

Reg. No.: 21BCE1808

Name :



VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test I – May 2023

Programme	: B.Tech CSE	Semester	: Fall Inter 2022-23
		Code	: BCSE353E
Course	: Information Security Analysis and Audit	Class Nbr	: CH2022232501115, CH2022232501112, CH2022232501117, CH2022232501107, CH2022232501111, CH2022232501109, CH2022232501116, CH2022232501106, CH2022232501113, CH2022232501108, CH2022232501105, CH2022232501110, CH2022232501114
Faculty	: Dr.S.Sandosh, Dr. N Ganesh, Dr. Suvidha Rupesh Kumar, Dr.A.Sheik Abdullah, Dr.Joshan Athanesious J, Dr.R.Priyadarshini, Dr.Padmavathy T V, Dr.S.Brindha, Dr. Shruti Mishra, Dr.S.Abirami, Dr.S. Radhika Selvamani, Dr N.M.Elango, Dr. K. Palani Thanaraj	Slot	: TB1
Time	: 90 Minutes	Max. Marks	: 50

Answer ALL the questions

Q.No.	Sub. Sec.	Questions	Marks
1.	a	Imagine you receive an email from an unknown sender with an attachment. When you download and open the attachment, your computer starts behaving strangely and slows down significantly. You also notice that the files are replicated. Identify and define the type of malicious program which infected your computer.	4
	b	Discuss in detail about the various types of malicious programs which are recognized as harmful to the computer.	6
2.	a	Today, you have received a phone call from someone who masquerade himself and claims to be a representative from your bank. He has asked you to verify your account information for security purposes and requested you to provide username, password, and social security number over the phone.	5

After providing this information, you started noticing unauthorized transactions on your bank account. Identify and illustrate the type of attack.

✓ 2. The webserver of your company is experiencing a sudden increase in traffic, causing it to slow down significantly. As you investigate further, you observe that the incoming traffic is originating from different IP addresses that targets the webserver. When you start solving it, you also notice that incoming traffic appears distributed because they are originating from multiple IP addresses simultaneously to attack the webserver. Illustrate the above attacks. 5

✓ 3. Alice is a customer who regularly performs online banking transactions. She wants to transfer a significant amount of money from her account to Bob's account, who is her business partner. However, Alice and Bob are concerned about the security of the transaction and the possibility of unauthorized access or tampering. Help Alice and Bob to understand the need of Confidentiality, Integrity, Availability, Authentication and Authorization in this sensitive banking transaction. 10

✓ 4. A top MNC named KANINI SOFTWARE SOLUTIONS, has faced an unauthorized individual gain access to the corporate network and potentially compromises the confidential data. This shows the importance of identifying system vulnerabilities in the MNC. As a cyber security specialist, insist your company to train the employees on the various types of vulnerabilities and the steps to protect your business from the vulnerabilities. 10

✓ 5. One day, you notice unusual network activities in the restricted areas of your network including multiple failed login attempts and repeated access attempts. From the above activities you suspect there would be an ongoing cyber-attack or an unauthorized user trying to gain access. As a network administrator in this scenario suggest the tool or technique you would use to identify and respond to the potential security breach. 10

⇔ ⇔ ⇔