	RV College of Engineering® **Department of Computer Science and Engineering** **CIE - I: Test Paper**

Course & Code	**INTRODUCTION TO CYBER SECURITY (CS124BTF)**		**Semester: II**
Date: 15/05/2024	**Duration:**90 minutes	**Max.Marks** : 50 Marks	
USN :	**Name :**		

NOTE: ***Answer all the questions***

Sl.no.	**Questions**	**Marks**	**BT**	**CO**
1.a	Cyber Security is all about securing the Cyber Space. What you mean by Cyber Space. Trace the evaluation of Cyber space from the early computing era of mainframe to present mobile communication. Identify the technical revolutions happened in each transition.	05	L2	CO1
1.b	Distinguish between Cyber Security and Information Security.	05	L1	CO1
2.a	List and explain different types of cyber security threats.	06	L2	CO1
2.b	Identify and explain in brief the steps involved in the Security System Development Life Cycle (SecSDLC).	04	L2	CO1
3.a	Define passive attack. List and explain the any three tools used in passive attack.	06	L2	CO5
3.b	Explain Pay-per-click business model with all the stake holders of this model and also discuss the fraud activities involved in this model.	04	L3	CO2
4.a	What are proxies? How and why attackers use proxies.	06	L3	CO3
4.b	Mr. Bhaskar needs to fill an online application for a government job which needs to pay the application fee in web portal itself. Mr. Bhaskar plans to fill online application in a Cybercafé, identify and discuss the safety measures he needs to follow while filling and after filling the application.	04	L3	CO2
5.a	In a large financial institution, the accounting department notices small, unauthorized transactions occurring across multiple accounts over some time. Upon investigation, it's revealed that these transactions were orchestrated by an employee who manipulated financial records to siphon off small amounts of money from various accounts. Identify and explain the type of cyber-attack described in the scenario.	06	L3	CO4
5.b	Explain the following in detail i. Shoulder surfing ii. Dumpster Driving	04	L2	CO3

	L1	**L2**	**L3**	**L4**	**L5**	**L6**	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	05	25	20	***	***	***	20	08	10	06	06

Department of Computer Science and Engineering

Academic year 2023-2024 (Even Semester)

CIE 2: Question Paper

Course	**Introduction to cyber security**		
Date	June 2024	Maximum Marks	50
Course Code	CS124BT	Duration	90 Min
Sem	II	CIE – II	

Sl.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 cyber security is a matter of concern for e-commerce?	5	L2	CO2
2.a	Consider the case study: XYZ Online Retailer is a popular E-commerce platform offering a wide range of products to customers worldwide. Recently, the company experienced a significant data breach resulting in the exposure of thousands of customer records, including personal information and payment details. As a cybersecurity consultant, analyze the situation and answer the following questions: • What are the potential consequences of the data breach for XYZ Online Retailer and its customers? • What vulnerabilities or security weaknesses may have contributed to the data breach? • What steps can XYZ Online Retailer take to improve its E-commerce security posture and enhance customer trust? • How can XYZ Online Retailer communicate effectively with affected customers and stakeholders regarding the incident?	10	L3	CO4
3.a	Explain the key differences between digital wallets and traditional payment methods. Mention advantages and disadvantages of each of the methods.	5	L2	CO2
3.b	Describe the role of payment gateways in digital transactions.	5	L3	CO2
4.a	Discuss any 5 modes of digital payments that are available to the society.	5	L2	CO3
4.b	Define digital security. Differentiate between digital information security and cyber security	5	L3	CO4
5	A university's network was compromised due to multiple faculty and student laptops being infected with ransomware. This led to significant data loss and disruption of academic activities. On this case, answer the following questions: 1. What are various digital devices involved in this scenario? 2. What are the potential weaknesses in the university's network security that could have allowed ransomware to spread? 3. How can antivirus software, firewalls, and regular software updates help in preventing such attacks? 4. What should be the university's immediate response to a ransomware attack to minimize data loss and restore affected systems?	10	L4	CO5

Course Outcomes: After completing the course, the students will be able to:-	
CO 1	Understand the cyber-attacks and their principles for different domains- social media,E-commerce, and digital devices.
CO 2	Analyse vulnerabilities in different domains that the attacker capitalizes for attack.
CO 3	Applydifferent attacking techniques that make use of vulnerabilities available in various domains.
CO 4	Evaluate methods to cover different vulnerabilities to safeguard the systems against cyber-attacks.
CO 5	Investigate modern tools and technologies available to mitigate cybercrime attacks.

BT-Blooms Taxonomy, CO-Course Outcomes, M-Marks

Marks Distribution	Particulars		CO1	CO2	CO3	CO4	CO5	L1	L2	L3	L4
	Test	Max Marks	5	15	5	15	10	--	20	20	10

	RV College of Engineering® **Department of Computer Science and Engineering** **CIE 3 (Improvement Test)**		
Course & Code	**INTRODUCTION TO CYBER SECURITY** **(CS124BTF)**		**Semester: II**
Date: 03/07/2024	**Duration:**120 minutes	**Max.Marks**: 60 Marks)	
USN :	**Name :**		

NOTE: ***Answer all the questions from Part-A (10 M) and Part-B (50 M)***

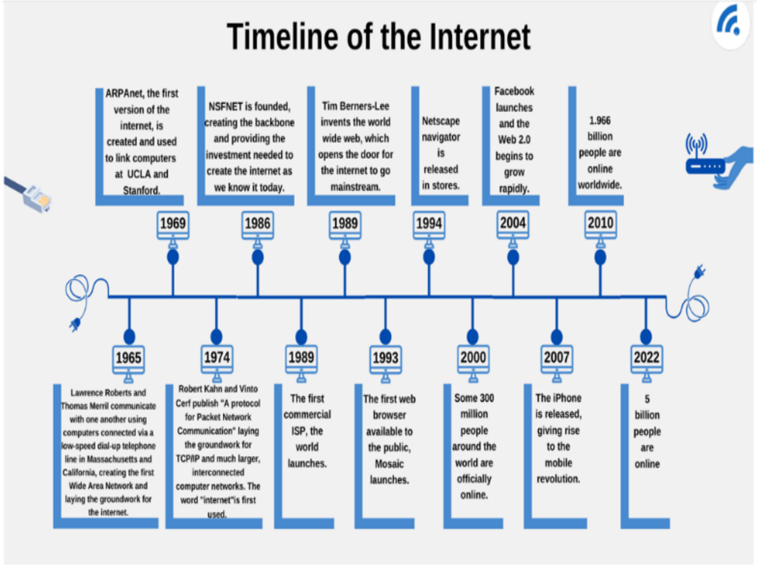
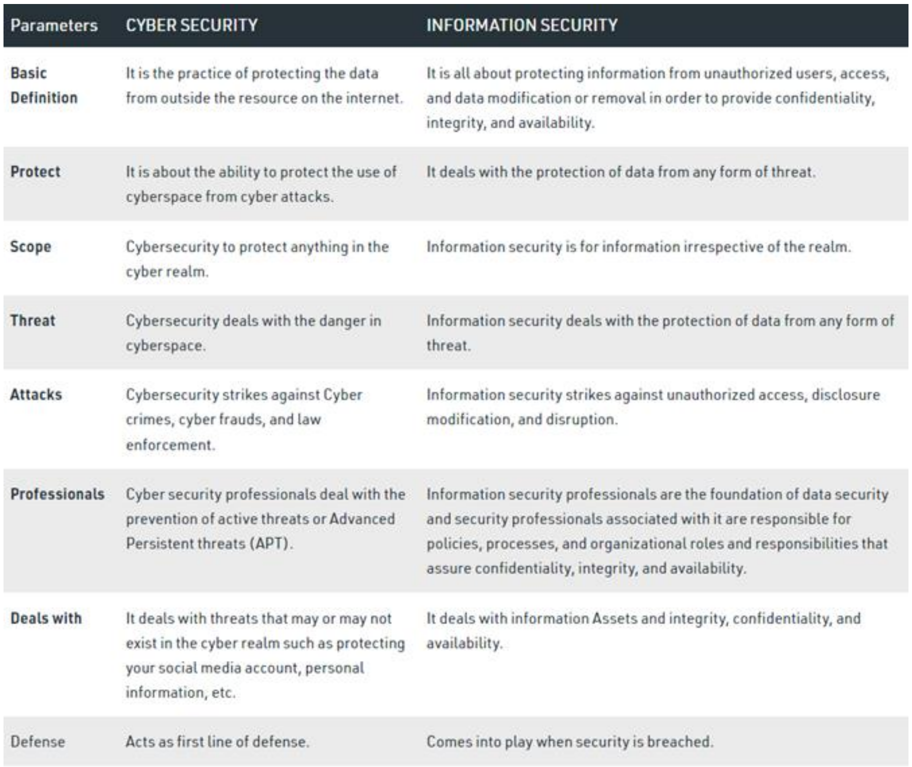
Sl.no	PART - A	Marks	BT	CO
1	X is a metaphorical name given to a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks such as sending spam emails, launch DoS attacks of one sort or another under remote direction. What is X?	1	L2	CO1
2	Consider the following scenarios. **Email X** – where an attacker forges the sending address of an email. **IP address X** – where an attacker alters the source IP address in a network packet to hide their identity. **Biometric X -** where an attacker produces a fake biometric sample to pose as another user. **MAC X** – where an attacker modifies the Media Access Control (MAC) address of their network interface to pose as a valid user on a network. Identify the word **X**___________________	1	L2	CO2
3	____________ is a techniques where every possible combination of letters, numbers and symbols in an attempt to guess the password.	1	L1	CO1
4	Access social networking sites using ____________ protocol to safeguard your username, password and other information you post.	1	L1	CO1
5	Anytime an unknown device is used to sign into your Google account, the user must provide a verification code in addition to the password. This is known as_________	1	L1	CO1
6	To enhance social media privacy, users should regularly update their ______ settings to control who can see their information.	1	L1	CO1
7	This is a Debian-derived Linux distribution managed and funded by Offensive Security Ltd, designed for digital forensics and penetration testing. Which is this very famous OS majorly developed for Hackers and software testers?	1	L2	CO2
8	The word X is a combination of the words “robot” and “network”. It is a number of Internet-connected devices, each of which is running one or more bots. This can be used to perform DDoS attacks, steal data, send spam. Identify the word X?	1	L2	CO3

9	Bob Thomas, working at BBN, wrote a program named X which infected the ARPANET. He later wrote the program Y to destroy X. What are X and Y?	1	L2	CO2
10	___________ is a form of malware that uses social engineering to cause shock, anxiety, or the perception of a threat to manipulate users into buying unwanted software.	1	L1	CO2

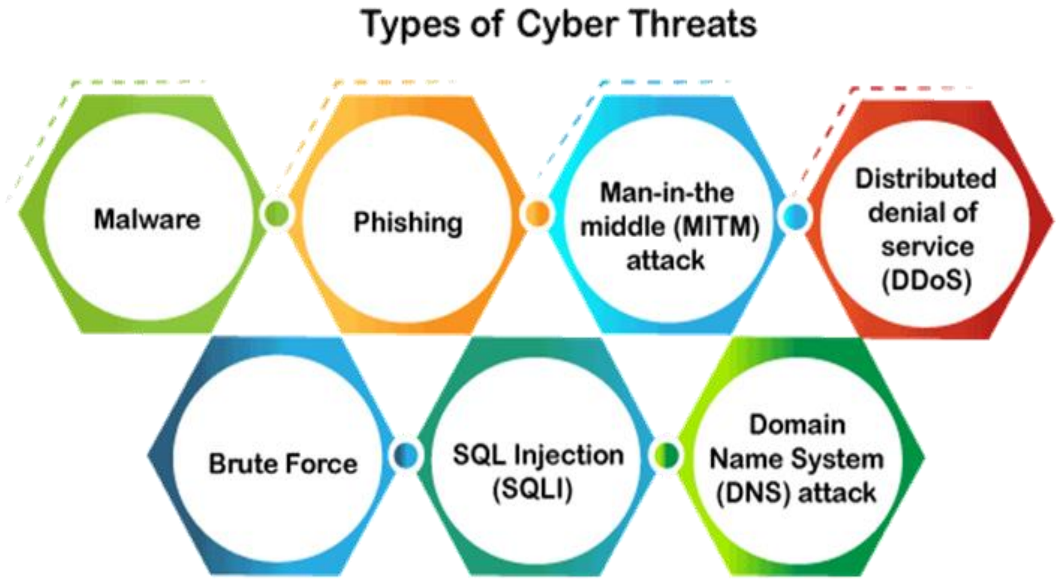
Sl.no.	PART - B	Marks	BT	CO
1.a	Explain the categories of cybercrime. Give examples.	5	L2	CO1
1.b	Define cyber space. Why cyber security is important.	5	L2	CO1
2.a	Identify the type of cybercrime behind the following scenarios i) Joining the same groups and forums on the online media as the victim and posting the messages. ii) Promising the victim a reward in return for sensitive information or knowledge of its whereabouts. iii) Use of Zbot, to harvest banking credentials and financial information from users of infected devices. Once the data was collected, attackers used the bots to send out spam and phishing emails that spread the Zeus Trojan. iv) Attacker delegates a subdomain, and configures his machine as the subdomain's authoritative DNS server. v) !!Urgent! Your number has been selected for a 500000 prize guaranteed! To claim your prize call +423697497459.	5	L3	CO2
2.b	Propose any FIVE significant reasons that prompt for the commitment of cybercrime at Cyber café in India.	5	L2	CO2
3.a	I am starting a new startup software development company with 20 employees. List the five important cybersecurity solutions that my business needs with justification. Consider solutions to protect Employees, Network, Data, Privacy and Attacks.	6	L3	CO4
3.b	Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.	4	L3	CO5
4	Define cybercrime. List and briefly explain different types of cybercrimes.	10	L2	CO1
5.a	Describe any FIVE categories of social media, using at least one app or website as an example for each.	5	L2	CO1
5.b	Identify and justify any FIVE risks that may raise due to the use of Social Networks without the knowledge of vulnerabilities exits in social networks.	5	L3	CO3

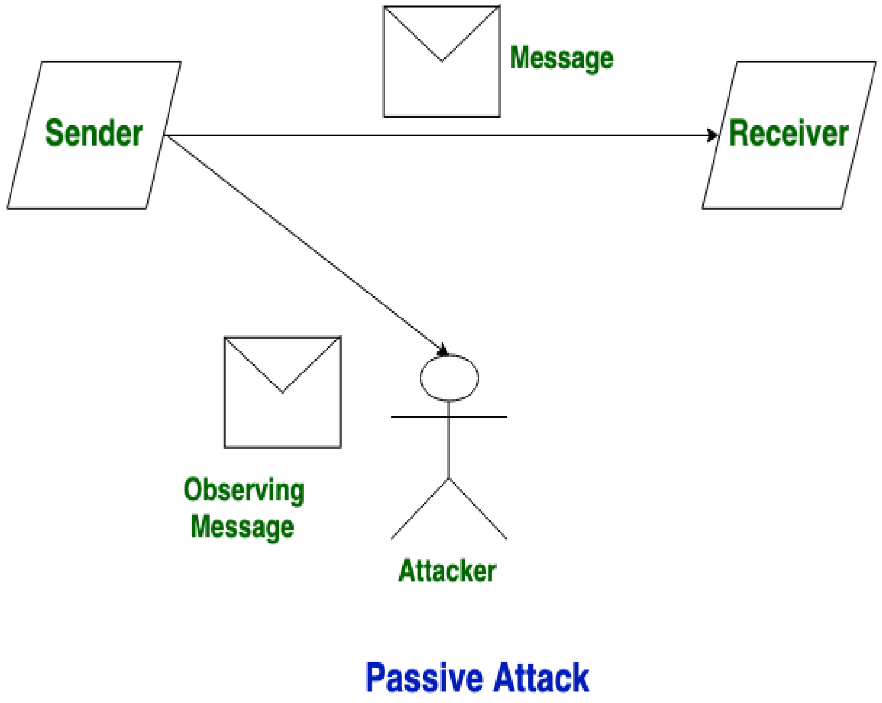
	L1	**L2**	**L3**	**L4**	**L5**	**L6**	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Part-A & B	**5**	**35**	**20**	*******	*******	*******	**30**	**14**	**06**	**06**	**04**

	RV College of Engineering® **Department of Computer Science and Engineering** **CIE - I: Test Paper**	
Course & Code	**INTRODUCTION TO CYBER SECURITY (CS124BTF)**	**Semester: II**
Scheme & Solutions		

Sl.no.	**Questions**	**Marks**
1.a	Evolution phase of the Internet  Timeline of the Internet 1969 ARPAnet, the first version of the internet, is created and used to link computers at UCLA and Stanford. 1986 NSFNET is founded, creating the backbone and providing the investment needed to create the internet as we know it today. 1989 Tim Berners-Lee invents the world wide web, which opens the door for the internet to go mainstream. 1994 Netscape navigator is released in stores. 2004 Facebook launches and the Web 2.0 begins to grow rapidly. 2010 1.966 billion people are online worldwide. 1965 Lawrence Roberts and Thomas Merril communicate with one another using computers connected via a low-speed dial-up telephone line in Massachusetts and California, creating the first Wide Area Network and laying the groundwork for the internet. 1974 Robert Kahn and Vinto Cerf publish "A protocol for Packet Network Communication" laying the groundwork for TCP/IP and much larger, interconnected computer networks. The word "internet"is first used. 1989 The first commercial ISP, the world launches. 1993 The first web browser available to the public, Mosaic launches. 2000 Some 300 million people around the world are officially online. 2007 The iPhone is released, giving rise to the mobile revolution. 2022 5 billion people are online	06
1.b		04

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

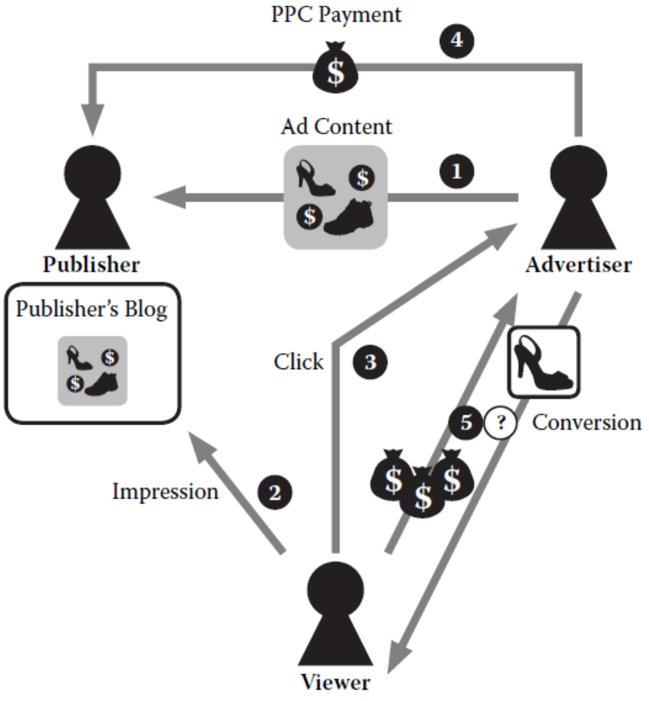
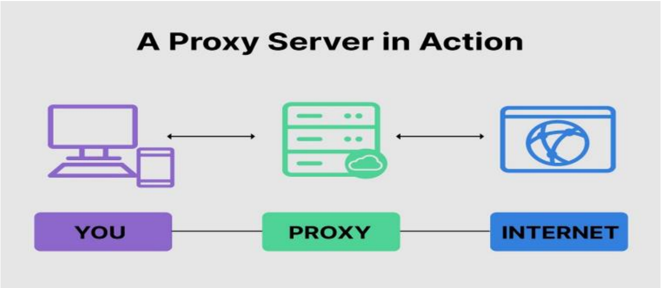
2.a	A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupt digital life in general. *List of all threats- 02 marks, explanation – 06 marks*  Types of Cyber Threats Malware Phishing Man-in-the middle (MITM) attack Distributed denial of service (DDoS) Brute Force SQL Injection (SQLI) Domain Name System (DNS) attack	06
2.b	Security System Development Life Cycle (SecSDLC) is defined as the set of procedures that are executed in a sequence in the software development cycle (SDLC). It is designed such that it can help developers to create software and applications in a way that reduces the security risks at later stages significantly from the start. SecSDLC eliminates security vulnerabilities. Its process involves identification of certain threats and the risks they impose on a system as well as the needed implementation of security controls to counter, remove and manage the risks involved. ---2 M Phases involved are as follows: 1.System Investigation 2.System Analysis 3.Logical Design 4.Physical Design 5.Implementation 6.Maintenance ---2 M	04
3.a	Passive attacks • Gathering information about a target without his/her knowledge • Internet searches or by googling. Passive Attacks: Passive Attacks are the type of attacks in which, The attacker observes the content of messages or copy the content of messages. Passive Attack is a danger for Confidentiality. Due to passive attack, there is no any harm to the system. The most important thing is that In passive attack, Victim does not get informed about the attack.	06



In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.

- In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
- In passive attacks, information remains unchanged.
- Unlike active attacks, in passive attacks, victims do not get informed about the attack.
- The passive attacks do not harm the system.
- In passive attacks, the system resources remain unchanged.
- They can be dangerous for confidentiality of the message.
- In active attacks, attention is on prevention.
- It involves traffic analysis, the release of a message.
- Unlike active attacks, passive attacks are easy to prohibit.

Passive attack and explanation – 3 marks
3 tools with explanation – 3 marks

3.b	 PPC Payment 4 $ Ad Content 1 Publisher Advertiser Publisher's Blog Click 3 5 ? Conversion Impression 2 Viewer - Pay-per-click is a model of digital advertising where the advertiser pays a fee each time one of their ads is clicked. - Stake holders involved in this model and their role are - Advertiser, Publisher, and the Viewer - The advertiser is a company that produces content it would like to display to potential customers. - The publisher is a creative outlet that produces content that will draw visitors to its medium - Visitors view the ad and, ideally, purchase the advertised product or service. *Diagram – 2 marks Explanation – 2 marks*	
4.a	 In computer networking, a proxy server is a server application that acts as an intermediary between a client requesting a resource and the server Attackers use proxies to: 1.IP address masking 2.Anonymity 3.Geographical obfuscation 4.Access control bypass 5.Traffic encryption	06

4.b	**While filling the application:** • Stay with computer: should not leave system un-attended. • Be alert: careful about the shoulder snooping for username and password. • Use Virtual Keyboard: Better to use s/w keyboard to avoid the hacking for pin. • while doing online fee payment. • Security warnings: warning messages posted by financial organizations while accessing the financial accounts in cyber cafe 2 **marks** **After filling the application:** • Always logout: Logout of the services that were used with username and password credentials • Change password: Change the password / pin of the financial account on your personal lap-top or Desktop 2 **marks**	
5.a	Analyze the steps involved in “How the criminals plan their attack” Justify your answer.	06
5.b	Explanation for Shoulder surfing -2 marks Dumpster Driving -2 marks	04

Academic year 2023-2024 (Even Semester)

CIE 2: Scheme of Solutions

Course	**Introduction to cyber security**		
Date	June 2024	Maximum Marks	50
Course Code	CS124BT	Duration	90 Min
Sem	II	CIE – II	

Sl.No.	Solutions	M	BT	CO
1.a	**1*5=5** **Business-to-Consumer (B2C):** In this model, businesses sell products or services directly to individual consumers. Examples: Amazon, Walmart, eBay, Best Buy, Flipkart. **Business-to-Business (B2B):** In B2B E-commerce, businesses sell products or services to other businesses. Examples: Alibaba, ThomasNet, Grainger, Office Depot. **Consumer-to-Consumer (C2C):** C2C E-commerce involves transactions between individual consumers, facilitated by a third-party platform. Examples: eBay (auction-style sales), Craigslist, Facebook Marketplace, Airbnb (for short-term rentals). **Consumer-to-Business (C2B):** In this model, individual consumers offer products or services to businesses. Examples: Freelancer, Upwork, Fiverr (for freelance services), UserTesting (for user feedback). **Business-to-Government (B2G):** B2G E-commerce involves businesses selling products or services to government agencies or departments. Examples: Government procurement portals, such as GSA Advantage (for U.S. federal government procurement).	5	L3	CO2
1.b	Cyber security is essential for e-commerce because cyber attacks can result in loss of revenue, of data and of overall viability for businesses. Cyber criminals use advanced tactics to steal information from businesses. With e-commerce, it's not just your data that you're protecting; it's your customers' data that you need to be careful with. A breach in your cyber security systems could mean the loss of your customer's information. And that could cost your business the trust and reputation that you've worked to build up.	5	L2	CO1
2.a	**Analysis** **Consequences: …3M** **For retailers:** □ Loss of customer trust and reputation damage leading to decreased sales and revenue. □ Legal and regulatory consequences, including fines and penalties for non-compliance with data protection laws. □ Costly remediation efforts, such as investigating the breach, notifying affected customers, and implementing security improvements. **For Customers:** □ Risk of identity theft, fraud, and financial losses due to exposure of personal and payment information. □ Potential harm to personal and professional reputation if sensitive data is misused by	10	L3	CO2

	cybercriminals. **Vulnerabilities:..3M** Inadequate Data Protection Measures, Weaknesses in Network Security, Human Error and Insider Threats **Steps to improve:..2M** mplement Strong Encryption and Access Controls, Enhance Network Security Measures, Provide Ongoing Employee Training and Awarenes **Effective Communication with Affected Customers and Stakeholders..2M** Timely notification, Transparency and accountability, Regular updates and followup,			
3.a	Digital wallets store payment information and allow users to make transactions electronically, often via mobile devices, without the need for physical cards or cash. They typically offer features such as transaction history, rewards, and enhanced security (e.g., encryption and tokenization). Traditional payment methods, like cash and credit/debit cards, require physical presence and can lack some of the security and convenience features of digital wallets… 2M **Advantages and Disadvantages of digital payment**:…2M **Advantages**: Convenience and speed, Enhanced Security, Cost efficiency, Integration with other services **Disadvantages**: Security risks, Technical issues, Privacy concerns, Accessibility issues **Advantages and disadvantages of Traditional method:…2M** A**dvantages**: Universal acceptance, No need of technology, Immediate settlement, Familiarity and trust **Disadvantages:** Theft and loss, Check fraud, Time consuming, Manual handling, Limited flexibility.	6	L3	CO3
3.b	Payment gateways are services that facilitate online transactions between customers and merchants by securely transmitting payment information from the customer to the acquiring bank…1M They play a crucial role in verifying the authenticity of the transaction, ensuring that the customer has sufficient funds, and protecting sensitive information through encryption and other security measures….2M Payment gateways provide a seamless and secure link between the E-commerce website and the payment processor, enabling smooth and efficient digital transactions…1M	4	L2	CO1
4.a	Explanation any 5 of :Banking cards, USSD, AEPS, UPI, Mobile wallets, POS, Internet banking, Mobile banking, MicroATMS	5	L3	CO3
4.b	Digital Security: refers to the measures and practices implemented to protect digital information, systems, and networks from unauthorized access, attacks, damage, or theft…1M Difference..4M Digital Information Security encompasses measures and practices designed to protect digital information from unauthorized access, alteration, destruction, or disclosure. It primarily focuses on the confidentiality, integrity, and availability of data, regardless of the environment in which the data resides. Cyber Security is the practice of protecting systems, networks, and programs from digital attacks. These attacks are typically aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.	5	L3	CO4
5	1. Various Digital devices: Gateways, servers, mobile phones, laptops…1M 2. Potential Weaknesses in the University's Network Security: Lack of Regular Software Updates and Patch Management, Inadequate Antivirus and Anti-malware Protection, Weak User Authentication and Access Controls, Poor Network Segmentation, Insufficient User Training and Awareness.. 3M 3. Role of antiviruses, firewalls, regular software updates: Detection and prevention of threats, Network traffic monitoring, Intrusion prevention, Patch vulnerabilities.3M 4. Immediate response: Isolate infected system, Shutdown the systems, Block Malicious IPs and Domains, Investigate Affected Systems, Inform IT Staff and Administration, Verify Backups, Engage with Cybersecurity Experts..3M	10	L4	CO4

Course Outcomes: After completing the course, the students will be able to:-	
CO 1	Understand the cyber-attacks and their principles for different domains- social media,E-commerce, and digital devices.
CO 2	Analyse vulnerabilities in different domains that the attacker capitalizes for attack.
CO 3	Applydifferent attacking techniques that make use of vulnerabilities available in various domains.
CO 4	Evaluate methods to cover different vulnerabilities to safeguard the systems against cyber-attacks.
CO 5	Investigate modern tools and technologies available to mitigate cybercrime attacks.

BT-Blooms Taxonomy, CO-Course Outcomes, M-Marks

Marks Distribution	Particulars		CO1	CO2	CO3	CO4	CO5	L1	L2	L3	L4
	Test	Max Marks	5	15	5	15	10	--	20	20	10

CIE 3 *Scheme and solution*

Sl.no	PART - A	Marks	* BT	*CO
1	Zombie "Zombie" is the term used when an attacker takes control of your computer without your knowledge. A zombie attack aimed either to steal your sensitive information or to make your computer do things that it normally shouldn't.	1	L1	CO1
2	Spoofing: Spoofing happens when cybercriminals use deception to appear as another person or source of information.	1	L1	CO1
3	Brute-Force Attack	1	L2	CO2
4	HTTPS	1	L1	CO2
5	OTP / 2-step verification system	1	L1	CO1
6	Privacy / password	1	L2	CO2
7	Kali Linux	1	L2	CO1
8	Botnet	1	L1	CO1
9	X- Creeper, Y- Reaper	1	L2	CO1
10	Scareware	1	L1	CO1

Sl.no.	PART - B
1.a	Cybercrime can be categorized based on • The target of the crime • Whether the crime occurs as a single event or as a series of events 1. Crimes targeted at individuals 2. Crimes targeted at property 3. Crimes targeted at organizations 4. Single event of cybercrime *5.* Series of events *5 marks – Listing + explanation for each*

1.b	"Cyberspace refers to the virtual space that provides the infrastructure, electronic medium and related elements necessary for online global communication" • Cyber Security is not a one-time process to achieve • It is an ever-growing challenge encountered from time to time • When old problems are fixed and rectified, new targeted attacks challenge the Cyberspace • Cyber security is a process by itself and not the end *Definition – 1 Mark, why cyber security is important -4 Marks*
2.a	i) Cyber stalk ii) Social Engineering iii) Botnet / DDoS iv) DNS tunnelling v) Phishing against Mobile Devices 1 **mark X 5=5 marks**
2.b	Use of **pirated software** like OS, office tools **Use of Deep Freeze** S/W which wipe out all the activities carried out on computer which destroys the evidence of crime **Use of out-dated version of antivirus**: these S/W may allow to install malware on computers **Un-blocked websites** with indecent contents: These websites may contain most provoking contents to commit crime **Police** (cybercrime dept.) may not visit the cyber centre periodically **Cyber owner** have very less awareness about cyber law, IT security and IT Governance and with intension of making profit, they may ignore the conduction of crime **1 mark X any 5 points = 5 marks**
3.a	Employee: Access control, anti-virus Network: Firewall Data: Access control, Encryption Privacy: Password Attacks: DOS prevention software.
3.b	**Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.** *Global cooperation required in fighting against cybercrime-4 Marks*
4	**Define cybercrime. List and briefly explain different types of cybercrimes.** Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal

possession [and] offering or distributing information by means of a computer system or network.

Computer-related crime is considered as any illegal, unethical, or unauthorized behaviour relating to the automatic processing and the transmission of data.

1. Cyber pornography
2. Sale of illegal articles
3. Online gambling
4. Intellectual Property crimes
5. Email spoofing
6. Forgery
7. Cyber Defamation:
8. Cyber stalking
9. Unauthorized access to computer systems or networks
10. Theft of information contained in electronic form
11. Email bombing
12. Data diddling
13. Salami attacks
14. Denial of Service attack
15. Virus / worm attacks
16. Logic bombs
17. Trojan attacks
18. Internet time theft
19. Web jacking
20. Theft of computer system
21. Physically damaging a computer system

Definition-1 Mark, List – 1 mark, Explain any 4 types in detail with example - 8 Marks

5.a

Social connections. This is a type of social network where people stay in touch with friends, family members, acquaintances or brands through online profiles and updates, or find new friends through similar interests. Some examples are Facebook, Myspace and Instagram.

Professional connections. Geared toward professionals, these social networks are designed for business relationships. These sites can be used to make new professional contacts, enhance existing business connections and explore job opportunities. LinkedIn, Microsoft Yammer and Microsoft Viva

News or informational. This type of social networking allow users to post news stories, informational or how-to content and can be general purpose or dedicated to a single topic. Ex. Reddit.

Communication. Here, social networks focus on allowing the user to communicate directly with each other in one-on-one or group chats, Ex. WhatApp, Telegram.

Educational. Educational social networks offer remote learning, enabling students and teachers to collaborate on school projects, conduct research, and interact through blogs and forums. Google Classroom 5 marks

5.b	**Addiction:** Now days irrespective of age group the people are addicting to social networks and becoming victims for the cyber attackers **Identity theft :** Social networking sites encourage users to enter and share as much data as possible. An imposer may collect as much information as they need from your posts and plan their attack. **Cyber Bulling and Blackmail:** Social networking sites are common places for cyber bullying to occur. Bullies may use these websites as a way of sending you malicious emails. **Phishing Attacks:** Social network user may receive an email that seems to be from a social networking site, but it actually encourages you to visit fake websites. **Loss of Privacy:** Large websites like social networking sites back up their databases regularly. Therefore, information about you collected over time or posted by yourself never disappears completely **Any 5 risks with justification 5 marks**

CS114BTF / CS124BTF / 22EM206

USN | 1 | R | V | 2 | 3 | C | D | 0 | 0 | 3 |

RV COLLEGE OF ENGINEERING®

(An Autonomous Institution Affiliated to VTU)

I/II Semester B. E. Regular / Supplementary Examinations Aug-2024

INTRODUCTION TO CYBER SECURITY

Time: 03 Hours *Maximum Marks: 100*

Instructions to candidates:

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

			M	BT	CO
1	1.1	In the 1970s, the true birth of cybersecuity began with a project called ________.	01	1	1
	1.2	________ protects internet-connected systems such as hardware, software, and data from cyber-attacks. It aims to reduce cyber-attacks against the system, network, and technologies by reducing unauthorized exploitation, vulnerability, and threats.	01	1	3
	1.3	Give two examples for cyber-squatting.	01	2	2
	1.4	What do you mean by Cyber Law?	01	1	3
	1.5	The term ________ has been replaced with 'electronic signature' to make the Information Technology (Amendment) Act, 2008 more technology neutral.	01	2	1
	1.6	________ on infected mobile devices are waiting for orders from their owners. It starts a DDoS flood attack after receiving the owner's instructions. As a result, calls are not connected or data is not sent.	01	2	2
	1.7	________ are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.	01	1	5
	1.8	The cyber stalking cases are dealt in India by the ________ and ________ acts respectively.	02	3	3
	1.9	What is the purpose of two-factor authentication?	01	1	3
	1.10	In ________, we create our online communication sites through which we can share information, images, ideas, audio and video files, as well as other content with our friends, family members, and business partners.	01	2	1
	1.11	After withdrawing money from *ATM*, the user usually throws the receipt in which the total amount and account details are mentioned. This type information becomes helpful to a hacker, the technique used is called as ________.	01	1	3
	1.12	________ exploits *SMS*/text messages that may contain links and other personal info that may be exploited.	01	2	1
	1.13	________ an umbrella organization for operating retail payments and settlement systems in India, is an initiative of Reserve Bank of India (*RBI*) and Indian Banks' Association (*IBA*) under the provisions of the Payment and Settlement systems Act, 2007.	01	1	3
	1.14	The innovative payment service on ________ channel allows mobile banking transactions using basic feature mobile phone, there is no need to have mobile internet data facility.	01	1	2
	1.15	________ is an 11 digit alphanumeric code that uniquely identifies a bank-branch participating in the *NEFT* system.	01	3	5

1.16	Cracking digital identity of any individual or doing identity theft comes under section ________ of the *IT* Act.	01	2	2
1.17	________ is a violent act done using the Internet, which either threatens any technology user or leads to loss of life or otherwise harms anyone in order to accomplish political gain.	01	2	3
1.18	________ is a popular tool used for discovering networks as well as in security auditing.	01	3	1
1.19	Suppose you sent $500 to an authorized person and in between a Man in the Middle (MiTM) attack takes place and the value has tampered to $50. ________ element of the *CIA* model is compromised in the above example.	01	4	5

PART-B

2	a	Give the difference between Cyber Security and Information Security.	06	2	1
	b	Demonstrate the *CIA* model.	04	3	2
	c	Discuss the different areas of cyber-crime, where Cyber Law is used.	06	2	3
3	a	Explain the categories of cybercrime.	06	2	2
	b	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* group emailed new account information and instructions to the hospital. 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.	06	4	4
	c	Discuss Dumpster diving and shoulder surfing with an example for each.	04	2	3
		OR			
4	a	Discuss the three main proxy types in detail.	06	2	3
	b	Explain any four benefits of using tunneling in your network.	04	2	2
	c	Illustrate the three phases involved in planning a cyber-attack.	06	3	4
5	a	Investigate the social media challenges. Also suggest appropriate solution for each of the challenges.	10	4	4
	b	What is a Viral Content? Discuss the ways to create a Viral Content.	06	2	3
		OR			
6	a	Illustrate the social media privacy issues for the following: i) Data mining for identity theft ii) Privacy setting loopholes iii) Location settings iv) Harassment and cyber bullying v) False information	10	4	4

	b	What is flagging and reporting of inappropriate content? Discuss the laws regarding posting of inappropriate content.	06	2	3
7	a	Discuss the Elements of *E*-Commerce Security.	06	2	1
	b	The main reason for increase in digital payments is demonetization. Discuss about demonetization, its advantages and disadvantages.	04	4	3
	c	Demonstrate the following Security Threats in the E-Commerce Environment: i) Malicious code ii) Hacking iii) Cybervandalism iv) Data breach	06	3	4
		OR			
8	a	Characterize the advantages and disadvantages of *E*-Commerce.	06	3	1
	b	Discuss the barriers in digital payments.	04	2	3
	c	Demonstrate the following Security Risks in Digital Payment Systems: i) Phishing, smishing and vishing ii) Fake identity fraud iii) UPI Frauds iv) Refund Frauds	06	4	4
9	a	Illustrate the four main techniques hackers can use to get hold of your password.	06	3	2
	b	What is third-party software? List the pros and cons of using third-party software.	04	2	3
	c	Discuss the different types of Digital Security.	06	2	4
		OR			
10	a	What is security patch management? Explain the three types of patch management.	06	2	3
	b	Write the differences between Firewall and Antivirus.	04	2	2
	c	Give the brief description about the following digital security tools: i) Instant Message Encryption Tools ii) Navigation Privacy Tools iii) Telephone Encryption Tools	06	3	4