Reg. No.																

Question Paper Code	13036

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2024

Sixth Semester

Artificial Intelligence and Data Science

20AIEL601 - ETHICAL HACKING AND SYSTEM DEFENCE

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (20 × 1 = 20 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	The following tool which performs foot printing undetected is _____ (a) Trace route (b) Ping sweep (c) Whois search (d) Host scanning	1	K1	CO1
2.	_____ is the practice of secretly listening in on conversations in order to gather crucial information. (a)Impersonation (b) Piggybacking (c)Tail gating (d) Eavesdropping	1	K1	CO1
3.	Which is not the Social Engineering Attack? (a) Human based (b) Mobile based (c) Computer based (d) Society based	1	K1	CO1
4.	The other name for Backdoors is _____. (a) Trap doors (b) Front doors (c) Cover doors (d) Back entry	1	K1	CO2
5.	_____ is an attack which is a compiled list of meaningful words, compared against the password field till a match is found (a) Hybrid (b) Dictionary (c) Brute force (d) Password guess	1	K1	CO2
6.	_____ is the dangerous type of rootkit. (a) Library level (b) System level (c) Kernel level (d) Application level	1	K1	CO2
7.	Which protocol is commonly used in a ping sweep? (a) HTTP (b) ICMP (c) TCP (d) UDP	1	K1	CO3
8.	TCP sequence number field is of _____. (a) 8 bit (b) 16 bit (c) 24 bit (d) 32 bit	1	K1	CO3
9.	_____is suitable for IoT devices. (a) IPV4 (b) IPV6 (c) IPV5 (d) IPV2	1	K1	CO3
10.	What is the meaning of the acronym "DoS"? (a) Denial of Service (b) Distribution of Server (c) Distribution of Service (d) Denial of Server	1	K1	CO4
11.	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
12.	What is the main advantage of TCP over UDP? (a) Guaranteed in-order delivery of data. (b) Low latency and overhead. (c) Ability to handle large amounts of data (d) All of the mentioned	1	K1	CO4
13.	Which tool is commonly used for vulnerability scanning and assessment? (a) Nmap (b) Snort (c) Nessus (d) Nikto	1	K1	CO5
14.	A router works in _____. (a) Physical layer (b) Datalink layer (c) Network layer (d) Transport layer	1	K1	CO5
15.	What type of attack involves flooding a network or server with excessive traffic to disrupt its normal operation? (a) DDoS Attack (b) SQL Injection Attack (c)Spoofing Attack (d) Cross-Site Scripting Attack	1	K1	CO5
16.	Desktops and mobile pc come under the category of (a) clients (b) hosts (c)servers (d) none of the mentioned	1	K1	CO5

17.	A security token that generates a one-time password (OTP) used for authentication is known as: (a) Smart card (b) Biometric device (c)Security token (d) Hardware token	*1*	*K1*	*CO6*
18.	Which of the following is a preventive security measure against data loss? (a) Data backup (b) Antivirus software (c) Intrusion Prevention System (d) Virtual Private Network	*1*	*K1*	*CO6*
19.	Which of the following is a system that is created to lure and detect hackers? (a) Honeyd (b) Firewall (c) Honey trap (d) IDS	*1*	*K1*	*CO6*
20.	A honey pot is an example of _____ software. (a) Intrusion-detection (b) Virus (c) Encryption (d) Security-auditing	*1*	*K1*	*CO6*

PART - B (10 × 2 = 20 Marks)

Answer ALL Questions

21.	Define foot printing.	*2*	*K1*	*CO1*
22.	What are the different types of social engineering?	*2*	*K1*	*CO1*
23.	What do you understand by rootkits?	*2*	*K1*	*CO2*
24.	What are different types of Trojans?	*2*	*K1*	*CO2*
25.	Define TCP protocol header format with neat diagram.	*2*	*K1*	*CO3*
26.	Define Scripting.	*2*	*K1*	*CO3*
27.	List out some vulnerabilities in the Windows Operating System.	*2*	*K1*	*CO4*
28.	What is Buffer flow?	*2*	*K1*	*CO4*
29.	What is firewall?	*2*	*K1*	*CO5*
30.	What are the counter measures against the port scanning?	*2*	*K1*	*CO6*

PART - C (6 × 10 = 60 Marks)

Answer ALL Questions

31.	a)	Explain phases of ethical hacking in detail with diagram.	*10*	*K2*	*CO1*
		OR			
	b)	Explain enumeration and its techniques in detail.	*10*	*K2*	*CO1*
32.	a)	Discuss password cracking technique in detail.	*10*	*K2*	*CO2*
		OR			
	b)	Describe the in detail various password-cracking tools.	*10*	*K2*	*CO2*
33.	a)	Explain the TCP Three-way handshake with neat diagram and steps in detail.	*10*	*K2*	*CO3*
		OR			
	b)	What is scanning? List and explain the types of scanning performed.	*10*	*K1*	*CO3*
34.	a)	Discuss in detail about Linux OS Vulnerabilities.	*10*	*K2*	*CO4*
		OR			
	b)	Discuss various tools for identifying vulnerabilities in Windows OS.	*10*	*K2*	*CO4*
35.	a)	Compare and contrast the operation of a traditional router and a modern multi-layer switch.	*10*	*K2*	*CO5*
		OR			
	b)	Explain any attack which you know about penetrating the IDS.	*10*	*K2*	*CO5*
36.	a)	Explain the rootkit in detail along with counter measure.	*10*	*K2*	*CO6*
		OR			
	b)	Explain the effectiveness of Intrusion Detection and Prevention Systems (IDPS) in complementing firewall security.	*10*	*K2*	*CO6*