CB 60:40

## TILAK MAHARASHTRA VIDYAPEETH, PUNE BACHELOR OF COMPUTER APPLICATIONS (B.C.A.)/ SPECIALIZATION IN CYBER SECURITY (CS)

**EXAMINATION: MAY-2024** 

**SEMESTER - V** 

**Sub:** Cyber Security - III (BCA – 544-18/BCA-CS-544-20)

Date: 24/05/2024 Total Marks: 60 Time: 2.00 pm to 4.30 pm

## Instructions:

- 1. All questions are compulsory unless and otherwise stated.
- 2. Bold figures to the right of every question are the maximum marks for that question.
- 3. Candidates are advised to attempt questions in order.

	<ul><li>4. Answers written illegibly are likely to be marked zero.</li><li>5. Use of scientific calculators, Log tables, Mollier Charts is allowed.</li></ul>		
	6. Draw neat and labelled diagrams	wherever necessary.	
Q.1.	Fill in the blanks.		(05)
1.	, or the unsolicited sending of bulk email for commercial purposes, is		
	unlawful to varying degrees.		
	a) Identity Theft	b) Harassment	
	c) Spam	d) Malware	
2.	aims at redirecting the website used by the customer to another bogus website by hijacking the victim's DNS server.		
	a) Identity Theft	b) Harassment	
	c) Internet Pharming	d) Malware	
3.	Administrative shares are considered hidden shares, and they all have the character appended to their names.		
	a) #	b) @	
	c) %	d) \$	
4.	Objects or information of potential probative value that is associated with physical items are called as		
	a) Digital Evidence	b) data objects	
	c) Duplicate Digital Evidence	d) Physical Items	
5.	is used to capture the keystroke logs, screen dumps and clipboard data along with application logs.		
	a) Virus	b) Keylogger	
	c) Worm	d) Trojan	
0.2	State Tune/Felge		(05)
<b>Q.2.</b> 1.	State True/False.  Cyber Stalking in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources.		(05)
2.	Router creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed.		
3.	4. Digital evidence is said to be fragile.		
4.			
5.	Section 66 provides the punishment for Hacking with intent or knowledge.		
Q.3.	Answer the following. (Solve any 5)		(10)
1.	What is digital evidence?		
2.	* *		
3.	Define the term "Hash".		
4.	What is expert report?		

- 5. Define the term "Denial of Service Attacks".
- 6. Define the term "Phishing".

## Q. 4. Answer the following in detail. (Solve any 6)

(30)

- 1. Define the term "Cyber Crime". Explain any two types of Cyber Crime.
- 2. Explain the procedure of reviewing IIS logs with example.
- 3. Write a short note on "Event Viewer".
- 4. Write down the steps involved in computer crime investigation.
- 5. Explain any two types of digital evidence.
- 6. Explain in detail steps involve in computer forensics.
- 7. Explain the five basic ways computer criminal use to get information of the companies they attack.

## Q. 5. Answer the following in detail. (Solve any 1)

(10)

- 1. What are the six steps, in order, that a computer crime investigator would normally follow?
- 2. Explain any five types of Cyber Crime.

Cyber Security Level- III (BCA – 544-18/BCA-CS-544-20) ALD/I