| Reg. No. | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| Question Paper Code | 14094 |
|---|---|

**B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025**

Third Semester

**Computer Science and Engineering (Cyber security)**

**24SCPC301 - CYBER SECURITY ESSENTIALS**

Regulations - 2024

Duration: 3 Hours | Max. Marks: 100

**PART - A (MCQ) (10 × 1 = 10 Marks)**

Answer ALL Questions

| | | Marks | K – Level | CO |
|---|---|---|---|---|
| 1. | Identify the option that is NOT an example of malware.<br>(a) Trojan horse (b) Worm (c) Phishing (d) Ransomware | 1 | K1 | CO1 |
| 2. | Making sure a system is accessible to authorized users when needed relates to:<br>(a) Confidentiality (b) Integrity (c) Availability (d) Authorization | 1 | K1 | CO1 |
| 3. | Digital certificates are issued by:<br>(a) Certificate Authority (CA) (b) Internet Service Provider (ISP)<br>(c) Firewall vendor (d) Antivirus software | 1 | K1 | CO2 |
| 4. | The main purpose of a digital signature is to:<br>(a) Encrypt the data only (b) Verify authenticity and integrity of a message<br>(c) Compress large files (d) Hide IP addresses | 1 | K1 | CO2 |
| 5. | Identify the OWASP Top 10 vulnerability related to improperly sanitized user input.<br>(a) Insecure Deserialization (b) Injection<br>(c) Broken Access Control (d) Sensitive Data Exposure | 1 | K1 | CO3 |
| 6. | In DevSecOps, security responsibility is:<br>(a) Only with security teams (b) Shared across developers, operations & security<br>(c) Only with developers (d) Only with testers | 1 | K1 | CO3 |
| 7. | Which forensic principle ensures that evidence remains in its original form and is admissible in court?<br>(a) Chain of Custody (b) Root Cause Analysis<br>(c) Threat Hunting (d) Intrusion Detection | 1 | K1 | CO4 |
| 8. | An organization wants to detect brute-force login attempts in real time. Which solution is most appropriate?<br>(a) SIEM log correlation (b) Network scanning with Nmap<br>(c) Packet capture with Wireshark (d) Exploitation with Metasploit | 1 | K1 | CO4 |
| 9. | Which feature of blockchain enhances cybersecurity?<br>(a) Centralized control (b) Immutable ledger<br>(c) Weak authentication (d) Single-point-of-failure | 1 | K1 | CO5 |
| 10. | Select the correct set of core functions in the NIST Cybersecurity Framework.<br>(a) Identify, Protect, Detect, Respond, Recover (b) Plan, Do, Check, Act<br>(c) Confidentiality, Integrity, Availability (d) Monitor, Backup, Restore, Audit | 1 | K1 | CO6 |

**PART - B (12 × 2 = 24 Marks)**

Answer ALL Questions

| | | Marks | K – Level | CO |
|---|---|---|---|---|
| 11. | Compare ransomware and phishing attacks. | 2 | K2 | CO1 |
| 12. | What is a cybersecurity policy? Give two examples of cyber security policies in organizations. | 2 | K1 | CO1 |
| 13. | Give examples for symmetric and asymmetric key algorithms. | 2 | K2 | CO2 |
| 14. | Outline what is firewall and what is PKI. | 2 | K1 | CO2 |
| 15. | Differentiate between static and dynamic code analysis. | 2 | K2 | CO3 |
| 16. | Infer what does “shifting security left” mean in Secure SDLC. | 2 | K2 | CO3 |
| 17. | Interpret the two types of scans supported by Nmap. | 2 | K2 | CO4 |

| | | | | | |
|---|---|---|---|---|---|
| 18. | Illustrate the primary function of Meta sploit. | 2 | K2 | CO4 |
| 19. | Interpret what is the main role of AI in cybersecurity. | 2 | K2 | CO5 |
| 20. | Outline why is strong authentication important in IoT security? State one best practice for securing IoT devices. | 2 | K2 | CO5 |
| 21. | What does GDPR stand for, and where is it applicable? Mention two individual rights under GDPR. | 2 | K1 | CO6 |
| 22. | Classify the purpose of PCI DSS? Mention any two PCI DSS requirements. | 2 | K2 | CO6 |

**PART - C (6 × 11 = 66 Marks)**

Answer ALL Questions

| | | | | | | |
|---|---|---|---|---|---|---|
| 23. | a) | Apply the concept of the CIA Triad to a real-world cyber security scenario and illustrate how each component (Confidentiality, Integrity and Availability) is implemented. | 11 | K3 | CO1 |
| | | **OR** | | | |
| | b) | Identify different types of vulnerabilities in a university network system. Apply appropriate security measures to reduce the risk of cyber threats exploiting these weaknesses. | 11 | K3 | CO1 |
| 24. | a) | Illustrate the application of cryptographic techniques with suitable real-life examples. | 11 | K3 | CO2 |
| | | **OR** | | | |
| | b) | Implement the steps involved in creating a digital signature for document verification. | 11 | K3 | CO2 |
| 25. | a) | Analyze how DevSecOps practices improve collaboration between developers and security teams, ensuring continuous security in the development pipeline. | 11 | K4 | CO3 |
| | | **OR** | | | |
| | b) | Evaluate the relationship between code analysis techniques and secure coding practices, highlighting how static and dynamic analyses complement each other. | 11 | K4 | CO3 |
| 26. | a) (i) | Use Wireshark to capture and inspect network packets for suspicious activity. | 5 | K3 | CO4 |
| | (ii) | Apply packet analysis techniques to detect and prevent potential network intrusions. | 6 | K3 | CO4 |
| | | **OR** | | | |
| | b) (i) | Identify and outline the key stages of an ethical hacking penetration test. | 5 | K3 | CO4 |
| | (ii) | Demonstrate how each stage helps evaluate the organization's overall security posture. | 6 | K3 | CO4 |
| 27. | a) | Investigate the reasons why AI systems are often better at identifying zero-day attacks than manual threat detection methods. | 11 | K4 | CO5 |
| | | **OR** | | | |
| | b) | Categorize the cybersecurity applications of block chain under three areas: identity management, data integrity, and secure transactions, and explain how each benefits from block chain properties. | 11 | K4 | CO5 |
| 28. | a) | Apply the principles of the NIST Cyber security Framework on a ransom ware-affected university network to showcase how it assists in prevention, response, and recovery. | 11 | K3 | CO6 |
| | | **OR** | | | |
| | b) | Evaluate how the enforcement of GDPR principles strengthens individual rights and influences corporate data protection policies. | 11 | K3 | CO6 |