Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India
(Autonomous College Affiliated to University of Mumbai)

End Semester Examination

May 2022

Max. Marks : 60 **Duration: 120 Minutes**
Class : TE Computer/ TE IT **Semester: VI**
Course Code : IT 321 **Branch : CS/IT**
Name of the Course: Ethical Hacking **Date-17th May 2022**

Instructions:

(1) All Questions are Compulsory
(2) Draw neat diagrams
(3) Assume suitable data, if necessary

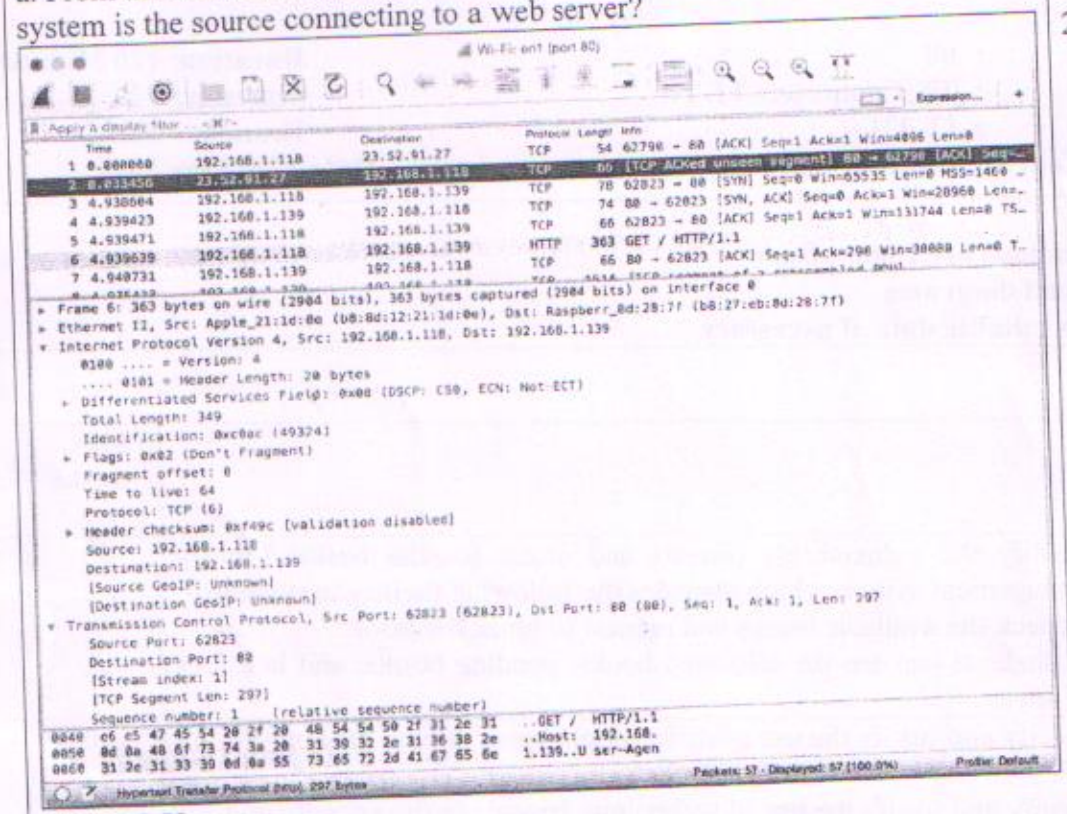
Question No.		Max. Marks	BL	CO
1	a) Identify the vulnerability ,threats and attack for the online Library management system which provides the following facility to students- i) check the available books and request to block the book. ii) students can see the allocated books, pending books, and late fees (if any).	10	4	1
	b) Specify and justify the use of different phases of ethical hacking OR b) Specify and justify the use of technology triangle in the security and also differentiate between the ethical hacker and unethical hacker	10	3	1
2	a) With the help of examples, list and define the different types of Virus and Trojan and also specify the life cycle for Virus and Trojan.	10	3	2
	b) ,Specify the different ways to attack the system using session hijacking and justify the avoidance mechanism for the same	10	2	2
3	a) How are legitimate websites compromised with SQL injections and Malicious Advertisements? Give proper justification along with the avoidance of such attacks.	7	2	4
	b) Suppose that Alice's system employs the NX bit method of protecting against buffer overflow attacks. If Alice's system uses software that is known to harbor multiple buffer overflows, would it be possible for Trudy to conduct a denial of service attack against Alice by exploiting one of these buffer overflows? Explain.	8	5	3

Sardar Patel Institute of Technology

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai-400058-India

(Autonomous College Affiliated to University of Mumbai)

1	a. From the information given in the Wireshark pcap file, what operating system is the source connecting to a web server?	2	4	2
	b. What must a user have in order to sniff the full stack of wireless traffic?	1.5	2	3
	c. Which of the following can be used to check for wireless signals?	1.5	1	4



A. OS X
B. Microsoft
C. Linux
D. Raspbian

b. What must a user have in order to sniff the full stack of wireless traffic?

A. Wireless device set to promiscuous mode
B. Wireless device that has 2.4 GHz and 5 GHz set to read only
C. Wireless device set to monitor mode
D. Ettercap set to clone

c. Which of the following can be used to check for wireless signals?

A. AirCheck
B. Netcheck
C. Ncat
D. AirWare

xxxxxxx