

Section A

Q.-1. Respond to any three of the following questions in brief. (30)

- (1) What is an Advanced Persistent Threat (APT)? Discuss its intentions, common threat vectors, and defending strategies.
- (2) Detail the offences and corresponding penalties prescribed under the Indian Information Technology Act, 2000 (Sections 65 to 71).
- (3) Explain the components and working of a Public Key Infrastructure (PKI), including the roles of the Certificate Authority and Registration Authority.
- (4) Explain the NIST Cybersecurity Framework, detailing its five core functions and how organizations can use it to manage risk.
- (5) Classify and describe cybercrimes against individuals, property, organizations, and society as outlined in the sources.

Section B

Q.-2. Write short notes on any four of the following topics. (20)

- (1) Explain the "Persistent" nature of an Advanced Persistent Threat (APT).
- (2) Briefly describe the "Plan-Do-Check-Act" (PDCA) model used in ISO/IEC 27001.
- (3) Define the "Chain of Custody" and why it is vital for digital evidence in court.
- (4) Differentiate between a Network Intrusion Detection System (NIDS) and a Host-based one (HIDS).
- (5) What are the four general classes of Cybercrime?
(1) (2) Explain the concept of "Nonrepudiation" in digital transactions.

Section C

Q.-3. Tick (✓) the correct alternative (10)

(1) What is the security property that provides proof of delivery and identity so neither party can deny processing the data?

- | | |
|------------------|-------------------|
| A) Authorization | B) Nonrepudiation |
| C) Integrity | D) Availability |

(2) Which type of attack involves the attacker intercepting information but with the intent of only reading it and not modifying it?

- | | |
|------------------|-------------------|
| A) Active Attack | B) Passive Attack |
| C) Masquerade | D) Replay Attack |

(3) In Linux iptables, which chain is used for packets that are neither destined for nor originate from the host computer, but are routed by it?

- | | |
|------------|---------------|
| A) INPUT | B) OUTPUT |
| C) FORWARD | D) PREROUTING |

(4) Which SELinux mode prints warnings but does not actually enforce the security policy?

- | | |
|--------------|---------------|
| A) Enforcing | B) Permissive |
| C) Disabled | D) Targeted |

(5) Which W3AF plugin type is specifically used to find URLs where injection points occur?

- | | |
|------------------|-----------------|
| A) Audit plugin | B) Crawl plugin |
| C) Attack plugin | D) Grep plugin |

(6) Which security level in the Damn Vulnerable Web App (DVWA) is used to compare vulnerable code with secure source code?

- A) Low
- B) Medium
- C) High
- D) Impossible

(7) What is the process of extracting knowledge or design information from a man-made object to reproduce it?

- A) Web Scraping
- B) Reverse Engineering
- C) Social Engineering
- D) Data Mining

(8) In the Indian IT Act 2000, which section covers the offence of hacking with a computer system and provides for up to 3 years imprisonment?

- A) Section 65
- B) Section 66
- C) Section 67
- D) Section 68

(9) What is the term for the chronological documentation of electronic evidence, including its collection and transfer, to maintain its integrity?

- A) Digital Forensics
- B) Metadata
- C) Chain of Custody
- D) Hash Analysis

(10) Which type of analysis examines the malware binary without actually running it to achieve larger code coverage?

- A) Static Analysis
- B) Dynamic Analysis
- C) Behavioral Analysis
- D) Forensic Analysis

Section D

Q.-4. State whether the following statements are true or false (10)

- (1) Integrity refers to ensuring that stored data is accurate and has not undergone unauthorized modifications.
- (2) The MD5 algorithm processes data in 512-bit blocks and produces a 128-bit message digest.
- (3) Spearphishing is a phishing attack specifically targeted at individuals within a particular organization.
- (4) Unlike viruses, Trojans are designed to be self-replicating programs.
- (5) Ransomware typically uses cryptoviral extortion and demands payment in bitcoin for file recovery.
- (6) A Zero-Day Exploit occurs after a vulnerability is announced but before a patch is implemented.
- (7) The Cyber Kill Chain consists of seven technical phases, beginning with Reconnaissance.
- (8) Packet filtering firewalls are considered "stateful" because they monitor the entire history of a connection.
- (9) Intrusion Detection Systems (IDS) are designed to automatically block malicious traffic as their primary function.
- (10) WEP encryption uses a 24-bit pseudo-random number known as an Initialization Vector (IV).
