Reg. No.															

Question Paper Code	12741

B.E. / B.Tech. - DEGREE EXAMINATIONS, APRIL / MAY 2024

Sixth Semester

Artificial Intelligence and Data Science

20AIEL601 - ETHICAL HACKING AND SYSTEM DEFENSE

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (10 × 2 = 20 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	What is the difference between ethical hacking and malicious hacking?	2	K1	CO1
2.	How does social engineering play a role in ethical hacking?	2	K1	CO1
3.	What is foot printing? How is it performed?	2	K1	CO2
4.	List out two password hacking techniques commonly used by hackers.	2	K1	CO2
5.	Define ping sweeps.	2	K1	CO3
6.	Differentiate Rootkits, Trojans and Backdoors.	2	K2	CO3
7.	List out the tools for identifying vulnerabilities in windows.	2	K1	CO4
8.	Describe the concept of port scanning and its significance in ethical hacking.	2	K2	CO4
9.	How does TCP/IP addressing work?	2	K1	CO5
10.	What are honeypots and how are they used in network protection systems?	2	K1	CO5

PART - B (5 × 13 = 65 Marks)

Answer ALL Questions

				Marks	K – Level	CO
11.	a)	i)	Explain the phases involved in ethical hacking and briefly discuss the significance of each phase.	13	K2	CO1
			OR			
	b)	i)	Explain the steps in hacking the server through virtual machine.	8	K2	CO1
		ii)	List out the task where performing a penetration test for a small business. Discuss how you would use scanning and enumeration techniques to identify weaknesses in their network security.	5	K2	CO1
12.	a)		Describe the various techniques used in launching denial of service (DoS) attacks and analyze the potential impact of such attacks on critical infrastructure, such as financial institutions or government agencies. Propose effective mitigation strategies that organizations can implement to minimize the risk of DoS attacks and ensure the continuity of their services in the face of evolving cyber threats.	13	K2	CO2
			OR			

b)	i)	Explain any one password hacking techniques with example.	3	K2	CO2
	ii)	Explain the differences between rootkits, Trojans, backdoors, viruses, worms, and sniffers, and discuss how each of these types of malware can pose significant cyber security threats to both individuals and organizations. Additionally, provide examples of real-world incidents where the deployment of these malicious programs has resulted in severe data breaches or system compromises.	10	K2	CO2
13. a)	i)	Consider a scenario where a network administrator detects unusual port scanning activities on their organization's network. Describe the typical methods employed by attackers when conducting port scanning, and analyze the potential motives behind such activities. Subsequently, propose a comprehensive response plan outlining the steps the administrator should take to investigate, mitigate, and prevent future port scanning incidents, ensuring the security and integrity of the network infrastructure.	9	K2	CO3
	ii)	How do different port scanning tools, such as Nmap, Masscan, and ZMap, vary in their methodologies and capabilities? Compare and contrast their features, including their scanning speed, stealthiness, and ability to detect open ports accurately. Additionally, discuss the implications of selecting a specific port scanning tool based on the security objectives and constraints of an organization.	4	K2	CO3
		OR			
	b)	Explain the fundamental concepts of TCP/IP, including its layered architecture and the functions of each layer. Subsequently, delve into the concept of port scanning within the TCP/IP framework, detailing the significance of ports and the methodologies used by attackers to perform port scans. How does an understanding TCP/IP concept enhance one's ability to detect and respond to port scanning activities effectively?	13	K2	CO3
14.	a)	List and analyze three significant vulnerabilities commonly found in Windows operating systems. Discuss the potential impact of each vulnerability on system security and the broader organizational infrastructure. Furthermore, propose a comprehensive risk mitigation strategy that includes proactive measures to prevent exploitation of these vulnerabilities, as well as reactive steps to address and remediate any successful attacks targeting Windows OS systems.	13	K1	CO4
		OR			
	b)	Discuss in detail about the desktop and server OS vulnerabilities with example.	13	K2	CO4
15. a)	i)	How do penetration testing and ethical hacking contribute to the overall understanding of security vulnerabilities within an enterprise information security program? Explain the differences between these	9	K2	CO5

two approaches and discuss how they complement each other in identifying weaknesses and assessing the resilience of an organization's security infrastructure.

ii) Evaluate the effectiveness of risk analysis tools for firewalls in identifying and prioritizing security risks within an organization's network infrastructure. *4 K5 CO5*

OR

b) i) Compare and contrast the functionalities of routers and firewalls in network protection systems. Explain how routers and firewalls contribute to enhancing network security, and discuss their respective roles in controlling traffic flow, enforcing access policies, and mitigating potential threats. *7 K2 CO5*

ii) Explain the concept of honeypots within the context of network security, including their deployment strategies and the types of attacks they are designed to attract. *6 K2 CO5*

PART - C (1× 15 = 15 Marks)

16. a) Explain in detail a simulated network environment; implement a comprehensive network protection strategy that integrates routers, firewalls, and intrusion detection and prevention systems (IDPS). Outline the configuration settings and rule sets for each component, considering the organization's security requirements and risk analysis findings. Evaluate the efficacy of your network protection system in mitigating common cyber threats, such as denial of service attacks and unauthorized access attempts. *15 K2 CO6*

OR

b) Explain in detailabout utilizing the knowledge gained from the phases of ethical hacking, including footprinting, social engineering, and scanning, design and execute a penetration testing plan targeting a simulated corporate network environment. Detail the steps involved in each phase, from gathering initial information about the network to exploiting identified vulnerabilities, and assess the effectiveness of your approach in uncovering potential security weaknesses. *15 K2 CO6*