Reg. No. : | | | | | | | | | | | | |

Question Paper Code: U8401

B.E. / B.Tech. DEGREE EXAMINATION, NOV 2024

Professional Elective

Computer Science and Engineering

21ITV401 ETHICAL HACKING

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	List the Six types of flags in TCP Segment?	CO1 -U	
2.	Analyze the impact of a Distributed Denial of Service (DDoS) attack on an organization's network infrastructure.	CO3 -Ana	
3.	You are required to scan a network to identify open ports and the services running on them. Describe the type of scan you would perform?	CO2 -App	
4.	Outline on firewall	CO1 U	
5.	Analyze the impact of insufficient enumeration of network services on a penetration test. What could be the consequences if a tester fails to fully enumerate all network services on a target system?	CO3-Ana	
6.	Outline about NetBIOS enumeration	CO1 U	
7.	List the components of web application hacking	CO1 U	
8.	You encounter a high number of false positives in the CGI Scan report. How would you differentiate between false positives and Genuine Vulnerabilities?	CO2-App	
9.	What are the different types of intrusion detection systems	CO1 -U	
10.	Analyze the impact of misconfigurations in firewall rules on the security of a network	CO1 -U	

PART – B (5 x 16= 80 Marks)

11.	(a)	Explain in detail about TCP/IP Protocol Layers and discuss how intruders use these Layers for their Attack?	CO1 -U	(16)

Or

	(b)	How to protect the system from Malware attack and Explain it in detail?	CO1 -U	(16)
12.	(a)	You have been hired by a company to perform a security assessment on their network. Describe the steps you would take during the foot printing phase to gather information about the company's external-facing assets. Which tools would you use, and what specific information would you be looking to collect?	CO2 -App	(16)
		Or		
	(b)	You have been asked to perform a network scan on a client's internal network to identify potential security vulnerabilities. Describe the steps you would take, the types of scans you would perform. What information would you expect to gather from these scans?	CO2 -App	(16)
13.	(a)	Explain in detail about the Enumeration Concepts?	CO1 -U	(16)
		Or		
	(b)	Explain the purpose and importance of vulnerability assessment?	CO1 -U	(16)
14.	(a)	You are part of an ethical hacking team hired to conduct a penetration test on a government website. During the reconnaissance phase, What are the things you discover that the website is vulnerable to multiple types of web attacks?	CO2 -App	(16)
		Or		
	(b)	You're an IT security consultant for a medium-sized company that has recently experienced a security breach due to war driving. Unauthorized users gained access to the company's Wi-Fi network, leading to the theft of sensitive customer data. What are the data to identify vulnerabilities and recommend appropriate solution to the company?	CO2 -App	(16)
15.	(a)	Explain in detail about the Risk Analysis Tools for Firewalls and Routers	CO1 -U	(16)
		Or		
	(b)	Explain the following techniques of firewall identification: (a) Port scanning (b) Banner grabbing (c) Fire walking	CO1 -U	(16)