RV College of Engineering®
Mysore Road, RV Vidyaniketan Post,
Bengaluru - 560059, Karnataka, India

Department of Computer Science and Engineering

Date: 18.06.25	Test - 2	Max. Marks:
Semester: II	UG	Duration: $1\frac{1}{2}$ Hrs
Course: Introduction to Cybersecurity		Course Code:CS124BT

Q. No.	Questions	M	BT	CO
1.a	Discuss the various types of E-commerce models and provide examples for each.	5	L2	CO1
1.b	Why should e-commerce platforms prioritize cybersecurity?	5	L2	CO4
2.a	What are the key challenges, potential benefits, and common risks associated with online social networks?	6	L2	CO4
2.b	Describe the role of payment gateways in digital transactions.	4	L2	CO1
3.a	Using a labelled diagram, explain the concept and working of tunnelling techniques.	6	L2	CO3
3.b	Discuss how digital wallets differ from conventional payment methods. Include the pros and cons of both approaches.	4	L2	CO4
4	LMN Mart is a fast-growing E-commerce application that allows users to purchase electronics, clothing, and groceries through its web and mobile platforms. Recently, LMN Mart detected a spike in fraudulent transactions where attackers used stolen payment card data to place high-value orders. Many genuine customers reported unauthorized charges and account misuse. As a cybersecurity consultant, analyze the scenario and answer the following questions: i. What are the potential consequences of the payment fraud for LMN Mart and its customers? ii. What vulnerabilities or security weaknesses in LMN Mart's system may have contributed to the success of the fraudulent transactions? iii. What measures should LMN Mart take to strengthen its fraud detection mechanisms and enhance overall transaction security? iv. How should LMN Mart communicate effectively with the affected users and payment partners to address the issue and rebuild trust?	10	L4	CO4
5	Explain how attackers exploit proxies. Discuss various techniques for detecting proxy usage.	10	L2	CO5

****

USN	1	R	V	2	4	C	S	0	3	1

R V College of Engineering

R V Vidyanikethan Post
Mysuru Road Bengaluru - 560 059

I / II Semester B.E. Regular/ Supplementary Examinations- July/August - 2025.
Common to All Programs.
Course : Introduction To Cyber Security CS114BTF/CS124BTF

Time : 3 Hours

Maximum Marks : 100

Instructions to the students

1. Answer all questions from Part A. Part A questions should be answered in first three pages of the answer book only.
2. Answer FIVE full questions from Part B. In Part B question number 2 is compulsory. Answer any one full question from 3 and 4, 5 and 6, 7 and 8, 9 and 10.

Part A

Question No	Question	M	CO	BT
1.1	Define the term Cyberspace.	01	1	1
1.2	State any two key differences between a hacker and a cracker.	02	2	2
1.3	During a forensic investigation of a compromised mobile device, it was discovered that a malicious third-party app accessed user data without consent. What legal or policy measure could have prevented this issue?	01	4	2
1.4	Differentiate between spam and phishing emails.	02	2	2
1.5	How do attackers use custom or local proxies to conceal their identity, and why are these hard to detect?	02	3	2
1.6	Why is it important to flag or report inappropriate content on social media?	02	2	2
1.7	An organization has implemented a strong password policy, but several accounts were still compromised due to credential stuffing attacks. Which additional security measure would best complement the password policy?	02	3	4
1.8	In E-commerce what does "C2B" stand for?	01	2	1
1.9	Under which IT Act clause can RBI penalize banks for UPI frauds?	01	1	2
1.10	List two examples of B2C E-Commerce platforms.	02	2	2
1.11	What is the role of 'Application Whitelisting' in endpoint security? Give an example.	02	3	1
1.12	A hospital uses legacy antivirus software and skips updates. How does this affect endpoint security?	02	2	4

Part B

Question No	Question	M	CO	BT
2a	Ravi's company hires a professional to test the security of its network by trying to hack into it and find any weaknesses. a) What type of hacker was hired? b) What is the goal of such hacking?	06	2	4

c) State benefits of hiring such hackers.

An employee misused his system access to delete critical company data after a dispute with management.

2b Identify the type of cyber-attack and suggest two ways such attacks can be prevented. 04 3 3

A small, rural hospital contracted with an emergency medical group for emergency department (ED) coverage. The group was paid monthly by EFT from the hospital's account to the ED group's account. In June, the hospital received an email invoice from the ED group with instructions to send payment to a new account. The hospital sent the $200,500 payment to the new account on July 10. On July 12, the payment was returned because the new account was frozen. On July 16, the ED

2c group emailed new account information and instructions to the hospital. 06 4 4

The hospital sent the $200,500 payment to the new account. In early August, the ED group sent the next monthly invoice by email with instructions to send the funds to another new account. The hospital sent the $206,500 payment on August 13. Identify and explain the type/types of fraud involved in the above incident. Also discuss the preventive measures to be taken by the hospital.

An attacker gathers employee details from public sources and sends a fake government email with a malicious file to an HR executive at a pharma company. The file installs spyware that records data. Later, the attacker accesses internal systems and steals research files using anonymous proxies and encrypted tunnels.

3a Answer the following : 08 3 3

i) Mention two attack vectors used.

ii) Identify and explain two types of attacks involved.

iii) Name two tools or techniques used.

iv) Suggest two preventive measures.

A security team at a financial services firm notices abnormal but encrypted DNS traffic leaving the internal network. After investigation, it is revealed that an insider had been gathering sensitive financial records over several weeks. The data was being exfiltrated in small chunks using DNS tunneling. The insider had earlier performed passive reconnaissance using internal tools and company manuals, and had disabled basic logging to avoid detection. To further cover tracks, the attacker used a local proxy configured on their system, which rerouted all monitoring tools to false outputs.

3b Answer the following questions based on the scenario : 08 3 3

i) Identify the two attack types used.

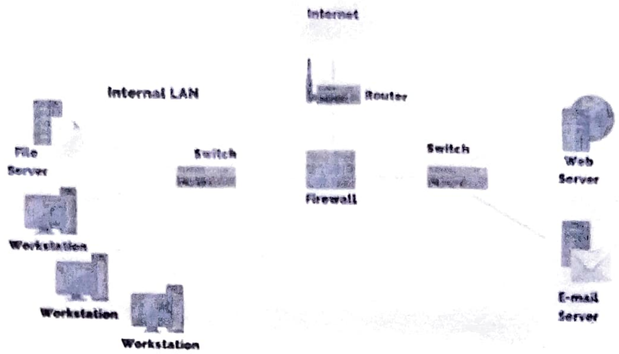
ii) Mention two antiforensics techniques applied in this case.

iii) Name and explain two tools or methods used in passive reconnaissance or tunneling.

iv) Suggest two advanced preventive controls that could detect or prevent this attack.

OR

4a Consider an enterprise network highlighting the security features involved in it. 06 2 4



List out the occurrence of possible vulnerabilities that the hackers would look into to breach the network.

4b Differentiate between phishing, vishing, and smishing attacks. Provide one example each. 06 2 4

4c What is tunneling in cyberattacks? Explain how attackers use it to avoid detection. 04 4 2

5a A student creates a fake LinkedIn profile impersonating a professor and uses it to solicit money from students under false pretenses. How should victims detect and report impersonation? How does the platform respond? Outline the legal consequences. 08 3 3

5b Anita, a college student, notices a fake Instagram profile impersonating her friend and sharing offensive content using her name and photos. Several students have started commenting negatively on the posts, believing it to be real. Anita decides to report the profile but is unsure about the correct steps and how the platform will handle her report. 08 3 4

As a cybersecurity student, explain to Anita the steps she should take to report the impersonation. Also describe how the social media platform's moderation system (both automated and manual) would process her report, and what actions the platform may take after verifying the violation. Highlight the importance of community guidelines in this context.

OR

6a Illustrate a case study on social media misuse and its legal consequences. 10 3 3

6b Define social media. Explain the different types of social media. 06 2 2

7a Describe any four major digital payment frauds in India. Explain how each is executed and list the specific counter measures to prevent them 10 3 3

7b **Scenario:** At an ATM, a "helpful stranger" saw Divya struggling to withdraw cash. He offered assistance and watched her enter the PIN. Next day, her account was empty. 06 3 4

Questions:

i) What scam occurred here?

ii) List two safe ATM practices

	iii) Which banking regulation protects victims? iv) Name one safer alternative to ATM cards			
	OR			
8a	Discuss the working of Aadhar Enabled Payment System(AEPS) and its role in promoting financial inclusion. Compare AEPS with at least two other payment methods.	10	2	2
8b	Illustrate any three essential security features for online shopping sites. List three common online banking threats that is seen in todays world.	06	2	2
9a	What are the best practices for securing wireless communications?	08	3	3
9b	What guidelines should be followed when setting a strong password?	08	2	2
	OR			
10a	Assume , you are starting a new workplace with 5 employees.Identify four tools that has to be installed to protect workspace from threats and give reason.	06	4	4
10b	A digital marketing team uses third-party browser plugins to track analytics. One plugin leaked customer data. How should plugin management be handled securely?	04	3	4
10c	A government department issued smartphones to employees for official use. Although devices had encryption and screen locks enabled, several employees delayed system updates, ignored app permission warnings, and installed news apps from unofficial sources. Later, it was discovered that a malicious app exploited an unpatched vulnerability, exposing sensitive government emails and user location data to external servers. Evaluate the security failures in the above situation with reference to patch management and mobile device security. Propose three corrective actions to prevent such incidents in future deployments.	06	3	4