22EM106: INTRODUCTION TO CYBER SECURITY
(2022 SCHEME)

MODEL QUESTION PAPER - I

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer all questions from Part A. Part A questions should be answered in first three pages of the answer book only.
2. Answer FIVE full questions from Part B. In Part B question number 2 is compulsory. Answer any one full question from 3 and 4, 5 and 6, 7 and 8, and 9 and 10.

		PART-A	
1	1.1	_____ 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.	01
	1.2	Define vulnerability. Give an example.	02
	1.3	_____ is a code injecting method used for attacking the database of a system or website.	01
	1.4	This is a Debian-derived Linux distribution managed and funded by Offensive Security Ltd, designed for digital forensics and penetration testing. Which is this very famous OS majorly developed for Hackers and software testers?	01
	1.5	The word X is a combination of the words “robot” and “network”. It is a number of Internet-connected devices, each of which is running one or more bots. This can be used to perform DDoS attacks, steal data, send spam. Identify the word X?	01
	1.6	Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called_____	01
	1.7	_____command is used to see if a computer has connectivity with another computer on the same network segment.	01
	1.8	A strong password should contain different combinations of _____and _____	02
	1.9	A group of students created a fake social network account for one of their classmates. On the page for this account, the students presented the classmate falsely and posted hateful messages. What two terms describe this harassment?	01
	1.10	A person is using an ATM, the person behind them is standing behind them but just to the side watching what they are doing. Identify type of social engineering attack.	01
	1.11	Access social networking sites using _____ protocol to safeguard your username, password, and other information you post.	01
	1.12	Name any two popularly used web Browser.	01
	1.13	It can be a software program or a hardware device that filters all data packets	01

		coming through the internet, a network, etc. it is known as the_____	
	1.14	_____ protocol is most widely used in Wi-Fi Security.	01
	1.15	DNS translates a Domain name into _____	01
	1.16	_____ is the world's most popular vulnerability scanner used in companies for checking vulnerabilities in the network.	01
	1.17	Packet filtering firewalls are vulnerable to _____	01
	1.18	_____ helps in protecting corporate data, communications, and other assets.	01
PART-B			
UNIT-I			
2	a	Define the term Internet. List and briefly explain the applications of the Internet.	08
	b	Define cybercrime. List and briefly explain different types of cyber crimes.	08
UNIT-II			
3	a	Define Active attack. List and briefly explain the tools used in passive attack.	10
	b	Differentiate between cyber security and information security.	06
OR			
4	a	Define Attack Vector. Explain why attackers use proxies and types of proxies.	10
	b	What are Botnets? Explain How Botnets involved in cybercrimes.	06
UNIT-III			
5	a	List and explain different types of social media and its uses.	08
	b	Explain the following in detail. i. Social media addiction ii. Cyberbullying	08
OR			
6	a	List and briefly explain the pitfalls of social networking.	08
	b	Define hashtag in social media. Explain how to use hashtags effectively on social media.	08

UNIT-IV			
7	a	Define Unified Payment Interface(UPI). Explain the working of UPI.	08
	b	Define E-commerce Security. Explain different types of threats and issues in E-Commerce.	08
OR			
8	a	Define digital payment fraud. How does it happen? Explain types of digital payments.	10
	b	Differentiate between electronic wallets and bank accounts.	06

UNIT-V			
9	a	How does the attack occur in Wi-Fi Environment ? Explain different types of	10

		attacks and guidelines for securing wireless communications.	
	b	Explain the following in detail. i. E-mail security ii. Anti-virus	06
OR			
10	a	List and explain different types of firewalls along with advantages and disadvantages.	10
	b	List and briefly explain digital security tools.	06