B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Seventh Semester

18EEE433T - 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. Minimizing the number of incidents is a function of which of the following? — 1　1　1
   (A) Incident response testing　　　(B) Forensic analysis
   (C) Risk management　　　　　　　(D) Security investments

2. Which of the following have the capability of spreading itself and doesn't require the host and human support to spread? — 1　1　1
   (A) Virus　　　　(B) Trojan
   (C) Worm　　　　(D) Bug

3. Which of the following belong to Categories of Cybercrimes? — 1　1　1
   (A) Cybercrimes against People　　　(B) Cybercrimes against Property
   (C) Cybercrimes against Government　(D) All the above

4. Which of the below does not constitute a cybercrime? — 1　1　1
   (A) refusal of service　　(B) Man in the middle
   (C) Phishing　　　　　　(D) Advanced Encryption Standard

5. Which of the following attack types best describes a targeted attack that successfully obstructs functionality? — 1　1　2
   (A) Spam attack　　(B) Malware attack
   (C) DDoS attack　　(D) Killer attack

6. Expand DoS Attacks _____ — 1　1　2
   (A) Denial of Service　　　(B) Disk operating System
   (C) Duplication of Service　(D) Duplication of system

7. What is a grey hat hacker? — 1　1　2
   (A) Black Hat Hacker　　　　　　　　　(B) White Hat Hacker
   (C) Combination of White and black hat hackers　(D) None

8. Which of the following describes malicious computer programs such as viruses, worms, and Trojan horses? — 1　1　2
   (A) Software piracy　　(B) Malware
   (C) Larceny　　　　　(D) Arson

9. Which of the following is not a strong security protocol? — 1　1　3
   (A) SSL　　　(B) HTTPL
   (C) SMTP　　(D) SFTP

10. Which of the below is a hacking technique in which cybercriminals create fictitious web pages or domains to deceive or obtain more traffic — 1　1　3
    (A) Pharming　　(B) Mimicking
    (C) Spamming　　(D) Website-Duplication

11. Which of the below is a popular victim of cyber attackers looking to gain the IP address of a target or victim user?   1   1   3
    (A) emails   (B) websites
    (C) IP tracer   (D) web pages

12. HTTPS is abbreviated as _____   1   1   2
    (A) Hypertexts Transfer Protocol   (B) Secured Hyper Text Transfer
        Secured   Protocol
    (C) Hyperlinked Text Transfer Protocol (D) Hyper Text Transfer Protocol
        Secured   Secure

13. An act to injure, corrupt, or threaten a system or network is characterized as which of   1   1   3
    the below?
    (A) Digital crime   (B) Threats
    (C) System hijacking   (D) Cyber Attack

14. A _____ can be a hardware device or a software program that filters all the   1   1   3
    packets of data that comes through a network, the internet, etc.
    (A) Firewall   (B) Antivirus
    (C) Malware   (D) Cookies

15. CCFP stands for?   1   1   3
    (A) Cyber Certified Forensics   (B) Certified Cyber Forensics
        Professional   Professionalt
    (C) Certified Cyber Forensics Program   (D) Certified Cyber Forensics Product

16. Computer forensics also known as?   1   1   4
    (A) digital forensic science   (B) computer crime
    (C) computer forensic science   (D) computer forensics investigations

17. Which one option is not a type of cybercrime?   1   1   4
    (A) Data theft   (B) Forgery
    (C) Damage to data and systems   (D) Installing antivirus for protection

18. Computer forensics also is used in civil proceedings.   1   2   5
    (A) Yes   (B) No
    (C) Can be yes or no   (D) Cannot say

19. Any company or agency's IT protection is managed and maintained by?   1   1   5
    (A) Software Security Specialist   (B) CEO of the organization
    (C) Security Auditor   (D) IT Security Engineer

20. Which of the below is an internet fraud in which a consumer is digitally persuaded to   1   2   6
    reveal personal data by cybercriminals?
    (A) MiTM attack   (B) Phishing attack
    (C) Website attack   (D) DoS attack

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

	Marks	BL	CO
21. Mention the Need of Cybersecurity.	4	1	1
22. Write short note on motive of cyber attackers.	4	2	2
23. Define: a) Authentication b) Biometrics	4	1	3
24. Write short notes on SOAP Services .	4	2	4
25. Discuss about the challenges to Indian cyber laws.	4	1	5
26. Write about Digital Forensics.	4	2	6
27. What are the limitations of firewalls?	4	1	5

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

		Marks	BL	CO

28. (a) What is the concept of internet governance, and how does it influence the development, management, and regulation of online spaces? — 12 4 1

(OR)

(b) What is the potential impact of cyber warfare on critical infrastructure, and how do nations prepare to defend against or respond to cyber-attacks that target essential systems?

29. (a) Define an Intrusion. Discuss the Intrusion Detection System — 12 1 2

(OR)

(b) Explain briefly about Complex Network Architectures.

30. (a) Discuss in brief the main features of HTTP. — 12 1 3

(OR)

(b) Explain detail about web application.

31. (a) Explain the approaches for Digital Signatures based on Public Key Encryption. — 12 1 4

(OR)

(b) Write a detail note on firewall design principles and types of firewalls.

32. (a) Explain about Cyber Forensics and digital evidence. — 12 1 5

(OR)

(b) Explain about the Cybercrime and punishments in India.

* * * * *