Name: Enrolment No:	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course:	**IT Systems and Network Security**	**Semester:**	**VI**
Program:	**B. Tech CSE+ IT-Infra**	**Time**	**03 hrs.**
Course Code:	**CSEG 3022**	**Max. Marks:**	**100**

SECTION A

1. **Each Question will carry 5 Marks**
2. **Instruction: Complete the statement / Select the correct answer(s)**

S. No.	Question	CO
1	A network administrator is testing a new monitoring application that uses multiple Internet Control Message Protocol (ICMP) messages to host systems. The application is reported on IEV as a network attack. This alarm is referred to as a a) False positive b) False negative c) True positive d) True negative	CO1
2	Lack of access control policy is a _____ a) Bug b) Threat c) Vulnerability d) Attack	CO2
3	Possible threat to any information cannot be _____ a) reduced b) transferred c) protected d) ignored	CO3
4	Which of the following combinations can support RAID 05? a) 2 sets with 3 disks each b) 3 sets with 2 disks each c) 2 sets with 4 disks each d) 4 sets with 1 disk each	CO5
5	Which of the following terminology is inappropriate from network security perspective? a)Threat b)Malfunction c)Vulnerability d)Attack	CO4
6	Which of the following is not the type of access control? a)DAC b)MAC c)RBA d)VVD	CO1

SECTION B

1. **Each Question will carry 10 marks**
2. **Instruction: Write short/brief notes**

7	What are the IT company's top risks, how severe is their impact and how likely are they to occur? How do you measure the effectiveness of any IT company in managing its top risks?	CO3, CO4
8	Define the following terms briefly. A. Heuristic analysis	CO2, CO5

	B. Signature-based detection C. Host-based detection D. Pattern matching E. Flood decode analysis	
9	What is a security policy? Discuss the Hierarchy of a Security Policy. List various characteristics of a Good Security Policy	CO4
10	What is VPN Concentrators? Explain various functions of a VPN Concentrator.	CO5
11	List various advantages of network traffic monitoring and analysis. Is it possible to have router-based monitoring technique? If yes, explain with an example. Also, discuss the role of network traffic signatures in network traffic monitoring. **OR** Discuss the important Data Backup Strategies/Plans. How will you select the Backup Media. List various data backup options and discuss RAID-level approach in detail.	CO1
SECTION C **1. Each Question carries 20 Marks.** **2. Instruction: Write long answer.**		
12	A. List the roles and responsibilities of Incident Response Team Members. Who is First Responder? Discuss the role of First Responder in University IT Network and Services. B. How to calculate needed disk space in sectors for a striped volume. Explain with an example. **OR** A) Discuss with suitable diagram Incident handling and response process flow. B) Discuss RAID storage architecture and enlist its advantages and disadvantages.	CO2, CO3