APJ ABDULKALAM TECHNOLOGICAL UNIVERSITY

08 PALAKKAD CLUSTER

Q. P. Code : CSE0821311C-I (Pages: 2)

Name: ....

Reg. No: ....

THIRD SEMESTER M.TECH. DEGREE EXAMINATION DECEMBER 2021

Branch: Computer Science and Engineering Specialization: Computer Science and Engineering

08CS 7011(C) ETHICAL HACKING

(Common to CSE)

Time: 3 hours **Max. Marks: 60**

Answer all six questions.

Modules 1 to 6: Part 'a' of each question is compulsory and answer either part 'b' or part 'c' of each question.

Q. No.	Module 1	Marks
1. a	Comment on Threat, Vulnerability and Risk.	3
	Answer b or c	
b	Explain in detail about computer fraud classification according to data processing model.	6
c	What are the different methods for managing the insider threat?	6

Q. No.	Module 2	Marks
2. a	How can a hacker inside or outside a network impersonates the conversations of a trusted computer?	3
	Answer b or c	
b	Explain about the prominent cyberattacks in Domain Name System?	6
c	How does an attacker perform DDOS attack? Explain about DDOS Models.	6

Q. No.	Module 3	Marks
3. a	Write a sample batch program to create a folder bomb (i.e. creates infinite folders)	3
	Answer b or c	
b	Compare and contrast packet filter firewall and packet inspection firewall	6
c	Discuss in detail about application proxy firewalls.	6

Q. No.	Module 4	Marks
4. a	What is rainbow table attack? How can it be prevented?	3
	Answer b or c	
b	Being an expert in hacking, you are asked to analyze the free, open source software being used to run FTP services on a server. You noticed that there is an excessive number of fgets() and gets() on the source code. These C++ functions do not check bounds. What kind of attack is this program susceptible to? Comment on your recommendation to prevent this attack?	6
c	While testing a web application of www.ente.com, you login using your credentials (admin and pass). During the login process, you see a request for the following URL appear in your intercepting proxy: http://www.ente.com/app?action=login&uname=admin&password=pass Comment atleast two vulnerabilities that you can diagnose without probing any further?	6

Q. No.	Module 5	Marks
5. a	A pentester and a hacker want to hack Twitter. How different will be their approach?	4
	Answer b or c	
b	Organization A needs to use an intrusion detection mechanism that monitors the traffic on its network segment as a data source whereas organization B needs to detect the intrusion that take place on a single host system. Suggest them which device to use. Explain them about its strength and weakness.	8
c	Explain in detail the phases of penetration testing process.	8

Q. No.	Module 6	Marks
6. a	You are given a hard disk belonging to a suspected criminal. Explain the steps to make a forensic copy of hard disk.	4
	Answer b or c	
b	What do you mean by Journaling? Explain the journaling for UNIX operating system.	8
c	How do neural networks help with fraud detection? Discuss it's advantages and disadvantages?	8