

Dr. Babasaheb Ambedkar Open University
Term End Examination January – 2026

Course	: MSCCS	Date	: 23/02/2026
Subject Code	: MSCCS-203	Time	: 11:30 am to 01:45 pm
Subject Name	: Application and Network Security	Duration	: 02:15 Hours
		Max. Marks	: 70

Section A

Answer the following (Attempt any three) (30)

1. Explain Operating System Security mechanisms. Discuss access control models, privilege management, and kernel security features.
2. Describe Programming Bugs and Malicious Code. Explain buffer overflow, race condition, logic bombs, viruses, worms, and trojans with suitable examples.
3. Discuss Network Security Models and Network Security Threats. Explain OSI security architecture, common attack vectors, and risk mitigation strategies.
4. Explain Public Key Infrastructure (PKI). Discuss digital certificates, certificate authorities, digital signatures, and key management lifecycle.
5. Explain Wireless Network Security. Discuss security issues in Wi-Fi networks and methods to secure wireless infrastructure.

Section B

Answer the following (Attempt any four) (20)

1. Write a note on Desktop Security and endpoint protection mechanisms.
2. Explain Database Security. Discuss threats such as SQL injection, privilege abuse, and database auditing techniques.
3. Differentiate between Firewall and Intrusion Detection/Prevention Systems.
4. Explain Web Application Security threats and mitigation strategies.
5. Discuss E-Commerce Security requirements and secure transaction mechanisms.
6. Explain Mobile Device Security challenges and countermeasures

Section C

Part – A (Multiple Choice Questions) (10)

- 1 Which of the following is an example of malicious code?
A Compiler B Trojan Horse
C Firewall D Patch
- 2 SQL Injection is primarily a threat to:
A Operating System B Database
C Hardware D Router
- 3 WPA3 is related to:
A Database Security B Wireless Network Security
C Web Browser Security D PKI
- 4 A Firewall mainly operates at which layer?
A Network/Transport Layer B Application Layer only
C Physical Layer D Presentation Layer

- 5 Digital Certificates are issued by:
A Firewall B Intrusion Detection System
C Certificate Authority D Proxy Server
- 6 Buffer overflow is categorized as:
A Cryptographic attack B Programming bug
C Social engineering D Physical attack
- 7 HTTPS provides security using:
A FTP B SSL/TLS
C SNMP D SMTP
- 8 IDS stands for:
A Internal Data Security B Intrusion Detection System
C Internet Data Server D Integrated Defense Solution
- 9 Phishing attacks are commonly associated with:
A E-mail Security B Firewall Configuration
C Disk Partitioning D BIOS
- 10 The main purpose of PKI is to provide:
A Data compression B Authentication and Encryption
C File sharing D Network routing

Part – B (Do as Directed)

(10)

State whether the following statements are true or false

- 1 A worm requires a host file to propagate.
2 A firewall can prevent all types of cyber attacks.
3 Digital signatures provide integrity and non-repudiation.
4 WPA2 is used in wireless network security.
5 SQL injection is a web application attack.
6 IDS can actively block malicious traffic.
7 Public and private keys are identical in asymmetric cryptography.
8 Mobile devices are immune to malware.
9 HTTPS is more secure than HTTP.
10 Desktop security includes antivirus and patch management.
