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: II		
Regulation:PVP20	Maximum Marks:10Marks		Session: F.N		
A.Y:2025-26	Date:03/11/25	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**

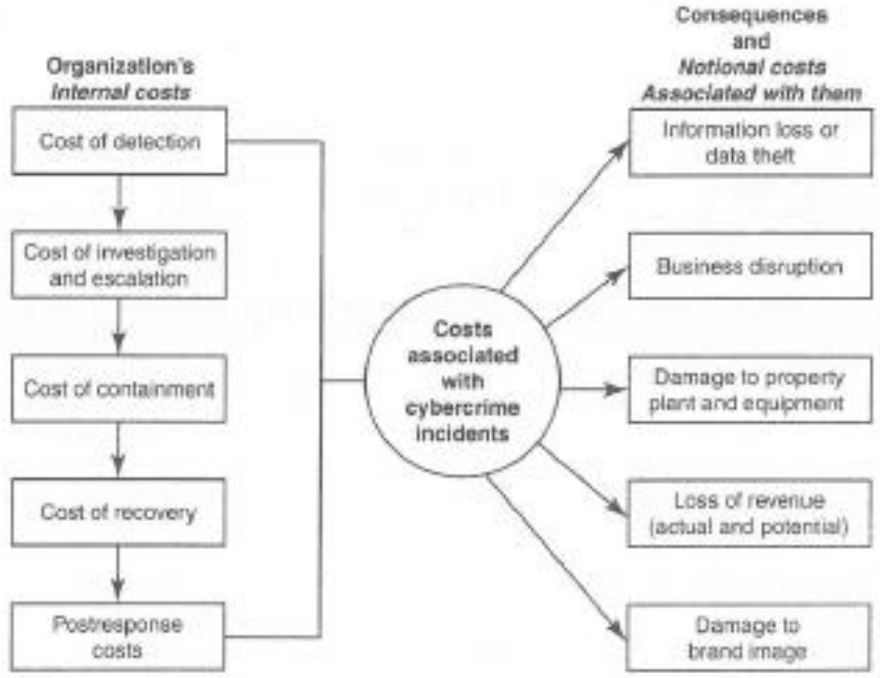
S.No	Question	CO	Level	Answer
1.	IMEI full form: a) Identifiable Mobile Equipment Information b) Internal Mobile Equipment Identification c) Internal Mobile Encryption Identity d) International Mobile Equipment Identity	CO1	L1	D
2.	_____ is a combination of mobile phone & Pishing. a) Hashing b) Smishing c) Mishing d) Vishing	CO1	L1	C
3.	It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers a) Bluejacking b) Bluesnarfing c) Bluebugging d) Car Whisperer	CO1	L1	B
4.	_____is a tool that attempts to make activity on the Internet untraceable. a) Anonymizer b) Proxy server c) IDS d) Firewall	CO1	L1	A
5.	Which is the purpose of a proxy server a) Speed up access to a resource b) Filter unwanted content c) IP address multiplexer d) All	CO1	L2	D
6.	It is a subsidiary of Google and provides Internet ad-serving services and paid search products listing (DART Search) and utilize the cookies, which are called DART cookie. a) Google Cookie b) G-Zapper c) DoubleClick d) None	CO1	L1	C
7.	_____is a tool that can detect the keylogger installed on the computer system and can remove the tool. a) Delogger b) Antikeylogger c) Nologger d) Mislogger	CO1	L1	B
8.	It infects the storage media on which OS is stored (e.g., hard drives) and which is used to start the computer system a) Boot sector viruses b) Program viruses c) Stealth viruses d) Polymorphic viruses	CO1	L1	A
9.	Different types of offline password attacks are a) Dictionary Attack b) Hybrid Attack c) Brute force Attack d) All	CO1	L1	D
10.	_____is a means of access to a computer program that bypasses security mechanisms a) Pishing b) Password cracking c) Backdoor d) DoS Attack	CO1	L1	C
11.	_____is the practice of concealing (hiding) a file, message, image, or video within another file, message, image, or video. a) Encryption b) Steganography c) Pishing d) None	CO1	L1	B
12.	_____ is an attempt to make a computer resource (i.e., information systems) unavailable to its intended users a) DoS attack b) Steganography c) Pishing d) None	CO1	L1	A
13.	These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack a) Bandwidth attacks b) Protocol attacks c) Unintentional DoS attack d) Logic attacks	CO1	L1	D

PTO...

14.	_____is an DoS attack where fragmented packets are forged to overlap each other when the receiving host tries to reassemble them				**CO1**	**L1**	**C**
	a) Flood attack	b) Ping of death attack	c) Teardrop attack	d) SYN attack			
15.	_____ is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker				**CO1**	**L2**	**B**
	a) Sequence Injection	b) Blind SQL Injection	c) Tear Injection	d) None			
16.	A _____ insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability				**CO1**	**L2**	**A**
	a) malicious	b) careless	c) tricked	d) None			
17.	_____ is a dimension of privacy				**CO1**	**L1**	**D**
	a) Informational/ data privacy	b) Personal privacy	c) Communication privacy	d) All			
18.	Most often quoted reasons by employees, for use of pirated software are				**CO1**	**L1**	**D**
	a) Cheaper and more readily available.	b) Many others use	c) Latest versions are available faster	d) All			
19.	_____ are the costs associated with Cyber security incidents				**CO1**	**L2**	**D**
	a) Detection costs	b) Post response costs	c) Cost of containment	d) All			
20.	_____ is a type of mobile workers/remote workers.				**CO1**	**L1**	**D**
	a) Remote worker	b) Roaming User	c) Nomad	d) All			

P.V.P Siddhartha Institute of Technology						
Department of Computer Science and Engineering						
Course: B.Tech	Year: IV	Semester: I	Descriptive:II	A.Y:2025-26		
Subject Code: 20CS4702C	Subject Name: CYBER SECURITY			Regulation:PVP20		
Duration:1 hr 30 min	Maximum Marks:15 Marks			Date: 03/11/25	Session: F.N	
Answer all the Questions. Each Question carries 5 Marks				3×5M=15M		

Q.No			Marks	CO	Level
1.	a)	What kinds of attacks are possible on mobile/cell phones? Explain with examples **ANSWER: (Explanation on any 2 = 2 * 2.5 M= 5 M)** • Mobile Phone Theft • Mobile Viruses • Mishing / Vishing / Smishing • Pretexting / Sexting • VoIP Spam • Bluetooth Attacks	5	CO3	L3
2.	a)	What is SQL injection and what are the different countermeasures to prevent the attack? **ANSWER: (Definition : 1 M** **Two prevention mechanisms 2 * 0.5M = 1 M)** Structured Query Language (SQL) is a database computer language designed for managing data in relational database management systems (RDBMS). SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. SQL injection attacks occur due to poor website administration and coding. The following steps can be taken to prevent SQL injection. 1. **Input validation** • Replace all single quotes to two single quotes. • Sanitize the input: User input needs to be checked and cleaned of any characters or strings that could possibly be used maliciously. For example, character sequences such as ; , --, select, insert and xp_ can be used to perform an SQL injection attack. • Numeric values should be checked while accepting a query string value. Function –IsNumeric() for Active Server Pages (ASP) should be used to check these numeric values. • Keep all text boxes and form fields as short as possible to limit the length of user input. **2. Modify error reports:** • SQL errors should not be displayed to outside users 3. **Other preventions** • The default system accounts for SQL server 2000 should never be used. • Isolate database server and web server. • Most often attackers may make use of several extended stored procedures	2	CO2	L3

	b)	How can key-loggers be used to commit a cybercrime? **ANSWER: (Definition: 1 M** **Software & Hardware Keyloggers: 2 M)** Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored. It can be classified as software keylogger and hardware keylogger. **Software Keyloggers** ▪ Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. ▪ Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places (i.e., cybercafés, etc) and can obtain the required information about the victim very easily. A keylogger usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes. **Hardware Keyloggers** ▪ Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device.	3	CO2	L2
3.	a)	Are there any costs associated with cyber-crimes? What are the typical components of those costs? Explain. **ANSWER: (Explanation: 2 M)** • **Organizational Internal costs** • **Consequenses and national costs associated with them**	2	CO4	L3
					

	b)	What are some of the key challenges to organizations in handling web usage? Describe them briefly. **ANSWER: (Explantion on any three: 3 * 1 M = 3 M)** Organizations need not be hapless about handling these challenges to mitigate he associated risks for each of these challenges. 1. Employee Time Wasted on Internet Surfing 2. Enforcing Policy Usage in the Organization 3. Monitoring and Controlling Employees' Internet Surfing 4. Keeping Security Patches and Virus Signatures Up to Date 5. Surviving in the Era of Legal Risks 6. Bandwidth Wastage Issues 7. Mobile Workers Pose Security Challenges 8. Challenges in Controlling Access to Web Applications 9. The Bane of Malware 10. The Need for Protecting Multiple Offices and Locations	3	CO4	L3