SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA
School of Computer Science & Engineering
B. Tech. (All Branches under AEC Category) /Major Examination (Even) 2023-24

Entry No: | | | | | | | | | |

Total Number of Pages: [01]

Date: 24.05.2024

Total Number of Questions: [15]

Course Title: Introduction to Cyber Security
Course Code: CSL AE102

Time Allowed: 3.0 Hrs.

Max Marks: [50]

Instructions / NOTE

i. Attempt All Questions.
ii. Support your answer with neat freehand sketches/diagrams, wherever appropriate.
iii. Assume any missing data to suit the case / derivation / answer.
iv. Show every step while solving a numerical/analytical/design based question.

	Section-A	
Q1.	Which of the following act violates cyber security? a) Exploit b) Attack c) Threat d) Vulnerability	[01]
Q2.	Which of the following do Cyber attackers commonly target for fetching IP address of a target or victim user? a) ip tracker b) emails c) websites d) web pages	[01]
Q3.	They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are "they" referred to here? a) White Hat Hackers b) Black Hat Hackers c) Hactivists d) Gray Hat Hackers	[01]
Q4.	Which of the following term refers to a group of hackers who are both white and black hat? a) Yellow Hat hackers b) Grey Hat hackers c) Red Hat Hackers d) White-Black Hat Hackers	[01]
Q5.	Which of the following DDoS in mobile systems wait for the owner to trigger the cyber attack? a) botnets b) programs c) virus d) worms	[01]
Q6.	Define the term cyberspace precisely.	[02]
Q7.	Point out the key standard measures to establish confidentiality in cyber security.	[02]
Q8.	Define the term DNS spoofing precisely with an example.	[02]
Q9.	Define the term Phishing from cyber security perspective. Point out key types of phishing.	[02]
Q10.	Write short note on Non-state actors from cyber security perspective.	[02]
	Section-B	
Q11.	Define the term "Cyber Security" and "Cyber Threat". Explain Evolution of Cyber Security and cyber threats with the help of proper diagrams.	[07]
Q12.	What is significance of New Model of digital security? Explain Tactical Security integration with the help of proper diagram. Point out key Future Technology to be Designed with Security.	[07]
Q13.	Explain cyber security hierarchy in India in proper tabular form. Also describe Recommendations on Cyber security Framework for States.	[07]
Q14.	Explain key five layers in Cyber Security Planning. What are smart security solutions towards 2025 in Indian scenario?	[07]
Q15.	Let you are leading a team of cyber security experts responsible for solving a critical security breach case where you don't have any clue except the breach. What key steps you will follow for solving the case. Explain in detail.	[07]

SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA
School of Computer Science & Engineering
B. Tech. (Common to all) Mid-Sem Examination (Even) 2024-25

Entry No: | | | | | | | | | |

Total Number of Pages: [02]

Date: 20th March, 2025

Total Number of Questions: [09]

Course Title: Introduction to Cyber Security

Course Code: CSL AE102

Time Allowed: 1 hour 30 minutes

Max Marks: [20]

Instructions / NOTE

i. Attempt All Questions.

ii. It's mandatory to support your answer with detailed stepwise solutions along with neat freehand sketches/diagrams, wherever appropriate.

	Section – A (Attempt All questions)		
Q1.	1.Which of the following best describes the principle of least privilege in cyber security? a. Users are granted minimal access rights necessary to perform their tasks b. Users are allowed temporary access rights c. Users have complete access to all system resources d. Users are restricted from accessing any resources	[01]	CO1
Q2.	A user receives an email from an unknown source asking for sensitive information. What is this type of attack called? a. Phishing b. Man-in-the-middle attack c. DoS attack d. DDoS attack	[01]	CO2
Q3.	Which of the following options best defines an attack vector in terms of cyber security? a. A software tool used by ethical hackers to test system vulnerabilities b. A hardware component that helps prevents denial-of-service attacks c. A technique to encrypt sensitive data during transmission d. A method or avenue used by cyber threats to gain unauthorized access to a system or network	[01]	CO1
Q4.	Which of the following is a common type of social engineering attack? a. Brute force attack b. Distributed Denial of Service (DDoS) attack c. Phishing attack d. SQL injection attack	[01]	CO2
	Section – B		
Q5.	Briefly describe the types of spyware. How does a spyware work?	[04]	CO1
Q6.	Differentiate DoS attack from DDoS attack. Give two examples of DoS attack.	[04]	CO2
Q7.	Discuss different types of hackers along with their intentions and approach.	[04]	CO1
Q8.	Discuss life cycle of an APT. What makes it different from logic bomb. OR	[04]	CO2
Q9.	Describe zero-day vulnerability and software patches. List some of the common vulnerabilities in cybersecurity.	[04]	CO2

Examination (Even) 2024-25

Entry No: 2 4 1 5 E C 0 5 5

Date: 29th July, 2025

Total Number of Pages: [01]

Total Number of Questions: [10]

Course Title: Introduction to Cyber Security

Course Code: CSL AE102

Time Allowed: 3 hour

Max Marks: [40]

Instructions / NOTE

i. Attempt All Questions.

ii. It's mandatory to support your answer with detailed stepwise solutions along with neat freehand sketches/diagrams, wherever appropriate.

	Section – A (Attempt All questions)		
Q1	Briefly define cyberspace and attack surface.	2	CO1
Q2	_____ malware replicate itself and require host file but _____ malware is self-dependent for its replication.	2	CO2
Q3	Briefly define personal and non-personal data.	2	CO4
Q4	Discuss, how bigdata is different from data?	2	CO4
Q5	Differentiate data protection from data privacy.	2	CO4
	Section – B		
Q6	Discuss in detail the ethical and legal concerns associated with use of AI and generative AI now a days.	6	CO3
Q7	Explain the major adoption with the implementation of IT act 2000 in India. Discuss the limitations of this act as well.	4+2	CO3
Q8	Discuss Phishing, Vishing and Smishing along with suitable examples.	2+2+2	CO2
Q9	Describe threat, risk and vulnerability in context of cyber security. Discuss some common vulnerabilities of password-based authentication.	4.5+1.5	CO2
Q10	Discuss Email Scams, Online Job fraud and Online Payment Fraud with suitable examples.	2+2+2	CO5

SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA
School of Computer Science & Engineering
B. Tech. (All Branches under AEC Category) /Minor-1 Examination (Odd) 2024-25

Entry No: | | | | | | | | | |

Date: 26.02.2024

Total Number of Pages: [01]

Total Number of Questions: [07]

Course Title: Introduction to Cyber Security

Course Code: CSL AE102

Time Allowed: 1.0 Hrs.

Max Marks: [20]

Instructions / NOTE

i. Attempt All Questions.
ii. Support your answer with neat freehand sketches/diagrams, wherever appropriate.
iii. Assume any missing data to suit the case / derivation / answer.
iv. Show every step while solving a numerical/analytical/design based question.

	Section-A	
Q1.	Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information? (A) Cyber attack (B) Computer security (B) Cryptography (D) Digital hacking	[01]
Q2.	Which of the following is a type of cyber security? (A) Cloud Security (B) Network Security (C) Application Security (D) All of the above	[01]
Q3.	What are the features of cyber security? (A) Compliance (B) Defense against internal threats (C) Threat Prevention (D) All of the above	[01]
Q4.	Define the term Digital Signatures. Give a most common example of digital signatures.	[02]
	Section-B	
Q5.	Define the term "Cyber Crime". Point out various Cyber Crimes. How you can combat cyber crimes?	[05]
Q6.	What do you understand by Cyber Threats? Point out Various Types of Cyber Threats. Also point out key tips for cyber safety.	[05]
Q7.	Define the term "Computer Virus". Why Do people Create These Viruses? Classify Various Types of Viruses. Is it legal or illegal to create computer viruses?	[05]

SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA
School of Computer Science & Engineering
B. Tech. (All Branches under AEC Category) /Minor-2 Examination (Odd) 2024-25

Entry No: | | | | | | | | | |

Total Number of Pages: [01]

Date: 08.04.2024

Total Number of Questions: [07]

Course Title: Introduction to Cyber Security
Course Code: CSL AE102

Time Allowed: 1.0 Hrs.

Max Marks: [20]

Instructions / NOTE

i. Attempt All Questions.
ii. Support your answer with neat freehand sketches/diagrams, wherever appropriate.
iii. Assume any missing data to suit the case / derivation / answer.
iv. Show every step while solving a numerical/analytical/design based question.

	Section-A	
Q1.	Which of the following type of data, phishers cannot steal from its target victims? (A) bank details (B) phone number (C) passwords (D) apps installed in the mobile	[01]
Q2.	A _____ tries to formulate a web resource occupied or busy its users by flooding the URL of the victim with unlimited requests than the server can handle. (A) Phishing attack (B) DoS attack (C) Website attack (D) MiTM attack	[01]
Q3.	DNS stands for _____ (A) Data Name System (B) Domain Name Server (C) Domain Name System (D) Domain's Naming System	[01]
Q4.	What is Ransomware in cyber security? What do's and don'ts you will take in such matter?	[02]
	Section-B	
Q5.	What are key causes of Cyber attack? What precautions you will take to secure your Mobile Device? Point out each.	[05]
Q6.	What exactly a malware is? Give 5 Examples of Malware. Differentiate Computer Virus, Network worm and Trojan Horse.	[05]
Q7.	What is significance of social engineering from cyber security perspective? Describe MHA Recommendations to maintain proper Cyber Security.	[05]