Reg. No.															

Question Paper Code	13485

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

Sixth Semester

Artificial Intelligence and Data Science

(Common to Computer Science and Engineering (AIML))

20AIEL601 - ETHICAL HACKING AND SYSTEM DEFENSE

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 a passive reconnaissance technique used in ethical hacking? (a) Port Scanning (b) Social Engineering (c) Sniffing (d) SQL Injection	1	K1	CO1
2.	Suppose an ethical hacker manipulates an application's input to cause unexpected behavior. What type of attack is this? (a) SQL injection (b) Buffer overflow (c) Cross-site scripting (XSS) (d) Brute force attack	1	K1	CO1
3.	Wireshark is also known as _____ (a) Ethereal (b) Packet Sniffer (c) Etherpeek (d) Ethertop	1	K1	CO2
4.	_____ occurs when an attacker impersonates another device or user on a network. (a) Sniffing (b) Spoofing (c) Phishing (d) Encryption	1	K1	CO2
5.	Which protocol is primarily used to synchronize clocks across computer networks? (a) SNMP (b) FTP (c) NTP (d) LDAP	1	K1	CO3
6.	Lightweight Directory Access Protocol functions over the _____ port to access distributed directory services. (a) TCP port 21 (b) TCP port 80 (c) TCP port 389 (d) TCP port 143	1	K1	CO3
7.	Which of the following refers to a technique for bypassing all security measures to gain unauthorized access to a computer program or an entire computer system? (a) Backdoor (b) Masquerading (c) Phishing (d) Trojan Horse	1	K1	CO4
8.	_____ are the types of scanning. (a) Port, network, and services (b) Network, vulnerability and port (c) Passive, active, and interactive (d) Server, client, and network	1	K1	CO4
9.	Which tool is commonly used for vulnerability scanning and assessment? (a) Nmap (b) Snort (c) Nessus (d) Nikto	1	K1	CO5
10.	_____ is a type of intrusion detection system. (a) Signature-based IDS (b) Password-based IDS (c) Password-based IDS (d) Authentication-based IDS	1	K1	CO6

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	Define SMTP enumeration? Give one example.	2	K1	CO1
12.	Differentiate Threat and Attack.	2	K2	CO1
13.	Assess how hash passwords stored in Microsoft security accounts manager are.	2	K2	CO2
14.	What are the different types of password attacks?	2	K1	CO2
15.	Infer how a SYN scan differs from a FIN scan.	2	K2	CO3
16.	Define TCP three-way handshake with a neat diagram?	2	K1	CO3
17.	List out some vulnerabilities in the Linux Operating System.	2	K1	CO4
18.	What does Zero day Vulnerability mean?	2	K1	CO4

19.	Differentiate between stateful and stateless firewalls.		*2*	*K2*	*CO5*
20.	What does the term Honey Pot mean?		*2*	*K1*	*CO5*
21.	What is the role of firewalls in preventing backdoor attacks?		*2*	*K1*	*CO6*
22.	Interpret the countermeasures against Rootkits with example.		*2*	*K2*	*CO6*

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain phases of ethical hacking in detail with diagram.	*11*	*K2*	*CO1*
		OR			
	b)	Summarize the impact of Social Engineering attack on an organization.	*11*	*K2*	*CO1*
24.	a)	Discuss a solution to store hash passwords in Microsoft security accounts manager. Explain Microsoft authentication mechanism.	*11*	*K2*	*CO2*
		OR			
	b)	Describe in detail about Rootkits and Backdoors with example.	*11*	*K2*	*CO2*
25.	a) (i)	Draw and explain TCP protocol header format.	*6*	*K2*	*CO3*
	(ii)	Demonstrate the use of a port scanning tool (e.g., Nmap) to scan a local network.	*5*	*K2*	*CO3*
		OR			
	b) (i)	Describe the structure, features, and advantages of IPv6.	*6*	*K2*	*CO3*
	(ii)	Explain about Ping Sweeps with fping and hping.	*5*	*K2*	*CO3*
26.	a)	Identify Windows OS Vulnerabilities with real time example.	*11*	*K3*	*CO4*
		OR			
	b)	Construct the case study on Stuxnet.	*11*	*K3*	*CO4*
27.	a)	Explain in detail about risk analysis tools for firewall and routers.	*11*	*K2*	*CO5*
		OR			
	b)	Compare and contrast the advantages and limitations of signature-based and behaviour-based approaches in intrusion detection and prevention system.	*11*	*K2*	*CO5*
28.	a)	Explain the best practices for hardening windows systems in Windows OS Vulnerabilities.	*11*	*K2*	*CO6*
		OR			
	b)	Describe the Intrusion Detection and Prevention systems in detail.	*11*	*K2*	*CO6*