Reg. No.															

Question Paper Code	13520

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

Sixth Semester

Computer Science and Engineering (Cyber Security)

20SCPC604 - PENETRATION TESTING AND ETHICAL HACKING

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	Define the primary use of penetration testing. (a) Software testing (b) Finding vulnerabilities (c) Speed enhancement (d) Data encryption	1	K1	CO1
2.	Label the best description of ethical hacking. (a) Unauthorized access (b) Legal security testing (c) Network disruption (d) Data theft	1	K1	CO1
3.	Select the tool used to perform network discovery and vulnerability scanning. (a) Nmap (b) Maltego (c) Netcat (d) Hydra	1	K1	CO2
4.	Name the open-source tool commonly used for mapping relationships and connections between different entities during information gathering. (a) Maltego (b) Nmap (c) Burp Suite (d) Netcat	1	K1	CO2
5.	Name the port scanning technique commonly used to detect open ports without establishing a full connection: (a) TCP Connect scan (b) UDP scan (c) SYN scan (d) Xmas scan	1	K1	CO3
6.	Fingerprinting is used for: (a) Identifying open ports (b) Detecting services and OS versions (c) Analyzing network topology (d) Mapping DNS records	1	K1	CO3
7.	Define the primary goal of exploiting vulnerabilities in penetration testing. (a) To verify system security weaknesses (b) To permanently damage the target system (c) To delete critical system files (d) To prevent security measures	1	K1	CO4
8.	Choose the purpose of lateral movement. (a) Spread access (b) Remove malware (c) Notify admins (d) Patch issues	1	K1	CO4
9.	Select a key goal of post-exploitation. (a) Lateral movement (b) Blocking users (c) Encrypting data (d) Updating software	1	K1	CO5
10.	Choose the primary goal of a penetration testing report. (a) Communicating vulnerabilities (b) Encrypting system logs (c) Deleting security issues (d) Blocking attackers	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Explain the primary goal of penetration testing.	2	K2	CO1
12.	List any two ethical and legal implications of hacking.	2	K1	CO1
13.	Label two sources used for gathering OSINT about a target system.	2	K1	CO2
14.	Explain the role of Nmap in network scanning during the information gathering phase.	2	K2	CO2
15.	Name the difference between manual and automated enumeration techniques.	2	K1	CO3
16.	Explain the significance of vulnerability scanning in spotting weaknesses in systems.	2	K2	CO3
17.	Name two techniques used to keep access to a hacked system (persistence methods).	2	K1	CO4

18.	Outline how attackers steal (exfiltrate) important data from systems after exploitation.	*2*	*K2*	*CO4*
19.	Point out two serious issues caused by reporting vulnerabilities incorrectly.	*2*	*K1*	*CO5*
20.	Describe two main sections usually found in a penetration testing report.	*2*	*K2*	*CO5*
21.	Classify the major elements typically found in a penetration testing report.	*2*	*K2*	*CO6*
22.	Discuss two key cyber security compliance standards that organizations must follow.	*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the different phases of a penetration test.	*11*	*K2*	*CO1*
		OR			
	b)	Describe the role of social engineering in penetration testing and types of social engineering attacks in detail.	*11*	*K2*	*CO1*
24.	a)	Identify how DNS interrogation helps gather information about a target.	*11*	*K3*	*CO2*
		OR			
	b)	Classify how Google Dorking is used to uncover public sensitive information.	*11*	*K3*	*CO2*
25.	a)	Apply TCP, UDP, and SYN scanning to a sample network and identify which finds open ports more effectively.	*11*	*K3*	*CO3*
		OR			
	b)	Determine the steps involved in service enumeration and list how they help in finding system weaknesses.	*11*	*K3*	*CO3*
26.	a)	Describe how buffer overflow attacks work and their effects on software.	*11*	*K2*	*CO4*
		OR			
	b)	Explain how SQL injection and XSS attacks affect web applications.	*11*	*K2*	*CO4*
27.	a)	Discuss about compliance standards that guide penetration testing, such as GDPR, PCI-DSS, and ISO 27001, and describe how they influence security evaluations.	*11*	*K2*	*CO5*
		OR			
	b)	Detail the steps involved in documenting and reporting findings during penetration testing and justify the value of detailed documentation for cybersecurity.	*11*	*K2*	*CO5*
28.	a)	Summarize the main elements found in a penetration testing report and mention their role in security evaluations.	*11*	*K2*	*CO6*
		OR			
	b)	Describe how security reports assist organizations in recognizing and resolving system weaknesses.	*11*	*K2*	*CO6*