(8 pages) **Reg. No. :** .....

Code No. : 8389 **Sub. Code : WCAE 31**

M.C.A. (CBCS) DEGREE EXAMINATION, NOVEMBER 2024

Third Semester

Computer Application

Elective – V — CYBER SECURITY

(For those who joined in July 2023 onwards)

Time : Three hours Maximum : 75 marks

PART A — (15 × 1 = 15 marks)

Answer ALL questions.

Choose the correct answer :

1. What is the primary reason for the commission of cybercrime?
   (a) Curiosity (b) Financial gain
   (c) Boredom (d) Entertainment

2. Cyberstalking is classified under which type of cybercrime?
   (a) Financial crime (b) Social crime
   (c) Cyber harassment (d) Cyber terrorism

3. Which type of malware replicates itself to spread to other computers?
   (a) Trojan Horse (b) Worm
   (c) Spyware (d) Adware

4. Which of the following is a good practice when making purchases online?
   (a) Using public Wi-Fi networks
   (b) Using a credit card or secure payment method
   (c) Sharing personal information freely
   (d) Ignoring website security features

5. How often should you clear your browser cache?
   (a) Never
   (b) Once a year
   (c) Periodically, depending on usage
   (d) Only when your browser slows down

6. What is phishing?
   (a) A method to secure emails
   (b) A type of email scam to steal personal information
   (c) A technique to organize emails
   (d) A way to filter spam emails

7. Which of the following best describes the role of law enforcement officers in cybercrime investigation?

(a) Developing cybersecurity software

(b) Collecting and preserving digital evidence

(c) Providing legal defense for accused individuals

(d) Educating the public about internet safety

8. What is a key step in incident response?

(a) Ignoring security breaches

(b) Containing and mitigating the threat

(c) Publicly announcing the breach immediately

(d) Deleting all affected data

9. What does WiFi RF scanning involve?

(a) Scanning for radio frequencies used by WiFi networks

(b) Disabling all WiFi networks in the area

(c) Blocking WiFi signals

(d) Interfering with WiFi communications

10. Which of the following is a key step in the digital evidence seizure methodology?

(a) Destroying all digital evidence

(b) Ensuring proper documentation and chain of custody

(c) Ignoring encryption on seized devices

(d) Handling evidence without gloves

11. Which of the following is an alternative to seizing entire hardware?

(a) Imaging the hard drive

(b) Copying physical documents

(c) Shutting down the computer

(d) Disconnecting the network

12. What has the explosion of networking led to in terms of cybercrime?

(a) Decrease in cybercrime cases

(b) Increase in opportunities for cybercriminals

(c) Elimination of digital evidence

(d) Reduced need for cybersecurity measures

13. Which of the following is the first phase of digital forensics?

(a) Examination (b) Analysis

(c) Collection (d) Reporting

14. Which of the following tasks is performed during the analysis phase?

(a) Data preservation

(b) Data recovery and interpretation

(c) Data collection

(d) Data destruction

15. What type of cybercrime is often targeted at government agencies?

(a) Online shopping fraud

(b) Cyber espionage and data breaches

(c) Social media harassment

(d) Email phishing campaigns

PART B — (5 × 4 = 20 marks)

Answer ALL questions, choosing either (a) or (b).

Each answer should not exceed 250 words.

16. (a) What are the different classifications of cybercrimes with examples?

Or

(b) How do digital signatures enhance the security of online transactions?

17. (a) Why is it important to clear your browser cache before making an online purchase?

Or

(b) Mention some major security issues associated with using a Wireless LAN (WLAN).

18. (a) Explain some legal issues associated with intercepting Wi-Fi transmissions.

Or

(b) What techniques are commonly used for eavesdropping on WiFi networks?

19. (a) Discuss about some alternatives to the wholesale seizure of hardware when collecting digital evidence.

Or

(b) Describe some common threads or principles that should be followed during the seizure of digital evidence.

20. (a) Explain the digital forensics, and why is it important in the context of cybercrime investigations.

Or

(b) Define the main phases of digital forensics and the purpose of each phase.

PART C — (5 × 8 = 40 marks)

Answer ALL questions, choosing either (a) or (b).

Each answer should not exceed 600 words.

21. (a) Explain the role and different types of authentication methods in cybersecurity.

Or

(b) Discuss the importance, advantage and disadvantage of encryption in ensuring data security.

22. (a) List out some comprehensive safe browsing guidelines for social networking sites.

Or

(b) Describe the importance, guidelines and measures of smartphone security.

23. (a) Write a short note on the role, responsibilities and unique skills of a cybercrime investigator.

Or

(b) Describe the process and steps of analyzing a computer system compromised by the Hacker Defender rootkit.

24. (a) Explain the role of IP addresses in cyber investigations and explain the use of IP addresses.

Or

(b) Why is effective interpersonal communication important in cyber investigations and discuss its role.

25. (a) What are the primary challenges and considerations involved in the collection of digital evidence?

Or

(b) Mention the types of cybercrimes are commonly targeted at government agencies with examples.

———————