Reg. No															

B.Tech DEGREE EXAMINATION, DECEMBER 2023

Seventh Semester

18CSE493T - CYBER CRIMES AND CYBER SECURITY

(For the candidates admitted during the academic year 2020 - 2021 & 2021 - 2022)

Note:

i. **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

PART - A (20 × 1 = 20 Marks)

Answer **all** Questions

		Marks	BL	CO
1.	IPC inspiration derived from (A) Japan penal code and code of korea (B) french penal code and code of Louisiana in the US (C) USA penal code and code of newyork (D) UK penal code and code of french	1	1	1
2.	Chief justice and other judges of supreme court are directly appointed by (A) Prime Minister of India (B) Home Minister of India (C) Vice President of India (D) President of India	1	1	1
3.	India comes under which legislature (A) uni-cameral (B) tri-cameral (C) bi-cameral (D) one-chamber	1	1	1
4.	Match the following terms: (i) India - a. parliament (ii) Japan - b. congress (iii) UK - c. diet (iv) USA - d. sansad (A) i – d, ii – b, iii – a, iv - c (B) i – a, ii – b, iii – c, iv - d (C) i – d, ii – c, iii – a, iv - b (D) i – a, ii – d, iii – c, iv - b	1	1	1
5.	Which of the following is NOT covered by the Information Technology Act, 2000? (A) Cybercrime and electronic fraud (B) Data protection and privacy (C) Regulation of social media platforms (D) Digital signatures and electronic records	1	1	2
6.	Choose the international court is responsible for settling disputes between states, including issues of jurisdiction? (A) International Criminal Court (ICC) (B) International Court of Justice (ICJ) (C) International Tribunal for the Law of the Sea (ITLOS) (D) European Court of Human Rights (ECHR)	1	1	2
7.	What is the significance of a digital signature under the Information Technology Act, 2000? (A) It is legally binding and equivalent to a physical signature. (B) It is optional and not recognized by law. (C) It is required only for government documents. (D) It is used only for email communication.	1	1	2

8. What is the principle of "Sovereign Immunity" in international law? 1 1 2

(A) States can be held accountable for any action in international courts.
(B) Diplomats enjoy immunity from prosecution for any crime.
(C) States have absolute immunity from any legal actions.
(D) Heads of state are immune from prosecution in all cases.

9. _____ is the primary goal of threat analysis in cybersecurity? 1 1 3

(A) To prevent all cyber threats
(B) To detect and respond to cyber threats
(C) To identify potential vulnerabilities
(D) To secure physical assets

10. In threat analysis, what does the term "attack vector" refer to? 1 1 3

(A) A type of firewall
(B) The path or method used by a threat actor to exploit a vulnerability
(C) A security policy
(D) An antivirus program

11. Which type of threat involves manipulating or altering data to deceive or mislead users or systems? 1 1 3

(A) Data breach
(B) Data leakage
(C) Data manipulation
(D) Data encryption

12. How do you describe digital forensics in cybersecurity? 1 1 3

(A) Investigating physical security breaches
(B) Analyzing computer systems, networks, and digital devices for evidence of cybercrimes
(C) Recovering lost passwords
(D) Predicting future cyber threats

13. Which of the following is an example of a common authentication factor? 1 1 4

(A) Something you know
(B) Something you are
(C) Something you see
(D) Something you hear

14. _____ is the purpose of a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)? 1 1 4

(A) To authenticate users
(B) To authorize access to resources
(C) To prevent automated bots from accessing a system
(D) To encrypt data transmissions

15. Which OSI layer does a firewall primarily operate at? 1 1 4

(A) Layer 1 (Physical layer)
(B) Layer 2 (Data Link layer)
(C) Layer 3 (Network layer)
(D) Layer 7 (Application layer)

16. Choose the type of IDS monitors network traffic in real-time and can detect patterns or anomalies indicative of an intrusion. 1 1 4

(A) Host-based IDS (HIDS)
(B) Network-based IDS (NIDS)
(C) Firewall IDS (FIDS)
(D) Anti-malware IDS (AMIDS)

17. Among the following, choose the best option that describes Trusted Computing. 1 1 5

(A) A computing model that ensures all data is encrypted
(B) A concept that focuses on securing hardware components like CPUs and TPMs
(C) A security framework that relies on user authentication only
(D) A method for securing network communication

18. What is the Bell-LaPadula model in Multilevel Security? 1 1 5

(A) A model for encrypting data at rest
(B) A model for controlling access to classified information based on security clearances
(C) A model for network intrusion detection
(D) A model for securing network communication

19.	In cybersecurity training, what is the purpose of conducting simulated security incidents or drills? (A) To confuse employees (B) To test the effectiveness of security policies (C) To identify potential threats (D) To decrease employees' awareness	1	1	5
20.	Which physical security control restricts access to a secure area based on an individual's security clearance level? (A) Access control list (ACL) (B) Perimeter fencing (C) Mantrap (D) Biometric authentication	1	1	5

PART - B (5 × 4 = 20 Marks)
Answer **any 5** Questions

		Marks	BL	CO
21.	Write short notes on Indian penal code 1860?	4	1	1
22.	What is morality? Explain the relation between morals and law.	4	1	1
23.	Explain the components of security threat correlation along with the data sources.	4	1	3
24.	Discuss the various types of threats that can occur in the cyber space along with examples.	4	2	3
25.	What is a firewall? Discuss various types of firewalls that are commonly implemented.	4	2	4
26.	Discuss the various types of Intrusion Detection Systems and the working in detail.	4	2	4
27.	Elucidate some key components typically included in email and internet usage policies.	4	3	5

PART - C (5 × 12 = 60 Marks)
Answer **all** Questions

		Marks	BL	CO
28.	(a) Explain the salient features of Indian judiciary. **(OR)** (b) Illustrate the structure of courts in India and its function with neat diagram.	12	1	1
29.	(a) (i). What is jurisdiction with respect to cyberspace? Discuss the issues of jurisdiction that one has looked upon. (8) (ii). Discuss the jurisdiction under the Information Technology Act 2000. (4) **(OR)** (b) Explain the purpose of Information technology act 2000 along with the chapters involved with the act.	12	1	2
30.	(a) Elucidate the Security Correlation steps in a Corporate Network given below. Background: XYZ Corporation is a large financial institution that handles sensitive customer data and financial transactions. They have a complex network infrastructure with multiple security devices and systems in place, including firewalls, intrusion detection systems (IDS), and antivirus software. The security team is responsible for monitoring and protecting the network from cyber threats. **(OR)** (b) ACME Inc. is a medium-sized e-commerce company that recently experienced a data breach. Customer personal information, including names, addresses, and credit card numbers, was stolen. The company's cybersecurity team suspects a breach in their web server but needs to conduct a thorough forensic analysis to determine the scope of the breach and the extent of the data exposed. Perform the forensic analysis steps in order to identify the level of data exposure.	12	4	3

31.	(a) How important is security monitoring and auditing in cyber security? Discuss he key aspects of monitoring and auditing in the cyberspace.	12	3	4
	(OR)			
	(b) XYZ Corporation is a large multinational company with a complex network infrastructure. They have sensitive corporate data and customer information stored on their servers. To maintain security, XYZ Corporation employs strong authentication and authorization mechanisms. Discuss the authentication and authorization approaches the corporation should adhere to, in order to provide a secure access to the network.			
32.	(a) What is Role-based Access Control (RBAC) security model? Explain the working and the key components involved in RBAC along with the challenges in implementing it.	12	2	5
	(OR)			
	(b) Explain the concept of trusted computing and multilevel security with respect to cyber security along with their key components in detail.			

* * * * *