Course Code: 23CS1004

R23

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY:: PUTTUR
(AUTONOMOUS)
Siddharth Nagar, Narayanavanam Road – 517583
QUESTION BANK (DESCRIPTIVE)

Subject with Code: Principles of Cyber security (23CS1004) **Course & Branch**: B.Tech – CIC

Regulation: R23 **Year & Sem:** III - B.Tech & I-Sem

UNIT –I
INTRODUCTION TO CYBER SECURITY

1	a	What is meant by the term cybersecurity?	[L1][CO1]	[2M]
	b	Describe cybercrimes and the methods used to prevent them.	[L2][CO1]	[2M]
	c	Explain who cyber criminals are and discuss the types of damage they cause.	[L2][CO1]	[2M]
	d	Enumerate some common cyber threats.	[L1][CO1]	[2M]
	e	Outline the classification of cybercrimes and briefly discuss the related terms.	[L1][CO1]	[2M]
2		Explain the various categories of cybercrime cases under the Information Technology Act, 2000. Discuss the different types of cybercrimes covered under the Act, their legal provisions, and suitable examples. Explain how the Act helps prevent and address cyber offenses in India.	[L2][CO1]	[10M]
3		Discuss the concept of cybercrime in detail. Explain the different types of cybercrimes and the corresponding security measures used to prevent and mitigate them. Describe the importance of cybersecurity practices in protecting individuals, organizations, and digital assets.	[L2][CO1]	[10M]
4	a	List and explain the important sections and rules of the Information Technology Act, 2000. Discuss their significance in addressing cybercrimes, regulating electronic transactions, and ensuring information security.	[L1][CO1]	[5M]
	b	Explain the global impact and perspective of cybercrime. Discuss its effects on individuals, organizations, governments, and the	[L2][CO1]	[5M]

		global economy. Describe the international efforts and strategies adopted to combat cybercrime and enhance cybersecurity.		
5		Explain the concept of cybercrime in detail. Classify the different types of cybercrimes and describe their characteristics with suitable examples. Discuss their impact on individuals, organizations, and society.	[L2][CO1]	[10M]
6	a	Provide a brief overview of cybercrime from the legal perspective. Explain the laws, regulations, and legal provisions governing cybercrimes, along with their role in preventing, investigating, and prosecuting cyber offenses.	[L2][CO1]	[5M]
	b	Discuss cybercrime with reference to the Indian legal framework. Explain the key provisions of the Information Technology Act, 2000 and other relevant laws for preventing, investigating, and prosecuting cyber offenses in India.	[L2][CO1]	[5M]
7		Explain the differences between Information Security and Cybersecurity. Compare their objectives, scope, and key features with suitable examples.	[L4][CO1]	[10M]
8		Discuss the importance of Information Security Management. Explain its objectives, key components, and implementation process in protecting organizational information assets. Describe benefits and challenges of Information Security Management	[L2][CO1]	[10M]
9		Discuss the importance of Cyber Security Management. Explain its objectives, key components, and implementation process in protecting organizational networks, systems, and digital assets. Describe benefits and challenges of Cyber Security Management.	[L2][CO1]	[10M]
10	a	Discuss the cybercrime cases covered under the different sections of the Indian Penal Code (IPC). Explain the relevant IPC provisions applicable to cyber offenses, their legal significance, and suitable examples.	[L2][CO1]	[5M]
	b	Examine the prevalence of cybercrimes in major cities. Discuss the common types of cybercrimes, contributing factors, and their impact on individuals and organizations. What are the measures to reduce Cybercrime in Cities.	[L4][CO1]	[5M]

11	What are the different classifications of cybercrimes on the Internet? Explain each classification with its characteristics, common types, and suitable examples. Discuss their impact on individuals, organizations, and society.	[L2][CO1]	[10M]

UNIT –II
Information Security (IS) within Lifecycle Management

1	a	Provide a brief explanation of social engineering in the context of cybercrime.	[L1][CO2]	[2M]
	b	Explain cyberstalking using an appropriate example.	[L2][CO2]	[2M]
	c	Explain how botnets facilitate cybercriminal activities.	[L2][CO2]	[2M]
	d	Write any two examples of cybercrimes commonly committed through cyber cafés.	[L1][CO2]	[2M]
	e	What do you mean by an attack vector in cybersecurity?	[L2][CO2]	[2M]
2	Explain the Information Security Life Cycle in detail. Describe each phase, including planning, risk assessment, implementation, monitoring, incident response, and continuous improvement.		[L2][CO2]	[10M]
3	Discuss the various information security tools in detail. Explain their features, functions, and advantages in protecting systems, networks, and data from cyber threats.		[L2][CO2]	[10M]
4	What do you mean by the Operational Threat Environment? Explain its key components, types of threats, vulnerabilities, and risk factors. Discuss its importance in identifying and mitigating cyber threats to protect organizational information assets.		[L2][CO2]	[10M]
5	Discuss the different classes of attacks in information security. Explain their characteristics, types, and methods used to compromise information systems.		[L2][CO2]	[10M]
6	What is a vulnerability in information security? Explain its concept, types, causes, and potential impact on information systems. Discuss how vulnerabilities can be identified, assessed, and mitigated to enhance cybersecurity.		[L2][CO2]	[10M]

7	a	What do you mean by access attacks in information security? Explain the concept, types, and techniques used to gain unauthorized access to systems and data. Discuss their impact on information security and the measures used to prevent them.	[L2][CO2]	[5M]
	b	Explain reconnaissance attacks in information security. Describe their objectives, techniques, and different types used to gather information about target systems. Discuss their impact and the security measures used to detect and prevent them.	[L2][CO2]	[5M]
8	What is risk management in cybersecurity? Explain its objectives, key processes, and importance in identifying, assessing, and mitigating security risks. Discuss how effective risk management helps protect organizational information assets and ensures business continuity.		[L2][CO2]	[10M]
9	a	What is Cyber Threat Intelligence? Explain its concept, objectives, and the different types of CTI. Discuss sources and benefits of Cyber Threat Intelligence.	[L2][CO2]	[5M]
	b	Explain malware and phishing in detail. Discuss their types, methods of attack, and their impact on information systems and users. Describe the preventive measures and best practices to protect against malware and phishing attacks.	[L2][CO2]	[5M]
10	Distinguish between risks, threats, and vulnerabilities in cybersecurity. Explain their meanings, key differences, and interrelationship with suitable examples. Discuss their role in information security and risk management.		[L4][CO2]	[10M]
11	Briefly discuss Distributed Denial-of-Service (DDoS) attacks. Also distinguish between DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks.		[L4][CO2]	[10M]

Course Code: 23CS1004 **R23**

UNIT –III
Incident Response

1	a	List any two security threats associated with mobile devices.	[L1][CO3]	[2M]
	b	Briefly describe credit card fraud associated with mobile and wireless devices.	[L2][CO3]	[2M]
	c	How do registry settings help improve the security of mobile operating systems?	[L2][CO3]	[2M]
	d	State any two types of attacks on mobile devices.	[L1][CO3]	[2M]
	e	Why are organizational security policies essential for mobile computing?	[L2][CO3]	[2M]
2	Explain the different categories of cybersecurity incidents. Discuss the different categories of cybersecurity incidents with examples.		[L2][CO3]	[10M]
3	a	What is incident response in cybersecurity? Explain its objectives, key phases, and importance in detecting, managing, and recovering from cybersecurity incidents. Discuss how an effective incident response process minimizes damage and ensures business continuity.	[L2][CO3]	[5M]
	b	What is incident recovery in cybersecurity? Explain its objectives, key activities, and importance in restoring systems, data, and services after a cybersecurity incident. Discuss how effective incident recovery supports business continuity and organizational resilience.	[L2][CO3]	[5M]
4	Explain Identity and Access Management (IAM) in cybersecurity. Discuss its objectives, key components, authentication and authorization mechanisms, and access control models. Describe how IAM helps protect organizational resources and ensures secure access to information systems.		[L2][CO3]	[10M]
5	Discuss the ports and protocols used in cybersecurity. Explain their functions, common types, and significance in secure network communication. Describe how they contribute to protecting data and ensuring reliable information exchange.		[L2][CO3]	[10M]

6		Explain data assets in detail. Discuss their types, characteristics, and importance in information security and organizational operations. Describe the methods used to classify, protect, and manage data assets throughout their lifecycle.	[L2][CO3]	[10M]
7		Briefly explain protection technologies in cybersecurity. Discuss the various technologies used to safeguard information systems, networks, and data from cyber threats. Describe the importance of Protection Technologies.	[L2][CO3]	[10M]
8	a	Why is digital data security important? Explain its significance in protecting sensitive information, ensuring confidentiality, integrity, and availability, and preventing unauthorized access, data breaches, and cyber threats.	[L2][CO3]	[5M]
	b	What are the different types of digital security? Explain each type, its key features, and its role in protecting digital systems, networks, applications, and information from cyber threats.	[L2][CO3]	[5M]
9		Differentiate between Digital Information Security and Cyber Security. Compare their objectives, scope, key features, and areas of application. Discuss how each contributes to protecting digital information, systems, and organizational assets.	[L4][CO3]	[10M]
10		Explain digital security and its different types. Discuss with examples each type in protecting digital devices, networks, applications, and information from cyber threats.	[L2][CO3]	[10M]
11		What is configuration management in cybersecurity? Explain its objectives and various components in configuration management in Cyber security. Discuss how effective configuration management helps reduce vulnerabilities and enhance overall cybersecurity.	[L2][CO3]	[10M]

Course Code: 23CS1004 **R23**

UNIT –IV
Threat Detection and Evaluation

1	a	Write a short note on the role of a proxy server in cybercrime.	[L1][CO4]	[2M]
	b	Compare a virus and a worm in cybersecurity.	[L4][CO4]	[2M]
	c	Explain the term SQL Injection in cybersecurity.	[L2][CO4]	[2M]
	d	Define keyloggers in the context of cybersecurity.	[L1][CO4]	[2M]
	e	Write any two approaches used by attackers to perform identity theft.	[L1][CO4]	[2M]
2		Explain Vulnerability Management in Cyber Security in detail. Describe its objectives, importance, and the various stages involved in identifying, assessing, prioritizing, remediating, and monitoring security vulnerabilities. Discuss the tools, challenges, and best practices for implementing an effective vulnerability management process.	[L2][CO4]	[10M]
3	a	What are Security Logs in Cyber Security? Explain their purpose, importance, and the different types of security logs generated by systems, networks, applications, and security devices.	[L2][CO4]	[5M]
	b	What are Alerts in Cyber Security? Explain their purpose, importance, and the different types of alerts generated by security systems.	[L2][CO4]	[5M]
4	a	Examine the various web threats faced by organizations in detail. Explain the different types of web-based attacks, their impact on organizational security, and the methods used by attackers. Discuss the preventive measures and best practices to protect organizations from web threats.	[L2][CO4]	[5M]
	b	List out the major roles or impacts of cyber threats on organizations and information systems.	[L1][CO4]	[5M]
5		Explain Monitoring Tools and Appliances in Cyber Security in detail. Describe their purpose, types, key features, and their role in monitoring networks, systems, and security events. Discuss how these tools help	[L2][CO4]	[10M]

		detect threats, improve performance, and strengthen an organization's overall security.		
6		Explain the classification of Cyber Threats in detail. Describe the different types of cyber threats based on their source, nature, and attack methods, along with their characteristics and examples. Discuss their impact on information systems and organizational security.	[L2][CO4]	[10M]
7	a	Discuss the various threat detection techniques used in Cyber Security. Explain the different methods, tools, and technologies for identifying and analyzing cyber threats, and describe their role in protecting information systems and networks from security attacks.	[L2][CO4]	[5M]
	b	What is Threat Evaluation in Cyber Security? Explain its purpose, importance, and the process of assessing and prioritizing cyber threats based on their likelihood, impact, and potential risks.	[L2][CO4]	[5M]
8		What is Packet Capture Analysis in Cyber Security? Explain its purpose, importance, and the process of capturing and analyzing network packets to detect security threats, troubleshoot network issues, and investigate cyber incidents.	[L2][CO4]	[10M]
9		What is Network Traffic Analysis in Cyber Security? Explain its purpose, importance, and the techniques used to monitor and analyze network traffic for detecting suspicious activities, identifying security threats, and improving network performance.	[L2][CO4]	[10M]
10		What is Vulnerability Assessment in Cyber Security? Explain its purpose, importance, and the process of identifying, analyzing, and evaluating security vulnerabilities in systems, networks, and applications. Discuss how vulnerability assessment helps strengthen an organization's overall security posture.	[L2][CO4]	[10M]
11		Differentiate between Vulnerability Assessment and Vulnerability Management in Cyber Security. Compare their objectives, processes, scope, and outcomes.	[L4][CO4]	[10M]

Course Code: 23CS1004 **R23**

UNIT –V
Introduction to backdoor System and security

1	a	Write a short note on IPR issues in cybercrime.	[L1][CO5]	[2M]
	b	Mention any two common web-based threats affecting organizations.	[L1][CO5]	[2M]
	c	Explain the term social computing briefly.	[L2][CO5]	[2M]
	d	What are two common security concerns related to social media marketing?	[L1][CO5]	[2M]
	e	What is the economic impact of cybercrime on organizations?	[L1][CO5]	[2M]
2		Explain the concept of a Backdoor System in Cyber Security in detail. Describe its purpose, types, methods of installation, associated security risks, and how attackers exploit backdoors to gain unauthorized access. Discuss the preventive measures and best practices for detecting and eliminating backdoors from computer systems and networks.	[L2][CO5]	[10M]
3		Explain how to protect devices from Backdoor Attacks in Cyber Security. Discuss the preventive measures, security tools, and best practices used to detect, prevent, and remove backdoors, and explain their importance in maintaining system security and data integrity.	[L2][CO5]	[10M]
4		Explain the concept of Operating System Hardening in Cyber Security. Discuss its objectives, importance, key techniques, and best practices used to strengthen the security of an operating system and protect it from cyber threats and unauthorized access.	[L2][CO5]	[10M]
5	a	Explain the concept of a Single Firewall in Cyber Security. Describe its architecture, working principle, advantages, limitations, and its role in protecting computer networks from unauthorized access and cyber threats.	[L2][CO5]	[5M]
	b	Explain the concept of a Dual Firewall in Cyber Security. Describe its architecture, working principle, advantages, limitations, and how it provides enhanced network security by using two layers of firewall protection against cyber threats and unauthorized access.	[L2][CO5]	[5M]

6		Explain the concept of a Ransomware Attack in Cyber Security. Describe its working mechanism, types, methods of infection, impact on individuals and organizations, and the preventive measures used to protect systems from ransomware attacks.	[L2][CO5]	[10M]
7		What is a Demilitarized Zone (DMZ) in Cyber Security? Explain its architecture, purpose, components, and how it enhances network security by isolating public-facing services from an organization's internal network.	[L2][CO5]	[10M]
8		What are Backdoor Trojans in Cyber Security? Explain their features, methods of infection, and how they enable attackers to gain unauthorized remote access to compromised systems. Discuss their impact on system security and the measures used to detect, prevent, and remove them.	[L2][CO5]	[10M]
9	a	What is Metasploit in Cyber Security? Explain its purpose, architecture, key features, and the various components used for penetration testing and vulnerability assessment.	[L2][CO5]	[5M]
	b	Explain the significance of Digital Signatures in Cyber Security. Discuss their purpose, key features, and the role they play in ensuring authentication, integrity, non-repudiation, and secure communication in digital transactions.	[L2][CO5]	[5M]
10		What is System Hardening in Cyber Security? Explain its objectives, types, steps used, benefits and challenges of System Hardening in Cyber Security.	[L2][CO5]	[10M]
11		What is Network Hardening in Cyber Security? Explain its objectives, steps used, key techniques, and best practices used and challenges in Network Hardening in Cyber Security.	[L2][CO5]	[10M]