PVP 20

Code: 20IT6401

II B.Tech - II Semester – Regular Examinations – MAY 2024

CYBER SECURITY AND ETHICAL HACKING
(HONORS in INFORMATION TECHNOLOGY)

Duration: 3 hours Max. Marks: 70

Note: 1. This paper contains questions from 5 units of Syllabus. Each unit carries 14 marks and have an internal choice of Questions.
2. All parts of Question must be answered in one place.

BL – Blooms Level CO – Course Outcome

			BL	CO	Max. Marks
UNIT-I					
1	a)	What are the primary classifications of cybercrimes, and how do they impact individuals, organizations and society?	L1	CO1	7 M
	b)	Identify who are cybercriminals, and what motivates them to engage in illegal activities in cyberspace?	L2	CO1	7 M
OR					
2	a)	Discuss the legal perspectives surrounding cybercrimes, including the Indian IT Act 2000 and its implications for cybersecurity in India.	L2	CO1	7 M
	b)	Explain the global perspective on cybercrimes, highlighting significant trends, challenges and initiatives aimed at combating cyber threats worldwide.	L2	CO1	7 M

UNIT-II					
3	a)	Explain the concept of social engineering and its role in cybercrime, providing examples of common social engineering tactics used by cybercriminals.	L2	CO1 CO2	7 M
	b)	Discuss the significance of botnets in facilitating cybercrimes, including their characteristics, functionalities and the challenges they pose to cybersecurity.	L2	CO1 CO2	7 M
OR					
4	a)	Identify the role of cyber cafes in enabling cybercrimes, including their impact on anonymity, accessibility to cybercriminals and regulatory challenges.	L2	CO1 CO2	7 M
	b)	Describe the attack vectors commonly exploited by cybercriminals, including vulnerabilities in software, networks and human behavior.	L1	CO1 CO2	7 M
UNIT-III					
5	a)	Describe the role of proxy servers and anonymizers in facilitating cybercrimes, including their use for anonymity, bypassing censorship and evading detection.	L2	CO1 CO3	7 M
	b)	Discuss the various types of malware used in cybercrimes, including viruses, worms, trojans & spyware, and explain their functionalities and impacts on compromised systems.	L2	CO1 CO3	7 M
OR					

6	a)	Explain the phishing technique used by cybercriminals to deceive individuals into divulging sensitive information and discuss countermeasures for phishing prevention.	L2	CO1 CO3	7 M
	b)	Explain the different types of cyber-attacks, such as DoS and DDoS attacks, SQLI and buffer overflow.	L3	CO1 CO3	7 M
UNIT-IV					
7	a)	Discuss the ethical considerations and legal implications associated with ethical hacking, including compliance with relevant laws and regulations.	L2	CO1 CO4	7 M
	b)	Explain the required skill set for Ethical Hacking and also identify types of ethical hacking.	L2	CO1 CO4	7 M
OR					
8	a)	Explain the reconnaissance phase of ethical hacking, including information gathering methodologies and tools used to gather intelligence on target systems.	L2	CO1 CO4	7 M
	b)	Illustrate ethical hacking and explain its significance in cybersecurity, including its role in identifying and mitigating vulnerabilities in computer systems.	L3	CO1 CO4	7 M
UNIT-V					
9	a)	Classify the common types of passwords used in system security, and how do they differ in terms of strength and vulnerability to hacking?	L2	CO1 CO4	7 M

	b)	Discuss the concept of keyloggers and other spyware technologies, including their functionalities, methods of deployment and implications for user privacy and security.	L2	CO1 CO4	7 M
OR					
10	a)	Explain the process of cracking a password, including the various techniques and tools used by hackers to gain unauthorized access to password-protected systems.	L2	CO1 CO4	7 M
	b)	Differentiate between overt and covert channels used by trojans and backdoors to infiltrate systems.	L2	CO1 CO4	7 M