Reg. No.																

Question Paper Code	14027

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 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.	In which type of cyber attack does a criminal use the internet to threaten or harass someone repeatedly? a) Phishing b) Cyber stalking c) Spoofing d) Cyber terrorism	*1*	*K1*	*CO1*
2.	When an attacker modifies the sender’s IP address to impersonate another host, which spoofing is being used? a) DNS spoofing b) IP spoofing c) Email spoofing d) ARP spoofing	*1*	*K1*	*CO1*
3.	Social engineering attacks succeed mostly by manipulating which aspect of individuals? a) Cloud storage b) Network protocols c) Encryption strength d) Human psychology	*1*	*K1*	*CO2*
4.	Name the OSINT tool commonly used to discover exposed servers and IoT devices online. a) Shodan b) Maltego c) The Harvester d) Nmap	*1*	*K1*	*CO2*
5.	Identify the well-known computer worm from the options below. a) ZEUS b) MELISSA c) ILOVEYOU d) CRYPTOLOCKER	*1*	*K1*	*CO3*
6.	Which type of malicious code operates directly within a computer’s memory instead of being stored on the hard drive? a) Trojan b) Ransomware c) Rootkit d) Fileless malware	*1*	*K1*	*CO3*
7.	In Nmap, which scan uses empty TCP packets with no flags set to identify open or closed ports? a) SYN scan b) ACK scan c) NULL scan d) TCP connect	*1*	*K1*	*CO4*
8.	Select the tool that is primarily usedfor detecting system vulnerabilities. a) Nessus b) Photoshop c) Excel d) VMware	*1*	*K1*	*CO4*
9.	Pick the tool that is most suitable for conducting web application security testing. a) Wireshark b) Burp Suite c) Photoshop d) Docker	*1*	*K1*	*CO5*
10.	At what stage of penetration testing are system ports and running applications identified? a) Scanning b) Enumeration c) Reconnaissance d) Reporting	*1*	*K1*	*CO6*

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11.	Classify cyber-attacks based on their target or intent.	*2*	*K2*	*CO1*
12.	Outline the term phishing and state its core purpose.	*2*	*K2*	*CO1*
13.	For what reason do cyber criminals usually direct Quid Pro Quo attacks toward company staff?	*2*	*K2*	*CO2*
14.	List any two popular OSINT tools and mention their primary uses.	*2*	*K2*	*CO2*
15.	Recall the general objectives of malware developers.	*2*	*K1*	*CO3*
16.	State the reasons that make zero-day exploits hard to detect and prevent.	*2*	*K2*	*CO3*
17.	Mention any two common network vulnerabilities that attackers exploit.	*2*	*K1*	*CO4*
18.	Outline the significance of using tools like Nmap in network discovery.	*2*	*K2*	*CO4*
19.	In what ways do web attacks leverage application vulnerabilities?	*2*	*K2*	*CO5*
20.	How does a security misconfiguration increase the risk of web application vulnerabilities?	*2*	*K2*	*CO5*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

21. Given a network testing task, decide whether black-box or white-box testing is more suitable and justify your choice. *2 K2 CO6*

22. Enlist the goals of vulnerability scanning differ from those of penetration testing. *2 K2 CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23. a) Discuss the major types of cybercrimes, citing suitable examples from current incidents. *11 K2 CO1*

OR

b) Explain the working principle of DoS attack. Also, summarize the preventive mechanisms and mitigation strategies against DoS attacks. *11 K2 CO1*

24. a) Demonstrate the common types of social engineering attacks and outline the measures that can be adopted to prevent them. *11 K2 CO2*

OR

b) Outline the sequential stages involved in OSINT methodology and discuss how it aids in detecting and reducing cyber threats. *11 K2 CO2*

25. a) Illustrate the different stages involved in the malware lifecycle and analyze how attackers sustain their control from infection to data exfiltration. *11 K2 CO3*

OR

b) Depict the characteristics and behavioral patterns of various malware types, and review their impact on system performance along with preventive measures. *11 K2 CO3*

26. a) Outline the goals of network scanning and summarize the basic mechanics behind popular scanning methods. *11 K2 CO4*

OR

b) Paraphrase the purpose of Network Enumeration and review the various enumeration techniques with relevant examples. *11 K2 CO4*

27. a) A university portal allows student comments, uses cookie-based authentication, and embeds an external payment widget in an iframe. A security review finds unvalidated comment input, no CSRF tokens on state-changing forms, and the site permits framing by any origin. Identify which browser attacksare possible, give short PoC sketches for each, propose practical server- and client-side fixes with justification, and describe how you would test the remediations. *11 K3 CO5*

OR

b) A web application hosted on a university server is found to be vulnerable due to improper configuration of access permissions and input validation. During penetration testing, attackers exploited directory traversal to access confidential student data and later attempted brute force login attacks on the admin panel. Apply your knowledge of security misconfigurations to analyze the root causes of these vulnerabilities and propose suitable countermeasures to prevent such attacks in real-world deployment. *11 K3 CO5*

28. a) Explain with suitable examples the major causes leading to common network vulnerabilities and analyze their possible consequences. *11 K2 CO6*

OR

b) Summarize the functional principles behind any two well-known network vulnerability scanning tools. *11 K2 CO6*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create