23ICPC308

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Sixth Semester B.E Degree Examination

Ethical Hacking

Time: 3 Hours(180 Minutes) **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	C
Q1	a.	Define the terms vulnerability, threat and exploit.	06	L2	CO1
	b.	Discuss the various types of Hacker Attacks	06	L2	CO1
	c.	Explain the phases in Information-Gathering Methodology for footprinting. List out any 3 tools used for the same.	08	L2	CO1
		OR			
Q2	a.	Explain the five phases that make up an attack.	06	L2	CO1
	b.	What is meant by Hacktivism? Explain the four hacker classes.	06	L2	CO1
	c.	Explain the primary utility and a specific example tool for three of the following network information gathering tools: WHOIS Tools, DNS Information Tools, Network Range Locator Tools, Email spiders, Locating Network Activity	08	L2	CO1
		Module- 2			
Q3	a.	Discuss the different types of scanning and its objectives.	06	L2	CO2
	b.	Explain about proxy servers. What are the different ways through which proxy servers are used for attacking.	06	L2	CO2
	c.	Discuss the steps involved in scanning a network. List out any three live system scanning tools.	08	L2	CO2
		OR			
Q4	a.	Explain the various countermeasures to make scanning unsuccessful.	06	L2	CO2
	b.	Discuss about the operating system fingerprinting and its types.	06	L2	CO2
	c.	Explain the phases in Information-Gathering Methodology for footprinting. List out any three fingerprinting tools.	08	L2	CO2
		Module - 3			
Q5	a.	Discuss briefly the steps taken by an attacker in enumeration technique. What are the types of information enumerated by attackers?	06	L2	CO3
	b.	Explain about Null sessions in windows, its counter measures and tools used.	06	L2	CO3
	c.	Explain briefly about Web enumeration techniques.	08	L2	CO3
		OR			
Q6	a.	Explain UNIX enumeration process and tools used for the same.	06	L2	CO3
	b.	Explain about SNMP enumeration techniques and its countermeasures including tools	06	L2	CO3
	c.	Discuss about Default Password Enumeration and tools used.	08	L2	CO3
		Module - 4			
Q7	a.	Explain four types of password attacks	06	L2	CO4
	b.	Discuss about password guessing done by hackers.	06	L2	CO4

	c.	Discuss about steganography and any 3 tools used for the same.	08	L2	CO4
OR					
Q8	a.	What are the different types of passwords? Explain the characteristics of a strong password.	06	L2	CO4
	b.	Discuss about keyloggers and any 3 tools used for the same. What are the countermeasures for keyloggers?	06	L2	CO4
	c.	Explain how an attacker covers the tracks after an attack is made.	08	L2	CO4
Module - 5					
Q9	a.	Briefly explain the Security Assessments made in the penetration testing phase.	06	L2	CO5
	b.	Compare Passive Reconnaissance and Active Reconnaissance	06	L2	CO5
	c.	Elaborate the Phases of Penetration Testing.	08	L2	CO5
OR					
Q10	a.	Explain types of Penetration Testing.	06	L2	CO5
	b.	Discuss about enumerating devices in the Penetration testing process.	06	L2	CO5
	c.	What is a threat? Discuss its impacts in Business and the three levels of severities.	08	L2	CO5

-*****-