Reg. No.															

Question Paper Code	13547

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2025

Fifth Semester

Computer Science and Engineering (Cyber Security)

20SCPC503 – CYBER ATTACKS

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Which of the following is an example of a DoS attack? (a) Phishing (b) Port scanning (c) Email spoofing (d) SYN flood	1	K1	CO1
2.	What is the primary goal of cyber terrorism? (a) Financial gain (b) Intellectual property theft (c) Disruption for political motives (d) Surveillance	1	K1	CO1
3.	In social engineering, which attack involves pretending to be someone trustworthy to get information? (a) Tailgating (b) Quid Pro Quo (c) Pretexting (d) Shoulder Surfing	1	K1	CO2
4.	What is "Quid Pro Quo" in the context of social engineering? (a) Gaining access via phishing (b) Offering something in exchange for information (c) Following someone into a secure area (d) Faking an identity online	1	K1	CO2
5.	Which OSINT tool specializes in discovering open ports and services exposed to the internet? (a) Shodan (b) Harvester (c) Wireshark (d) Nessus	1	K1	CO3
6.	What is the main purpose of Maltego in OSINT? (a) Malware analysis (b) Social network mapping (c) Virus detection (d) Phishing prevention	1	K1	CO3
7.	Which type of malware hides its existence from detection software? (a) Ransomware (b) Rootkit (c) Trojan (d) Worm	1	K1	CO4
8.	What distinguishes fileless malware from traditional malware? (a) It is larger in size (b) It doesn't require internet (c) It runs in memory only (d) It is a form of spyware	1	K1	CO4
9.	Which scanning method helps to identify open ports on a networked system? (a) Vulnerability scanning (b) Port scanning (c) Enumeration (d) Spoofing	1	K1	CO5
10.	What is the goal of a brute force attack? (a) Prevent access to a website (b) Steal source code (c) Crack passwords (d) Redirect traffic	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Define cyber stalking.	2	K2	CO1
12.	Differentiate between DoS and spoofing attacks.	2	K2	CO1
13.	List the major types of social engineering attacks.	2	K2	CO2
14.	Explain the term impersonation with an example.	2	K2	CO2
15.	Define OSINT and mention two of its applications.	2	K2	CO3
16.	List two features of Shodan as an OSINT tool.	2	K2	CO3
17.	Explain the malware lifecycle.	2	K2	CO4

18.	State any two characteristics of ransom ware.	*2*	*K2*	*CO4*
19.	Mention any two common network vulnerabilities.	*2*	*K2*	*CO5*
20.	Differentiate between port scanning and vulnerability scanning.	*2*	*K2*	*CO5*
21.	What is clickjacking?	*2*	*K2*	*CO6*
22.	How does directory traversal exploit web servers?	*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a) (i)	Explain the different types of cybercrimes with suitable examples.	*11*	*K2*	*CO1*
	(ii)	Describe various types of cyber-attacks and their impacts on organizations.	*11*	*K2*	*CO1*
		OR			
	b) (i)	Showcase phishing and spoofing techniques used in modern cyber threats.	*11*	*K2*	*CO1*
	(ii)	Differentiate between software piracy and cyber terrorism with examples.	*11*	*K2*	*CO1*
24.	a)	Explain the social engineering life cycle and discuss common human-based Social Engineering attacks.	*11*	*K2*	*CO2*
		OR			
	b)	Discuss phishing techniques and suggest ways to mitigate impersonation attacks in enterprises.	*11*	*K2*	*CO2*
25.	a)	Illustrate the methodologies used in OSINT and compare the applications of Maltego and Shodan.	*11*	*K2*	*CO3*
		OR			
	b)	Analyze the application of The Harvester and Shodan in cyber reconnaissance.	*11*	*K2*	*CO3*
26.	a)	Describe the lifecycle of malware and analyze the impact of zero-day exploits with real-world examples.	*11*	*K2*	*CO4*
		OR			
	b)	Compare and contrast the characteristics of viruses, trojans, and worms.	*11*	*K2*	*CO4*
27.	a)	Explain various network scanning methods and discuss the use of vulnerability scanners in security assessments.	*11*	*K2*	*CO5*
		OR			
	b)	Briefly discuss common network vulnerabilities and suggest mitigation strategies.	*11*	*K2*	*CO5*
28.	a)	Identify and evaluate different types of web application attacks with their preventive measures.	*11*	*K2*	*CO6*
		OR			
	b)	Explain Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks with practical examples.	*11*	*K2*	*CO6*