Continuous Assessment Test (CAT) – I - FEB 2024

Programme	:	B. Tech CSE and its specialization	Semester	:	WINTER 23-24
Course Code & Course Title	:	BCSE354E Information Security Management	Slot	:	TB1
Faculty	:	Dr. Prasad M Dr. Joshan Athanesious J Dr. Sendhil R Dr. Ganesh N Dr. Avuthu Avinash Dr. Leki Chom Thungon Dr. Brindha V Dr. Muthumanikandan V Dr. Padmanaban R	Class Number	:	CH2023240503287 CH2023240503222 CH2023240503288 CH2023240503215 CH2023240503223 CH2023240503285 CH2023240503224 CH2023240503286 CH2023240503221
Duration	:	90 Mins	Max. Mark	:	50

General Instructions:

Write only your registration number on the question paper in the box provided and do not write other information.

- Use statistical tables supplied from the exam cell as necessary.
- Use graph sheets supplied from the exam cell as necessary.
- Only non-programmable calculator without storage is permitted.

Answer all questions

Q. No	Sub Sec.	Description	Marks
1.		Consider you are working as a Network Administrator of an Organization. You are requested to create an infrastructure and solutions help enterprises establish secure, productive and efficient access to technology resources and developer should not be allowed to have admin rights on production system. Find out the suitable security tool to implement the same. Explain in detail about that tool.	10
2.		<p>You are given the role of security manager in organization 'Zinc Security Solution', which is planning to construct secured network architecture. It has hosted with the following security levels given in Table. By considering the proposed design of network architecture, answer the following questions;</p> <ol style="list-style-type: none"> Identify the security devices you would use for your organization? (1 mark) How many zones are required and explain the types of hosts present in each zone. (2 marks) Elucidate the use of deploying a firewall for the above scenario. (1 mark) Explain the type of firewall that can be used and its working. (3 marks). 	10

		<p>✓ If you deploy firewall, what type of architecture you will suggest and explain it. (3 marks)</p> <table border="1"> <thead> <tr> <th>No. of host</th><th>Type of host</th><th>Security level</th></tr> </thead> <tbody> <tr> <td>20</td><td>Database server</td><td>High security can't be accessed by external network</td></tr> <tr> <td>10</td><td>Printer server</td><td>High security can't be accessed by external network</td></tr> <tr> <td>10</td><td>Financial server</td><td>High security can't be accessed by external network</td></tr> <tr> <td>10</td><td>Web server</td><td>Medium security will be accessed by clients through their browser</td></tr> <tr> <td>200</td><td>Employee desktop computers</td><td>Internal network with low level security can't be accessed by external network</td></tr> <tr> <td>50</td><td>Application server</td><td>Medium security will be accessed by external network</td></tr> <tr> <td>1</td><td>Dual homed host computers</td><td>Which can access both internal network and external network</td></tr> </tbody> </table>	No. of host	Type of host	Security level	20	Database server	High security can't be accessed by external network	10	Printer server	High security can't be accessed by external network	10	Financial server	High security can't be accessed by external network	10	Web server	Medium security will be accessed by clients through their browser	200	Employee desktop computers	Internal network with low level security can't be accessed by external network	50	Application server	Medium security will be accessed by external network	1	Dual homed host computers	Which can access both internal network and external network	
No. of host	Type of host	Security level																									
20	Database server	High security can't be accessed by external network																									
10	Printer server	High security can't be accessed by external network																									
10	Financial server	High security can't be accessed by external network																									
10	Web server	Medium security will be accessed by clients through their browser																									
200	Employee desktop computers	Internal network with low level security can't be accessed by external network																									
50	Application server	Medium security will be accessed by external network																									
1	Dual homed host computers	Which can access both internal network and external network																									
3 ✓		<p>VITCC-SCOPE has received a project to set up a network for BitsnBytes company whose requirement is to provide distinct access towards the network based on their departments. For example, the organization may have departments that require network access to employees, customers, top level management and staff members which allow them to communicate with only insiders. No outsiders are allowed to communicate with the insiders. Elaborate the steps you would take to configure the firewall for the above scenario with the help of neat diagram.</p>	10																								
4 ✓		<p>Create a network security model for a banking environment by choosing appropriate security mechanisms from the following list. Analyse the efficiency before and after deployment.</p> <ul style="list-style-type: none"> i) ✓ Behavioural analytics (2 marks) ii) ✓ Data loss prevention (2 marks) iii) ✓ Email security (2 marks) iv) ✓ Network segmentation (2 marks) v) ✓ Mobile device security (2 marks) 	10																								
5 ✓		<p>An organization 'ebay' have network systems with four LANs and it is connected to WAN (that consists of 4LANs and a WAN). For the given scenario, with the help of topological representation, answer the following :</p> <ul style="list-style-type: none"> i) ✓ Identify the security device that can be used to connect LAN and WAN. (2) ii) ✓ Elucidate the different types of attacks which would occur on this device (2) iii) ✓ Illustrate the ways through which the attack can occur. (2) iv) ✓ What security measures can be taken to prevent the attack?(1) v) ✓ The CEO of the organization doesn't want his identity to be known when he access the internet. Identify the system which he would require to hide his identity. Explain how it works. (3) 	10																								