APJ ABDULKALAM TECHNOLOGICAL UNIVERSITY

08 PALAKKAD CLUSTER

Q. P. Code : 3AC-16-1 **(Pages: 2)** **Name**

Reg. No:

THIRD SEMESTER M.TECH. DEGREE EXAMINATION DEC 2016

Computer Science and Engineering

08CS 7011(C) ETHICAL HACKING

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

Answer all six questions. Part 'a' of each question is compulsory.

Answer either part 'b' or part 'c' of each question.

Q.no.	Module 1	Marks
1.a	Write short note on Fraud Triangle.	3
	Answer b or c	
b	Explain in detail about computer fraud classification according to data processing model.	6
c	Write in detail about Framework for Understanding and Predicting Insider Attacks.	6

Q.no.	Module 2	Marks
2.a	Write short note on port scanning. Name one tool used to perform port scanning.	3
	Answer b or c	
b	With the help of a neat diagram, explain the difference between full open scan and half open Scan.	6
c	An attacker uses a distributed group of computers to shutdown a single machine or network, making it inaccessible to its intended users. Explain the attack with a neat diagram. What are the ways to prevent this attack?	6

Q.no.	Module 3	Marks
3.a	Write short note on the limitations of packet filters.	3
	Answer b or c	
b	Compare Packet filtering Vs Application Level Firewall Technology.	6
c	An organization need to evaluate network packets for valid data at the application	6

layer before allowing a connection. Suggest and explain the firewall technology that suits their need.

Q.no.	Module 4	Marks
4.a	What type of password attack would be most successful against the password A42k#s23B? Justify your answer. What defensive measures will you take to protect your network from this type of attack.	3
	Answer b or c	
b	An attacker writes a program that attempts to put data outside the bounds of a block of allocated memory. Explain this attack and the best practices to prevent it.	6
c	You are appointed as a security consultant for an MNC. One of their web applications is having SQL injection vulnerability. Explain about this vulnerability and demonstrate to the senior management on how an attacker exploit this and delete records in a database.	6

Q.no.	Module 5	Marks
5.a	Explain in detail about vulnerability assessment phases.	4
	Answer b or c	
b	Suggest and explain an existing framework to identify and mitigate the risks associated with ICF.	8
c	An organization needs to detect the intrusion that take place on a single host system. Suggest them which device to use. Explain them about its working, applications, strength and weakness.	8

Q.no.	Module 6	Marks
6.a	Write short note on journaling. Discuss the journaling for firewalls.	4
	Answer b or c	
b	Discuss the advantages and disadvantages of neural network based misuse detection system.	8
c	What do you mean by novelty detection? Explain the concept of SaffronOne associative memory.	8