Name: **Enrolment No:**	UPES UNIVERSITY OF TOMORROW

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2022

Course: IT Systems & Network Security **Semester : VI**
Program: BT-CSE-Spz-IT-INFRA **Time : 03 hrs.**
Course Code: CSEG 3022 **Max. Marks: 100**

Instructions: (i) Start answer to a new question on a fresh page, (ii) Scattered part answers will not be evaluated, (iii) Use and exchange of mobile phone, calculator or any other item is not allowed and (iv) Exam is close book.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Differentiate between Network, Web and Mobile Penetration Testing.	**5**	**CO1**
Q 2	What are the response codes that can be received from a Web Application?	**5**	**CO2**
Q 3	What is the difference between VA(Vulnerability Assessment) and PT(Penetration Testing)?	**5**	**CO3**
Q 4	What makes a script fully undetectable (FUD) to antivirus software? How would you go about writing a FUD script?	**5**	**CO4**
Q 5	What are some of the common Cyberattacks?	**5**	**CO5**

SECTION B
(4Qx10M= 40 Marks)

Q 6	You're tasked with setting up an email encryption system for certain employees of a company. What's the first thing you should be doing to set them up? How would you distribute the keys?	**10**	**CO4**
Q 7	Write out the most common threats to web security discussed in OWASP. What is the source of these risks and dangers? Make a plan for how to protect your web-Cyberspace from the threats outlined in OWASP.	**10**	**CO5**
Q 8	Describing the hardening process. Then explain what the nmap utility does and how youwould use the information it provides in the hardening process	**10**	**CO1, CO2**
Q 9	Answer the following questions: a) What is DMZ? Describe the devices you need to setup a DMZ and what type of servicesyou'd likely place in DMZ. b) Name and explain the different functionalities in the network security? c) Can a firewall block attacks using server scripts, such as the attack in which the user could change a price on an item offered	**10**	**CO3, CO4**

	by an e-commerce site? Why or why not? OR One form of IDS starts operation by generating an alert for every action. Over time, the administrator adjusts the setting of the IDS so that common, benign activities do not generate alarms. What are the advantages and disadvantages of this design for an IDS?		
	SECTION-C **(2Qx20M=40 Marks)**		
Q	Wi-Fi is a wireless technology that provides simple broadband access using a laptop and an access point to which the laptop has authenticated itself. Suppose an attacker has a modified Wi-Fi card designed to intercept data. All information coming from the access points within wireless range can be read. Suppose an attacker wishes to authenticate to a corporate access point they should not be able to use. In a man-in-the-middle attack the attacker sets up a bogus access point: • The bogus access point identifies a real corporate access point in advance. • When a corporate laptop sees the bogus access point and tries to associate to it the bogus access point copies all the messages it receives to the valid corporate access point, substituting its own Medium Access Control (MAC) address for the source address. • The bogus access point copies all the messages received from the valid access point back to the mobile device again substituting its own Medium Access Control (MAC) address for the source address. This intervention is possible even when the data is encrypted and without the enemy knowing the secret keys. Considering the above scenario, answer the following: a) If the message content is encrypted very little can be achieved without some knowledge of the contents of the messages before they were encrypted. Is it the only possible solution? If no, discuss the other solutions. b) More can be achieved if the attacker is allowed to replay captured messages. Discuss the possibilities and defense approaches in detail. c) In particular, if a simple challenge response scheme were used for authentication by replaying captured messages the bogus access point could associate itself to the corporate access point. Is it true? Justify your answer.	**20**	**CO5, CO2**
	Write Short note on following: a) Can encrypted e-mail provide verification to a sender that a recipient has read an email message? Why or why not? b) What are the advantages and disadvantages of an e-mail program that automatically applies and removes protection to e-	**20**	**CO1,CO 3,CO4**

	mail messages between sender and receiver? c) In what ways is denial of service (lack of availability for authorized users) a vulnerability to users of single-user personal computers? d) List three different sources of water to a computing system, and state a control for each. e) Cite three security controls that could have both positive and negative effects. OR Answer the following: a) For an airline, what are its most important assets? What are the minimal computing resources it would need to continue business for a limited period (up to two days)? What other systems or processes could it use during the period of the disaster? b) Investigate your university's or employer's security plan to determine whether its security requirements meet all the conditions listed in this chapter. List any that do not. When was the plan written? When was it last reviewed and updated?		