C
00G-MAPM5

CNFCCT305062602

Pages: 2

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S5 (S,FE) Examinations June 2026 (2019 Scheme)

Course Code: CCT305
Course Name: SYSTEMS & NETWORK SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

(Answer all questions; each question carries 3 marks) Marks

1		What do you understand by the term attack? Mention the different types of attacks	3
2		Explain the concept of subnetting.	3
3		Explain the protection mechanisms against malcode in a Windows workstation.	3
4		List any four appropriate times when the security posture of a Windows system should be re-evaluated.	3
5		What is meant by Privacy and Security?	3
6		What are the key security measures that a Web-based application dealing with sensitive data must address?	3
7		Explain the practical aspects of digital signatures?	3
8		What are the common device security issues in wireless networks?	3
9		Discuss the major security issues in GPRS.	3
10		What is the purpose of SSL(Secure Socket Layer) Alert Protocol?	3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

11	a)	Explain how the principles of network security contribute to protecting network resources.	7
	b)	Explain the concept of Network Address Translation (NAT) and describe its primary functions.	7
12	a)	Explain the steps involved in the Address Resolution Protocol (ARP) when a host needs to communicate with another host on the same network.	7
	b)	Explain the working of DHCP (Dynamic Host Configuration Protocol) with a neat diagram.	7

Module -2

13	a)	Explain the different types of system upgrades and patches with suitable examples	7
	b)	What measures should be followed to create and maintain secure passwords in Windows systems?	7
14	a)	Explain the process of Linux system hardening and its importance in maintaining system security.	6
	b)	Discuss the best practices for maintaining the physical security of a Linux system. Highlight the importance of backups and operating Linux securely	8

Module -3

15	a)	Define the Domain Name System (DNS) and discuss its significance.	7
	b)	Discuss various techniques of web hacking.	7
16	a)	Explain the working of HTTP with a neat diagram?	7
	b)	Explain the common methods employed by attackers to target users.	7

Module -4

17	a)	Discuss the difference between proprietary and open-source algorithms.	7
	b)	Describe how steganography is used to hide information, giving an example.	7
18	a)	Describe the different types of digital watermarking.	8
	b)	Explain how confidentiality, integrity and availability are related to steganography?	6

Module -5

19	a)	Explain the working of IP Security.	7
	b)	Explain Wireless Transport Layer Security (WTLS) and the features provided by WTLS.	7
20	a)	Compare and contrast the different categories of firewalls	6
	b)	Explain the different phases of penetration testing.	8

***