

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

: TE Computer/ TE IT

Course Code

Class

: IT 321

Name of the Course: Ethical Hacking

Duration: 120 Minutes

Semester: VI Branch : CS/IT Date-17th May 2022

Instructions:

(1) All Questions are Compulsory

(2) Draw neat diagrams

(3) Assume suitable data, if necessary

Quest ion No.		Max. Marks	BL	СО
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
10	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
	 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)

a.	From the information given in the wireshark peap 1777			
arti	From the information given in the Wireshark pcap file, what operating stem is the source connecting to a web server?	2	4	2
-	Wo Fe and (part 80)	2		-
110				
100	Time Scotte Operination 7(P 54 62798 + 88 (ACK) Seqr.1 Acks.1 Winn4895 Lens 8	1.5	2	13
525	2 8.033456 23.52.01.27 120.156.1.139 TCF 78 62823 - 00 [SYN] Segre Winner 75 100.156.1.139 TCF 78 62823 - 00 [SYN] Segre Winner 75 100.156.1.139		2	-
	4 4.939423 192.160.1.139 192.160.1.139 TCF 66 62823 - 80 [ACK] Seq=1 ACK92 WIRELES			
95	6 4.839639 192.166.1.118 192.168.1.119 TCP 66 80 - 62823 [ACK] Segel Ack=296 Win=38688 Lenes 1.	DE LISTA	1	1
-	AND	1.5	1	
	Ethernet II, 5rc: hpyte_atatatatatatatatatatatatatatatatatata	omare !		
	8180 = Version: a			
	bifferentiated Services Fleig! exed (DSF) Cast			
11	Identification: 0xc0ec (49374) + Flags: 0x02 (Don't Fragment)		Rene	
	Fragment offset: 0 Time to live: 64		mel	
	Protocol: TCP (6) > Header checksum: 8xf49c [validation disabled]		100	
	Source: 192.168.1.118 Ocstination: 192.168.1.129			
	in the control teamson!			
	[Destination GeolP: Unknown] Transmission Control Protocol, Src Port: 62833 (62823), Dat Part: 68 (88), Seq: 1, Ack: 3, Len: 297 Source Part: 62823	11-		
	Destination Port: 88 [Stream index: 1]			1
- 11	[TCP Segment Len: 297]	1		
	20 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
	anda Ad Da 48 OT 72 74 38 50 21 22 24 57 55 56 1 139 U Ser-Agen			
	he56 8d 8a 48 67 73 74 3a 55 73 65 72 2d 41 67 65 6c 1.139U ser-Agen Peckets: \$3 - Displayed: \$7 (100.01%) Product Cortout.			
1	9856 84 08 46 07 73 74 38 56 72 26 41 67 65 66 1.139 U ser-Agen Peckets: 57 - Displayed: 57 (100.01%) Profile: Defoult (C) 7 - Hypersed Treasler Positional Position (C) 27 Byrins			
	Peckets: 57 - Discharged: 57 (100.0%) Product Default. OS X			
I	Peckets: 57 - Deschared: 57 (100.01%) Product Default OS X Microsoft			
H	Pecket: 57 - Decket: 57 - Decke			
1	Peckett: 57 - Deschared: 57 / 100 /			
1	A. OS X B. Microsoft Linux Raspbian Raspbian What must a user have in order to sniff the full stack of wireless traffic?			
1	A. OS X B. Microsoft Linux C. Raspbian D. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic?			
1	A. OS X B. Microsoft C. Linux D. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only			
1	A. OS X B. Microsoft Linux C. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only			
1	A. OS X B. Microsoft Linux C. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode			
	A. OS X B. Microsoft Linux Raspbian What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode Ettercap set to clone			
	A. OS X B. Microsoft Linux Raspbian What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode Ettercap set to clone			
	A. OS X B. Microsoft C. Linux C. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode B. Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode Ettercap set to clone C. Which of the following can be used to check for wireless signals?			
	A. OS X B. Microsoft Linux C. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode Ettercap set to clone Which of the following can be used to check for wireless signals? A. AirCheck			
	A. OS X B. Microsoft C. Linux C. Raspbian D. What must a user have in order to sniff the full stack of wireless traffic? Wireless device set to promiscuous mode B. Wireless device that has 2.4 GHz and 5 GHz set to read only Wireless device set to monitor mode Ettercap set to clone C. Which of the following can be used to check for wireless signals?			