K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

Feb – Mar – 2024

Program: BTECH (COMP/AIDS/IT/EXTC Scheme II
Examination: TY   Semester: V
Course Code: HCSC501 and   Course Name: Ethical Hacking

Supplementary exam

Date of Exam: 22-02-2024   Duration: 2.5 Hours   Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight:	12		
i)	Which of the layer is responsible for end-to-end reliable data transfer with error recovery and flow control?	2	CO1	U
ii)	Summarize the concept of biometric authentication	2	CO2	U
iii)	Which type of data cannot be retrieved about the target source/website using whois database lookup?	2	CO3	U
iv)	What is account harvesting?	2	CO4	U
v)	Define side channel attacks?	2	CO5	U
vi)	Describe in brief functionality of DVWA?	2	CO6	U
vii)	What is packet sniffing?	2	CO4	U
viii)	What type of information is gathered using port scanning?	2	CO3	U
Q.2	Solve any four questions out of six.	16		
i)	Is the following statement is true/false about TCP statement if yes/no justify your answer Statement -"It allows cross platform communication among heterogeneous networks"	4	CO1	U
ii)	Illustrate with example about substitution cipher?	4	CO2	U
iii)	Describe about the types of Mobile based social engineering attacks with examples?	4	CO3	U

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

Feb – May 2024

Program: BTECH (COMP/AIDS/IT/EXTC Scheme II
Examination: TY   Semester: V
Course Code: HCSC501 and   Course Name: Ethical Hacking

Date of Exam: 22-02-2024   Duration: 2.5 Hours   Max. Marks: 60

iv)	Illustrate the concept of Error based and Blind SQL Injection.	4	CO4	U
v)	Describe about the physical probing and black box testing in hardware attacks?	4	CO5	U
vi)	How host discovery can be performed using the TCP Sweep?	4	CO6	Ap
Q.3	Solve any two questions out of three.	16		
i)	Consider a big single network having ip address 200.1.2.0. Divide this network in to two subnets. Use the concept of ip subnetting?	8	CO1	Ap
ii)	Write a short note on SQL injection authentication Bypass?	8	CO4	U
iii)	What is hardware trojan?Describe about its types and trojan detection.	8	CO5	U
Q.4	Solve any two questions out of three.	16		
i)	Demonstrate the steps of capturing packets in wireshark	8	CO6	Ap
ii)	Draw the architecture of DES algorithm and explain its steps with the help of example	8	CO2	Ap
iii)	Explain the types of DDOS attacks	8	CO3	U

****