U.S.N.										

B.M.S. College of Engineering, Bengaluru-560019

Autonomous Institute Affiliated to VTU

August 2024 Supplementary Examinations

Programme: B.E. **Semester: VII**
Branch: Artificial Intelligence and Machine Learning **Duration: 3 hrs.**
Course Code: 22AM7PEEHP **Max Marks: 100**
Course: Ethical Hacking Principles

Instructions: 1. Answer any FIVE full questions, choosing one full question from each unit.
2. Missing data, if any, may be suitably assumed.

Important Note: Completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages. Revealing of identification, appeal to evaluator will be treated as malpractice.

		UNIT - I	*CO*	*PO*	**Marks**
1	a)	Identify the types of penetration test and frame the rules for report writing.	*CO1*	*PO1*	**10**
	b)	Discuss the rules of engagement for the ethical hacking.	*CO 1*	*PO 1*	**05**
	c)	Interpret the difference between OSSTMM and OWASP methodologies.	*CO 2*	*PO 2*	**05**
		UNIT - II			
2	a)	With neat schematic diagram illustrates the working of a TCP SYN scan and TCP connect scan works	*CO 2*	*PO2*	**10**
	b)	Elaborate how can DNS clients effectively communicate with DNS servers to ensure efficient interaction and optimal functionality?	*CO 3*	*PO3*	**10**
3		**UNIT - III**			
	a)	Interpret the types of sniffing with an example.	*CO 1*	*PO1*	**05**
	b)	Analysis the mechanics of DHCP spoofing, and explain potential benefits and drawbacks associated with this technique?	*CO 1*	*PO 1*	**05**
	c)	Elucidate the process involved in session hijacking through a Man-in-the-Middle (MITM) attack, and what are the potential pros and cons associated with this method?	*CO 2*	*PO6*	**10**
		OR			
4	a)	Illustrate the occurrence of client-side exploitation in the context of DNS cache snooping, and write a case study exemplifying this method?	*CO 2*	*PO1*	**10**
	b)	With schematic diagram, explain different ways of ARP attacks	*CO 2*	*PO6*	**10**

			UNIT - IV			
	5	a)	Analyses the distinctions between text-based and binary protocols and provide examples that illustrate the characteristics of each type?	*CO 1*	*PO1*	**5**
		b)	Explain how does PDF hacking occur and with a schematic diagram to visually depict the various stages involved?	*CO 2*	*PO2*	**5**
		c)	Develop a case study on Metasploit Framework on popular interfaces and its utilities	*CO 3*	*PO3*	**10**
			UNIT - V			
	6	a)	Analyze the steps involved in utilizing the aircrack-ng tool for cracking WEP security, and how straightforward is the process in terms of ease and efficiency?	*CO 3*	*PO3*	**10**
		b)	Apply the SSRF vulnerability manifest in practical applications, and can you present a well-organized schematic diagram to elucidate the operational dynamics of SSRF within an application context?	*CO 2*	*PO6*	**10**
			OR			
	7	a)	Analyze the functionality of a wireless adapter supporting packet injection to be demonstrated in a real-world scenario and provide a specific case study illustrating its application?	*CO 1*	*PO1*	**10**
		b)	Illustrate real-world instances where SQL injection attacks have occurred in practical applications, and provide a case study highlighting the distinct types of SQL injection vulnerabilities involved?	*CO 2*	*PO6*	**10**

******