

Term End Examination January – 2026

Course	: BSCCS	Date	: 25/02/2026
Subject Code	: BSCCS-304	Time	: 11:30am to 01:45pm
Subject Name	: Principles of Cyber Security	Duration	: 02.15 Hours
		Max. Marks	: 70

Section A

Answer the following (Attempt any three) (30)

1. Explain the CIA Triad (Confidentiality, Integrity, and Availability) in detail. How do these three pillars serve as the foundation for information security?
2. Compare and contrast Packet Filtering, Stateful Packet Inspection, and Application Level Gateways. Which one is considered most secure and why?
3. Discuss the workflow of the W3AF (Web Application Attack and Audit Framework). Explain the specific roles of its Crawl, Audit, and Attack plugins.
4. Define Cybercrime and explain its classification into four major categories: crimes against individuals, property, organizations, and society.
5. Explain the concept of the Cyber Kill Chain. Detail all seven technical phases from Reconnaissance to Actions on Objective.

Section B

Answer the following (Attempt any four) (20)

1. List and briefly describe at least three key initiatives launched by the Government of India to create a safe cyber ecosystem (e.g., NCCC, CERT-In, NCIIPC).
2. Explain the three main iptables chains (INPUT, OUTPUT, and FORWARD) used in a Linux firewall and describe the purpose of each.
3. What is a Man-in-the-Middle (MitM) attack in a wireless network? Describe the steps an attacker takes to set up a rogue access point.
4. Define SQL Injection. Provide a sample malicious query and list two methods used to prevent such attacks in web applications.
5. Differentiate between Static Analysis and Dynamic Analysis in the context of malware forensics.
6. Explain the "Rights of Ownership" as defined under Intellectual Property Law in the cyber world.

Section C

Part – A (Multiple Choice Questions) (10)

- Which property ensures that information is not denied later by the sender?
A Integrity
B Non-repudiation
C Availability
D Authentication
- The National Critical Information Infrastructure Protection Center (NCIIPC) was created under which section of the IT Act?
A Section 66
B Section 70A
C Section 43
D Section 67
- Which type of firewall is considered "stateless"?
A Packet Filter
B Proxy Server
C Stateful Inspection
D Circuit Level

- 4 In the Linux filesystem, which partition is similar to the C:/ drive in Windows?
A home B etc
C root D bin
- 5 Which 802.11 standard operates at a frequency of 5 GHz and provides speeds up to 1.3 Gbps?
A 802.11b B 802.11g
C 802.11n D 802.11ac
- 6 The tool used to find insecure files and programs specifically on a web server is:
A Nikto B John the Ripper
C Hydra D Snort
- 7 Which NIST Cyber security Framework function enables the "timely discovery" of events?
A Protect B Detect
C Respond D Recover
- 8 Which malware is a self-contained program that propagates across networks without needing to attach to a host file?
A Virus B Worm
C Trojan D Logic Bomb
- 9 Which port is used by default for SSH traffic?
A 80 B 443
C 22 D 21
- 10 The 2008 amendment to the Indian IT Act primarily focused on:
A Digital Signatures B Cybercrimes and Electronic Devices
C E-Commerce D Intellectual Property

Part – B (Do as Directed)

(10)

State whether the following statements are true or false

- 1 Encryption is used in APTs to bypass security devices that cannot read encrypted payloads.
- 2 A Trojan horse has the ability to self-replicate just like a computer virus.
- 3 The "Plan-Do-Check-Act" (PDCA) model is used to construct and set up ISMS processes.
- 4 WEP is a wireless security protocol that stands for Wired Equivalent Privacy.
- 5 Symmetric encryption uses two different keys (public and private) for data transmission.
- 6 HIPAA Title 2 is known as Administrative Simplification and deals with electronic healthcare standards.
- 7 A "Zero-Day Exploit" occurs before a patch or solution is implemented for a known vulnerability.
- 8 Digital signatures have no legal validity under the Indian IT Act, 2000.
- 9 SELinux operates in three modes: Enforcing, Permissive, and Disabled.
- 10 The "Salami Attack" involves collecting small increments of money over time to avoid detection
