SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK

V SEMESTER

1923501 – CYBER SECURITY & DIGITAL FORENSICS

Regulation – 2019

Academic Year 2022-2023 (Odd Semester)

Prepared by

Ms. K. R. Nandhashree, A.P (O.G) / CYS

Ms. R. Sivasankari, A.P (O.G) / CYS

Ms. S. Priyanka, A.P (O.G) / CYS

SUBJECT: 1923501 - CYBER SECURITY & DIGITAL FORENSICS
SEM/YEAR : V / III

UNIT I - INTRODUCTION TO CYBER SECURITY
Introduction – Computer Security – Threats – Harm – Vulnerabilities – Controls – Authentication – Access Control and Cryptography – Web—User Side – Browser Attacks – Web Attacks Targeting Users – Obtaining User or Website Data – Email Attacks.

PART - A

Q.No	Question	Level	Competence
1	Explain Computer Security?	BTL3	Applying
2	Point out the assets that deserves security protection.	BTL4	Analyzing
3	List the three aspects that make the system valuable.	BTL1	Remembering
4	Discuss values of assets with a relevant example of your own.	BTL2	Understanding
5	Interpret the term Access Control .	BTL2	Understanding
6	List the properties of C-I-A traid.	BTL1	Remembering
7	Define Vulnerability.	BTL1	Remembering
8	List the kinds of Threats.	BTL1	Remembering
9	Explain about access control on reference monitors	BTL2	Understanding
10	Define Threat.	BTL1	Remembering
11	Generalize your view about control.	BTL6	Creating
12	Analyze Risk Management.	BTL4	Analyzing
13	Define cryptography.	BTL3	Applying
14	List the components of the digital signature.	BTL2	Understanding
15	Write a note on RSA algorithm.	BTL3	Applying
16	When does overflow occur?	BTL5	Evaluating
17	List the ways to deal with Harm.	BTL1	Remembering
18	Define backdoor.	BTL4	Analyzing
19	Explain the term Malware.	BTL6	Creating
20	Write a note on working of virus detectors.	BTL5	Evaluating
21	Give the list of authentication mechanisms to confirm an user's identity.	BTL1	Remembering
22	Name some types of browser attacks.	BTL1	Remembering
23	Differentiate between Authentication and Identification.	BTL4	Analyzing
24	Write a note on i) web bugs ii) click jacking.	BTL1	Remembering
25	List the independent classes of Control. Give example of each type of control.	BTL2	Understanding

PART – B

Q.No	Question	Level	Competence
1	Explain Method- Opportunity-Motive. (13)	BTL1	Remembering
2	(i) Distinguish between vulnerability, threat, and control. (06) (ii) Do you currently use any computer security control measures? If so, what? Against what attacks are you trying to protect? (07)	BTL1	Remembering
3	Theft usually results in some kind of harm. For example, if someone steals your car, you may suffer financial loss, inconvenience (by losing your mode of transportation), and emotional upset (because of invasion of your personal	BTL1	Remembering

	Property and space). List three kinds of harm a company might experience from theft of computer equipment. (13)		
4	Write a brief note on CIA triad with their respective criteria. (13)	BTL2	Understanding
5	Discuss vulnerabilities and countermeasures to overcome in detail. (13)	BTL2	Understanding
6	Give a brief note on authentication and its mechanism to confirm a user's identity. (13)	BTL1	Remembering
7	Explain i) Password usage (05) ii) Password attacks (04) iii) Protecting password attacks (04)	BTL3	Applying
8	Briefly explain i) Problems with Use of Biometrics (07) ii) False positive and false negative (06)	BTL4	Analyzing
9	Discuss i) Federated Identity Management scheme (07) ii) Effective Policy Implementation (06)	BTL4	Analyzing
10	i) Distinguish between Procedure-Oriented and Role-Based Access Control. (7) ii) List the advantages and disadvantages of stream and block encryption algorithms. (6)	BTL2	Understanding
11	Explain Cryptography and its types in detail. (13)	BTL3	Applying
12	Give a brief note on i) Addressing potential problems of vulnerability in an application (07) ii) Time-of-Check to Time-of-Use (06)	BTL6	Creating
13	Discuss malware and Types of Malicious Code (13)	BTL 5	Evaluating
14	Explain the harms caused by the malicious codes to various subjects (13)	BTL4	Analyzing
15	Write a brief note on attacks seeking sensitive data. (13)	BTL4	Analyzing
16	Discuss i) Web bugs (04) ii) Clickjacking (04) iii) Drive-by-download (05)	BTL6	Creating

17	Write a note on attacks through e-mail.	(13)	BTL4	Analyzing
18	Explain types of attacks in the web-user side in detail.	(13)	BTL6	Creating

PART – C			
Q.No	**Question**	**Level**	**Competence**
1	Write a brief note on DES : Data Encryption Standard	BTL5	Evaluating
2	Explain in detail about Signatures and how it is used?	BTL6	Creating
3	Discuss Email Attacks in details with suitable examples.	BTL6	Creating
4	Give a brief on countermeasures for user and security with respect to malware attacks.	BTL5	Evaluating
5	Write a brief note on AES : Advanced Encryption System	BTL5	Evaluating

UNIT II - SECURITY IN OPERATING SYSTEM & NETWORKS			
Security in Operating Systems – Security in the Design of Operating Systems –Rootkit – Network security attack– Threats to Network Communications – Wireless Network Security – Denial of Service – Distributed Denial–of–Service.			
PART – A			
Q.No	**Question**	**Level**	**Competence**
1	Define Operating System.	BTL1	Remembering
2	Analyze about Object Sanitization.	BTL4	Analyzing
3	What is Rootkit?	BTL2	Understanding
4	What are the advantages of Multitasking?	BTL1	Remembering
5	Brief about Sandbox.	BTL5	Evaluating
6	Discuss about Kernel and list its functions.	BTL2	Understanding
7	Analyze the term Honeypot.	BTL6	Creating
8	List the types of Threats in Network Communications.	BTL1	Remembering
9	Explain “Trusted Systems” and the user’s expectations towards the Trusted Systems.	BTL2	Understanding
10	What are the dimensions of concerns about Packet Sniffing.	BTL1	Remembering
11	Analyze the Segmentation Concept.	BTL6	Creating
12	Define Hypervisor.	BTL 3	Applying
13	Generalize on the factors of Paging.	BTL4	Analyzing
14	Differentiate between Substitution attack and insertion attack.	BTL1	Remembering
15	Define Fence.	BTL3	Applying
16	Define Frame and what are the fields present in a frame?	BTL5	Evaluating
17	Explain Session Hijack.	BTL1	Remembering
18	What are Zombies?	BTL2	Understanding
19	Generalize Reference Monitor.	BTL3	Applying
20	What are the effects of Splicing.	BTL4	Analyzing
21	Analyze the term “Wire Tapping”.	BTL1	Remembering
22	Explain how TCB (Trusted Computing Base) works.	BTL1	Remembering
23	List the vulnerabilities in Wireless Networks.	BTL2	Understanding

24	Analyze WEP.	BTL4	Analyzing
25	Discuss about DoS Attacks.	BTL2	Understanding

PART - B			
Q.No	**Question**	**Level**	**Competence**
1	i)Explain the Structure of Operating System. (05) ii) List and explain the security features of an Operating System. (08)	BTL1	Remembering
2	Elaborate the History of operating System. (13)	BTL2	Understanding
3	Describe in detail about the layered design of Operating System to protect objects. (13)	BTL1	Remembering
4	Discuss about the tools used to implement security functions in an Operating System. (13)	BTL3	Applying
5	Explain the Concept Segmentation in detail. (13)	BTL2	Understanding
6	i) Elaborate Paging. (08) ii)Brief "Combined Paging with Segmentation". (05)	BTL1	Remembering
7	Describe about the Kernelized design of Operating System in detail. (13)	BTL3	Applying
8	i)What are Trusted Systems? List its Characteristics. (06) ii) Brief the History of Trusted Systems. (07)	BTL4	Analyzing
9	List and elaborate the Functions of Trusted Computing Base (TCB), its Design and Implementation. (13)	BTL4	Analyzing
10	Discuss in detail about Rootkits. (13)	BTL2	Understanding
11	Brief the Network Terms: i) Cable (03) ii) Packet Sniffing (03) iii) Radiation (03) iv) Cable Splicing (04)	BTL1	Remembering
12	Briefly explain Addressing and Routing. (13)	BTL6	Creating
13	List and elaborate the Threats to Network Communications. (13)	BTL2	Understanding
14	Brief Port Scanning. (02) What are the Port Scanning Tools used? (03) Discuss about Port Scanning Results. (04) Brief the harms from Port Scanning. (04)	BTL4	Analyzing

15	Explain in detail about how security is applied to Wireless Networks.	(13)	BTL5	Evaluating
16	List and explain the vulnerabilities in Wireless Networks.	(13)	BTL6	Creating
17	Explain in detail about the Failed Counter Measure : WEP.	(13)	BTL5	Evaluating
18	Describe in detail about Denial of Service Attacks.	(13)	BTL3	Analyzing

PART – C				
Q.No	**Question**		**Level**	**Competence**
1	Explain the Denial Of Service by addressing Failures in detail.	(15)	BTL6	Creating
2	Describe in detail about Traffic Redirection.	(15)	BTL5	Evaluating
3	Explain in detail about i) TCP Hijack. ii) Session Hijack.	 (07) (08)	BTL5	Evaluating
4	Explain how WPA is a stronger Protocol suite.	(15)	BTL6	Creating
5	Explain in detail about Distributed DoS Attacks.	(15)	BTL5	Evaluating

UNIT – III : DEFENCES: SECURITY COUNTERMEASURES

Cryptography in Network Security – Firewalls – Intrusion Detection and Prevention Systems – Network Management – Databases – Security Requirements of Databases – Reliability and Integrity – Database Disclosure – Data Mining and Big Data.

PART – A

Q.No	**Question**	**Level**	**Competence**
1	Define Cryptography.	BTL1	Remember
2	List the two classes of Encryption	BTL1	Remember
3	Why is Network Encryption needed? What are the modes of Network Encryption?	BTL4	Analyze
4	What is a Firewall?	BTL1	Remember
5	Explain about Guard. How does it work?	BTL5	Evaluate
6	Analyze what firewalls can / cannot block?	BTL4	Analyze
7	Define Onion Routing.	BTL1	Remember
8	What do you mean by ESP? Why is it formed?	BTL6	Create
9	Why is VPN created?	BTL5	Evaluate
10	Summarize two styles of Intrusion Detection	BTL2	Understand
11	List the goals of Intrusion Detection System.	BTL1	Remember
12	Classify the types of IDS.	BTL3	Apply
13	Discover the limitations of IDS.	BTL3	Apply
14	Define Database.	BTL1	Remember

15	Give the components of Databases.	BTL2	Understand
16	Analyze Select-Project-Join query.	BTL4	Analyze
17	Demonstrate the factors which can make data sensitive.	BTL3	Apply
18	Discuss how Network Management is implemented?	BTL2	Understand
19	Assess the various types of Disclosures.	BTL5	Evaluate
20	Summarize Direct Inference.	BTL2	Understand
21	Discuss about Direct Attack.	BTL2	Understand
22	Demonstrate Data mining.	BTL3	Apply
23	Analyze Security versus Precision.	BTL4	Analyze
24	What do you mean by Big Data?	BTL1	Remember
25	Data on activities or behavior abound. Are they accurate?	BTL6	Create

PART – B

Q.No	Question		Level	Competence
1	List the Modes of Network Encryption and discuss in detail.	(13)	BTL1	Remember
2	Compare the various Encryption Methods.	(13)	BTL4	Analyze
3	Explain the concept of Browser Encryption.	(13)	BTL1	Remember
4	Demonstrate Virtual Private Networks in detail.	(13)	BTL3	Apply
5	Illustrate the design of Firewalls in detail.	(13)	BTL3	Apply
6	Demonstrate the various types of Firewalls in detail.	(13)	BTL3	Remembering
7	a) List the various types of Firewalls. b) Compare the various types of Firewalls.	(03) (10)	BTL2	Understand
8	Summarize the Intrusion Detection and Prevention System.	(13)	BTL2	Understand
9	Discuss in detail about Network Management.	(13)	BTL2	Understand
10	Analyze Data Loss Prevention.	(13)	BTL4	Analyze
11	Describe the Model of Intrusion Detection System.	(13)	BTL1	Remember
12	List and explain the various types of IDS.	(13)	BTL1	Creating
13	• a) Elaborate Onion Routing. • b) With a neat sketch, explain the system architecture of VPN.	(06) (07)	BTL5	Evaluate
14	a) List the advantages of using Databases. • b) Assess the security requirements of Databases.	(05) (08)	BTL5	Evaluate
15	• Describe in detail about Reliability and Integrity in Databases.	(13)	BTL2	Understand
16	• Describe the concept of Database Disclosure in detail.	(13)	BTL1	Remember
17	• Elaborate Data Mining and Big Data.	(13)	BTL5	Evaluate
18	• Analyze Big Data Application Framework: Apache Hadoop.	(13)	BTL4	Analyze

PART – C

Q.No	Question		Level	Competence
1	Summarize how IPsec implements encryption and authentication in the Internet protocols.	(15)	BTL5	Evaluate
2	Explain (i) Stateful Inspection Firewall. (ii) Application Proxy (iii) Personal Firewall	(05) (05) (05)	BTL5	Evaluate
3	Explain Two-Phase Update with an Example.	(15)	BTL5	Evaluate

4	Formulate the major security issues dealt with at each level of the OSI protocol stack. (15)	BTL6	Create
5	Design a Network load balancing which directs incoming traffic to resources with available capacity. (15)	BTL6	Create

UNIT IV - DIGITAL FORENSICS

Introduction to Digital Forensics, Open Source Examination Platform – Using Linux and Windows as the Host, Disk and File System Analysis, Media Analysis Concepts , Sleuth Kit, Partitioning and Disk Layouts, Special Containers, Hashing, Forensic Imaging, Internet Artifacts, Browser & Mail Artifacts, File Analysis, Image, Audio, Video, Archives, Documents, Graphical Investigation Environments, PyFLAG, Fiwalk, Forensic Ballistics and Photography,Face, Iris and Fingerprint Recognition.

PART – A

Q.No	Question	Level	Competence
1	What is Digital Forensics ?	BTL-1	Remember
2	What is computer Forensics?	BTL-1	Remember
3	Define Forensics Readiness.	BTL-1	Remember
4	What are the uses of computer Forensics?	BTL-1	Remember
5	Recall Digital Forensics analysis?	BTL4	Analyze
6	Explain the three A's of digital forensics?	BTL3	Apply
7	Describe Media Analysis Concepts.	BTL2	Understand
8	Explain Sleuth Kit.	BTL5	Evaluating
9	List the purpose of Sleuth Kit.	BTL3	Applying
10	What is Forensics imaging.	BTL3	Applying
11	What is RAID?	BTL5	Evaluating
12	List out the Traditional problems associated with Computer Crime.	BTL6	Creating
13	List the Levels of RAID.	BTL1	Remembering
14	What is hashing?	BTL6	Creating
15	Differentiate Internet Artifacts, Browser & Mail Artifacts.	BTL1	Remembering
16	Explain the rules for computer forensics in investigation.	BTL3	Applying
17	What is Internet Artifacts?	BTL1	Remembering
18	How will you find out the hidden data in forensics technology?	BTL2	Understanding
19	What is Browser Artifacts?	BTL4	Analyzing
20	Define RAID data acquisition.	BTL1	Remembering
21	What is Mail Artifacts?	BTL1	Remembering
22	Differentiate master boot record(MBR) and master file table(MFT)	BTL3	Applying
23	How will you create new technology file system?	BTL1	Remembering
24	Define hashing algorithms for forensic purpose.	BTL3	Applying
25	Explain the rules for computer forensics in investigation.	BTL5	Evaluating

PART – B			
Q.No	**Question**	**Level**	**Competence**
1	Explain File System Abstraction Model in detail. (13)	BTL1	Remembering
2	Explain Sleuth Kit and its tools in detail. (13)	BTL3	Applying
3	Explain in detail about computer Forensics and its four stages. (13)	BTL1	Remembering
4	What is RAID and explain in detail about its various levels. (13)	BTL3	Applying
5	Explain Forensics imaging. (13)	BTL6	Creating
6	Discuss the steps for investigating routers. (13)	BTL5	Evaluating
7	Explain e-mail forensic investigation methods. (13)	BTL4	Analyzing
8	Briefly explain each of the following: Qualified forensic duplicate, restored image, mirror image. (13)	BTL4	Analyzing
9	Explain the process of investigating e-mail crimes and violation. (13)	BTL1	Remembering
10	Explain importance of forensic duplication and its methods. (13)	BTL2	Understanding
11	Write short note on NTFS disk. (13)	BTL4	Analyzing
12	Write short note on laws related to computer forensics. (13)	BTL2	Understanding
13	How will you trace the crime which has been happened through email using tools? (13)	BTL1	Remembering
14	Describe the levels of culpability. (13)	BTL2	Understanding
15	Differentiate and explain in detail about Internet artifacts, Brower and mail artifacts. (13)	BTL2	Understanding
16	Give the methods for steganalysis attack. (13)	BTL3	Applying
17	Explain about pslogedo and netstatn. (13)	BTL5	Evaluating
18	Summarize Forensic Ballistics and Photography in detail. (13)	BTL6	Creating

PART – C			
Q.No	**Questions**	**Level**	**Competence**
1	Briefly explain the role of the following tools in digital forensics: i) netstat ii) pslogedon iii)tcptrace iv) netcat v) cryptcat (15)	BTL5	Evaluating
2	Write a short note on: 1) CFAA. 2) Storage layer of file system. (15)	BTL6	Creating
3	Briefly explain the role of Windows registry in collecting forensic evidence. (15)	BTL5	Evaluating
4	Briefly explain how the following roles are applied in investigation in E-mail investigations and E-mail client and server. (15)	BTL 6	Creating
5	How will you generalize the modes of protection. (15)	BTL 6	creating

UNIT V - LAWS AND ACTS			
Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.			
PART – A			
Q.No	**Question**	**Level**	**Competence**
1	What is cyber law?	BTL4	Analyzing
2	What are the cyber laws in India?	BTL1	Remembering
3	What is section 43 in cyber law?	BTL3	Applying
4	What is section 66 and 66B in cyber law?	BTL1	Remembering
5	What is section 66C and 66D in cyber law?	BTL5	Evaluating
6	What are the four 4 ethical issues of cyber ethics?	BTL1	Remembering
7	What are the cyber laws in ethics ?	BTL2	Understanding
8	What is electronic Communication Privacy ACT.	BTL2	Understanding
9	What is Indian Evidence ACT.	BTL4	Analyzing
10	What is Evidence?	BTL2	Understanding
11	What is Indian Evidence IPC?	BTL3	Applying
12	What is DOS attack?	BTL1	Remembering
13	What is Indian Evidence CrPC.	BTL6	Creating
14	Explain the term cyber terrorism.	BTL1	Remembering
15	Explain the term cyber theft.	BTL2	Understanding
16	How to write an incident report.	BTL3	Applying
17	How will you plan the most critical aspects of computer evidence?	BTL1	Remembering
18	Explain ethics for computer user.	BTL5	Evaluating
19	What is ethics for Information services.	BTL4	Analyzing
20	Explain Software Piracy.	BTL6	Creating
21	Write a note on Unauthorized Access.	BTL2	Understanding
22	What is code of ethics?	BTL3	Applying
23	Why the need of Cyber law arises?	BTL4	Analyzing
24	Explain IT Act in brief.	BTL5	Evaluating
25	List any four legal policies.	BTL1	Remembering

PART - B				
Q.No	**Question**		**Level**	**Competence**
1	Explain cyber laws.	(13)	BTL1	Remembering
2	Explain the four 4 ethical issues of cyber ethics.	(13)	BTL2	understanding
3	Explain the various sections of cyber laws.	(13)	BTL1	Remembering
4	Explain the various Procedures for Evidence Handling.	(13)	BTL3	Applying
5	Explain the Indian Evidence ACT.	(13)	BTL1	Remembering
6	Explain following terms as mentioned in the IT Act 2000.	(13)	BTL2	Understanding
7	Explain the various benefits of cyber laws.	(13)	BTL2	understanding
8	Describe about Digital Evidence and its characteristics.	(13)	BTL3	Applying

9	What are the challenges in evidence handling. (13)	BTL1	Remembering
10	What is incident and what are the goals of incident response?. (13)	BTL4	Analyzing
11	Classify the different categories of cyber crime with examples of each. Identify the type of cyber-crime for each of the following situations: (i)Hacking into a web server and defacing legitimate Web pages (04) (ii)Introducing viruses, worms, and other malicious code into a network or computer (04) (iii)Unauthorized copying of copyrighted software, music, movies, arts, books. (iv)Internet gambling and trafficking (05)	BTL4	Analyzing
12	What is Evidence ? explain the types of Evidence . (13)	BTL4	Analyzing
13	What is DOS attack? How to achieve recovery from DOS attack. (13)	BTL5	Evaluating
14	Explain the term cyber terrorism with example. (13)	BTL6	Creating
15	Explain the guidelines for incident report writing. (13)	BTL3	Applying
16	Explain the procedures to investigate routers . (13)	BTL5	Evaluating
17	Explain the cyber theft and its various types. (13)	BTL2	understanding
18	Summarize the Electronic Communication Privacy ACT in detail. (13)	BTL6	Creating

PART – C			
Q.No	**Question**	**Level**	**Competence**
1	Explain the basics of Indian Evidence ACT IPC and CrPC in detail . (15)	BTL6	Creating
2	Explain about cyber laws ,various sections of law and its advantages in detail (15)	BTL5	Evaluating
3	Explain about electronic Communication Privacy ACT. (15)	BTL5	Evaluating
4	List out the various Legal Policies (15)	BTL6	Creating
5	Explain about digital evidence and its benefits (15)	BTL6	Creating