REG.NO.:

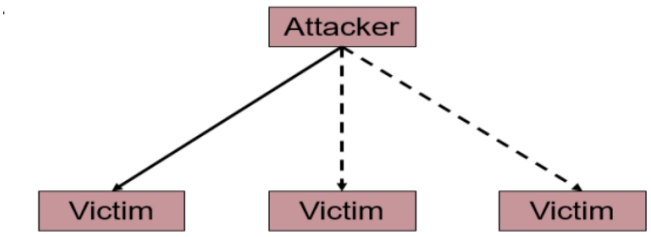
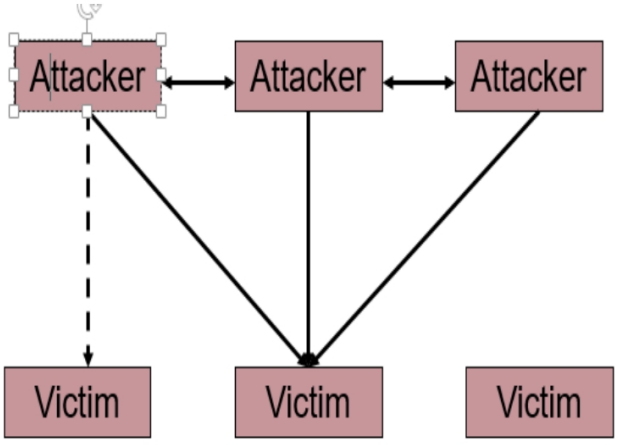
SLOT:C1+TC1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

Programme Name & Branch : **B.Tech & CSE**
Course Code and Course Name : **Cyber Security-BCSE410L**
Faculty Name(s) : **ALL**
Class Number(s) : **ALL**
Date of Examination : **19-08-2025**
Exam Duration : **90 minutes** **Maximum Marks: 50**

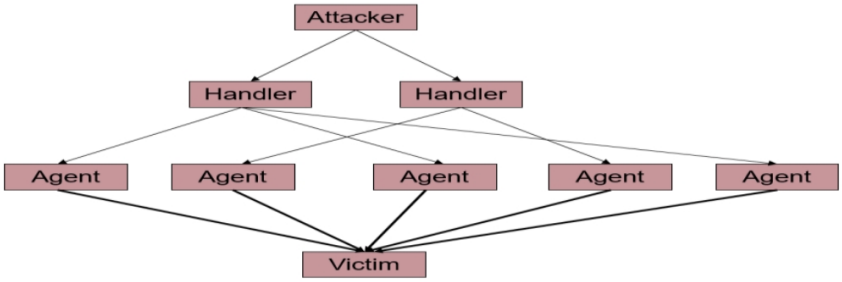
General instruction(s): Answer All Questions

- Course Outcomes:
  CO1: Understand the emerging cyber security attacks and their adversarial risk.
  CO2: Identify the emerging vulnerabilities and attacks, and countermeasures in cyber-physical systems.

Q. No	Question	M	CO	BL
1.	Identify the following attacks and suggest appropriate preventive measures for each. a) A type of attack makes a service unusable by overloading the server or network with excessive traffic. Discuss the different categories of this attack using a suitable diagram (7 Marks) **1. Simple DoS**  **2.Coordinated DoS**  3.Distributed DoS	10	1	3

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

	 b) A type of attack can be controlled by reducing the application's access privileges to the database. (3 Marks) **SQL Injection (SQLi)** 1. Use Parameterized Queries (Prepared Statements) 2. Use Stored Procedures 3. Input Validation and Sanitization 4. Least Privilege Principle 5. Error Handling and Messages 6. Use ORM (Object-Relational Mapping) Libraries 7. Regular Security Audits and Code Reviews			

2.	Even though firewalls allow traffic only to legitimate hosts and services, attacks like Code Red on IIS can still occur. Explain how this problem can be solved, and describe the types of systems used to monitor and detect such attacks based on their operation.
	• Firewalls allow traffic only to legitimate hosts and services
	• Traffic to the legitimate hosts/services can have attacks
	  • CodeReds on IIS
	• Solution?
	  • Intrusion Detection Systems
	  • Monitor data and behavior
	  • Report when identify attacks
	Types of IDS
	Signature-based IDS
	Anomaly-based IDS
	Network-basedIDS
	Host-based IDS
		10	1	4

3.	Your organization is worried about cyber-attacks on its online banking system. As a cyber - security consultant, use an attack tree model to analyze how attackers might compromise customer accounts. a) Identify and briefly describe three main attack paths to reach the root goal. (5 Marks) **1. Phishing Attacks** • Attackers send fraudulent emails or messages impersonating the bank to trick customers into revealing login credentials.	10	2	4

- Methods may include fake login pages, urgent warnings, or fake rewards.

2. Web Application Exploits

- Attackers target vulnerabilities in the bank's website or mobile app.
- Techniques may include:
  - SQL Injection (to access user data),
  - Cross-Site Scripting (to hijack sessions),
  - Exploiting weak authentication mechanisms.

3. Malware Installation

- Attackers use malware (e.g., keyloggers or trojans) on customers' or employees' devices.
- These can capture login details or hijack sessions without the victim's knowledge.

b) Explain how an attack tree helps in finding vulnerabilities and planning mitigations. (5 Marks)

1. Visual Mapping of Threats

Breaks down the root goal into all possible attack methods, showing the full picture of potential security weaknesses.

2. Identifies Vulnerabilities Clearly

Highlights specific areas (e.g., user behavior, software flaws, system design) where attacks could succeed.

3. Prioritizes Risks and Responses

Helps security teams focus on the most likely or most damaging attack paths and apply mitigations accordingly.

4. Supports Layered Defense

Encourages multiple protective strategies such as:

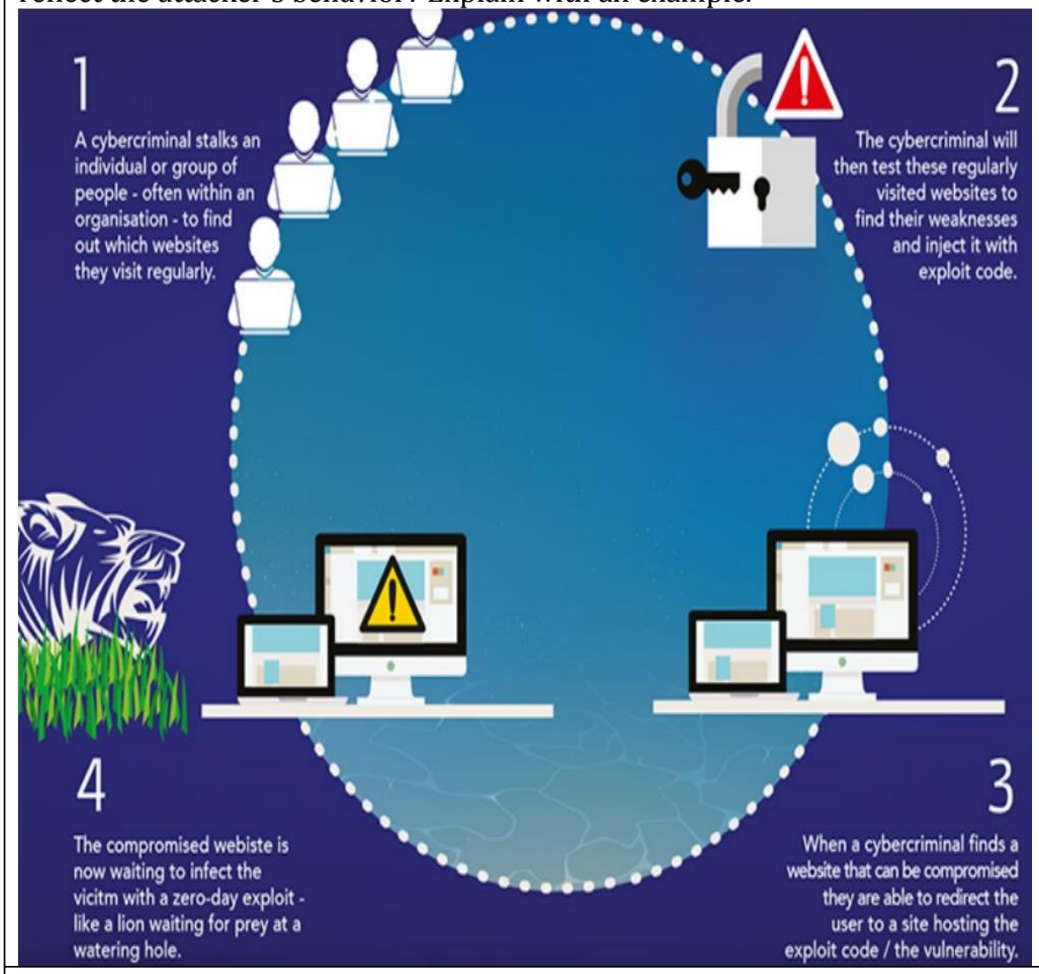
User training (to combat phishing),

Secure coding practices (to prevent exploits),

Antivirus/malware protection (to detect threats).

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

	5. Improves Communication Easy to present and understand across technical and non-technical teams, helping with security planning and decision-making.			
4.	a) Which type of social engineering attack is best described by the phrase "Like lions hidden in the savannah grass, they then lay and lurk," and how does this reflect the attacker's behavior? Explain with an example.  	5	2	4
	b) Which phishing tactic involves using names of popular companies like Google or PayPal? Explain why attackers use this method and how the attack works.	5		

				
5.	Explain the different phases of the Penetration Testing Execution Standard (PTES) and describe the role each phase plays in conducting a structured penetration test. Penetration Testing is a way to simulate the methods that an attacker might use to circumvent security controls and gain access to a system." 1. **Pre-Engagement** 2. **Intelligence Gathering** 3. **Threat Modeling** 4. **Vulnerability Analysis** 5. **Exploitation** 6. **Post Exploitation** 7. **Reporting**	10	2	2