Question Paper

Exam Date & Time: 12-Jul-2023 (02:30 PM - 05:30 PM)

MANIPAL ACADEMY OF HIGHER EDUCATION

VIth SEMESTER B.TECH
MAKEUP EXAMINATION
JULY 2023

CYBER SECURITY [ICT 4306]

Marks: 50 **Duration: 180 mins.**

A

Answer all the questions.

Instructions to Candidates: Answer ALL questions Missing data may be suitably assumed

1)	A)	Explain how Single Sign-on (SSO) strengthens security measures and mitigates identity theft and password-related breaches. Additionally, discuss common challenges and limitations that arise during the implementation of single sign-on and potential solutions for addressing these issues.	(5)
	B)	Analyze the various types of Cross-Site Scripting (XSS) attacks that are commonly employed, and evaluate the potential impact of these attacks on users and organizations.	(3)
	C)	Evaluate the effects of software piracy on software vendors and users, considering the potential legal and financial ramifications associated with the use of pirated software.	(2)
2)	A)	Interpret the relationship between security services and mechanisms. Also, with suitable examples justify how security services and mechanisms work together to protect against common cyber threats.	(5)
	B)	Compare and contrast computer viruses with other types of malware such as worms, trapdoors, and zombies, highlighting their differences. Analyze the mechanisms by which these threats spread and propagate, and evaluate common techniques employed by attackers to distribute and infect targets.	(3)
	C)	Differentiate between cross-site scripting (XSS) and cross-site request forgery (CSRF), and assess how these vulnerabilities can jeopardize web applications.	(2)
3)	A)	Examine the relationship between the Same Origin Policy and other web security mechanisms, such as Client Access Policy and Cross-Origin Resource Sharing, and evaluate how they can be utilized in tandem to enhance security measures against common attacks.	(5)
	B)	Explain the differences between digital forensics investigations and traditional investigations that involve physical evidence and witnesses. Additionally, discuss the ethical and legal considerations that forensic investigators need to consider when conducting digital forensics investigations to ensure that their approach is defensible.	(3)
	C)	Define ethical hacking and differentiate it from traditional hacking. Explain how organizations can integrate ethical hacking into their security strategy.	(2)
4)	A)	Discuss the benefits of using digital signatures over traditional signatures, as well as the challenges and limitations of using digital signatures. With suitable proofs of concept discuss how digital signatures have impacted security and privacy.	(5)

	B)	Explain the typical features and functionalities of a Web application Firewall, and compare and contrast it with other security solutions such as intrusion detection and prevention systems (IDPS), highlighting their similarities and differences.	(3)
	C)	Identify some challenges and limitations in the enforcement of cybercrime laws and regulations, and explain how these can hinder the ability of law enforcement agencies to combat cybercrime effectively.	(2)
5)		Explain the working principles of Intrusion Detection Systems (IDS) and how they differ from Firewalls in detecting potential threats in an organization.	(5)
	A)		
	B)	Inspect the differences between an act, a code, an article, and a section in the Indian legal system, and how they are applied in practice.	(3)
	C)	Describe the process of collecting user data on websites and identify the two primary methods used for this purpose.	(2)

-----End-----