

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

(An Autonomous Institution)

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK



III SEMESTER

Coursecode COURSE NAME

Regulation – 2024

Academic Year 2024- 2025

Prepared by

Dr. V. Raghavendran,

Assistant Professor (SL. Gr)/MCA



SRM VALLIAMMAI ENGINEERING COLLEGE

DEPARTMENT OF COMPUTER APPLICATIONS

QUESTION BANK

SUBJECT :PMC505 -CYBER FORENSICS

SEM / YEAR: III/2026-27

UNIT I INTRODUCTION TO CYBER CRIME AND FORENSICS				
Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Role of ECD and ICT in Cybercrime - Classification of Cyber Crime. The Present and future of Cybercrime - Cyber Forensics -Steps in Forensic Investigation - Forensic Examination Process - Types of CF techniques - Forensic duplication and investigation - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.				
Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define cybercrime.	BTL -1	Remembering	CO 1
2.	What is traditional computer crime? Give one example.	BTL -2	Remembering	CO 1
3.	State any two problems associated with traditional computer crime.	BTL -2	Remembering	CO 1
4.	What is meant by ECD (Electronic Communication Devices)?	BTL -1	Remembering	CO 1
5.	Define ICT and mention its role in cybercrime.	BTL -2	Understanding	CO 1
6.	Classify cybercrime based on its target.	BTL -1	Remembering	CO 1
7.	Differentiate between traditional crime and cybercrime.	BTL -2	Understanding	CO 1
8.	What is cyber forensics? State its objective.	BTL -1	Remembering	CO 1
9.	List any four steps involved in forensic investigation.	BTL -2	Remembering	CO 1
10.	What is forensic examination?	BTL -1	Remembering	CO 1
11.	Name any four cyber forensic techniques.	BTL -1	Remembering	CO 1
12.	Define forensic duplication. Why is it necessary?	BTL -1	Understanding	CO 1
13.	What is meant by data acquisition in digital forensics?	BTL -2	Remembering	CO 1
14.	Mention any two forensic tools used in cyber investigations.	BTL -1	Remembering	CO 1
15.	State any two future trends in cybercrime.	BTL -2	Understanding	CO 1
16.	A company employee copies confidential customer data to a USB drive without permission. Identify the type of cybercrime.	BTL -2	Understanding	CO 1
17.	During an investigation, the examiner creates an exact copy of a suspect's hard disk before analysis. Why is this process important?	BTL -2	Understanding	CO 1

18.	A victim receives an email asking for banking credentials through a fake website. Identify the cybercrime involved.	BTL -1	Understanding	CO 1
19.	A forensic investigator collects RAM data before shutting down a compromised computer. Identify the process being performed.	BTL -1	Understanding	CO 1
20.	A government website is hacked and its homepage is altered. Under which category of cybercrime does this incident fall?	BTL -1	Understanding	CO 1
21.	A student illegally downloads licensed software from the Internet. Identify the type of computer crime.	BTL -2	Understanding	CO 1
22.	During evidence collection, the investigator ensures that the original hard disk is not modified. Explain why this practice is followed.	BTL -1	Understanding	CO 1
23.	An attacker uses a smartphone to send malicious links to several users. Explain the role of ECD in this cybercrime.	BTL -2	Understanding	CO 1
24.	A forensic analyst examines network traffic logs to identify the source of an attack. Which forensic technique is being used?	BTL -1	Understanding	CO 1
25.	A cybercriminal uses AI to create fake voice recordings and cheat bank customers. Explain how this reflects the future trend of cybercrime.	BTL -2	Understanding	CO 1
PART – B				
1.	Analyze the differences between traditional computer crimes and modern cybercrimes. Discuss how the evolution of ICT and electronic commerce has transformed the nature, scope, and complexity of cybercrime with suitable examples.	BTL -3	Analyzing (L4)	CO 1
2.	Evaluate the role of Information and Communication Technology (ICT) and Electronic Commerce Development (ECD) in facilitating both legitimate business operations and cybercriminal activities. Suggest appropriate preventive measures for organizations.	BTL -3	Evaluating (L5)	CO 1
3.	A multinational company experiences ransomware, phishing attacks, and insider data theft simultaneously. Analyze the different categories of cybercrime involved and recommend an appropriate response strategy for each category.	BTL -3	Analyzing + Applying (L4/L3)	CO 1
4.	Predict the future trends in cybercrime considering Artificial Intelligence, Cloud Computing, IoT, and Blockchain technologies. Design a cybersecurity strategy that organizations should adopt to combat future cyber threats.	BTL-3	Creating (L6)	CO 1
5.	During a cybercrime investigation, a forensic investigator discovers that evidence was collected without following proper forensic procedures. Evaluate the impact of improper evidence handling on the investigation and judicial process. Suggest corrective measures.	BTL-4	Evaluating (L5)	CO 1
6.	Design a comprehensive cyber forensic investigation framework for investigating a financial fraud involving unauthorized online banking transactions. Justify each phase of your proposed investigation.	BTL-5	Creating (L6)	CO 1
7.	A corporate employee is suspected of leaking confidential information through cloud storage services. Explain the complete forensic examination process that should be followed to preserve, acquire, examine, analyze, and present digital evidence.	BTL-4	Applying (L3)	CO 1

8.	Compare and critically analyze various computer forensic techniques such as live forensics, static forensics, memory forensics, and network forensics. Recommend the most suitable technique for investigating a ransomware attack.	BTL -4	Analyzing + Evaluating (L4/L5)	CO 1
9.	A cyber forensic investigator is required to duplicate a suspect's hard disk before investigation. Explain the forensic duplication process, challenges encountered, and methods for ensuring evidence integrity throughout the investigation.	BTL -3	Applying (L3)	CO 1
10.	Evaluate different forensic technologies and systems used in cybercrime investigations. Recommend the most appropriate forensic toolkit for investigating a large-scale cyber espionage case with proper justification.	BTL -4	Evaluating (L5)	CO 1
11.	Analyze the complete computer investigation process starting from incident reporting to courtroom presentation. Explain the significance of each stage with respect to maintaining the chain of custody.	BTL -3	Analyzing (L4)	CO 1
12.	A law enforcement agency receives a complaint regarding unauthorized deletion of confidential research data. Design a detailed data acquisition strategy ensuring forensic soundness and legal admissibility of digital evidence.	BTL -3	Creating (L6)	CO 1
13.	Critically evaluate the legal, ethical, and technical challenges faced during cyber forensic investigations. Recommend solutions to improve the effectiveness of digital forensic investigations in modern organizations.	BTL6	Evaluating (L5)	CO 1
14.	Analyze the impact of improper data acquisition methods on forensic investigations. Explain how forensic imaging, hashing algorithms, and chain of custody contribute to maintaining evidence integrity.	BTL6	Analyzing (L4)	CO 1
15.	An organization suspects that confidential documents have been exfiltrated using removable storage devices. Design a forensic investigation plan identifying the evidence sources, forensic tools, examination procedures, and reporting methodology.	BTL -3	Creating (L6)	CO 1
16.	Evaluate the effectiveness of cyber forensic investigations in solving cybercrimes compared to conventional criminal investigations. Support your arguments using suitable case scenarios and forensic principles.	BTL -4	Evaluating (L5)	CO 1
17.	A government organization experiences a cyberattack affecting multiple departments. Analyze the sequence of forensic investigation activities required to identify the attacker, recover digital evidence, and support legal prosecution.	BTL-6	Applying + Analyzing (L3/L4)	CO 1
18.	Develop a comprehensive cybercrime investigation model integrating cybercrime classification, forensic examination, forensic duplication, evidence preservation, and data acquisition. Justify how your model improves the efficiency and reliability of cyber forensic investigations.	BTL-6	Creating (L6)	CO 1

UNIT II EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes – Digital Evidence - Sources of Evidence - Working with File Systems. - Registry - Artifacts - Current Computer Forensics Tools: Software/ Hardware Tools - Forensic Suite - Acquisition and Seizure of Evidence from Computers and Mobile Devices – Chain of Custody- Forensic Tools

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define digital evidence . Give one example.	BTL-2	Remembering (L1)	CO 2
2.	What is meant by a crime scene in digital forensics?	BTL-2	Remembering (L1)	CO 2
3.	List any four common sources of digital evidence .	BTL-2	Remembering (L1)	CO 2
4.	What is the purpose of processing a digital crime scene ?	BTL-1	Understanding (L2)	CO 2
5.	Define a file system . Name any two commonly used file systems.	BTL-2	Remembering (L1)	CO 2
6.	Differentiate between FAT and NTFS file systems.	BTL-1	Understanding (L2)	CO 2
7.	What is the Windows Registry ?	BTL-1	Remembering (L1)	CO 2
8.	State any two uses of the Windows Registry in forensic investigations.	BTL-2	Understanding (L2)	CO 2
9.	What are digital artifacts ? Give two examples.	BTL-2	Remembering (L1)	CO 2
10.	Explain the difference between volatile and non-volatile evidence.	BTL-2	Understanding (L2)	CO 2
11.	Define Chain of Custody .	BTL-2	Remembering (L1)	CO 2
12.	Why is the Chain of Custody important in digital investigations?	BTL-1	Understanding (L2)	CO 2
13.	List any four computer forensic software tools .	BTL-2	Remembering (L1)	CO 2
14.	Give two examples of hardware forensic tools used during investigations.	BTL-1	Remembering (L1)	CO 2
15.	What is a forensic suite ? Mention one example.	BTL-2	Remembering (L1)	CO 2
16.	What is meant by forensic acquisition of digital evidence?	BTL-1	Remembering (L1)	CO 2
17.	Explain the purpose of write blockers during evidence acquisition.	BTL-2	Understanding (L2)	CO 2
18.	What precautions should be taken while seizing a computer as digital evidence?	BTL-1	Understanding (L2)	CO 2
19.	List any four sources of evidence that can be obtained from a mobile device .	BTL-1	Remembering (L1)	CO 2
20.	A forensic investigator finds a USB drive connected to a suspect's computer. What should be the first step before examining its contents?	BTL-1	Understanding (L2) (<i>Problem-based</i>)	CO 2
21.	During an investigation, a suspect's laptop is switched on. Why should the investigator avoid shutting it down immediately?	BTL-2	Understanding (L2) (<i>Problem-based</i>)	CO 2

22.	A forensic image of a hard disk has been created. Why is the original disk usually not examined directly?	BTL-1	Understanding (L2) (Problem-based)	CO 2
23.	A digital evidence bag has no documentation of who handled it. What forensic principle has been violated?	BTL-1	Understanding (L2) (Problem-based)	CO 2
24.	A deleted file is recovered from an NTFS partition. Which forensic concept makes this recovery possible?	BTL-1	Understanding (L2) (Problem-based)	CO 2
25.	A suspect deletes browser history before the investigator arrives. Name two alternative sources of evidence that may still reveal browsing activity.	BTL-2	Understanding (L2) (Problem-based)	CO 2
PART –B				
1.	Analyze the standard procedures involved in processing cybercrime and digital incident scenes. Explain how improper crime scene handling can compromise digital evidence and affect legal proceedings.	BTL5	Analyzing (L4)	CO 2
2.	A corporate office reports a cyberattack where multiple computers and servers are suspected to contain digital evidence. Design a systematic incident scene processing plan to ensure proper evidence collection, preservation, and documentation.	BTL -3	Creating (L6)	CO 2
3.	Explain the various sources of digital evidence available in a cybercrime investigation. Apply suitable evidence collection techniques for each source with relevant examples.	BTL -3	Applying (L3)	CO 2
4.	A suspect has attempted to delete incriminating files before the forensic team arrived. Analyze the possible sources from which digital evidence can still be recovered and justify their evidential value.	BTL -3	Analyzing (L4)	CO 2
5.	Evaluate the significance of file systems in digital forensic investigations. Compare FAT, NTFS, and EXT file systems with respect to forensic analysis and evidence recovery.	BTL-4	Evaluating (L5)	CO 2
6.	A forensic investigator is assigned to examine a hard disk containing multiple partitions with different file systems. Design an investigation methodology to identify, recover, and validate digital evidence from each partition.	BTL-4	Creating (L6)	CO 2
7.	Explain the role of the Windows Registry in forensic investigations. Analyze various Registry artifacts that can be used to reconstruct user activities during a cybercrime investigation.	BTL-3	Analyzing (L4)	CO 2
8.	A cybercriminal uses anti-forensic techniques to erase browser history and application logs. Evaluate how Registry artifacts and other system artifacts can still provide useful investigative evidence.	BTL-3	Evaluating (L5)	CO 2
9.	Differentiate between volatile and non-volatile digital artifacts. Apply appropriate forensic methods to collect and preserve each type of artifact during a live investigation.	BTL -3	Applying (L3)	CO 2
10.	Critically analyze the capabilities and limitations of current computer forensic software and hardware tools used in cybercrime investigations. Recommend suitable tools for investigating ransomware incidents.	BTL-4	Evaluating (L5)	CO 2
11.	A forensic laboratory plans to upgrade its investigation infrastructure. Design a forensic toolkit by selecting appropriate	BTL -3	Creating (L6)	CO 2

	software and hardware tools for investigating desktop, server, cloud, and mobile device-related cybercrimes. Justify your choices.			
12.	Compare different forensic suites available for digital investigations. Evaluate their features, strengths, limitations, and suitability for enterprise-level cybercrime investigations.	BTL -3	Evaluating (L5)	CO 2
13.	A suspect's computer and smartphone are seized during a cybercrime investigation. Explain the complete procedure for acquisition and seizure of digital evidence while ensuring forensic integrity and legal admissibility.	BTL-3	Applying (L3)	CO 2
14.	Design a detailed acquisition strategy for collecting evidence from computers, smartphones, and removable storage devices in a corporate espionage investigation. Explain how your strategy minimizes evidence contamination.	BTL-3	Creating (L6)	CO 2
15.	Analyze the importance of maintaining the Chain of Custody in digital forensic investigations. Explain how improper documentation can affect the admissibility of digital evidence in a court of law.	BTL-4	Analyzing (L4)	CO 2
16.	A digital forensic investigator discovers that evidence has changed during transportation due to improper handling. Evaluate the impact of this incident on the investigation and propose a revised Chain of Custody protocol to prevent similar issues.	BTL6	Evaluating (L5)	CO 2
17.	A multinational organization experiences a coordinated cyberattack involving laptops, cloud storage, and employee mobile devices. Develop a comprehensive digital evidence collection and forensic investigation plan, including evidence acquisition, forensic tools, documentation, and reporting.	BTL6	Creating (L6)	CO 2
18.	A financial institution reports unauthorized fund transfers carried out using compromised employee computers and mobile devices. Analyze the investigation process, identify appropriate forensic tools, describe evidence acquisition techniques, and recommend methods to ensure legal admissibility of digital evidence.	BTL6	Applying + Analyzing (L3/L4)	CO 2

UNIT III ANALYSIS AND VALIDATION

6

Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics - Analysis of Digital Evidence - Admissibility of Evidence - Cyber Laws in India – Case Studies

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define forensic data validation .	BTL-2	Remembering (L1)	CO 3
2.	Why is validation of digital evidence important in forensic investigations?	BTL-2	Understanding (L2)	CO 3
3.	What is meant by data hiding ?	BTL-2	Remembering (L1)	CO 3

4.	List any two data hiding techniques used by cybercriminals.	BTL-1	Remembering (L1)	CO 3
5.	Explain the term steganography .	BTL-2	Understanding (L2)	CO 3
6.	What is remote acquisition in digital forensics?	BTL-1	Remembering (L1)	CO 3
7.	State two advantages of performing remote acquisition .	BTL-1	Understanding (L2)	CO 3
8.	Define network forensics .	BTL-1	Remembering (L1)	CO 3
9.	Mention any two sources of evidence in network forensic investigations .	BTL-2	Remembering (L1)	CO 3
10.	Why are network logs important in network forensics?	BTL-1	Understanding (L2)	CO 3
11.	What is email forensics ?	BTL-2	Remembering (L1)	CO 3
12.	Name any two components of an email header used during forensic investigations.	BTL-1	Remembering (L1)	CO 3
13.	Explain why email headers are examined during an email investigation.	BTL-2	Understanding (L2)	CO 3
14.	What is mobile device forensics ?	BTL-1	Remembering (L1)	CO 3
15.	List any four types of evidence that can be recovered from a smartphone.	BTL-2	Remembering (L1)	CO 3
16.	Differentiate between logical acquisition and physical acquisition of a mobile device.	BTL-1	Understanding (L2)	CO 3
17.	Define analysis of digital evidence .	BTL-1	Remembering (L1)	CO 3
18.	What is meant by the admissibility of digital evidence ?	BTL-2	Understanding (L2)	CO 3
19.	Name any two requirements for digital evidence to be admissible in a court of law.	BTL-1	Remembering (L1)	CO 3
20.	Mention any two cyber laws in India that deal with cybercrime and digital evidence.	BTL-2	Remembering (L1)	CO 3
21.	A forensic investigator receives an image file suspected of containing hidden confidential information. Which forensic technique should be used to examine it?	BTL-1	Understanding (L2) (<i>Problem-based</i>)	CO 3
22.	A company server located in another city is compromised. Which forensic acquisition method is most suitable for collecting evidence without physically visiting the site?	BTL-2	Understanding (L2) (<i>Problem-based</i>)	CO 3
23.	During an investigation, the sender claims that an email was forged. Which part of the email should the investigator examine first to verify the sender's identity?	BTL-1	Understanding (L2) (<i>Problem-based</i>)	CO 3
24.	A suspect deletes all messages from a mobile phone before seizure. Mention one forensic approach that may help recover the deleted data.	BTL-1	Understanding (L2) (<i>Problem-based</i>)	CO 3
25.	During a cybercrime trial, the defense argues that the digital evidence was modified after collection. Which forensic principle helps establish the authenticity and admissibility of the evidence?	BTL-2	Understanding (L2) (<i>Problem-based</i>)	CO 3

PART –B				
1.	Analyze the importance of validating forensic data in a digital investigation. Explain various validation techniques used to ensure the integrity and authenticity of digital evidence with suitable examples.	BTL-3	Analyzing (L4)	CO 3
2.	A forensic investigator receives digital evidence from multiple storage devices with inconsistent hash values. Analyze the possible reasons for the mismatch and recommend appropriate validation procedures to ensure evidence integrity.	BTL-3	Analyzing + Evaluating (L4/L5)	CO 3
3.	Evaluate different data hiding techniques such as steganography, encryption, hidden partitions, and slack space. Recommend suitable forensic methods to detect and recover hidden information.	BTL-3	Evaluating (L5)	CO 3
4.	A cybercriminal is suspected of concealing confidential documents inside multimedia files before transmitting them over the Internet. Design a forensic investigation strategy to identify, extract, and validate the hidden data.	BTL-3	Creating (L6)	CO 3
5.	Explain the process of remote acquisition in digital forensics. Apply appropriate remote acquisition techniques to investigate a cyberattack on a geographically distributed corporate network while maintaining evidence integrity.	BTL-4	Applying (L3)	CO 3
6.	A multinational organization experiences a cyberattack on remote cloud servers. Develop a comprehensive remote evidence acquisition plan considering technical, legal, and security challenges.	BTL-3	Creating (L6)	CO 3
7.	Analyze the objectives, methodology, and challenges of network forensic investigations. Explain how network logs, packet captures, and firewall records contribute to cybercrime investigations.	BTL-3	Analyzing (L4)	CO 3
8.	An enterprise network experiences a Distributed Denial-of-Service (DDoS) attack. Analyze the network evidence available and recommend an investigation methodology to identify the attack source and preserve digital evidence.	BTL-4	Applying + Analyzing (L3/L4)	CO 3
9.	Evaluate the role of email forensics in investigating cybercrimes such as phishing, spoofing, and business email compromise. Discuss the forensic examination of email headers, metadata, and attachments.	BTL-3	Evaluating (L5)	CO 3
10.	A company receives fraudulent emails requesting unauthorized financial transactions. Design a complete email forensic investigation procedure to determine the origin, authenticity, and intent of the messages.	BTL-3	Creating (L6)	CO 3
11.	Explain the principles of mobile device forensics. Analyze the forensic acquisition techniques used for Android and iOS devices, highlighting their advantages and limitations.	BTL-3	Analyzing (L4)	CO 3
12.	A suspect involved in financial fraud has deleted call logs, messages, and documents from a smartphone. Develop a forensic investigation plan to recover, validate, and analyze the deleted evidence while ensuring legal admissibility.	BTL-3	Creating (L6)	CO 3

13.	Analyze the complete process of digital evidence analysis from acquisition to interpretation. Explain the challenges involved in correlating evidence from multiple digital sources.	BTL-3	Analyzing (L4)	CO 3
14.	Evaluate the legal requirements for admissibility of digital evidence in courts. Explain how chain of custody, hashing, documentation, and forensic standards contribute to evidence admissibility.	BTL6	Evaluating (L5)	CO 3
15.	A defense lawyer argues that the digital evidence presented in court has been tampered with after seizure. Evaluate the forensic procedures required to establish the authenticity and admissibility of the evidence.	BTL6	Evaluating (L5)	CO 3
16.	Analyze the major provisions of the Information Technology Act, 2000 (as amended) and other relevant cyber laws in India applicable to cybercrime investigations. Discuss their significance in prosecuting cyber offenders.	BTL6	Analyzing (L4)	CO 3
17.	Based on a real-world cybercrime case involving phishing, ransomware, or online banking fraud, analyze the investigation process, evidence collection, forensic analysis, and legal proceedings. Critically evaluate the effectiveness of the investigation.	BTL6	Analyzing + Evaluating (L4/L5)	CO 3
18.	A government organization experiences a sophisticated cyberattack involving hidden data, compromised email accounts, network intrusion, and mobile device misuse. Design a comprehensive digital forensic investigation model integrating forensic validation, remote acquisition, network forensics, email forensics, mobile forensics, evidence analysis, and compliance with Indian cyber laws. Justify each phase of your proposed investigation.	BTL6	Creating (L6)	CO 3

UNIT IV

ETHICAL HACKING

Introduction to Ethical Hacking – Foot printing and Reconnaissance – Scanning Networks - Enumeration - System Hacking - Malware Threats – Sniffing – Email Tracking

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define ethical hacking.	BTL-1	Remembering (L1)	CO 4
2.	State any two objectives of ethical hacking.	BTL-1	Remembering (L1)	CO 4
3.	Differentiate between an ethical hacker and a malicious hacker.	BTL-1	Understanding (L2)	CO 4
4.	What is footprinting?	BTL-1	Remembering (L1)	CO 4
5.	List any four information sources used during the footprinting phase.	BTL-1	Remembering (L1)	CO 4
6.	Explain the purpose of reconnaissance in ethical hacking.	BTL-1	Understanding (L2)	CO 4
7.	Define network scanning.	BTL-1	Remembering (L1)	CO 4

8.	Mention any two types of network scanning techniques.	BTL-2	Remembering (L1)	CO 4
9.	Why is port scanning performed during ethical hacking?	BTL-2	Understanding (L2)	CO 4
10.	What is enumeration in penetration testing?	BTL-2	Remembering (L1)	CO 4
11.	Name any four types of information that can be obtained during enumeration.	BTL-1	Remembering (L1)	CO 4
12.	Explain the difference between scanning and enumeration.	BTL-2	Understanding (L2)	CO 4
13.	What is meant by system hacking?	BTL-2	Remembering (L1)	CO 4
14.	List any four phases of system hacking.	BTL-2	Remembering (L1)	CO 4
15.	Define malware. Give any two examples.	BTL-2	Remembering (L1)	CO 4
16.	Explain the difference between a virus and a worm.	BTL-1	Understanding (L2)	CO 4
17.	What is packet sniffing?	BTL-1	Remembering (L1)	CO 4
18.	Differentiate between active sniffing and passive sniffing.	BTL-1	Understanding (L2)	CO 4
19.	What is email tracking?	BTL-2	Remembering (L1)	CO 4
20.	State any two purposes of analyzing an email header.	BTL-2	Understanding (L2)	CO 4
21.	A security administrator notices repeated connection attempts to several ports on a server. Which ethical hacking activity is most likely being performed?	BTL-1	Understanding (L2) (Problem-based)	CO 4
22.	During a penetration test, the tester collects employee information from social media without interacting with the target network. Which phase of ethical hacking does this represent?	BTL-2	Understanding (L2) (Problem-based)	CO 4
23.	A computer begins encrypting files and demands payment for decryption. Identify the type of malware involved.	BTL1	Remembering (L1) (Problem-based)	CO 4
24.	A network administrator suspects that login credentials are being captured on the local network. Which type of attack should be investigated first?	BTL2	Understanding (L2) (Problem-based)	CO 4
25.	An investigator examines the header of a suspicious email to identify its actual sender. What forensic information can be obtained from the email header?	BTL2	Understanding (L2) (Problem-based)	CO 4
PART –B				
1.	Analyze the objectives, phases, and methodologies of ethical hacking. Compare ethical hacking with malicious hacking, highlighting the ethical, legal, and technical differences.	BTL3	Analyzing (L4)	CO 4

2.	Evaluate the role of ethical hacking in protecting organizational information assets. Discuss its advantages, limitations, and legal implications with suitable examples.	BTL5	Evaluating (L5)	CO 4
3.	A financial institution plans to conduct an ethical hacking assessment of its network infrastructure. Design a comprehensive ethical hacking methodology covering planning, reconnaissance, exploitation, reporting, and remediation.	BTL4	Creating (L6)	CO 4
4.	Analyze the various footprinting and reconnaissance techniques used by ethical hackers to gather information about a target organization. Explain how organizations can defend against such reconnaissance activities.	BTL4	Analyzing (L4)	CO 4
5.	A company's website and employee information are publicly available on social media and search engines. Apply appropriate footprinting techniques to identify the information exposed and recommend suitable preventive measures.	BTL4	Applying (L3)	CO 4
6.	Design a reconnaissance strategy for assessing the security posture of a multinational organization's public-facing infrastructure while ensuring compliance with ethical and legal guidelines.	BTL3	Creating (L6)	CO 4
7.	Analyze different network scanning techniques such as TCP Connect Scan, SYN Scan, FIN Scan, NULL Scan, UDP Scan, and Banner Grabbing. Compare their advantages, limitations, and detection mechanisms.	BTL3	Analyzing (L4)	CO 4
8.	A security administrator detects unusual network scanning activity targeting organizational servers. Analyze the possible scanning techniques used by the attacker and recommend appropriate countermeasures.	BTL3	Applying + Analyzing (L3/L4)	CO 4
9.	Evaluate the importance of enumeration in penetration testing. Discuss different enumeration techniques for users, groups, shares, services, and network resources, and recommend methods to prevent information disclosure.	BTL4	Evaluating (L5)	CO 4
10.	A penetration tester has identified open ports on a target server. Design an enumeration strategy to identify users, services, shared resources, and vulnerabilities while minimizing detection by security monitoring systems.	BTL3	Creating (L6)	CO 4
11.	Analyze the phases involved in system hacking, including password attacks, privilege escalation, maintaining access, and covering tracks. Explain the corresponding defensive mechanisms for each phase.	BTL4	Analyzing (L4)	CO 4
12.	A server has been compromised through weak authentication and privilege escalation. Develop a systematic investigation and remediation plan to identify the attack vector, assess system compromise, and restore security.	BTL3	Creating (L6)	CO 4
13.	Evaluate different categories of malware, including viruses, worms, Trojans, ransomware, spyware, rootkits, and botnets. Discuss their attack mechanisms and suitable detection and prevention strategies.	BTL5	Evaluating (L5)	CO 4
14.	An organization experiences a ransomware attack affecting multiple departments. Analyze the malware lifecycle, identify	BTL4	Analyzing + Applying (L3/L4)	CO 4

	the likely infection vectors, and recommend a comprehensive incident response and recovery strategy.			
15.	Explain the principles of packet sniffing. Analyze active and passive sniffing techniques, their impact on network security, and the methods used to detect and prevent sniffing attacks.	BTL4	Analyzing (L4)	CO 4
16.	A network administrator suspects that confidential login credentials are being intercepted over the local network. Apply suitable forensic and security techniques to identify sniffing attacks and recommend effective countermeasures.	BTL6	Applying (L3)	CO 4
17.	Evaluate the techniques used in email tracking, email spoofing detection, and email header analysis. Discuss their significance in cybercrime investigations and phishing detection.	BTL6	Evaluating (L5)	CO 4
18.	A multinational organization reports suspicious emails, malware infections, unauthorized network scans, and compromised user accounts. Design a comprehensive ethical hacking and security assessment plan integrating reconnaissance, scanning, enumeration, system hacking analysis, malware investigation, sniffing detection, and email tracking. Justify each phase of your proposed solution.	BTL6	Creating (L6)	CO 4

UNIT – V APP IMPLEMENTATION IN CLOUD Cloud providers Overview – Virtual Private Cloud – Scaling (Horizontal and Vertical) – Virtual Machines, Ethernet and Switches – Docker Container – Kubernetes.

Q.No.	Question	Bloom's Taxonomy Level	Competence	Course Outcome
PART – A				
1.	Define social engineering.	BTL-1	Remembering (L1)	CO 5
2.	List any four common social engineering attacks.	BTL-1	Remembering (L1)	CO 5
3.	Why are employees considered the weakest link in information security?	BTL-2	Understanding (L2)	CO 5
4.	Define a Denial-of-Service (DoS) attack.	BTL-1	Remembering (L1)	CO 5
5.	Differentiate between DoS and Distributed DoS (DDoS) attacks.	BTL-1	Understanding (L2)	CO 5
6.	State any two objectives of a DoS attack.	BTL-2	Remembering (L1)	CO 5
7.	What is session hijacking?	BTL-1	Remembering (L1)	CO 5
8.	Mention any two methods used in session hijacking.	BTL-2	Remembering (L1)	CO 5
9.	Explain the purpose of session cookies in web applications.	BTL-2	Understanding (L2)	CO 5
10.	Define web server hacking.	BTL-2	Remembering (L1)	CO 5
11.	List any four common vulnerabilities found in web servers.	BTL-1	Remembering (L1)	CO 5
12.	Why should web servers be regularly patched and updated?	BTL-1	Understanding (L2)	CO 5

13.	What is meant by web application hacking?	BTL-1	Remembering (L1)	CO 5
14.	Name any four common web application attacks.	BTL-2	Remembering (L1)	CO 5
15.	Define SQL Injection (SQLi).	BTL-1	Remembering (L1)	CO 5
16.	Explain how SQL Injection can compromise a database.	BTL-2	Understanding (L2)	CO 5
17.	What is wireless network hacking?	BTL-1	Remembering (L1)	CO 5
18.	List any two wireless network security protocols.	BTL-2	Remembering (L1)	CO 5
19.	Why is WPA2 considered more secure than WEP?	BTL-2	Understanding (L2)	CO 5
20.	What is mobile platform hacking?	BTL-2	Remembering (L1)	CO 5
21.	A user receives a phone call requesting their online banking password from someone claiming to be a bank employee. Identify the type of attack.	BTL-2	Understanding (L2) (Problem-based)	CO 5
22.	A company's website becomes inaccessible after receiving millions of requests from different systems simultaneously. What type of cyberattack has most likely occurred?	BTL-2	Understanding (L2) (Problem-based)	CO 5
23.	A hacker steals a user's session cookie and accesses the user's account without entering the password. Which attack is being performed?	BTL-1	Understanding (L2) (Problem-based)	CO 5
24.	A login page accepts the input ' OR '1'='1 and grants unauthorized access to the database. Which web attack does this illustrate?	BTL-2	Understanding (L2) (Problem-based)	CO 5
25.	A mobile application downloaded from an unknown source starts sending sensitive user data to an external server. What type of security issue does this represent?	BTL-1	Understanding (L2) (Problem-based)	CO 5

PART –B

1.	Analyze the principles of social engineering and discuss various attack techniques such as phishing, pretexting, baiting, and tailgating. Recommend suitable countermeasures to reduce human vulnerabilities in organizations.	BTL-3	Analyzing (L4)	CO 5
2.	A multinational company experiences repeated phishing and social engineering attacks targeting employees. Design a comprehensive security awareness and technical defense program to minimize the success of such attacks.	BTL5	Creating (L6)	CO 5
3.	Evaluate different types of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. Compare their attack mechanisms, impact on organizations, and mitigation strategies.	BTL-3	Evaluating (L5)	CO 5
4.	An e-commerce website becomes unavailable after receiving an unusually high volume of malicious traffic from multiple locations. Analyze the attack, identify the	BTL-4	Applying + Analyzing (L3/L4)	CO 5

	probable DDoS technique, and recommend an incident response and mitigation strategy.			
5.	Analyze the concept of session hijacking and explain various techniques such as session fixation, session sidejacking, and cookie theft. Discuss suitable preventive mechanisms for secure session management.	BTL-4	Analyzing (L4)	CO 5
6.	A user's authenticated web session is compromised after connecting to an unsecured public Wi-Fi network. Design a forensic investigation and security enhancement plan to identify the attack and prevent similar incidents.	BTL-4	Creating (L6)	CO 5
7.	Evaluate common vulnerabilities found in web servers and explain how attackers exploit configuration errors, outdated software, and weak authentication. Recommend effective server hardening techniques.	BTL-4	Evaluating (L5)	CO 5
8.	A web server hosting confidential customer information is suspected to have been compromised. Apply appropriate ethical hacking techniques to identify vulnerabilities and propose suitable remediation measures.	BTL-3	Applying (L3)	CO 5
9.	Analyze the methodology used in web application hacking. Explain how authentication flaws, input validation errors, broken access control, and insecure configurations lead to successful attacks.	BTL-3	Analyzing (L4)	CO 5
10.	A university web portal allows unauthorized users to access student records. Design a secure web application architecture that minimizes common web application vulnerabilities and justifies your design choices.	BTL-3	Creating (L6)	CO 5
11.	Evaluate different SQL Injection attack techniques, including Union-based, Error-based, Blind, and Time-based SQL Injection. Discuss suitable detection and prevention mechanisms.	BTL-3	Evaluating (L5)	CO 5
12.	A banking application allows attackers to retrieve confidential customer records by manipulating SQL queries. Analyze the vulnerability, explain the attack process, and recommend secure coding practices to prevent SQL Injection.	BTL-4	Applying + Analyzing (L3/L4)	CO 5
13.	Analyze the security challenges of wireless networks. Compare WEP, WPA, WPA2, and WPA3 security protocols and discuss common wireless attacks with suitable countermeasures.	BTL-3	Analyzing (L4)	CO 5
14.	A corporate wireless network experiences unauthorized access despite password protection. Design a wireless network security framework that minimizes the risk of wireless attacks while maintaining usability.	BTL-4	Creating (L6)	CO 5
15.	Evaluate the major security threats affecting Android and iOS mobile platforms. Discuss malware, insecure applications, rooting/jailbreaking, and application permission misuse with suitable preventive measures.	BTL-3	Evaluating (L5)	CO 5
16.	A company's employees install applications from untrusted sources on their smartphones, resulting in confidential data leakage. Develop a comprehensive mobile security policy and technical control framework to prevent similar incidents.	BTL-4	Creating (L6)	CO 5
17.	Analyze the interrelationship between social engineering, session hijacking, SQL Injection, web application attacks, and	BTL-3	Analyzing (L4)	CO 5

	mobile platform attacks in a multi-stage cyberattack. Explain how each phase contributes to the overall compromise.			
18.	A financial institution experiences a coordinated cyberattack involving phishing emails, SQL Injection, web server compromise, session hijacking, DDoS attacks, wireless intrusion, and compromised employee mobile devices. Design a comprehensive ethical hacking and incident response strategy integrating vulnerability assessment, attack detection, forensic investigation, remediation, and organizational security improvements. Justify each phase of your proposed solution.	BTL6	Creating (L6)	CO 5

