PES University, Bengaluru

(Established under Karnataka Act No. 16 of 2013)

May 2019: End SEMESTER ASSESSMENT (ESA)

B.TECH. VI SEMESTER ELECTIVE CSE

UE16CS331: Computer Network Security

Time: 180 Mins | Answer All Questions | Max Marks: 100

		Questions	Marks
Q1.	A	Your friend has been hired by an organization to take care of the security of its computer network. He is feeling a bit nervous as he does not have any money to invest in new hardware / software like firewall/IDS/IPS. He has come to you, knowing that you have studied computer Network security in class. He asks your advice on simple measures that he can take to help prevent/minimise any intrusion attack. Please suggest four **simple** things that can tremendously help your friend limit the possibility of an intrusion attack?	8
Q1	B	Your company has decided to increase its authentication security by requiring employees to use a security token as well as a password to log onto the network. The employees are grumbling about the new requirements because they don't want to have to carry around the token with them and don't understand why it's necessary. Briefly explain the general ways that authentication can be performed. Then explain why your company has decided to use security tokens in addition to passwords.	8
Q1	C	What is WEP and WPA2 in the context of WiFi communication? Which one is better and why?	4
Q2	A	Explain the security principle of Defence in Depth with one example	4
Q2	B	Describe with a diagram the three-way handshake process used to initiate TCP connections.	8
Q2	C	From a security perspective, what is the SYN flooding? Explain with a diagram. What limitation of TCP protocol is misused to launch such attacks?	8
Q3	A1	"An impact is created when a threat exploits a vulnerability". In the context of Security Risk Management, can you explain with examples to your team members what is a vulnerability, threat and impact?	6

Q3	B	You have just completed a qualitative threat assessment of the computer security of your organization, with the impacts and probabilities of occurrence as follows. Properly place the threats in the table below into a three-by-three matrix with x axis showing probability and Y axis showing impact. Which of the threats should you take action on, which should you monitor, and which ones may not need your immediate attention?	14

Threat	Impact	Probability of occurrence
Virus Attacks	High	High
Internet Hacks	Medium	High
Disgruntled Employee hacks	High	Medium
Dial up- Hacks	High	Low
Week incidence response mechanism	Medium	Medium
Theft of information by a third-party contractor	Low	Medium
Competitor Hacks	High	Low
Inadvertent release of non-critical information	Low	Low
Wireless hacks	Low	High

Q4	A	In a discussion at work your co-worker says that Authentication and Authorization are alike. Do you agree? State Yes or NO. If you answer yes, please justify. If your answer is No, please explain.	4
Q4	B	What is an Intrusion Detection System (IDS)? What is the purpose/function of IDS? What is IDS Not?	9 4
Q4	C	What is Bluetooth? What are the two types of Bluetooth? Give one example for each type.	3

Q5	A	Your manager wants to move the inhouse applications of the organisation to the cloud. In particular she is worried about the following issues: 1) Use of unmanaged devices to access cloud 2) Storing sensitive data in Cloud 3) DLP – data leakage from inside the cloud IaaS, PaaS 4) Loss of Control as Data and apps now on the cloud 5) Multi-tenancy challenges Knowing that you have studied Cloud security, your manager approaches you to understand what the above five issues mean? Explain each issue in brief, concise and cogent sentences. Suggest what major controls can be applied to each issue in order to mitigate the same.	15
Q5	B	What is Access control List (ACL)? Can you propose a simple ACL for the question paper from the department of Computer Science and engineering?	5