U.S.N.										

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

Autonomous Institute Affiliated to VTU

January 2024 Semester End Main 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.

				CO	PO	Marks
			UNIT - I			
1	a)		What are the key steps involved in NIST penetration testing method and how does it differ from the OSSTMM method?	CO1	PO1	**8**
	b)		Briefly explain different types of Penetration Tests.	CO2	PO1	**6**
	c)		How do Rules of Engagement ensure ethical and legal boundaries in penetration test?	CO1	PO2	**6**
			UNIT - II			
2	a)		Explain how we can interact with DNS servers by using DNS clients.	CO2	PO2	**6**
	b)		Illustrate NULL, FIN, and XMAS Scans with appropriate sketches.	CO2	PO1	**6**
	c)		Why are traditional scan techniques considered less effective? List and explain various advanced evasion techniques used for bypassing firewall detection in the realm of network security.	CO1	PO2	**8**
			UNIT - III			
3	a)		How can BackTrack users leverage exploit-db for penetration testing, and what steps are involved in updating the exploit database within BackTrack?	CO1	PO2	**7**
	b)		In detail explain two ARP attack vectors.	CO2	PO1	**7**
	c)		How can Wireshark be utilized for capturing plain texts passwords transmitted over a network? Provide a step-by-step overview of the process.	CO3	PO5	**6**
			OR			
4	a)		Describe the various steps involved in the process of ARP poisoning a network using Cain and Abel in five steps.	CO1	PO3	**6**
	b)		As a penetration tester, describe why understanding network protocols are crucial in server exploitation phase? Provide a brief overview of each protocol.	CO3	PO2	**7**

		c)	Define Brute force attack. Explain different categories of Brute force attack.	*CO2*	*PO2*	**7**
			UNIT - IV			
	5	a)	Describe various steps involved in creating a backdoor from SET.	*CO2*	*PO3*	**7**
		b)	Explain the penetration testing methodology for setting up backdoor using Netcat during post-exploitation on a target system. Provide a step-by-step guide.	*CO3*	*PO2*	**6**
		c)	Provide a brief overview of how browser exploits within the PDF context work, highlighting the steps involved in executing such exploits for potential attacks.	*CO1*	*PO2*	**7**
			UNIT - V			
	6	a)	How can a rogue or fake access point be set up to redirect and control the victim's traffic? Provide step-by-step instructions using Social Engineering Toolkit (SET).	*CO1*	*PO3*	**6**
		b)	What is the agenda behind Evil Twin Attack? Explain how this can happen in real time?	*CO2*	*PO3*	**8**
		c)	Analyse and explain HTTP Basic Authentication and Form-Based Authentication.	*CO2*	*PO2*	**6**
			OR			
	7	a)	List two common flaws in CAPTCHA implementation, and how can they be exploited for potential security risks?	*CO3*	*PO2*	**6**
		b)	How does SQL injection exploit vulnerabilities in dynamic websites? Additionally, discuss the three types of SQL injection attacks.	*CO2*	*PO3*	**8**
		c)	How SSRF can it be exploited? Provide a brief explanation of how SSRF vulnerability works.	*CO3*	*PO3*	**6**

****