P.V.P Siddhartha Institute of Technology				
Department of Computer Science and Engineering				
Course: B.Tech	**Year: IV**	**Semester: I**	**Descriptive: I**	**A.Y:2025-26**
Subject Code: 20CS4702C	**Subject Name: CYBER SECURITY**			**Regulation:PVP20**
Duration:1 hr 30 min	**Maximum Marks:15 Marks**	**Date: 26-08-2025**		**Session: F.N**
Answer all the Questions. Each Question carries 5Marks				**3×5M=15M**

Q.No			Marks	CO	Level
1.	a)	Who are cyber criminals? How are they categorized into? Definition- (1 Mark) Cyber criminal's categorization – (1 Mark) • Type I: Cybercriminals-hungry for recognition • Type Il: Cybercriminals -not interested in recognition • Type III: Cybercriminals -the insiders	2	CO1	L2
	b)	Identify any six major types of cybercrimes targeting organizations. Explain each of them? Any six of the below. For each one – ½ mark (6 * ½M= 3 Marks) • Unauthorized accessing of Computer • Password Sniffing • Denial-of-service Attacks (DoSAttacks) • Virus attacks/dissemination of Viruses • E-Mail bombing/Mail bombs • Salami Attack/Salami technique • Logic Bomb • Trojan Horse • Data Diddling • Newsgroup Spam/Crimes emanating from Usenet newsgroup • Industrial spying/Industrial espionage • Computer network intrusions • Software piracy	3	CO1	L2
2.	a)	Define the concept of social engineering and critically examine the techniques used in underlying human-based social engineering attacks. Definition –(1 Mark) • Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action. Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes. Human Based Social Engineering techniques: (1 Mark) • Impersonating an employee or valid user • Posing as an important user • Using a third person • Calling technical support • Shoulder surfing • Dumpster diving	2	CO2	L3
	b)	Illustrate the different phases involved in planning a cybercrime, and explore the techniques of passive attack mechanisms used during the reconnaissance phase. Phases are involved in planning cybercrime: (1.5 Marks) • Reconnaissance (information gathering) is the first phase and is treated as passive attacks. • Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities. • Launching an attack (gaining and maintaining the system access). Passive attack mechanisms used during the reconnaissance phase: (1.5 Marks)	3	CO2	L3

		A passive attack involves gathering information about a target without his/her (individual‟s or company‟s) knowledge. • Internet searches or by Googling • Network sniffing			
3.	a)	Produce a holistic review of traditional versus modern credit card fraud techniques in wireless environment. Traditional Techniques (2.5 Marks) • ID theft • Financial fraud Modern Techniques (2.5 Marks) • Triangulation • Credit card generators	5	CO3	L3

P.V.P Siddhartha Institute of Technology				Signature of Invigilator with date:	Marks Obtained:
Department of Computer Science and Engineering					
Course: B.Tech	Year: IV	Semester: I	Objective: I		
Regulation:PVP20	Maximum Marks:10Marks		Session: F.N		
A.Y:2025-26	Date: 26-08-2025	Duration: 20 min			
Subject Code: 20CS4702C	Subject Name: Cyber Security				
Registered Number:		Name:			

Answer all the Questions. Each Question carries ½ Mark **20×½ M =10M**

S.No	Question	CO	Level	Answer
1.	A person who breaks into computers, to find vulnerabilities for a good cause is called a) Hacker b) Cracker c) Perverts d) All	CO1	L1	A
2.	A _____ hat hacker is one who thinks before acting or committing a malice or non-malice deed. a) Black b) White c) Brown d) Green	CO1	L1	C
3.	People who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent to are called_____ a) Pedophiles b) Spammers c) Cyber Terrorists d) Hackers	CO1	L1	A
4.	A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2/- or a few cents in a month) from the account of every customer such that it becomes un noticeable. a) Spamming b) Forgery c) Phishing d) Salami attack	CO1	L2	D
5.	A type of Cyber criminals who are hungry for recognition. a) Hobby Hackers b) Psychological Perverts c) organized criminals d) corporate espionage	CO1	L1	A
	Identify the types of Cyber Attacks/Crimes shown in the Figures(A to D) below			
6.	Figure A	Ans: **Dumpster diving**	CO1	L1
7.	Figure B	Ans: **Shoulder Surfing**	CO1	L1
8.	Figure C	Ans: **Web site Spoofing / Spoofing**	CO1	L1
9.	Figure D	Ans: **e-mail Spamming / Spamming**	CO1	L1

Figure-A

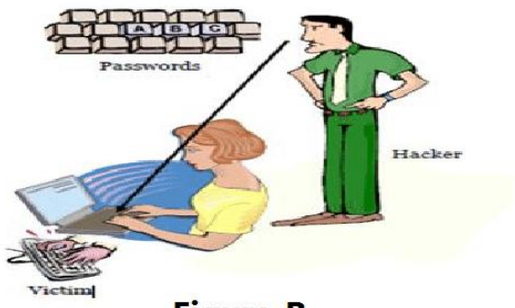

Figure-B

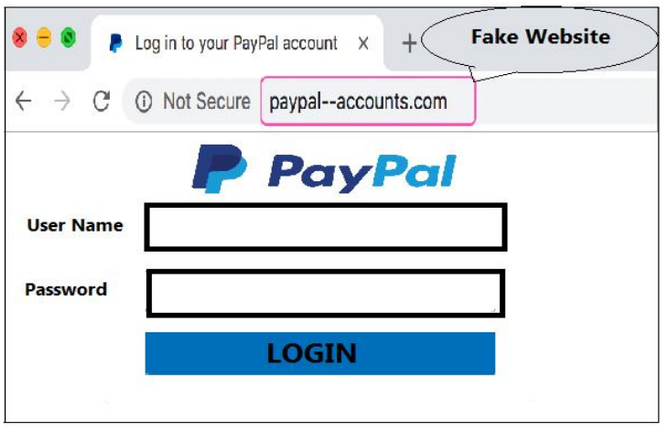

Figure-C

Figure-D

10.	_____is an automated program for doing some particular task, often over a network.				**CO1**	**L1**	**C**
	a) String	b) Query	c) Bot	d) Loop			
11.	Internet Time Theft, is a cybercrime against _____				**CO1**	**L1**	**C**
	a) individual	b) organization	c) property	d) society			
12.	A computing device installed in an automobile.				**CO1**	**L1**	**A**
	a) carputer	b) portable computer	c) fly fusion device	d) None			
13.	_____ is an act of finding something or somebody (especially to gain information about an enemy or potential enemy).				**CO1**	**L1**	**D**
	a) scanning	b) scrutinizing	c) attacking	d) Reconnaissance			
14.	_____ is used for Bandwidth Ping.				**CO1**	**L1**	**D**
	a) dig	b) Hmap	c)Hping	d) bing			
15.	_____ will restrict the results to documents containing that word in the URL.				**CO1**	**L1**	**B**
	a) link	b) inURL	c) cache	d) define			
16.	The tool is used on Windows and Unix to query domain name system (DNS) servers to find DNS derails, including IP addresses of a particular computer and other technical details such as mail exchanger (MX) records for a domain and name server (NS) servers of a domain.				**CO1**	**L2**	**C**
	a) whois	b) trace route	c) nslookup	d) HTTrack			
17.	_____ are the services provided by the cloud.				**CO1**	**L1**	**D**
	a) Infrastructure	b) platform	c) software	d) all			
18.	Signaling level attacks target _____				**CO1**	**L2**	**A**
	a) Session Initiation Protocol	b) Session Information Protocol	c) Secure Information Protocol	d) Standard Initiation Protocol			
19.	Which type of attack allows attacker to use a Brute-force approach?				**CO1**	**L1**	**B**
	a) Packet sniffing	b) Password Cracking	c) Denial of Service	d) Social Engineering			
20.	What are don't mechanisms of security in credit cards frauds.				**CO1**	**L1**	**A**
	a) Destroy credit card receipts by simply dropping into garbage box/dustbin.						
	b) Put your signature on the card immediately upon its receipt.						
	c) Make the photocopy of both the sides of your card and preserve it at a safe place						
	d) Reconcile your monthly invoice/statement with your receipts						