R4634

Sub. Code
25MCF2C1

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Second Semester

Cyber Forensics

OPERATING SYSTEM FOR CYBER SPACE

(CBCS – 2025 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct option.

1. Which component starts the OS during system booting (CO1, K2)

   (a) Complier (b) Kernel

   (c) Loader (d) Shell

2. Device drivers are mainly used to : (CO1, K1)

   (a) Compile programs (b) Control I/O devices

   (c) Manage memory (d) Create files

3. Message –oriented communication transfer data as : (CO2, K1)

   (a) Streams (b) Files

   (c) Message (d) Signals

4. Communication between processes is knows as :(CO2, K2)

(a) IPC

(b) DMA

(c) Paging

(d) Scheduling

5. NTP is mainly used for (CO3, K2)

(a) Process scheduling

(b) Memory allocation

(c) Time Synchronization

(d) File sharing

6. Why is clock synchronization difficult in distributed system? (CO3, K1)

(a) Limited storage

(b) Network delays

(c) CPU speed

(d) File Size

7. Memory coherence ensures that : (CO4, K2)

(a) All CPUs run at same speed

(b) Multiple copies of data remain consistent

(c) Memory is encrypted

(d) Data is compressed

8. Security is critical in distributed systems because: (CO4, K1)

(a) Systems are expensive

(b) Resources are shared over networks

(c) Memory is limited

(d) CPU are slow

9. IP tables in Linux are used for: (CO5, K2)

(a) File management

(b) User authentication

(c) Firewall configuration

(d) Process scheduling

10. GNU Privacy Guard (GPG) is used for : (CO5, K1)

(a) Network monitoring

(b) Data encryption

(c) Memory management

(d) Disk partitioning

Part B (5 × 5 = 25)

Answer **all** questions not more than 500 words each.

11. (a) Describe the booting process of an operating system step by step. (CO1, K3)

Or

(b) Discuss the role of command – line operation in managing files and directories. (CO1, K4)

12. (a) Describe the working of Remote Procedure Call (RPC) in a distributed environment. (CO2, K3)

Or

(b) Evaluate, the challenges involved in inter-process communication in distributed systems. (CO2, K5)

13. (a) Describe Lamport logical clocks and explain how they help in event ordering. (CO3, K4)

Or

(b) Evaluate the limitations of clock synchronization methods. (CO3, K5)

14. (a) Describe access control models used to protect distributed operating systems. (CO4, K4)

Or

(b) Evaluate the importance of security mechanism is distributed operating systems. (CO4, K5)

15. (a) Analyze the role of IP tables in securing Linux-based servers. (CO5, K5)

Or

(b) Evaluate the use of SSL and Open SSL in securing network communication. (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** questions not more than 1000 words each.

16. (a) Evaluate the difference between client operating systems an server operating systems with respect to functionality and use cases. (CO1, K5)

Or

(b) Design a basic operating system architecture showing interactions between kernel, Device drivers, and user interface. (CO1, K6)

17. (a) Evaluate message-oriented and stream-oriented communication models in distributed systems. (CO2, K5)

Or

(b) Design a communication model for inter-process communication in a distributed environment highlighting blocking and non-blocking modes. (CO2, K6)

18. (a) Evaluate the effectiveness of Network Time protocol (NTP) in large-scale distributed systems. (CO3, K5)

Or

(b) Constructs an event-ordering mechanism using Lamport and vector clocks for a distributed application (CO3, K4)

19. (a) Evaluate different security threats and external attacks in distributed operating systems. (CO4, K5)

Or

(b) Design a secure distributed operating system model incorporating authentication. authorization, and access control mechanism. (CO4, K4)

20. (a) Evaluate the role of IP tables and cryptographic services in protecting Linux – based systems. (CO5, K5)

Or

(b) Design a secure communication framework using SSL, Open SSL, and GNU Privacy Guard in an open – source environment (CO5, K6)

———————

R4635

Sub. Code
25MCF2C2

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Second Semester

Cyber Forensics

E GOVERNANCE & SECURITY

(CBCS – 2025 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the objective questions by choosing the correct option.

1. E-Governance primarily aims at: (CO1, K1)

   (a) Increasing governance revenue

   (b) Improving governance through ICT

   (c) Replacing government employees

   (d) Privatizing public services.

2. Government to Citizen (G2C) interaction mainly focuses on: (CO1, K2)

   (a) Internal administration

   (b) Business regulations

   (c) Service delivery to citizens

   (d) Inter-department communication

3. Which platform enables citizen participation in policy making? (CO2, K2)

(a) DigiLocker (b) MyGov

(c) e-Hospital (d) e-Courts

4. AEPS stands for : (CO2, K1)

(a) Aadhaar Enabled Payment System

(b) Advanced Electronic Payment Service

(c) Automated Electric Processing System

(d) Aadhaar Encrypted Payment Software

5. Blockchain in e-Governance mainly ensures. (CO3, K1)

(a) High Speed computation

(b) Transparency and immutability

(c) Reduced hardware cost

(d) Better graphics

6. Cloud computing in e-Governance helps in: (CO3, K2)

(a) Increasing paperwork

(b) Centralized data storage and scalability

(c) Reducing internet access

(d) Manual service delivery

7. Which is a major social challenge of e-Governance? (CO4, K1)

(a) High bandwidth

(b) Digital divide

(c) Server virtualization

(d) Cloud migration

8. Language barrier in e-Governance affects : (CO4, K2)

(a) Network Security (b) User accessibility

(c) Data encryption (d) Hardware performance

9. The UN e-Government Survey evaluates countries based on : (CO5, K1)

(a) Military strength

(b) Economic growth

(c) e-Governance development

(d) Population size

10. OSI in e-Governance ranking stands for : (CO5, K1)

(a) Online Service Index

(b) Online System Interface

(c) Organizational Security Index

(d) Online Security Infrastruture

Part B (5 × 5 = 25)

Answer **all** questions not more than 500 words each.

11. (a) Define e-Governance. Explain its objectives and goals with suitable example. (CO1, K3)

Or

(b) Describe the different types of interaction in e-Governance (G2C, G2B, G2G, G2E). (CO1, K4)

12. (a) List and explain the major components of the Digital India programme. (CO2, K4)

Or

(b) Explain the role of MyGov platform and Aadhaar Enabled Payment System (AEPS) in e-Governance. (CO2, K3)

13. (a) Define Cloud Computing and Blockchain technology in the context of e-Governance (CO3, K4)

Or

(b) Explain the concept and vision of India Enterprise Architecture (INDEA), (CO3, K5)

14. (a) List the major technical, social, and economic challenge of e-Governance in India. (CO4, K4)

Or

(b) Explain the role of privacy, security, and authentication in e-Governance applications. (CO4, K5)

15. (a) Discuss about the UN Government Survey? Mention its major indices. (CO5, K4)

Or

(b) Explain India's Position in global e-Governance ranking with reference to OSI and TII. (CO5, K4)

Part C (5 × 8 = 40)

Answer **all** questions not more than 1,000 words each.

16. (a) Critically evaluate the relevance of e-Governance theories such as Smog Theory, Kytoon Theory, Virga Theory, and Rainbow Theory in achieving good governance. (CO1, K5)

Or

(b) Analyze the advantages and disadvantages of e-Governance and examine its impact on urban and rural governance. (CO1, K4)

17. (a) Evaluate the effectiveness of major national e-Governance programs such as e-Kranti and Information for All in strengthening digital governance in India. (CO2, K5)

Or

(b) Analyze the different models of e-Governance including Broadcasting Model. Comparative Analysis Model, Critical Flow Model, and interactive Service Model. (CO2, K4)

18. (a) Critically evaluate the structure and reference models of INDEA and their importance for building a unified e-Governance architecture in India. (CO3, K5)

Or

(b) Illustrate how smart e-Government platforms use information technology to improve efficiency, transparency, and service delivery. (CO3, K4)

19. (a) Evaluate the effectiveness of capacity-building initiatives and IT Security audits in overcoming e-Governance challenges in Tamil Nadu. (CO4, K5)

Or

(b) Discuss the opportunities of e-Governance in Tamil Nadu with reference to initiatives such as e-Sevai and Tamil Nadu Blockchain Backbone.

(CO4, K5)

20. (a) Suggest suitable measure for improving India's e-Governance performance based on international best practices and global rankings. (CO5, K6)

Or

(b) Evaluate the e-Governance practices of any two leading countries such as Denmark, Singapore, South Korea, or Finland. (CO5, K5)

———————

R4636

Sub. Code
25MCF2C3

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Second Semester

Cyber Forensics

CYBER CRIME & INVESTIGATION

(CBCS – 2025 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective questions by choosing the correct option.

1. Which characteristic makes computer crime different from traditional crime? (CO1, K2)

   (a) Physical violence

   (b) Geographical boundaries

   (c) Requirement of weapons

   (d) Need for witnesses

2. Which of the following is NOT a type of computer crime? (CO1, K1)

   (a) Malware attack

   (b) Identity theft

   (c) Cyber stalking

   (d) Tax evasion without technology

3. Which of the following is the role of a cyber forensic expert during prosecution? (CO2, K2)

(a) Conduct interrogation

(b) Pronounce judgment

(c) Interpret digital evidence and submit expert opinion

(d) Register FIR

4. Before testifying in court, a cyber investigator should (CO2, K I)

(a) Review reports and evidence thoroughly

(b) Memorize the case

(c) Contact the accused

(d) Discuss case details publicly

5. Intercepting Wi-Fi transmissions without authorization primarily violates (CO3, K1)

(a) Hardware policies

(b) Backup procedures

(c) Privacy and communication laws

(d) Software licensing rules

6. Which factor makes Wi-Fi interception legally sensitive? (CO3, K3)

(a) High bandwidth

(b) Open-source protocols

(c) Limited range

(d) Presence of personal and private data

7. Mobile forensics mainly deals with (CO4, K2)

(a) Network traffic analysis

(b) Recovery of deleted files from hard disks

(c) Extraction and analysis of data from mobile devices

(d) Email header analysis

8. IMEI number is used to identify (CO4, K1)

(a) SIM card

(b) Mobile device

(c) Mobile network

(d) Mobile application

9. A forensic investigator finds deleted transaction records on a suspect's laptop. Which tool category is most useful? (CO5, K4)

(a) Network monitoring tools

(b) Password cracking tools

(c) Data recovery tools

(d) Encryption tools

10. The primary objective of financial fraud investigation is to (CO5, K2)

(a) Arrest the suspect immediately

(b) Recover lost money only

(c) Establish motive and opportunity

(d) Trace money trail and collect admissible evidence

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Define computer crime and explain its major characteristics. (CO1, K3)

Or

(b) Discuss the social and economic consequences of computer crimes. (CO1, K5)

12. (a) Explain the chain of custody process and its importance in ensuring evidence admissibility in court. (CO2, K2)

Or

(b) Illustrate the process of preparing a cybercrime case for prosecution, highlighting the responsibilities of cyber investigators. (CO2, K4)

13. (a) Explain the legal permissions required before intercepting wireless communications. (CO3, K4)

Or

(b) Illustrate how live forensic techniques are used in investigating a Wi-Fi-based security incident. (CO3, K3)

14. (a) Define mobile forensics and list out main steps involved in a typical mobile device forensic investigation process. (CO4, K2)

Or

(b) Analyze the challenges faced in Mobile forensics. (CO4, K4)

15. (a) Write down the steps carried out through investigation of financial frauds. (CO5, K3)

Or

(b) A suspect uses multiple SIM cards and mobile devices to conduct UPI fraud across different states. Analyze why such methods are used by fraudsters. List key mobile forensic artifacts useful in investigation. (CO5, K6)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Discuss about different types of computer crimes with suitable examples. (CO1, K5)

Or

(b) Design a comprehensive plan for handling an identity fraud case using CF techniques. (CO1, K6)

17. (a) Analyze the roles and responsibilities of cyber investigative professionals in cyber crime cases. (CO2, K4)

Or

(b) Evaluate the common challenges that can weaken a cyber crime case during prosecution. (CO2, K5)

18. (a) Demonstrate how live forensic tools can be used during a Wi-Fi-based cyber incident. (CO3, K3)

Or

(b) Explain the concept of incident response and its significance in cyber crime investigations. (CO3, K4)

19. (a) Illustrate how mobile forensic techniques are applied in a real cybercrime investigation. (CO4, K3)

Or

(b) Summarize in detail about Communication device-based investigation. (CO4, K5)

20. (a) A small business owner receives a phone call claiming to be from the bank's KYC department. Shortly after sharing details, multiple UPI transactions are made to unknown accounts.

(i) Identify the cybercrime and fraud technique used.

(ii) Analyze how social engineering enabled the fraud.

(iii) List the immediate steps an investigator should take after receiving the complaint. (CO5, K4)

Or

(b) Summarize in detail about Phishing and Ransomware. (CO5, K5)

———————

R4637	Sub. Code 25MCF2E1

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Second Semester

Cyber Forensics

Elective : IoT SECURITY

(CBCS – 2025 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the objective type questions by choosing the correct option.

1. In the IoT threat landscape, why are 'botnets' like Mirai considered a significant challenge? (CO1, K2)
   (a) They physically destroy the devices hardware sensors.
   (b) They exploit weak default credentials in millions of constrained devices to launch massive DDoS attacks.
   (c) They encrypt local user files to demand a ransom payment.
   (d) They replace the devices Wi-Fi chip with a malicious one.

2. What is a defining characteristic of Cyber-Physical Systems (CPS) that distinguishes them from basic IT systems? (CO1, K1)
   (a) A lack of connectivity to the public internet.
   (b) The exclusive use of wired fiber-optic connections.
   (c) The seamless integration of computational algorithms and physical components through a feedback loop.
   (d) The requirement for high-power desktop processors.

3. Why is the MQTT protocol often considered vulnerable if not implemented with TLS? (CO2, K2)

(a) It lacks a centralized broker, making identity verification impossible.

(b) It transmits data, including credentials, in plain text by default.

(c) It uses a request-response model that is easily blocked by firewalls.

(d) It requires high computational power that causes devices to crash.

4. What is the primary function of a 'Hardware Trojan' in an IoT integrated circuit? (CO2, K2)

(a) To encrypt data before it reaches the main CPU.

(b) To speed up the processor's clock cycle for better performance.

(c) To act as a physical shield against electromagnetic interference.

(d) To provide a covert channel for data leakage or to disable the device remotely.

5. How does Blockchain technology improve 'Identity Management' in an IoT ecosystem? (CO3, K1)

(a) By providing a decentralized, immutable ledger that removes the need for a central trusted authority.

(b) By centralizing all device identities in a single government-managed database.

(c) By physically hardening the hardware sensors against theft.

(d) By automatically generating passwords that are impossible for humans to read.

6. In the context of 'Secure Communication Protocols', what is a major benefit of using DTLS (Datagram Transport Layer Security) for IoT? (CO3, K2)

(a) It provides TLS-like security over UDP, which is the preferred transport for many constrained IoT devices.

(b) It eliminates the need for any hardware sensors.

(c) It makes the network speed ten times faster than standard internet.

(d) It allows devices to communicate without any wireless signal.

7. Which forensic domain deals with evidence from smart appliances such as smart locks, cameras and thermostats? (CO4, K1)

(a) Network forensics

(b) Mobile forensics

(c) Smart Home forensics

(d) Cloud forensics

8. Which of the following is a key legal and ethical concern in IoT forensics? (CO4, K2)

(a) Battery life of devices

(b) Device interoperability

(c) Network bandwidth

(d) User privacy and data ownership

9. What is the core principle of Zero Trust Architecture in IoT networks? (CO5, K2)

(a) Trust all internal devices

(b) Trust devices based on location

(c) Never trust, always verify

(d) Trust only cloud services

10. Which of the following techniques is used for privacy preservation in IoT systems? (CO5, K1)

(a) Data duplication

(b) Differential privacy

(c) Packet flooding

(d) Plaintext data transmission

Part B (5 × 5 = 25)

Answer **all** questions not more than 500 words each.

11. (a) Discuss the IoT threat landscape and how it affects consumer privacy. (CO1, K4)

Or

(b) Elaborate on the role of the Network Layer in IoT and its specific vulnerabilities. (CO1, K4)

12. (a) Describe the impact of ransomware on IoT-enabled critical infrastructure. (CO2, K3)

Or

(b) Explain the concept of "Device Vulnerabilities" in the context of resource-constrained hardware. (CO2, K4)

13. (a) Discuss how Secure Communication Protocols (like DTLS) protect data in transit. (CO3, K4)

Or

(b) Explain the role of Attribute-Based Access Control (ABAC) in managing IoT device permissions. (CO3, K5)

14. (a) Discuss the ethical considerations a forensic investigator must handle regarding user privacy in IoT data. (CO4, K4)

Or

(b) Explain the difference between cloud-based IoT forensics amid device-level forensics. (CO4, K3)

15. (a) Discuss the importance of Differential Privacy in protecting IoT data analytics. (CO5, K4)

Or

(b) Explain the concept of "Resilient IoT Systems" and how they differ from "Secure IoT Systems." (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** questions not more than 1000 words each.

16. (a) Analyze two major case studies of IoT breaches. What were the vulnerabilities and what was the impact? (CO1, K4)

Or

(b) Evaluate how the scale and heterogeneity of IoT devices contribute to the overall security risk of a smart city. (CO1, K5)

17. (a) Discuss the lifecycle of a Hardware Trojan, from insertion to activation and its consequences for IoT security. (CO2, K5)

Or

(b) Develop a threat model for a connected industrial environment (IIoT) identifying potential attack vectors and surfaces. (CO2, K4)

18. (a) Discuss the challenges and solutions for managing the identity of billions of heterogeneous IoT devices. (CO3, K5)

Or

(b) Analyze how various access control models can be implemented to prevent unauthorized physical and logical access to IoT gateways. (CO3, K5)

19. (a) Compare the forensic techniques used for Smart Home hubs versus those used for fitness trackers (Wearables). (CO4, K4)

Or

(b) Evaluate the current state of IoT forensic tools and identify the gaps that need to be addressed by future research. (CO4, K4)

20. (a) Discuss various privacy-preserving mechanisms (e.g.. Homomorphic Encryption, Kanonymity) and their feasibility in resource-constrained IoT. (CO5, K5)

Or

(b) Explore the future of IoT security: How will the shift toward Edge Computing change the way we detect and respond to threats? (CO5, K6)

———————

R4638

Sub. Code
25MCF2S1

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Second Semester

Cyber Forensics

EMBEDDED PROGRAMMING

(CBCS – 2025 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective type questions by choosing the correct option.

1. Which of the following is an external peripheral in an embedded system? (CO1, K2)

   (a) CPU core

   (b) GPIO controller

   (c) Cache memory

   (d) ALU

2. The memory map of an embedded system shows(CO1, K3)

   (a) Physical layout of memory chips

   (b) Software flow execution

   (c) Logical addressing of memory and peripherals

   (d) Power connections of the board

3. The function ledInit() is typically responsible for (CO2, K1)

(a) Turning the LED ON continuously

(b) Initializing GPIO pins connected to the LED

(c) Creating delay loops

(d) Handling interrupts

4. Which stage of the build process converts source code into object code? (CO2, K2)

(a) Loading (b) Locating

(c) Linking (d) Compiling

5. How does Direct Memory Access reduce CPU overhead? (CO3, K3)

(a) By allowing hardware peripherals to transfer data directly to memory without CPU intervention

(b) By simulating the hardware environment using an emulator

(c) By automatically fixing Endianness issues during transfer

(d) By increasing the clock speed of the processor

6. Which of the following problems is caused by endian mismatch? (CO3, K2)

(a) Memory overflow

(b) Slower execution

(c) Power failure

(d) Incorrect data interpretation

7. The main purpose of an Interrupt Service Routine is to (CO4, K1)

(a) Schedule tasks

(b) Handle an interrupt event quickly

(c) Manage memory

(d) Execute background tasks

8. Which of the following is NOT a function of an Operating System? (CO4, K2)

(a) Memory management

(b) Interrupt handling

(c) Direct hardware design

(d) Task scheduling

9. Which design approach is most critical for successful Big Data UI development? (CO5, K2)

(a) Hardware-centric design

(b) Code-first design

(c) Network-driven design

(d) User-centered design

10. Medical software systems must strictly follow regulations mainly to ensure (CO5, K1)

(a) Safety, privacy and reliability

(b) Better graphics

(c) Market competition

(d) Faster development

Part B (5 × 5 = 25)

Answer **all** the questions not more than 500 words each.

11. (a) Examine the PXA255 XScale Processor architecture. (CO1, K5)

Or

(b) Explain the concept of a Memory Map. (CO1, K2)

12. (a) Differentiate between compiling and linking stages in the embedded build process. (CO2, K4)

Or

(b) Illustrate in detail about delayms() function. (CO2, K3)

13. (a) Explain the steps involved in downloading a blinking LED program onto a target embedded system. (CO3, K4)

Or

(b) Differentiate between big-endian and little-endian memory representation. (CO3, K5)

14. (a) Discuss about interrupt Service Routine. (CO4, K4)

Or

(b) Explain the need for task synchronization in multitasking systems. (CO4, K3)

15. (a) How can data visualization techniques improve usability in a Big Data platform UI? (CO5, K3)

Or

(b) List out some business opportunities enabled by advancements in SpaceTech. (CO5, K5)

Part C (5 × 8 = 40)

Answer **all** the questions not more than 1000 words each.

16. (a) Describe the life of an embedded software developer. (CO1, K5)

Or

(b) Explain the various requirements that affect embedded system design choices. (CO1, K4)

17. (a) Explain the structure of a blinking LED program with suitable pseudo code. (CO2, K3)

Or

(b) Evaluate the importance of the infinite loop in embedded applications. (CO2, K5)

18. (a) Discuss in detail about the Usage of Flash Memory. (CO3, K3)

Or

(b) Examine various memory testing techniques used in embedded systems. (CO3, K5)

19. (a) Discuss in detail about the History and Purpose of Operating Systems in embedded Environments. (CO4, K4)

Or

(b) Explain about real-time characteristics of an RTOS. (CO4, K3)

20. (a) Discuss the system architecture and control mechanisms used in fuel-operated electrical heater platforms. (CO5, K4)

Or

(b) Examine how custom software in healthcare improves patient care and financial results through SDLC application. (CO5, K6)

———————

R5004

Sub. Code
556401

M.Sc. DEGREE EXAMINATION, APRIL – 2026

Fourth Semester

Cyber Forensics

REVERSE ENGINEERING AND MALWARE ANALYSIS

(CBCS – 2023 onwards)

Time : 3 Hours Maximum : 75 Marks

Part A (10 × 1 = 10)

Answer **all** the following objective type questions by choosing the correct option.

1. Which of the following is NOT a goal of malware reverse engineering (CO1, K2)

   (a) Understanding malware functionality

   (b) Identifying indicators of Compromise (IOCs)

   (c) Improving system performance

   (d) Developing detection signatures

2. Which tool is commonly used for static analysis of Windows executables? (CO1, K2)

   (a) Wireshark (b) IDA Pro

   (c) Process Monitor (d) TCPdump

3. Which of the following is NOT a type of malware? (CO2, K3)

   (a) Virus (b) Worm

   (c) Trojan (d) Compiler

4. Which component of malware is responsible for infection and replication? (CO2, K2)

(a) Payload

(b) Trigger

(c) Computer Infection Program

(d) Antivirus

5. A logic bomb is activated by (CO3, K1)

(a) Specific event or condition

(b) Network ping

(c) Random timer

(d) User login

6. Which of the following is a non-self-reproducing malware? (CO3, K2)

(a) Virus (b) Worm

(c) Trojan Horse (d) Conficker C

7. What is the primary function of the replicator in a virus? (CO4, K3)

(a) Hide the virus code

(b) Spread copies to new files or systems

(c) Activate payload on trigger

(d) Dispatch to network

8. The Linux permission model primarily helps in malware defense by (CO4, K2)

(a) Encrypting all files

(b) Hiding system processes

(c) Restricting unauthorized execution

(d) Monitoring network packets

9. Network monitoring during malware analysis is mainly used to detect (CO5, K1)

(a) Hardware failures

(b) Unauthorized outbound connections

(c) BIOS modifications

(d) File compression

10. Which component is MOST affected when malware attempts persistence? (CO5, K3)

(a) CPU cache

(b) Registry and startup entries

(c) Monitor resolution

(d) Keyboard buffer

Part B (5 × 5 = 25)

Answer **all** questions not more than 500 words each.

11. (a) Describe the typical behavior of malware during execution in an operating system environment. (CO1, K5)

Or

(b) Define reverse engineering and explain its importance in malware analysis. (CO1, K2)

12. (a) Discuss about the tools used in computer virology for malware detection. (CO2, K3)

Or

(b) Differentiate between virus nomenclature and worm nomenclature. (CO2, K5)

13. (a) Outline the key features of the Conficted C Worm. (CO3, K4)

Or

(b) List the main components required for implementing remote access in malware. (CO3, K5)

14. (a) Summarize about the brute force logical bomb. (CO4, K3)

Or

(b) Outline the basic steps for testing virus codes safely. (CO4, K4)

15. (a) Discuss about the concept of execution artefact capture. (CO5, K3)

Or

(b) Explain the importance of establishing an environment baseline before executing a malware specimen. (CO5, K4)

Part C (5 × 8 = 40)

Answer **all** questions not more than 1000 words each.

16. (a) Analyze the steps involved in static malware analysis. (CO1, K4)

Or

(b) Design a basic analysis lab setup for safe malware examination. (CO1, K3)

17. (a) Explain in detail about the various types of malware and their characteristic behaviors. (CO2, K5)

Or

(b) Describe the life cycle of a malware, Analyze how each stage helps the malware achieve its objective. (CO2, K4)

18. (a) Discuss in detail about non–self-reproducing malware. (CO3, K3)

Or

(b) Design a simple logic bomb implementation, including trigger conditions and payload. (CO3, K6)

19. (a) Explain about Security implications of designing shell-based malware under Linux. (CO4, K5)

Or

(b) Compare and contrast between the functions of replicator, concealer and dispatcher. (CO4, K4)

20. (a) Design a malware analysis workflow using an automated malware analysis framework. (CO5, K6)

Or

(b) Analyze the steps involved in setting up system and network monitoring for safe malware execution. (CO5, K4)

———————