	RV College of Engineering® Department of Computer Science and Engineering CIE - I: Test and Quiz Paper		
Course & Code	**INTRODUCTION TO CYBER SECURITY** **(22EM106)**		**Semester: I**
Date : Jan 2023	**Duration:**120 minutes	**Max.Marks**:(10+50)=60 Marks	**Staff :** MH
USN :	**Name :**		**Section : Physics cycle**

NOTE: *Answer all the questions from Part-A (10 M) and Part-B (50 M)*

Sl.no	PART - A	Marks	* BT	*CO
1	_____is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.	1	L1	CO1
2	_____ network developed prior to the internet.	1	L1	CO1
3	Define vulnerability. Give an example	1	L2	CO2
4	_____ is a code injecting method used for attacking the database of a system or website.	1	L1	CO2
5	The term_____ which denotes that only authorized users can access the information.	1	L1	CO1
6	In ethical hacking and cyber security, there are _____ types of scanning	1	L2	CO2
7	Who commits cyber-crimes. Give an example.	1	L2	CO1
8	List the important cyber security goals.	1	L1	CO1
9	Bob Thomas, working at BBN, wrote a program named X which infected the ARPANET. He later wrote the program Y to destroy X. What are X and Y?	1	L2	CO1
10	_____ is a form of malware that uses social engineering to cause shock, anxiety, or the perception of a threat to manipulate users into buying unwanted software.	1	L1	CO1

Sl.no.	PART - B	Marks	* BT	*CO
1.a	What is internet ? Explain the evaluation of the internet.	6	L2	CO1
1.b	Define cyber space. Why cyber security is important.	4	L2	CO1
2.a	List and briefly explain different types of cyber security threats.	6	L2	CO2
2.b	With block diagram explain security system development life cycle	4	L2	CO1
3.a	List the difference between cyber security and information security	6	L2	CO1
3.b	Explain in your own words what you understand about the global cooperation required in fighting against cybercrime.	4	L3	CO2
4	Define cybercrime. List and briefly explain different types of cybercrimes.	10	L3	CO2
5	Define passive attack. List and briefly explain the tools used in passive attack.	10	L3	CO2

COURSE OUTCOMES:

CO1:	Understand the cyber-attacks and their principles for different domains- social media, E-commerce, and digital devices.
CO2:	Analyse vulnerabilities in different domains that the attacker capitalizes for attack.
CO3:	Apply different attacking techniques that make use of vulnerabilities available in various domains.
CO4:	Evaluate methods to cover different vulnerabilities to safeguard the systems against cyber-attacks.
CO5:	Investigate modern tools and technologies available to mitigate cybercrime attacks.

	L1	L2	L3	L4	L5	L6	CO1	CO2	CO3	CO4	CO5
Part-A & B	6	30	24	***	***	***	27	33	***	***	***