



Jaywant Shikshan Prasarak Mandal's
RAJARSHI SHAHU COLLEGE OF ENGINEERING's
POLYTECHNIC



S.No.80, Pune-Mumbai Bypass Highway, Tathawade Campus, Pune.

Approved By AICTE & Govt. of Maharashtra, Affiliated to MSBTE

NBA ACCREDITED

DTE Code – 6141

MSBTE Inst. Code - 1620

“MASTER SOLUTIONS”

(MSBTE Question Paper with Solution as per I Scheme)

Class – Third Year Computer Engineering

Semester – CO6I

Subject: Network & Information Security

Subject Code – 22620

DEPARTMENT OF COMPUTER ENGINEERING



JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING,
POLYTECHNIC, TATHAWADE, PUNE-33



DEPARTMENT OF COMPUTER ENGINEERING

JSPM's RSCOE Polytechnic Institute Vision	JSPM's RSCOE Polytechnic Institute Mission
"To satisfy the aspirations of youth force, who want to lead the nation towards prosperity through techno-economic development."	"To provide, nurture and maintain an environment of high academic excellence, research and entrepreneurship for all aspiring students, which will prepare them to face global challenges maintaining high ethical and moral standards."
JSPM's RSCOE Polytechnic Department of Computer Engineering Vision	JSPM's RSCOE Polytechnic Department of Computer Engineering Mission
To impart value based technical education for developing competent computer engineers fulfilling expectations of industry and society.	M1- To provide sound theoretical education, practical knowledge and to train the students in association with industry. M2- To improve self awareness and ethical values among students along with technical proficiency. M3- To promote awareness about life-long learning and problem solving among students.
Program Specific Outcomes (PSOs)	Program Outcomes (POs)
PSO1.Computer Software and Hardware Usage; Use state of-the-art technologies for operation and application of computer software and hardware. PSO2.Computer engineering Maintenance; Maintain computer engineering related software and hardware system.	1. Basic and Discipline specific knowledge: Apply knowledge of basic mathematics, science and Engineering fundamentals and engineering specialization to solve the engineering problems. 2. Problem analysis: Identify and analyse well-defined engineering problems using codified standard methods. 3. Design/ development of solutions: Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs. 4. Engineering Tools, Experimentation and Testing: Apply modern engineering tools and appropriate technique to conduct standard tests and measurements. 5. Engineering practices for society, sustainability and environment: Apply appropriate technology in context of society, sustainability, environment and ethical practices. 6. Project Management: Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well-defined engineering activities. 7. Life-long learning: Ability to analyse individual needs and engage in updating in the context of technological changes.
Program Educational Objectives (PEOs)	
PEO1: Provide socially responsible, environment friendly solutions to Computer Engineering related broad-based problems adapting professional ethics. PEO2: Adapt state-of-the-art Computer engineering broad-based technologies to work in multi-disciplinary work environments. PEO3: Solve broad-based problems individually and as a team member communicating effectively in the world of work.	



Maharashtra State Board of Technical Education, Mumbai

Teaching and Examination Scheme for Post S.S.C. Diploma Courses

Program Name : Diploma in Computer Engineering / Diploma in Computer Technology / Diploma in Computer Science and Engineering

Program Code : CO/CM/CW

With Effect From Academic Year: 2017 - 18

Duration of Program : 6 Semesters

Duration : 16 Weeks

Semester : Sixth

Scheme : I

S. N.	Course Title	Course Abbre- viation	Course Code	Teaching Scheme		Credit (L+T+P)	Examination Scheme												Grand Total		
				L	T		P	Theory						Practical							
								Exam Duration in Hrs.	ESE		PA		Total		ESE		PA			Total	
									Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks	Max Marks	Min Marks		Max Marks	
1	Management	MGT	22509	3	-	-	3	90 Min	70*#	28	30*	00	100	40	--	--	--	--	--	100	
2	Programming with Python	PWP	22616	3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	150	
3	Mobile Application Development	MAD	22617	3	-	4	7	3	70	28	30*	00	100	40	25#	10	25	10	50	150	
4	Emerging Trends in Computer and Information Technology	ETI	22618	3	-	-	3	90 Min	70*#	28	30*	00	100	40	--	--	--	--	--	100	
Elective – II (Select Any One)																					
5	Web Based Application Development Using PHP	WBP	22619	3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	150	
	Network and Information Security	NIS	22620	3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	150	
	Data Warehousing with Mining Techniques	DWM	22621	3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	150	
6	Entrepreneurship Development	EDE	22032	2	-	2	4	--	--	--	--	--	--	--	50@	20	50~	20	100	100	
7	Capstone Project - Execution & Report Writing	CPE	22060	-	-	4	4	--	--	--	--	--	--	--	50#	20	50~	20	100	100	
Total				17	-	14	31	--	350	--	150	--	500	--	175	--	175	--	350	850	

Student Contact Hours Per Week: 31 Hrs.

Medium of Instruction: English

Theory and practical periods of 60 minutes each.

Total Marks : 850

Abbreviations: ESE- End Semester Exam, PA- Progressive Assessment, L - Lectures, T - Tutorial, P - Practical

@ Internal Assessment, # External Assessment, *# On Line Examination, ^ Computer Based Assessment

* Under the theory PA, Out of 30 marks, 10 marks are for micro-project assessment to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessment of the cognitive domain LOs required for the attainment of the COs.

~ For the courses having ONLY Practical Examination, the PA marks Practical Part - with 60% weightage and Micro-Project Part with 40% weightage shall be declared as
➤ If Candidate not securing minimum marks for passing in the "PA" part of practical of any course of any semester then the candidate shall be declared as "Detained" for that semester.



Program Name : Computer Engineering Program Group
Program Code : CO/CM/IF/CW
Semester : Sixth
Course Title : Network and Information Security
Course Code : 22620

1. RATIONALE

Computer network security is an important aspect in today's world. Now days due to various threats designing security in organization is an important consideration. It is essential to understand basic security principles, various threats to security and techniques to address these threats. The student will be able to recognize potential threats to confidentiality, integrity and availability and also able to implement various computer security policies. This course will introduce basic cryptographic techniques, fundamentals of computer/network security, Risks faced by computers and networks, security mechanisms, operating system security, secure System design principles, and network security principles. Also it will create awareness about IT ACT and different Cyber laws.

2. COMPETENCY

The aim of this course is to help the student to attain the following industry identified competency through various teaching learning experiences:

- **Maintain Network and Information security of an organization.**

3. COURSE OUTCOMES (COs)

The theory, practical experiences and relevant soft skills associated with this course are to be taught and implemented, so that the student demonstrates the following *industry oriented* COs associated with the above mentioned competency:

- Identify risks related to Computer security and Information hazard in various situations.
- Apply user identification and authentication methods.
- Apply cryptographic algorithms and protocols to maintain Computer Security.
- Apply measures to prevent attacks on network using firewall.
- Maintain secured networks and describe Information Security Compliance standards.

4. TEACHING AND EXAMINATION SCHEME

Teaching Scheme			Credit (L+T+P)	Examination Scheme													
L	T	P		Theory								Practical					
				Paper Hrs.	ESE		PA		Total		ESE		PA		Total		
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	
3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	20	

(*): Under the theory PA, Out of 30 marks, 10 marks are for micro-project assessment to facilitate integration of COs and the remaining 20 marks is the average of 2 tests to be taken during the semester for the assessment of the UOs required for the attainment of the COs.

Legends: L-Lecture; T – Tutorial/Teacher Guided Theory Practice; P -Practical; C – Credit,ESE -End Semester Examination; PA - Progressive Assessment

5. COURSE MAP (with sample COs, PrOs, UOs, ADOs and topics)

This course map illustrates an overview of the flow and linkages of the topics at various levels of outcomes (details in subsequent sections) to be attained by the student by the end of the



course, in all domains of learning in terms of the industry/employer identified competency depicted at the centre of this map.

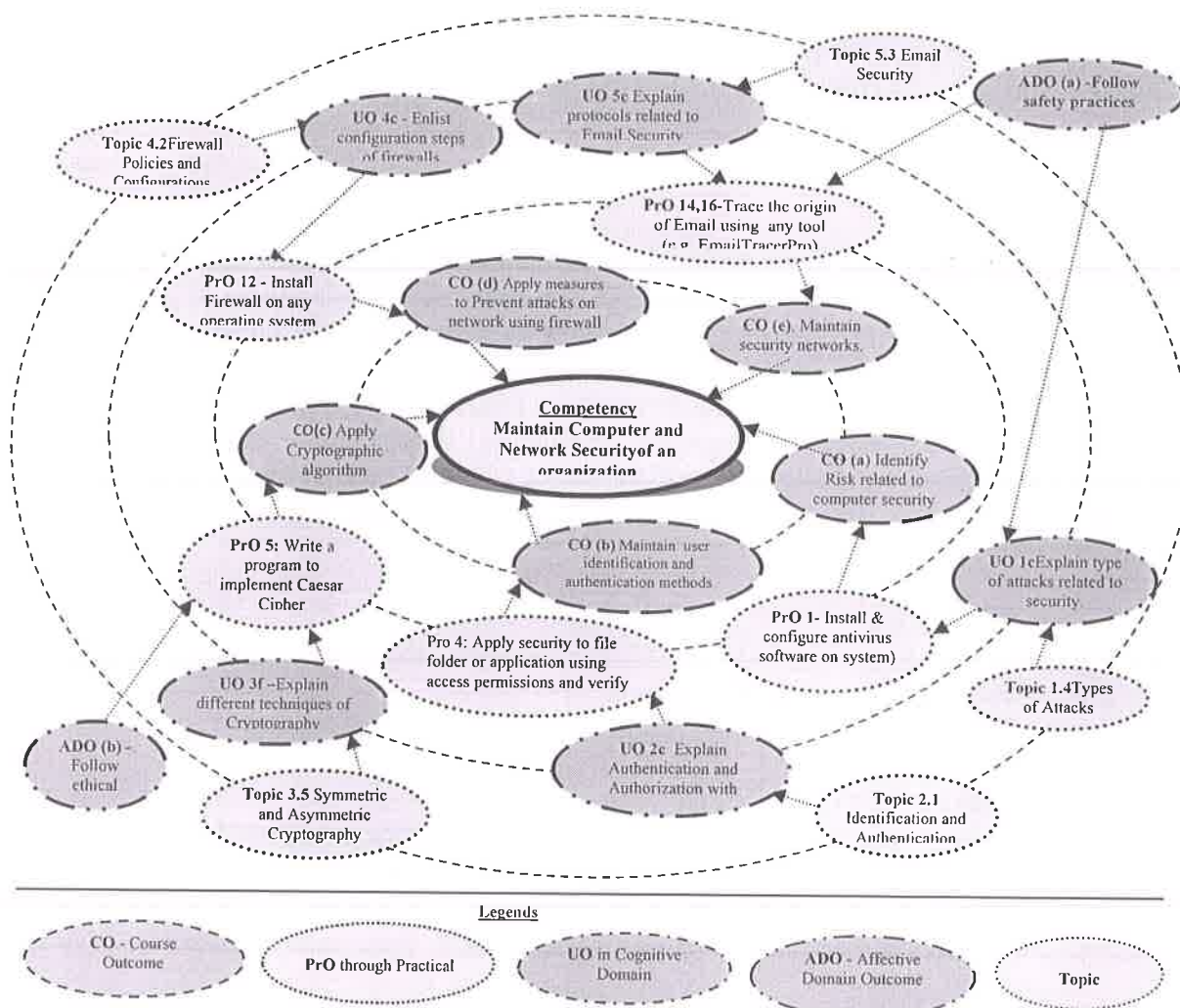


Figure 1 - Course Map

6. SUGGESTED PRACTICALS/ EXERCISES

The practicals in this section are PrOs (i.e. sub-components of the COs) to be developed and assessed in the student for the attainment of the competency.

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
1	a. Install and configure Antivirus software on system (any). b. Set up operating system Updates.	I	2
2	Perform Backup and Restore of the system.	I	2
3	Set up passwords to operating system and applications.	II	2
4	Apply security to file folder or application using access permissions and verify.	II	2
5	Write a program to implement Caesar Cipher	III	2
6	Write a program to implement Vernam Cipher	III	2
7	Create and verify Hash Code for given message	III	2
8	Write a program to implement Rail fence technique	III	2
9	Write a program to implement Simple Columnar Transposition technique	III	2

S. No.	Practical Outcomes (PrOs)	Unit No.	Approx. Hrs. Required
10	Create and verify digital signature using tool (e.g. Cryptool)	III	2
11	Use Steganography to encode and decode the message using any tool.	III	2
12	a. Install firewall on any operating system.	IV	2
	b. Configure firewall settings on any operating system.		
13	Create and verify Digital Certificate using tool (e.g. Cryptool)	V	2
14	Trace the origin of Email using any tool(e.g. emailTrackerPro)	V	2
15	Trace the path of web site using Tracert Utility	V	2
16	PGP Email Security	V	2
	a. Generate Public and Private Key Pair.		
	b. Encrypt and Decrypt message using key pair.		
Total			32

Note

- A suggestive list of PrOs is given in the above table. More such PrOs can be added to attain the COs and competency. All the above listed practical need to be performed compulsorily, so that the student reaches the 'Applying Level' of Blooms's 'Cognitive Domain Taxonomy' as generally required by the industry.
- The 'Process' and 'Product' related skills associated with each PrO are to be assessed according to a suggested sample given below:

S. No.	Performance Indicators	Weightage in %
1	Correctness of the flow of procedures.	40
2	Debugging ability.	20
3	Quality of input and output displayed (messaging and formatting)	10
4	Answer to sample questions	20
5	Submission of report in time	10
Total		100

The above PrOs also comprise of the following social skills/attitudes which are Affective Domain Outcomes (ADOs) that are best developed through the laboratory/field based experiences:

- Work collaboratively in team
- Follow ethical Practices.

The ADOs are not specific to any one PrO, but are embedded in many PrOs. Hence, the acquisition of the ADOs takes place gradually in the student when s/he undertakes a series of practical experiences over a period of time. Moreover, the level of achievement of the ADOs according to Krathwohl's 'Affective Domain Taxonomy' should gradually increase as planned below:

- 'Valuing Level' in 1st year
- 'Organization Level' in 2nd year.
- 'Characterization Level' in 3rd year.

7. MAJOR EQUIPMENT/ INSTRUMENTS REQUIRED

The major equipment with broad specification mentioned here will usher in uniformity in conduct of practicals, as well as aid to procure equipment by authorities concerned.



S. No.	Equipment Name with Broad Specifications	PrO. S. No.
1	Computer system (Any computer system with basic configuration)	All
2	Antivirus Software(any)	
3	Any compiler	6,7,8,9
4	Encryption Decryption tool(preferably Open source based)	10,13
5	Steganography Tools. (preferably Open source based)	11
6	E-mail tracing Tools. (preferably Open source based)	14
7	Web tracing Tools. (preferably Open source based)	15

8. UNDERPINNING THEORY COMPONENTS

The following topics/subtopics should be taught and assessed in order to develop UOs in cognitive domain for achieving the COs to attain the identified competency. More UOs could be added.

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit – I Introduction to Computer and Information Security	1a. Explain the importance of the given component of computer security. 1b. Explain the characteristics of the given type of threat. 1c. Explain the given type of attacks related with security. 1d. Describe the features of given type of update of operating system. 1e. Classify Information. 1f. Explain Principles of Information Security.	1.1 Foundations of Computer Security: Definition and Need of computer security, Security Basics: Confidentiality, Integrity, Availability, Accountability, Non-Repudiation and Reliability. 1.2 Risk and Threat Analysis: Assets, Vulnerability, Threats, Risks, Counter measures. 1.3 Threat to Security: Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan Horse, Intruders, Insiders. 1.4 Type of Attacks: Active and Passive attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, Spoofing, Man in the Middle, Replay, TCP/IP Hacking, Encryption attacks. 1.5 Operating system security: Operating system updates : HotFix, Patch, Service Pack. 1.6 Information, Need and Importance of Information, information classification, criteria for information classification, Security, need of security, Basics principles of information security.



Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit– II User Authenticati on and Access Control	2a. Explain techniques of the given type of attack on passwords. 2b. Explain mechanism of the given type of Biometric. 2c. Apply the relevant Authentication method for the given situation with an example. 2d. Describe features of the given access control policy.	2.1 Identification and Authentication: User name and Password, Guessing password, Password attacks-Piggybacking, Shoulder surfing, Dumpster diving. 2.2 Biometrics: Finger Prints, Hand prints, Retina, patterns, Voice patterns, Signature and Writing patterns, Keystrokes. 2.3 Access controls: Definition, Authentication Mechanism, principle-Authentication, Authorization, Audit, Policies: DAC, MAC, RBAC.
Unit– III Cryptograph y	3a. Encrypt/Decrypt the given text using different substitution techniques. 3b. Convert plain text to cipher text and vice versa using the given transposition technique. 3c. Convert the given message using steganography. 3d. Explain the given technique of cryptography using example.	3.1 Introduction: Plain Text, Cipher Text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption. 3.2 Substitution Techniques: Caesar's cipher, Modified Caesar's Cipher, Transposition Techniques: Simple Columnar Transposition. 3.3 Steganography : Procedure 3.4 Symmetric and Asymmetric cryptography: Introduction to Symmetric encryption, DES (Data encryption Standard) algorithm, Asymmetric key cryptography: Digital Signature.
Unit-IV Firewall and Intrusion Detection System	4a. Compare types of firewall on the given parameter(s). 4b. Explain function of the given type of firewall configuration. 4c. Compare various IDS techniques on the given parameter(s). 4d. Describe features of the given IDS technique.	4.1 Firewall : Need of Firewall, types of firewall- Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. 4.2 Firewall Policies, Configuration, limitations, DMZ. 4.3 Intrusion Detection System : Vulnerability Assessment, Misuse detection, Anomaly Detection, Network-Based IDS, Host-Based IDS, Honeypots
Unit –V Network Security, Cyber Laws and Compliance Standards.	5a. Explain the given component of Kerberos authentication protocol. 5b. Explain the given IP Security protocol with modes. 5c. Explain working of the given protocol for Email security. 5d. Describe the given component of Public Key Infrastructure. 5e. Classify the given Cyber crime.	5.1 Kerberos : Working, AS, TGS, SS 5.2 IP Security- Overview, Protocols- AH, ESP, Modes- transport and Tunnel. 5.3 Email security- SMTP, PEM, PGP. 5.4 Public key infrastructure (PKI): Introduction, Certificates, Certificate authority, Registration Authority, X.509/PKIX certificate format. 5.5 Cyber Crime: Introduction, Hacking , Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography , Identity Theft and Fraud , Cyber terrorism, Cyber Defamation. 5.6 Cyber Laws: Introduction, need,

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
	5f. Explain the specified Cyber law. 5g. Describe compliance standards for Information Security.	Categories: Crime against Individual, Government, Property. 5.7 Compliance standards: Implementing and Information Security Management System, ISO 27001, ISO 20000, BS 25999, PCI DSS, ITIL framework, COBIT framework.

Note: To attain the COs and competency, above listed UOs need to be undertaken to achieve the 'Application Level' of Bloom's 'Cognitive Domain Taxonomy'

9. SUGGESTED SPECIFICATION TABLE FOR QUESTION PAPER DESIGN

Unit No.	Unit Title	Teaching Hours	Distribution of Theory Marks			
			R Level	U Level	A Level	Total Marks
I	Introduction to Computer and Information Security	12	06	06	02	14
II	User Authentication and Access Control	06	04	04	02	10
III	Cryptography	06	02	04	08	14
IV	Firewall and Intrusion Detection System	12	04	06	08	18
V	Network Security, Cyber Laws and Compliance Standards.	12	06	06	02	14
Total		48	22	26	22	70

Legends: R=Remember, U=Understand, A=Apply and above (Bloom's Revised taxonomy)

Note: This specification table provides general guidelines to assist student for their learning and to teachers to teach and assess students with respect to attainment of UOs. The actual distribution of marks at different taxonomy levels (of R, U and A) in the question paper may vary from above table.

10. SUGGESTED STUDENT ACTIVITIES

Other than the classroom and laboratory learning, following are the suggested student-related **co-curricular** activities which can be undertaken to accelerate the attainment of the various outcomes in this course: Students should conduct following activities in group and prepare reports of about 5 pages for each activity, also collect/record physical evidences for their (student's) portfolio which will be useful for their placement interviews:

- Prepare journal of practicals.
- Undertake micro-projects.

11. SUGGESTED SPECIAL INSTRUCTIONAL STRATEGIES (if any)

These are sample strategies, which the teacher can use to accelerate the attainment of the various learning outcomes in this course:

- Massive open online courses (**MOOCs**) may be used to teach various topics/sub topics.
- 'L' in item No. 4 does not mean only the traditional lecture method, but different types of teaching methods and media that are to be employed to develop the outcomes.
- About **15-20% of the topics/sub-topics** which is relatively simpler or descriptive in nature is to be given to the students for **self-directed learning** and assess the

- development of the COs through classroom presentations (see implementation guideline for details).
- With respect to item No.10, teachers need to ensure to create opportunities and provisions for **co-curricular activities**.
 - Guide student(s) in undertaking micro-projects.
 - Demonstrate students thoroughly before they start doing the practice.
 - Encourage students to refer different websites to have deeper understanding of the subject.
 - Observe continuously and monitor the performance of students in Lab.

12. SUGGESTED MICRO-PROJECTS

Only one micro-project is planned to be undertaken by a student that needs to be assigned to him/her in the beginning of the semester. In the first four semesters, the micro-project is group-based. However, in the fifth and sixth semesters, it should be preferably be **individually** undertaken to build up the skill and confidence in every student to become problem solver so that s/he contributes to the projects of the industry. In special situations where groups have to be formed for micro-projects, the number of students in the group should **not exceed three**.

The micro-project could be industry application based, internet-based, workshop-based, laboratory-based or field-based. Each micro-project should encompass two or more COs which are in fact, an integration of PrOs, UOs and ADOs. Each student will have to maintain dated work diary consisting of individual contribution in the project work and give a seminar presentation of it before submission. The total duration of the micro-project should not be less than **16 (sixteen) student engagement hours** during the course. The student ought to submit micro-project by the end of the semester to develop the industry-oriented COs.

A suggestive list of micro-projects is given here. Similar micro-projects could be added by the concerned faculty:

- Case Studies in Secure Computing: Achievements and Trends.
- Implement Client/Server communication using cryptography tools in your laboratory.
- Create digital certificate for your departmental/ personal communication.
- Implement communication system using steganography. Encrypt image and message using any cryptography technique.
- Implement communication system using steganography using audio files. Encrypt audiofile and message using any cryptography technique.
- Implement Three Level Password Authentication System.
- Any other micro-projects suggested by subject faculty on similar line.

13. SUGGESTED LEARNING RESOURCES

S. No.	Title of Book	Author	Publication
1	Computer Security	Dieter Gollmann	Wiley Publication, New Delhi, ISBN : 978-0-470-74115-3
2	Cryptography and Network Security	Atul Kahate	McGraw Hill Education, New Delhi ISBN: 978-1-25-902988-2
3	Cyber Laws And IT Protection	Harish Chander	PHI Publication, New Delhi, 2012 ISBN: 978-81-203-4570-6
4	Implementing Information Security based on ISO 27001 / ISO 27002 (Best Practice)	Alan Calder	Van Haren Publishing ISBN-13: 978-9087535414 ISBN-10: 9087535414



14. SOFTWARE/LEARNING WEBSITES

- a) <http://nptel.ac.in/courses/106105162/>
- b) https://www.tutorialspoint.com//computer_security/computer_security_quick_guide.htm
- c) <http://learnthat.com/introduction-to-network-security/>
- d) <https://freevideolectures.com/course/3027/cryptography-and-network-security>
- e) <https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/>
- f) <http://stylesuxx.github.io/steganography/>
- g) <https://smartninja-pgp.appspot.com/>
- h) <http://www.cyberlawsindia.net/cyber-india.html>
- i) <https://www.upcounsel.com/cyber-law>
- j) <http://cyberlaws.net/cyber-law/>





JSPM's
Rajarshi Shahu College of Engineering,
Polytechnic, Tathawade, Pune-33



Academic Year 2024-25

MSBTE QUESTION PAPER ANALYSIS

Course: Network and Information Security

Course Code: 22620

Unit No.	Marks as per Teaching Scheme	Marks weightage in W-2024 QP	Marks weightage in S-2024 QP	Marks weightage in W-2023 QP	Marks weightage in S-2023 QP	Marks weightage in W-2022 QP	Marks weightage in S-2022 QP
Unit No. 1	14	20	24	24	22	22	20
Unit No. 2	10	14	14	10	12	14	14
Unit No. 3	14	20	22	26	20	22	22
Unit No. 4	18	28	26	26	26	26	26
Unit No. 5	14	20	16	16	22	18	20
Total Marks	70	102	102	102	102	102	102

Subject In-charge

(Mrs.N.N.Kawale)

DAC

(Mrs.S.U.Puri)

HOD

(Prof.V.T.Thakare)



JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING,
POLYTECHNIC

Department of Computer Engineering

Academic Year: 2024-25




UNIT-I (14 Marks)

MSBTE Question bank & Answer

Q.No	Question	Year	Marking																					
01.	Define following terms: i) Confidentiality ii) Accountability	S-22	2M																					
Answer:	i) Confidentiality: The principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message. ii) Accountability: The principle of accountability specifies that every individual who works with an information system should have specific responsibilities for information assurance. The tasks for which a individual is responsible are part of the overall information security plan and can be readily measurable by a person who has managerial responsibility for information assurance.																							
02.	Differentiate between viruses & worms (Any two).	S-22	2M																					
Answer:	<table><tr><th>S. No</th><th>Worms</th><th>Virus</th></tr><tr><td>1</td><td>The worm is code that replicate itself in order to consume resources to bring it down.</td><td>The virus is the program code that attaches itself to application program and when application program run it runs along with it</td></tr><tr><td>2</td><td>It exploits a weakness in an application or operating system by replicating itself</td><td>It inserts itself into a file or executable program.</td></tr><tr><td>3</td><td>It can use a network to replicate itself to other computer systems without user intervention.</td><td>It has to rely on users transferring infected files/programs to other computer systems.</td></tr><tr><td>4</td><td>Usually not. Worms usually only monopolize the CPU and memory.</td><td>Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.</td></tr><tr><td>5</td><td>Worm is faster than virus</td><td>Virus is slower than worm.</td></tr><tr><td>6</td><td>E.g. Code red</td><td>E.g. Macro virus, Directory virus, Stealth Virus</td></tr></table>	S. No	Worms	Virus	1	The worm is code that replicate itself in order to consume resources to bring it down.	The virus is the program code that attaches itself to application program and when application program run it runs along with it	2	It exploits a weakness in an application or operating system by replicating itself	It inserts itself into a file or executable program.	3	It can use a network to replicate itself to other computer systems without user intervention.	It has to rely on users transferring infected files/programs to other computer systems.	4	Usually not. Worms usually only monopolize the CPU and memory.	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.	5	Worm is faster than virus	Virus is slower than worm.	6	E.g. Code red	E.g. Macro virus, Directory virus, Stealth Virus	S-24	2M
	S. No	Worms	Virus																					
	1	The worm is code that replicate itself in order to consume resources to bring it down.	The virus is the program code that attaches itself to application program and when application program run it runs along with it																					
	2	It exploits a weakness in an application or operating system by replicating itself	It inserts itself into a file or executable program.																					
	3	It can use a network to replicate itself to other computer systems without user intervention.	It has to rely on users transferring infected files/programs to other computer systems.																					
	4	Usually not. Worms usually only monopolize the CPU and memory.	Yes, it deletes or modifies files. Sometimes a virus also changes the location of files.																					
	5	Worm is faster than virus	Virus is slower than worm.																					
6	E.g. Code red	E.g. Macro virus, Directory virus, Stealth Virus																						
		W-24	2M																					

03.	<p>Define following terms :</p> <p>(i) Operating System Security (ii) Hot fix (iii) Patch (iv) Service pack</p>	S-22 W-24	4M 4M
Answer:	<p>i) Operating System Security: The OS must protect itself from security breaches, such as runaway processes (denial of service), memory-access violations, stack overflow violations, the launching of programs with excessive privileges, and many others.</p> <p>ii) Hot Fix: Normally this term is given to small software update designed to address a particular problem like buffer overflow in an application that exposes the system to attacks.</p> <p>iii) Patch: This term is generally applied to more formal, larger s/w updates that may address several or many s/w problems. Patches often contain improvement or additional capabilities & fixes for known bugs.</p> <p>iv) Service Pack: <i>service pack</i> is a collection of updates and fixes, called patches, for an operating system or a software program. Many of these patches are often released before a larger service pack, but the service pack allows for an easy, single installation.</p>		
04.	<p>Define Information. Explain basic principle of Information security</p> <p>OR</p> <p>Describe CIA model with suitable diagram.</p> <p>OR</p> <p>Define CIA model of Security Basic.</p>	S-22 W-23 S-23 W-24	6M 4M 4M 2M
Answer:	<p>Information is organized or classified data, which has some meaningful values for the receiver. Information is the processed data on which knowledge, decisions and actions are based. For the decision to be meaningful, the processed data must qualify for the following characteristics</p> <ul style="list-style-type: none"> • Timely – Information should be available when required. • Accuracy – Information should be accurate. • Completeness – Information should be complete. 		

	<p>Basic Principles of information security</p>  <p>Fig: CIA Triad of information security</p> <ol style="list-style-type: none"> 1. Confidentiality: The goal of confidentiality is to ensure that only those individuals who have the authority can view a piece of information, the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message. 2. Authentication: It helps to establish proof of identities. Authentication process ensures that the origin of a message is correctly identified. Authentication deals with the desire to ensure that an individual is who they claim to be. 3. Integrity: Integrity is a related concept but deals with the generation and modification of data. Only authorized individuals should ever be able to create or change (or delete) information. When the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. 		
05.	<p>Explain DOS with neat diagram.</p> <p>Answer: Denial Of Service Attack: Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself. The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP</p>	<p>S-22 S-24</p>	<p>6M 4M</p>

	<p>networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems.</p> <p>In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come, as shown in Figure. The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.</p>		
<p>06.</p> <p>Answer:</p>	<p>Define computer security and state its need.</p> <p>Computer Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization.</p> <p>Need of computer Security:</p> <ol style="list-style-type: none"> 1. For prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc. 2. To make data remain safe and confidential. 3. To provide confidentiality which ensures that only those individuals should ever be able to view data they are not entitled to. 4. To provide integrity which ensures that only authorized individuals should ever be able change or modify information. 5. To provide availability which ensure that the data or system itself is available for use when authorized user wants it. 6. To provide authentication which deals with the desire to ensure that an authorized individual. <p style="text-align: center;"><u>OR</u></p> <p>The need of computer security has been threefold: confidentiality, integrity, and authentication—the “CIA” of security.</p>	W-22	2M

	<p>1. Confidentiality: the principle of confidentiality specifies that only sender and intended recipients should be able to access the contents of a message. Confidentiality gets compromised if an unauthorized person is able to access the contents of a message.</p> <p>2. Integrity: when the contents of the message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.</p> <p>3. Authentication: Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly identified.</p>		
<p>07.</p> <p>Answer:</p>	<p>State the meaning of hacking.</p> <p style="text-align: center;">OR</p> <p>Define Hacking. Explain different types of Hackers.</p> <p>State the meaning of hacking. Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. OR Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Hacking is not always a malicious activity, but the term has mostly negative connotations due to its association with cybercrime.</p> <p style="text-align: center;"><u>OR</u></p> <p>Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage. OR Hacking is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Hacking is not always a malicious activity, but the term has mostly negative connotations due to its association with cybercrime.</p> <p>Types of Hackers:</p> <ol style="list-style-type: none"> 1) Black Hat Hacker 2) White Hat Hacker 3) Grey Hat Hacker 	<p>W-22</p> <p>S-24</p>	<p>2M</p> <p>4M</p>

	<p>Black Hat Hacker Black-hat Hackers are also known as an Unethical Hacker or a Security Cracker. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.</p> <p>White Hat Hacker White hat Hackers are also known as Ethical Hackers or a Penetration Tester. White hat hackers are the good guys of the hacker world. These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.</p> <p>Grey Hat Hacker Grey hats Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system. In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.</p>		
08.	<p>Describe sniffing attack.</p> <p>Answer: This is software or hardware that is used to observe traffic as it passes through a network on shared broadcast media. It can be used to view all traffic or target specific protocol, service, or string of characters like logins. Some network sniffers are not just designed to observe the all traffic but also modify the traffic. Network administrators use sniffers for monitoring traffic. They can also use for network bandwidth analysis and to troubleshoot certain problems such as duplicate MAC addresses.</p>	W-22	2M
09.	<p>Define Risk. Describe qualitative and quantitative risk analysis.</p> <p>Answer: Risk: A computer security risk is any event or action that could cause a loss or damage to computer hardware, software, data, or information OR Risk is probability of threats that may occur because of presence of vulnerability in a system.</p> <p>Quantitative Risk Analysis: A Process of assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats. It is used to determine</p>	W-22	4M

	<p>potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation. In this 100% quantitative risk analysis is not possible.</p> <p>Qualitative Risk Analysis: A collaborative process of assigning relative values to assets, assessing their risk exposure and estimating the cost of controlling the risk. It utilizes relative measures and approximate costs rather than precise valuation and cost determination. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc. In this 100% qualitative risk analysis is feasible.</p>		
<p>10.</p> <p>Answer:</p>	<p>Explain any three criteria for classification of information.</p> <p style="text-align: center;">OR</p> <p>State the criteria for information classification. Explain information classification.</p> <p>Useful life A data is labeled „more useful“ when the information is available ready for making changes as and when required. Data might need to be changed from time to time, and when the „change“ access is available, it is valuable data. ii) Value of data This is probably the most essential and standard criteria for information classification. There is some confidential and valuable information of every organization, the loss of which could lead to great losses for the organization while creating organizational issues. Therefore, this data needs to be duly classified and protected. iii) Personal association It is important to classify information or data associated with particular individuals or addressed by privacy law. iv) Age The value of information often declines with time. Therefore, if the given data or information comes under such a category, the data classification gets lowered.</p> <p style="text-align: center;">OR</p> <p>1. Sensitivity: Sensitivity refers to the level of potential harm or damage that could result from unauthorized disclosure, alteration, or destruction of information.</p> <p>2. Confidentiality: Confidentiality measures the extent to which information should be kept secret and protected from unauthorized access.</p>	<p>W-22</p> <p>S-24</p> <p>W-23</p> <p>W-24</p>	<p>6M</p> <p>6M</p> <p>6M</p> <p>4M</p>

	<p>3. Criticality to Operations: Criticality relates to the importance of information for the organization's core business functions and operations.</p> <p>4. Legal and Regulatory Requirements: Legal and regulatory requirements may mandate specific levels of protection for certain types of information.</p> <p>8. Data Ownership: Definition: Consideration of the ownership of the information within the organization.</p> <p>5. Value to Competitors: Information that could provide a competitive advantage to other organizations if disclosed or misused.</p> <p>6. Risk of Financial Loss: Evaluate the financial consequences that may result from the compromise of specific information.</p> <p>7. Personal Identifiable Information (PII): Definition: PII refers to information that can be used to identify individuals, requiring special protection due to privacy concerns.</p> <p>8. Data Ownership: Definition: Consideration of the ownership of the information within the organization.</p>		
<p>11.</p> <p>Define virus and describe the phases of virus. OR Describe any three phases of virus with suitable example.</p> <p>Answer:</p> <p>Definition: Virus is a program which attaches itself to another program and causes damage to the computer system or the network. It is loaded onto your computer without your knowledge and runs against your wishes. During the lifecycle of virus it goes through the following four phases:</p> <p>1. Dormant phase: The virus is idle and activated by some event.</p> <p>2. Propagation phase: It places an identical copy of itself into other programs or into certain system areas on the disk.</p> <p>3. Triggering phase: The virus is activated to perform the function for which it was intended.</p> <p>4. Execution phase: The function of virus is performed</p>		<p>W-22</p> <p>S-23</p>	<p>6M</p> <p>6M</p>

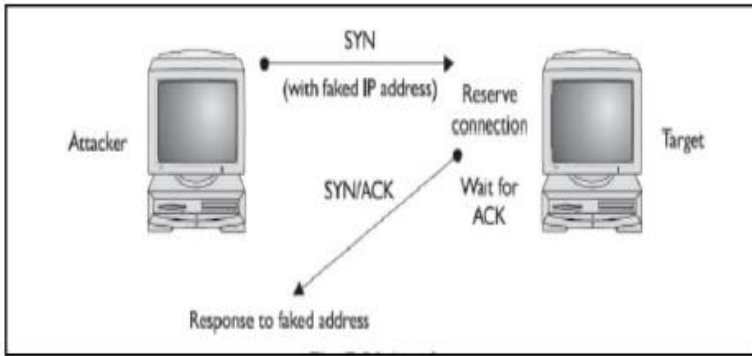
	<div>Example:</div> <div><div><div>Add i to j Print close end</div><div>Add i to j Virus job close end</div><div>Delete all files send copy to user return</div></div><div><div>Original code</div><div>Infected code due to virus</div><div>Virus Code</div></div></div> <td></td> <td></td>																							
<div>12.</div> <div>Answer:</div>	<div>Compare virus and logic bomb. (Any two points).</div> <table><tr><td>Characteristics</td><td>Virus</td><td>Logic Bomb</td></tr><tr><td>Nature</td><td>Self-replicating program that sticks to files</td><td>Code that stays quiet until a trigger</td></tr><tr><td>Replication</td><td>Makes copies of itself to move to other files</td><td>Doesn't make copies, stays put</td></tr><tr><td>Activation</td><td>Starts when you open an infected file</td><td>Wakes up when a specific event happens</td></tr><tr><td>Purpose</td><td>Created to spread and potentially harm</td><td>Used for specific attacks under conditions</td></tr><tr><td>Visibility</td><td>Often noticeable due to spreading behavior</td><td>Hidden until it's time to do something</td></tr><tr><td>Main Function</td><td>Spreads and may damage files/systems</td><td>Stays inactive until a specific trigger</td></tr></table>	Characteristics	Virus	Logic Bomb	Nature	Self-replicating program that sticks to files	Code that stays quiet until a trigger	Replication	Makes copies of itself to move to other files	Doesn't make copies, stays put	Activation	Starts when you open an infected file	Wakes up when a specific event happens	Purpose	Created to spread and potentially harm	Used for specific attacks under conditions	Visibility	Often noticeable due to spreading behavior	Hidden until it's time to do something	Main Function	Spreads and may damage files/systems	Stays inactive until a specific trigger	<div>S-23</div> <div>S-24</div>	<div>2M</div> <div>2M</div>
Characteristics	Virus	Logic Bomb																						
Nature	Self-replicating program that sticks to files	Code that stays quiet until a trigger																						
Replication	Makes copies of itself to move to other files	Doesn't make copies, stays put																						
Activation	Starts when you open an infected file	Wakes up when a specific event happens																						
Purpose	Created to spread and potentially harm	Used for specific attacks under conditions																						
Visibility	Often noticeable due to spreading behavior	Hidden until it's time to do something																						
Main Function	Spreads and may damage files/systems	Stays inactive until a specific trigger																						
<div>13.</div> <div>Answer:</div>	<div>Identify any four individual user responsibilities in computer security.</div> <div>Individual user responsibilities in computer security are:</div> <div><div>1. Lock the door of office or workspace.</div><div>2. Do not leave sensitive information inside your car unprotected.</div><div>3. Secure storage media in a secure storage device which contains sensitive information.</div><div>4. Shredding paper containing organizational information before discarding it.</div><div>5. Do not expose sensitive information to individuals that do not have an authorized need to know it.</div></div>	<div>S-23</div>	<div>2M</div>																					

<p>14.</p> <p>Answer:</p>	<p>List any two types of active and passive attacks.</p> <p style="text-align: center;">OR</p> <p>Enlist two Active & Passive attack each.</p> <p>Active Attack Types are:</p> <ol style="list-style-type: none"> 1. Release of message contents. 2. Traffic Analysis. <p>Passive Attack Types are:</p> <ol style="list-style-type: none"> 1. Interruption attack 2. Modification attack 	<p>S-23 W-24</p>	<p>2M 2M</p>
<p>15.</p> <p>Answer:</p>	<p>Describe the following terms:</p> <p>(i) Assets (ii) Vulnerability (iii) Risks</p> <p>(i)Assets: – Asset is any data, device, or other component of the environment that supports information-related activities. – Assets generally include hardware, software and confidential information.</p> <p>(ii) Vulnerabilities: – It is a weakness in computer system & network. The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful. – Vulnerability testing should be performed on an on-going basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed. – Such vulnerabilities are not particular to technology - they can also apply to social factors such as individual authentication and authorization policies. – Testing for vulnerabilities is useful for maintaining on-going security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise. – It is also invaluable for policy and technology development, and as part of a technology selection process; selecting the right technology early on can ensure significant savings in time, money, and other business costs further down the line.</p> <p>(iii) Risk: – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: 1. The adverse impacts that would arise if the circumstance or event occurs; 2. The likelihood of occurrence.</p>	<p>S-23</p>	<p>6M</p>

16.	List any four virus categories.	W-23	2M
Answer:	1. File Infector Viruses. 2. Boot Sector Viruses. 3. Macro Viruses. 4. Polymorphic Viruses		
17.	Give examples of Active & Passive Attacks (two each).	W-23	2M
Answer:	Active Attacks: <ul style="list-style-type: none"> • Man-in-the-Middle (MITM) Attack • Denial-of-Service (DoS) Attack Passive Attacks: <ul style="list-style-type: none"> • Eavesdropping • Traffic Analysis 		
18.	Explain any two password attacks.	W-23	4M
Answer:	1. Brute Force Attack Description: A brute force attack involves systematically guessing a password by trying every possible combination of characters until the correct one is found. This method relies on computing power to generate and test password combinations. How It Works: <ul style="list-style-type: none"> ○ The attacker uses automated tools to try different character combinations, starting from simple ones and progressing to more complex variations. ○ Strong passwords with greater complexity (e.g., a mix of upper- and lower-case letters, numbers, and symbols) take significantly longer to crack. Examples: <ul style="list-style-type: none"> ○ An attacker targets a web application login page by attempting thousands of passwords per second. ○ A local brute force attack on a hashed password file. Mitigation: Implementing account lockout policies after a certain number of failed attempts. Using CAPTCHAs to prevent automated attacks. Encouraging the use of long and complex passwords.		

	<p>2. Phishing Attack</p> <p>Description: A phishing attack involves tricking a user into voluntarily providing their password by impersonating a trusted entity (e.g., a bank, email provider, or company).</p> <p>How It Works:</p> <ul style="list-style-type: none"> ○ The attacker sends a fraudulent email or message containing a link to a fake website that resembles a legitimate one. ○ The victim is prompted to enter their password and other credentials, which are then captured by the attacker. <p>Examples:</p> <ul style="list-style-type: none"> ○ Receiving an email claiming to be from a bank, asking to verify account details on a fraudulent website. ○ SMS-based phishing (smishing), where the victim is tricked into providing credentials through a text message. <p>Mitigation: Educating users to identify phishing attempts (e.g., checking email addresses, URLs, and grammar). Using multi-factor authentication (MFA) to add an extra layer of security.</p>		
<p>19.</p> <p>Answer:</p>	<p>Explain the following attacks using an example: (i) Sniffing (ii) Spoofing (iii) Phishing</p> <p>(i) Sniffing: Sniffing is a type of network attack where an attacker intercepts and monitors data transmitted over a network. The attacker uses a packet sniffer or network analyzer tool to capture network traffic, including sensitive information like passwords, emails, and personal messages. This attack is particularly effective on unsecured networks, such as public Wi-Fi, where data is transmitted in clear text and is not encrypted.</p> <p>Example: Imagine you're using a public Wi-Fi network at a coffee shop, and you log into your online bank account. While you're browsing, an attacker sitting nearby uses a sniffer tool like Wire shark to capture the data packets transmitted over the network. Because the data is not encrypted, the attacker can see your login credentials, including your username and password. The attacker may then use this information to access your bank account.</p>	W-23	6M

	<p>(ii) Spoofing: Spoofing is an attack where an attacker impersonates another device, user, or system to gain unauthorized access or perform malicious actions. There are several types of spoofing, such as IP spoofing, email spoofing and DNS spoofing.</p> <p>Example (IP Spoofing): In IP spoofing, the attacker sends IP packets from a forged source address to appear as though the packets are coming from a trusted source. For example, an attacker may send a packet that appears to be from the IP address of a legitimate server, such as a bank's website, tricking the victim into trusting it. Imagine an attacker sends a malicious packet that appears to be from a legitimate banking website.</p> <p>(iii) Phishing: Phishing is a type of social engineering attack where an attacker impersonates a legitimate organization or individual, usually via email, to trick the victim into disclosing sensitive information such as passwords, credit card numbers, or personal details.</p> <p>Example: An attacker sends an email that looks like it's from a reputable company, such as a bank or an online store. The email contains a message warning the recipient about suspicious activity in their account and asks them to click a link to verify their account details. The link leads to a fake website that looks identical to the real site. Once the victim enters their personal information (such as username and password), the attacker captures this data and can use it to steal money or perform identity theft.</p>		
20.	Explain the term assets.	S-24	2M
Answer:	<p>Assets: Asset is any data, device, or other component of the environment that supports information related activities.</p> <p>Example: Assets generally include hardware, software and confidential information.</p>		
21.	Explain DOS with neat diagram.	S-24	4M
Answer:	<p>Denial Of Service Attack: Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself. The purpose of such an attack can be simply to prevent access to the target system, or the attack</p>		

	<p>can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems. In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come.</p>  <p style="text-align: center;">Fig: DOS Attack</p> <p>The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.</p>		
22.	Explain active attack & passive attack with suitable example.	S-24	6M
Answer:	<p>Passive Attack: A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.</p>		

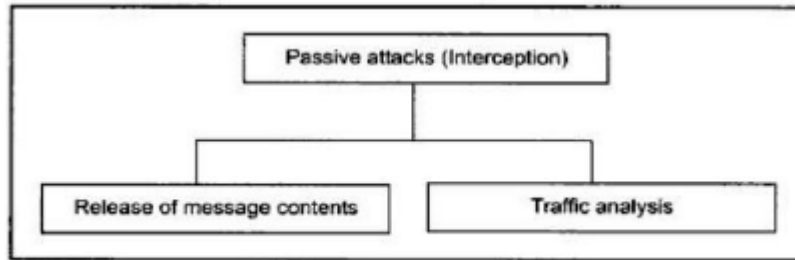


Fig Passive Attacks

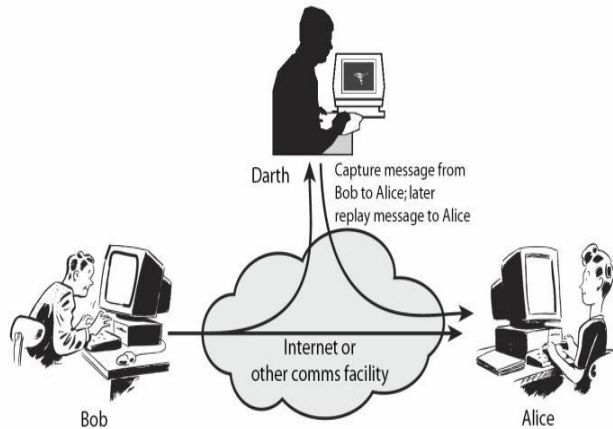
Passive attacks include:

- traffic analysis,
- release of message contents
- monitoring of unprotected communications,
- decrypting weakly encrypted traffic,
- Capturing authentication information such as passwords.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. The release of message contents is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions. A second type of passive attack, traffic analysis: Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern.

However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attack: In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.



Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Active attacks can be divided into four categories:

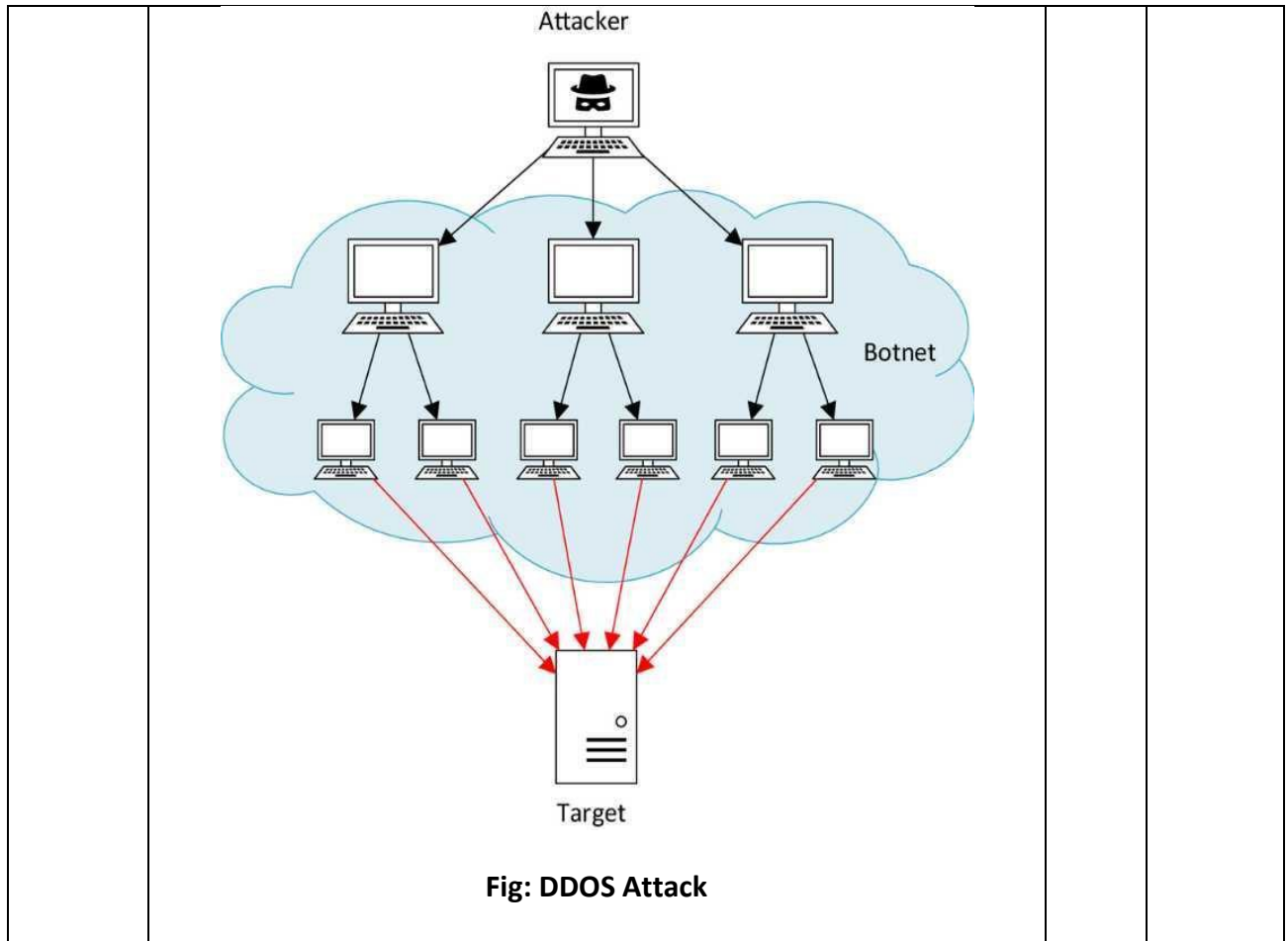
- masquerade,
- replay,
- modification of messages,
- Denial of Service (DoS)

A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. In replay attack, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning "Allow Ajay to read confidential accounts" is modified to mean "Allow Vijay to read confidential accounts."

23.	Draw & Explain DOS & DDOS attack in details	W-24	6M
<p>Answer:</p>	<p>Denial Of Service Attack: Denial of service (DOS) attack scan exploits a known vulnerability in a specific application or operating system, or they may attack features (or weaknesses) in specific protocols or services. In this form of attack, the attacker is attempting to deny authorized users access either to specific information or to the computer system or network itself. The purpose of such an attack can be simply to prevent access to the target system, or the attack can be used in conjunction with other actions in order to gain unauthorized access to a computer or network. SYN flooding is an example of a DOS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DOS attack. SYN flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems. In a SYN flooding attack, the attacker sends fake communication requests to the targeted system. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake the target will wait for responses that will never come.</p> <div data-bbox="394 1008 1144 1411" data-label="Diagram"> <pre> sequenceDiagram participant Attacker participant Target Attacker->>Target: SYN (with faked IP address) Note over Target: Reserve connection, Wait for ACK Attacker->>Target: SYN/ACK Target-->>Attacker: Response to faked address </pre> </div> <p>Fig: DOS Attack</p> <p>The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them, the system will quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be processed, the system will soon be reserving all its connections for fake requests. At this point, any further requests are simply dropped (ignored), and legitimate users who want to connect to the target system will not be able to. Use of the system has thus been denied to them.</p>		

	<p>A DDoS (Distributed Denial of Service) attack: It is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Unlike a regular DoS (Denial of Service) attack, which uses a single system to launch the attack, a DDoS attack utilizes multiple compromised systems, often distributed across various geographic locations, making it harder to defend against.</p> <p>DDoS Attacks Work:</p> <ol style="list-style-type: none"> 1. Botnet: Attackers typically use a network of compromised devices (known as a botnet) to carry out the attack. These devices could be anything from personal computers to IoT devices like smart cameras or routers that have been infected with malware. 2. Flooding Traffic: The botnet sends massive amounts of traffic (requests, data packets, etc.) to the target server or network, causing it to become overwhelmed and unable to function properly. 3. Target Impact: The result is that legitimate users cannot access the services, applications, or websites hosted by the target because the system has been overwhelmed and cannot respond to their requests. 		
--	---	--	--





JSPM's
**RAJARSHI SHAHU COLLEGE OF ENGINEERING,
POLYTECHNIC**
Department of Computer Engineering
Academic Year: 2024-25



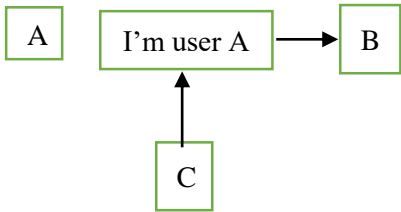
UNIT-II (10 Marks)

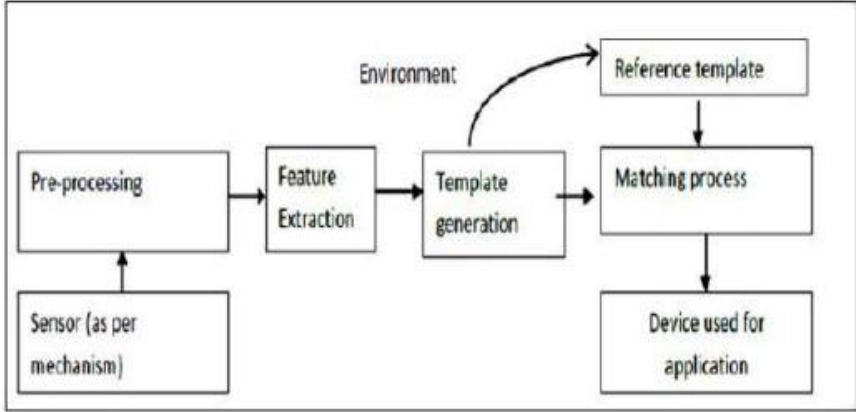
MSBTE Question bank & Answer

Q.No	Question	Year	Marking
01.	Explain the terms : (i) Shoulder surfing (ii) Piggybacking	S-22	2M
Answer:	<p>i) Shoulder surfing: It is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is a similar procedure in which attackers position themselves in such a way as to- be-able to observe the authorized user entering the correct access code.</p> <ul style="list-style-type: none">• Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. <p>ii) Piggybacking: Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission , it means when an authorized person allows (intentionally or unintentionally) others to pass through a secure door.</p>	S-23	4M

<p>02.</p> <p>Answer:</p>	<p>Explain the mechanism of fingerprint & voice pattern in Biometrics.</p> <div data-bbox="354 338 1198 936" data-label="Diagram"> <pre> graph LR Sensor[Sensor] --> Pre-processing[Pre-processing] Pre-processing --> FE[Feature Extractor] FE --> TG[Template Generator] TG -- "Test" --> M[Matcher] M --> AD[Application Device] TG -- "Enrollment" --> ST[Stored Templates] ST -- "Test" --> M subgraph Biometric_System [Biometric System] FE TG M end </pre> <p>The diagram illustrates the Biometric System mechanism. It starts with a Sensor block that feeds into a Pre-processing block. The output of Pre-processing goes to the Feature Extractor block. The Feature Extractor's output goes to the Template Generator block. The Template Generator has two paths: one labeled Enrollment (red arrow) that leads to Stored Templates, and another labeled Test (blue arrow) that leads to the Matcher block. The Stored Templates block also has a Test (blue arrow) path leading to the Matcher block. The Matcher block's output goes to the Application Device block. The Feature Extractor, Template Generator, and Matcher blocks are grouped within a green oval labeled Biometric System.</p> <p>Fingerprint registration & verification mechanism</p> <ol style="list-style-type: none"> 1. During registration, first time an individual uses a biometric system is called an enrollment. 2. During the enrollment, biometric information from an individual is stored. 3. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment. 4. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. 5. The 2nd block performs all the necessary pre-processing. 6. The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way. 7. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). 8. If a matching phase is being performed the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. 9. The matching program will analyze the template with the input. This will then be output for any specified use or purpose. </div>	<p>S-22</p>	<p>4M</p>
---	---	--------------------	------------------

	<p>Voice pattern :</p> <p>1. Biometric Voice Recognition is the use of the human voice to uniquely identify biological characteristics to authenticate an individual unlike passwords or tokens that require physical input.</p> <p>2. Voice biometric recognition works by inputting the voice of the individual whose identity has to be stored in the system. This input is kept as a print for authentication. The input print is made with software that can split the voice statement into multiple frequencies</p> <p>3. A voice biometrics tool collects a user's voice template it only checks who is speaking and what is speaking (Who you are and what you speak)</p>		
<p>03.</p> <p>Answer:</p>	<p>Describe the features of DAC access control policy.</p> <p>DAC (discretionary access control) policy utilizes user identification Procedures to identify and restrict object access .It restricts access to objects based on the identity of subjects and or groups to which they belongs to. The owner of information or any resource is able to change its permissions at his discretion .Data Owners can transfer ownership of information to other users .Data Owners can determine the type of access given to other users (read, write etc.)</p> <p>Features of DAC policy are as follows :-</p> <p>Flexible –In DAC policy owner of information or resource can change its permission.</p> <p>Backup - Discretionary access control allows organizations to backup security policies and data to ensure effective access points.</p> <p>Usability - Discretionary access control is easy to use. Data Owners can transfer ownership of information to other users easily.</p>	S-22	4M
<p>04.</p> <p>Answer:</p>	<p>Define access control & explain authentication mechanism for access control.</p> <p>Access Control – Access is the ability of a subject to interest with an object. Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to modify data or resources. Access control is to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.</p> <p>Authentication - Authentication helps to establish proof of identities. The Authentication process ensures that the origin of a message is correctly</p>	S-22	4M

	<p>identified. For example, suppose that user C sends a message over the internet to user B. however, the trouble is that user C had posed as user A when he sent a message to user B. how would user B know that the message has come from user C, who posing as user A? This concept is shown in fig. below. This type of attack is called as fabrication</p> <p>Authentication is the process of determining identity of a user or other entity. It is performed during log on process where user has to submit His / her username and password.</p> <p>There are three methods used in it.</p> <ol style="list-style-type: none"> 1. Something you know - User knows user id and password. 2. Something you have - Valid user has lock and key. 3. Something about you - Users unique identity like fingerprints, DNA etc.  <p>Fig: Absence of authentication.</p>		
05.	<p>Explain shoulder surfing attack.</p> <p>Answer: Shoulder surfing a similar procedure in which attackers position themselves in such a way as to- be-able to observe the authorized user entering the correct access code. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.</p>	w-22	2M
06.	<p>Explain working of biometric access control with any type of example.</p> <p style="text-align: center;">OR</p> <p>Enlist types of Biometrics & Explain any one Biometrics type in detail.</p> <p style="text-align: center;">OR</p> <p>Explain working of fingerprint mechanism & its limitations.</p> <p>Answer: Biometric refers study of methods for uniquely recognizing humans</p>	<p>w-22</p> <p>S-24</p> <p>S-24</p>	<p>4M</p> <p>4M</p> <p>4M</p>

	<p>based upon one or more intrinsic physical or behavioral characteristics. Biometric identification is used on the basis of some unique physical attribute of the user that positively identifies the user. Example: finger print recognition, retina and face scan technique, voice synthesis and recognition and so on.</p> <p>Different types of Biometrics are:</p> <ol style="list-style-type: none"> 1. Finger print recognition 2. Hand print recognition 3. Retina/iris scan technique 4. Face recognition 5. Voice patterns recognition 6. Signature and writing patterns recognition 7. Keystroke dynamics  <p>Fig. block diagram of biometric system</p> <p>Finger print recognition Above figure shows the block diagram of biometric system.</p> <p>Fingerprint registration & verification process</p> <ol style="list-style-type: none"> 1. During registration, first time an individual uses a biometric system is called an enrollment. 2. During the enrollment, biometric information from an individual is stored. 3. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment. 4. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. 5. The 2nd block performs all the necessary pre-processing 6. The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way. 7. If enrollment is being performed the template is simply stored Somewhere (on a card or within a database or both). 		
--	--	--	--

	<p>8. If a matching phase is being performed the obtained template is Passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm.</p> <p>9. The matching program will analyze the template with the input. This will then be output for any specified use or purpose.</p> <p>Limitations:-</p> <ol style="list-style-type: none"> 1) Using the fingerprint scanner does not take into consideration when a person physically changes 2) The cost of computer hardware and software programs can be expensive. 3) Using the fingerprint scanner can lead to false rejections and false acceptance. 4) It can make mistakes with the dryness or dirty of the fingers skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly. 		
<p>07.</p> <p>Answer:</p>	<p>Explain the term Authorization and Authentication with respect to security.</p> <p>Authorization: It is a process of verifying that the known person has the authority to perform certain operation. It cannot occur without authentication. It is nothing but granting permissions and rights to individual so that he can use these rights to access computer resources or information.</p> <p>Authentication. Authentication is the process of determining identity of a user or other entity. It is performed during log on process where user has to submit his/her username and password. There are three methods used in it. 1. Something you know User knows user id and password. 2. Something you have Valid user has lock and key. 3. Something about you Users unique identity like fingerprints, DNA etc.</p>	<p>W-22</p> <p>S-24</p>	<p>4M</p> <p>4M</p>

08.	Write short note on DAC & MAC.	W-22	4M
Answer:	<p>Discretionary Access control (DAC): Restricting access to objects based on the identity of subjects and or groups to which they belong to, it is conditional, basically used by military to control access on system. UNIX based System is common method to permit user for read/write and execute</p> <p>Examples- Permitting the Linux file operating system is an example of DAC.</p> <p>Mandatory Access control (MAC): It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity-based restriction, formal authorization subject to sensitivity. In MAC the owner or User cannot determine whether access is granted to or not. I.e. Operating system rights. Security mechanism controls access to all objects and individual cannot change that access.</p> <p>For example, the sender sends a message, such as an EFT, through the MAC algorithm, which generates a key and attaches a MAC data tag to the message.</p>	S-23	4M
09.	Describe any four password selection criteria.	S-23 W-24	4M 4M
Answer:	<p>Password: Password is a secret word or expression use authorized persons to prove their right to access, information.</p> <p>Components of good password :</p> <ol style="list-style-type: none"> 1. It should be at least eight characters long. 2. It should include uppercase and lowercase letters, numbers, Characters or punctuation marks. 3. It should not contain dictionary words. 4. It should not contain the user's personal information such a name, family member's name, birth date, pet name, phone number any other detail that can easily be identified. 5. It should not be the same as the user's login name. 6. It should not be the default passwords as supplied by the vendor such as password, guest and admin and so on 		
10.	List any four biometric mechanisms.	W-23	2M
Answer:	<ol style="list-style-type: none"> 1. Fingerprint Recognition 2. Facial Recognition 3. Iris Recognition 4. Voice Recognition 		

11.	<p>Describe: (i) Piggybacking (ii) Dumpster diving</p> <p>Answer: (i) Piggybacking: Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.</p> <p style="text-align: center;">OR</p> <p>Access of wireless internet connection by bringing one's own computer within range of another wireless connection & using that without explicit permission, it means when an authorized person allows (intentionally or unintentionally) others to pass through a secure door.</p> <p>(ii) Dumpster diving: Dumpster diving is a form of social engineering attack where an individual searches through physical trash or digital remnants to gather sensitive information. The information found can be used to breach security systems, steal identities, or commit other malicious acts.</p> <p>Examples Corporate Data Breach: An attacker retrieves confidential business records from improperly shredded documents found in a company's trash.</p>	W-23	4M
12.	<p>State the features of (i) DAC (ii) MAC</p> <p>Answer: i) DAC: DAC (discretionary access control) policy utilizes user identification procedures to identify and restrict object access restricts access to objects based on the identity of subjects groups to which they belongs to. The owner of information resource is able to change its permissions at his discretion Owners can transfer ownership of information to other users Owners can determine the type of access given to other users write etc.</p> <p>Features of DAC policy are as follows: - Flexible -In DAC policy owner of information or resource change its permission. Backup - Discretionary access control allows organization backup security policies and data to ensure effective access point Usability - Discretionary access control is easy to use. Data can transfer ownership of information to other users easily.</p> <p>ii) MAC: It is used in environments where different levels of security are classified. It is much more restrictive. It is sensitivity restriction, formal authorization subject to sensitivity. In MAC owner or User cannot determine whether access is granted to i.e. Operating system rights. Security mechanism controls access all objects and individual cannot change that access.</p>	W-23	4M

<p>13</p> <p>Answer:</p>	<p>State any four advantages of Biometrics.</p> <p>Advantages of biometrics</p> <ol style="list-style-type: none"> 1) Biometrics cannot be lost, stolen or forgotten. Barring disease or serious physical injury, the biometric is consistent and permanent. 2) It is also secure in that the biometric itself cannot be socially engineered, shared or used by others. 3) There is no requirement to remember password or pins, thus eliminating an overhead cost. 4) Coupled with a smart card, biometrics provides strong security for any credentials on the smart card. 5) It provides a high degree of confidence in user identity 6) Accuracy and precision are very high in biometrics 7) Efficiency is very high 8) Maintain Consistency 	<p>S-24</p>	<p>2M</p>
<p>14</p> <p>Answer:</p>	<p>Describe the dumpster diving with its prevention mechanism.</p> <p>Dumpster Diving is a term used in the context of information security and social engineering to describe the practice of searching through discarded materials—such as trash, recycling bins, or dumpsters—in order to find sensitive or confidential information that can be exploited for malicious purposes.</p> <p>In the context of cyber security and physical security, dumpster diving typically refers to scavenging discarded documents that may contain personal, financial, corporate, or security-related information. This can include sensitive data such as:</p> <ul style="list-style-type: none"> • Personal identification details (e.g., Social Security numbers, addresses, and phone numbers) • Financial information (e.g., bank statements, credit card details) • Corporate documents (e.g., employee records, confidential business strategies, trade secrets) • Login credentials (e.g., passwords, PINs) <p>Dumpster diving can be a precursor to more serious cyber-attacks or identity theft. Criminals, hackers, or corporate spies can use the information obtained to launch phishing attacks, perform identity theft, or gain unauthorized access to corporate systems.</p>	<p>W-24</p>	<p>4M</p>

	<p>Prevention Mechanisms for Dumpster Diving:</p> <p>To prevent the risk of dumpster diving and the potential data breaches that can occur from it, organizations and individuals can take several steps to properly handle and dispose of sensitive information.</p> <p>1. Shredding Documents:</p> <ul style="list-style-type: none"> - Paper Shredders: Ensure all sensitive paper documents, including financial statements, old tax records, and any materials containing personal data, are shredded before being disposed of. - Cross-cut Shredders: Use cross-cut shredders rather than strip-cut shredders to make it more difficult for someone to reconstruct the documents. <p>2. Proper Disposal of Digital Media:</p> <ul style="list-style-type: none"> - Wipe Hard Drives: Before disposing of old computers, hard drives, flash drives, or other digital media, use software tools that completely wipe the data. Simply deleting files does not remove the data from the disk special software can recover it. - Physical Destruction of Hard Drives: If wiping the data isn't feasible, physically destroy the hard drive (e.g., shredding, drilling, or crushing) to prevent data recovery. <p>3. Training and Awareness:</p> <ul style="list-style-type: none"> - Employee Education: For businesses, regularly train employees on the importance of safeguarding sensitive information and the risks associated with improper disposal. - Internal Policies: Develop clear internal policies about the disposal of sensitive documents, including mandatory shredding procedures and secure disposal of hardware. <p>4. Secure Waste Containers:</p> <ul style="list-style-type: none"> - Lockable Bins: For businesses, ensure that trash bins, recycling bins, and dumpsters are secure and locked to prevent unauthorized access. If the business deals with highly sensitive information, consider hiring security services to monitor waste disposal. - Confidential Waste Collection: Provide employees with secure bins for disposing of confidential documents that need to be shredded. Ensure that these bins are only accessible by authorized personnel or shredding service providers. <p>5. Use of Encryption:</p> <ul style="list-style-type: none"> - Encrypt Digital Documents: If storing sensitive data digitally, use strong encryption methods to protect it, ensuring that even if a document is accessed, it cannot be read without the decryption key. 		
--	--	--	--

	<p>-Secure Backup and Disposal: When backing up sensitive data, ensure that backup media is also securely disposed of once it's no longer needed.</p>		
<p>15</p> <p>Answer:</p>	<p>Describe following terms w.r.t biometric: (i) Finger Print Analysis (ii) Retina Scan (iii) Keystroke</p> <p>(i) Finger print Analysis Finger print registration & verification process are:</p> <ol style="list-style-type: none"> 1. During registration, first time an individual uses a biometric system is called an enrollment. 2. During the enrollment, biometric information from an individual is stored. 3. In the verification process, biometric information is detected and compared with the information stored at the time of enrolment. 4. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. 5. The 2nd block performs all the necessary pre-processing 6. The third block extracts necessary features. This step is an important step as the correct features need to be extracted in the optimal way. 7. If enrollment is being performed the template is simply stored Somewhere (on a card or within a database or both). 8. If a matching phase is being performed the obtained template is Passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm. 9. The matching program will analyze the template with the input. This will then be output for any specified use or purpose. <p>(ii) Retina Scan: A retina scan is a biometric security technology that uses the unique pattern of blood vessels in the retina, the thin layer of tissue at the back of the eye, to identify or authenticate an individual. It is considered one of the most accurate and reliable biometric methods for personal identification due to the uniqueness and stability of retinal patterns.</p> <p>How a Retina Scan Works:</p> <ol style="list-style-type: none"> 1. Light Source: A retina scanner uses near-infrared light to illuminate the eye. The infrared light is absorbed differently by the retina's blood vessels, creating a distinctive pattern of dark and light areas. 2. Capture the Image: The scanner captures a high-resolution image of the retina's blood vessel pattern. This process is usually non-invasive and does not require direct contact with the eye. The subject typically looks into a specialized device that records the retinal pattern. 	<p>W-24</p>	<p>6M</p>

	<p>3. Pattern Analysis: The captured image is analyzed using advanced algorithms to extract the unique patterns in the retina, such as the branching structure of the blood vessels.</p> <p>4. Matching and Authentication: The captured retinal pattern is compared with previously stored retinal scans (in a database or system) to verify the individual's identity. The system will match the pattern to an enrolled record and authenticate the individual if there's a match.</p> <p>(iii) Keystroke: Keystroke Dynamics in Biometric Network Security In the realm of biometric network security, keystroke dynamics is a behavioral biometric technique used for authentication, continuous identity verification, and threat detection based on the unique characteristics of how an individual types on a keyboard. This type of biometric authentication focuses on the rhythm and speed with which a person types, which can vary significantly from one person to another, making it a powerful tool for securing networked systems and applications. Keystroke dynamics is primarily used to enhance identity verification processes and continuously monitor user behavior in networked environments. It works as follows:</p> <p>1. Enrollment Phase: When a user first interacts with a system, they are required to type a sample phrase (often a specific password or passphrase) to "train" the system. This establishes the user's keystroke pattern or biometric template, which includes details like typing speed, dwell time (how long a key is pressed), and flight time (the time between key presses).</p> <p>2. Feature Extraction: The system analyzes the typing patterns, extracting key features such as: Dwell Time: The time a key is held down, Flight Time: The time it takes to move from one key to another, Typing Speed: The overall speed at which a user types.</p> <p>3. Authentication: Whenever the user interacts with the system again, the system compares their current keystroke dynamics with the stored template. If the typing patterns match within an acceptable threshold, the user is authenticated. This authentication can happen either at the login stage or during continuous session monitoring (more on this below).</p> <p>4. Continuous Authentication: Unlike traditional biometrics (like fingerprints or facial recognition), keystroke dynamics can be used for continuous authentication. This means that after the user logs in, the system keeps tracking their typing patterns throughout the session.</p>		
--	--	--	--



JSPM's
RAJARSHI SHAHU COLLEGE OF ENGINEERING,
POLYTECHNIC
Department of Computer Engineering
Academic Year: 2024-25



UNIT-III (14 Marks)

MSBTE Question bank & Answer

<div>01</div> <div>Answer:</div>	<div>Define term cryptography.</div> <div>Cryptography is art & science of achieving security by encoding messages to make them non-readable.</div> <div><div><div>Intelligible data</div><div>Cryptography</div><div>Un-Intelligible data</div></div></div>	<div>S-22</div> <div>w-22</div>	<div>2M</div> <div>2M</div>																								
<div>02</div> <div>Answer:</div>	<div>Differentiate between symmetric & asymmetric key cryptography.</div> <table><thead><tr><th>Categories</th><th>Symmetric Key</th><th>Asymmetric key</th></tr></thead><tbody><tr><td>Key used for encryption/ decryption</td><td>Same Key is used for encryption decryption</td><td>One key is used for encryption & another different key is used for decryption</td></tr><tr><td>Key processes</td><td>Ke=kd (same)</td><td>Ke#kd (not same)</td></tr><tr><td>Speed of encryption/ decryption</td><td>Very fast</td><td>slower</td></tr><tr><td>Size of resulting encrypted</td><td>Usually same as or less then</td><td>More than the original clear</td></tr><tr><td>Key agreement/exchange</td><td>A big problem</td><td>No problem at all</td></tr><tr><td>Usage</td><td>Mainly used for encryption & decryption, cannot be used for digital signatures</td><td>Can be used for encryption & decryption as well as for digital signatures</td></tr><tr><td>Efficiency in usage</td><td>Symmetric key cryptography is often used for long messages.</td><td>Asymmetric key cryptography is more efficient for short messages.</td></tr></tbody></table>	Categories	Symmetric Key	Asymmetric key	Key used for encryption/ decryption	Same Key is used for encryption decryption	One key is used for encryption & another different key is used for decryption	Key processes	Ke=kd (same)	Ke#kd (not same)	Speed of encryption/ decryption	Very fast	slower	Size of resulting encrypted	Usually same as or less then	More than the original clear	Key agreement/exchange	A big problem	No problem at all	Usage	Mainly used for encryption & decryption, cannot be used for digital signatures	Can be used for encryption & decryption as well as for digital signatures	Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.	<div>S-22</div> <div>S-24</div> <div>W-24</div>	<div>4M</div> <div>4M</div> <div>4M</div>
Categories	Symmetric Key	Asymmetric key																									
Key used for encryption/ decryption	Same Key is used for encryption decryption	One key is used for encryption & another different key is used for decryption																									
Key processes	Ke=kd (same)	Ke#kd (not same)																									
Speed of encryption/ decryption	Very fast	slower																									
Size of resulting encrypted	Usually same as or less then	More than the original clear																									
Key agreement/exchange	A big problem	No problem at all																									
Usage	Mainly used for encryption & decryption, cannot be used for digital signatures	Can be used for encryption & decryption as well as for digital signatures																									
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography is more efficient for short messages.																									

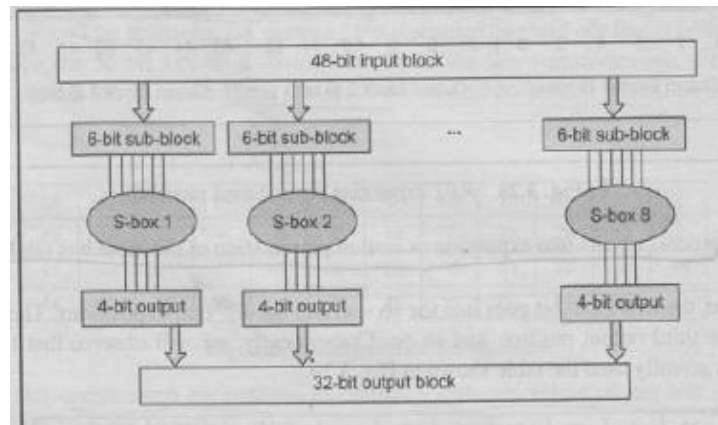
<p>03</p> <p>Answer:</p>	<p>Write & explain DES algorithm.</p> <div data-bbox="436 302 1042 751" data-label="Diagram"> <pre> graph TD A[Plain text (64 bits)] --> B[Initial Permutation (IP)] B --> C[LPT] B --> D[RPT] C --> E[16 rounds] D --> F[16 rounds] Key --> E Key --> F E --> G[Final Permutation (FP)] F --> G G --> H[Cipher text (64 bits)] </pre> </div> <p>Initial Permutation (IP): It happens only once. It replaces the first bit of the original plain text block with the 58th bit of the original plain text block, the second bit with the 50th bit of original plain text block and so on. The resulting 64-bits permuted text block is divided into two half blocks. Each half block consists of 32 bits. The left block called as LPT and right block called as RPT. 16 rounds are performed on these two blocks. Details of one round in DES</p> <div data-bbox="480 1075 1060 1495" data-label="Diagram"> <pre> graph TD A[Key Transformation] --> B[Expansion Permutation] B --> C[S-box substitution] C --> D[P-box Permutation] D --> E[XOR and swap] </pre> </div> <p>Step 1: key transformation: the initial key is transformed into a 56-bit key by discarding every 8th bit of initial key. Thus, for each round, a 56-bit key is available, from this 56-bit key, a different 48-bit sub key is generated during each round using a process called as key transformation Expansion Permutation Key Transformation</p> <p>S-box substitution XOR and swap P-box Permutation</p>	<p>S-22 w-22 W-24</p>	<p>4M 4M 4M</p>
--------------------------	--	-------------------------------	-------------------------

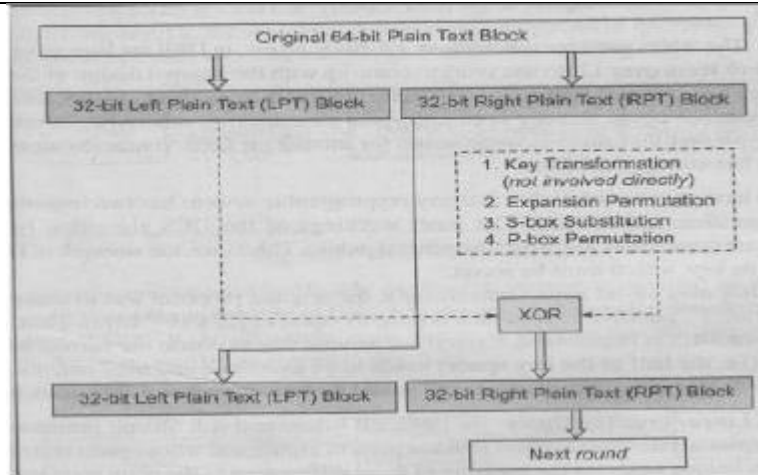
Step 2: Expansion permutation: During Expansion permutation the RPT is expanded from 32 bits to 48 bits. The 32-bit RPT is divided into 8 blocks, with each block consisting of 4-bits. Each 4-bits block of the previous step is then expanded to a corresponding 6-bit block, per 4-bit block, 2 more bits are added. They are the repeated 1st and 4th bits of the 4-bit block. The 2nd and 3rd bits are written as they were in the input. The 48 bit key is XOR ed with the 48-bit RPT and the resulting output is given to the next step.

Step 3: S-box substitution: It accepts the 48-bits input from the XOR operation involving the compressed key and expanded RPT and produces 32-bit output using the substitution techniques. Each of the 8 S-boxes has a 6-bit input and a 4-bit output. The output of each S-box then combined to form a 32-bit block, which is given to the last stage of a round

Step 4: P- box permutation: the output of S-box consists of 32-bits. These 32-bits are permuted using P-box. Step

5: XOR and Swap: The LPT of the initial 64-bits plain text block is XORed with the output produced by P box-permutation. It produces new RPT. The old RPT becomes new LPT, in a process of swapping.

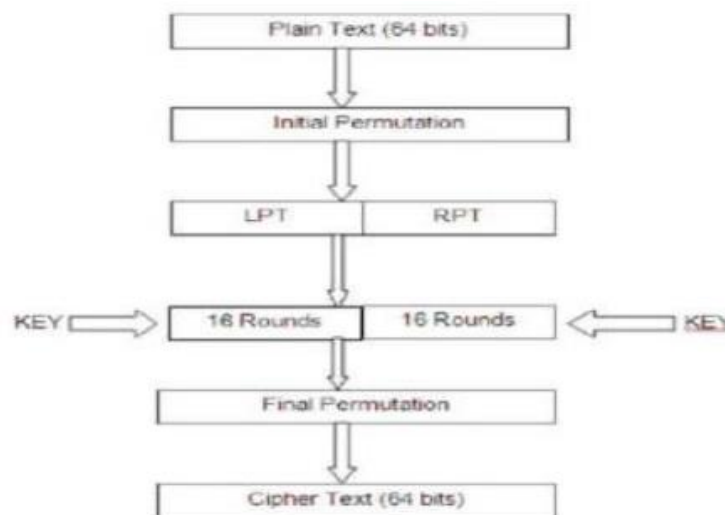




Final Permutation: At the end of 16 rounds, the final permutation is performed. This is simple transposition. For e.g., the 40th input bit takes the position of 1st output bit and so on.

OR

Data Encryption Standard is symmetric block cipher which takes input of 64-bit plain text along with 64-bit key and process it, to generate the 64-bit cipher text. The diagram below illustrates the working of DES.



DES Encryption:-

Step1: In the first step the 64-bit plain text undergoes initial permutation which rearranges the bits to produce two 32-bit permuted block which is called left plain text (LPT 32-bit) and right plain text (RPT 32-bit).

Step 2: Now, 16 rounds of DES encryption will be performed on this LPT and RPT with a 56-bit key.

Step 3: After the 16th round the 32-bit LPT and 32-bit RPT are integrated which forms a 64-bit block again and then the final permutation is applied to this 64-bit block, to obtain the 64-bit cipher text.

	<p>Rounds in Data Encryption Standard Each round of DES performs the same function. So, below are the steps of the function performed in each round of DES algorithm:</p> <p>1. Key Transformation: -In DES initial key size is 64-bit which is reduced to the 56-bit key. This is done by discarding every 8th bit from the 64-bit key. So, for each round of DES, this 56-bit key is used. In the key transformation step, this 56-bit is transformed to the 48-bit key.</p> <p>2. Expansion Permutation: -In the first step of encryption, during the initial permutation of DES, the 64-bit plain text is permuted and we have 32-bit LPT and 32-bit RPT. Now, the expansion permutation is performed on the 32-bit RPT which transforms it from 32-bit to 48-bit. The 32-bit LPT is untouched during the process.</p> <p>3. S-box Substitution:-The input to S-box is 48-bit resultant block of expansion permutation. In S-box substitution, the input 48-bit block is transformed to 32-bit block</p> <p>4. P-box Permutation:- The 32-bit output obtained from s-box substitution is provided as an input to P-box. Here, the 32-bit input is simply permuted and send to the next step.</p> <p>5. XOR and Swap:-In this step, the 32-bit LPT of the initial 64-bit plain text is XOR with the output of P-box permutation. The result of the XOR is the new RPT for next round and the old RPT is swapped with LPT.</p> <p>DES Decryption: - The same Data Encryption Standard algorithm used for encrypting the plain text is also used to decrypting the cipher text. But the algorithm is reversed, such as the initial and final permutation events are reversed. Even the sequence of the sub keys applied in 16 rounds of DES is also reversed.</p>		
04	<p>Consider plain text “COMPUTER ENGINEERING” & convert given plain text into cipher text using ‘Caesar Cipher’ with shift of position three - write down steps in encryption.</p>	S-22	4M
Answer:	<p>Caesar cipher technique is proposed by Julius Caesar. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. The Caesar cipher involves replacing each letter of the alphabet with the letter three places further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below</p>		

	<table><tr><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td></tr><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td></tr></table> <table><tr><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td><td>↑</td></tr><tr><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr></table> <p>PLAIN TEXT -COMPUTER ENGINEERING</p> <p>CIPHER TEXT–FRPSXWHU HQJLQHHULQJ</p>	A	B	C	D	E	F	G	H	I	J	K	L	M	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	0	1	2	3	4	5	6	7	8	9	10	11	12	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	13	14	15	16	17	18	19	20	21	22	23	24	25		
A	B	C	D	E	F	G	H	I	J	K	L	M																																																																					
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑																																																																					
0	1	2	3	4	5	6	7	8	9	10	11	12																																																																					
N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																																																					
↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑	↑																																																																					
13	14	15	16	17	18	19	20	21	22	23	24	25																																																																					
05	<p>Enlist substitution techniques & explain any one</p>	S-22	4M																																																																														
Answer:	<p>Substitution Techniques:- In substitution technique letters of plain text are replaced by the other letters or by numbers or by symbols. Substitution techniques are as follows:-</p> <p>a) Caesar cipher</p> <p>b) Modified version of Caesar cipher</p> <p>c) Mono-alphabetic cipher</p> <p>d) Vigeners cipher a Caesar cipher</p> <p>Caesar cipher:</p> <p>It is proposed by Julius Caesar. In cryptography Caesar cipher also known as Caesar cipher/code, shift cipher/code. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below.</p>																																																																																

	<table><tr><td>Plain</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>Cipher</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td></tr></table> <table><tr><td>Plain</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>Cipher</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr></table> <p>Using this scheme, the plain text “SECRET” encrypts as Cipher text “VHFUHW”. To allow someone to read the cipher text, you tell them that the key is 3</p> <p>For S:= (p + k)mod26 = (18 + 3) mod 26 = 21 = V</p> <p>To allow someone to read the cipher text, you tell them that the key is 3</p> <p>Algorithm to break Caesar cipher:</p> <ol style="list-style-type: none">1. Read each alphabet in the cipher text message, and search for it in the second row of the table above.2. When a match is found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table. (For example, if the alphabet cipher text is J, replace it with G).3. Repeat the process for all alphabets in the cipher text message.	Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Cipher	Q	R	S	T	U	V	W	X	Y	Z	A	B	C		
Plain	A	B	C	D	E	F	G	H	I	J	K	L	M																																														
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P																																														
Plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																														
Cipher	Q	R	S	T	U	V	W	X	Y	Z	A	B	C																																														
06	<p>Explain Digital Signature in Cryptography.</p> <p>Answer: Digital Signature:</p> <ol style="list-style-type: none">1. Digital signature is a strong method of authentication in an electronic form.2. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols.3. Digital Signature is used for authentication of the message and the ender to verify the integrity of the message.4. Digital Signature may be in the form of text, symbol, image or audio.5. In today’s world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster.	S-22 W-24	4M																																																								

	<p>6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature.</p> <p>7. Digital signature algorithms are divided into two parts</p> <p>a. Signing part: It allows the sender to create his digital signature.</p> <p>b. Verification part: It is used by the receiver for verifying the signature after receiving the message.</p> <p>Generation and Verification of digital signatures:</p> <p>Working:</p> <p>1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.</p> <p>2. The message digest is encrypted using users private key.</p> <p>3. Then, the sender sends this encrypted message digest with the plain text or message to the receiver.</p>																																																										
<p>07</p> <p>Answer:</p>	<p>Explain Ceaser’s Cipher substitution technique with suitable example.</p> <p>Caesar cipher technique is proposed by Julius Caesar. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. The Caesar cipher involves replacing each letter of the alphabet with the letter three places further down the alphabet. For example, with a shift of 3, A would be replaced by D, B would became E, and so on as shown in the table below</p> <table><tr><td>Plain text</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>Cipher text</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td></tr></table> <table><tr><td>Plain text</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>Cipher text</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr></table> <p>Example PLAIN TEXT - COMPUTER ENGINEERING</p> <p>Convert each alphabet in the plain text, using the table, the cipher text can be written as</p> <p>CIPHER TEXT – FRPSXWHU HQJLQHHULQJ</p>	Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M	Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P	Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	<p>W-22</p> <p>S-24</p> <p>W-24</p>	<p>4M</p> <p>4M</p> <p>4M</p>
Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M																																														
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P																																														
Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																														
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C																																														

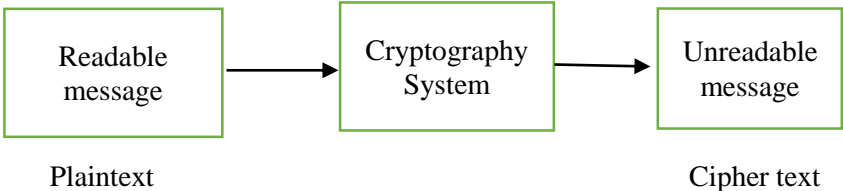
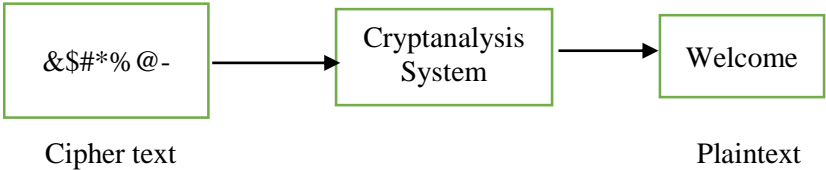
	<p>Algorithm to break Caesar cipher:</p> <p>1. Read each alphabet in the cipher text message, and search for it in the second row of the table above.</p> <p>2. When a match is found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table. (For example, if the alphabet cipher text is J, replace it with G).</p> <p>3. Repeat the process for all alphabets in the cipher text message.</p>																																
<p>08</p> <p>Answer:</p>	<p>Write an algorithm for simple columnar transposition technique and explain with example.</p> <p>Simple columnar transposition technique:</p> <p>Algorithm:</p> <p>1. The message is written out in rows of a fixed length.</p> <p>2. Read out again column by column according to given order or in random order.</p> <p>3. According to order write cipher text.</p> <p>Example The key for the columnar transposition cipher is a keyword e.g., ORANGE. The row length that is used is the same as the length of the keyword.</p> <p>To encrypt a below plaintext:</p> <p>COMPUTER PROGRAMMING</p> <table><tr><td>O</td><td>R</td><td>A</td><td>N</td><td>G</td><td>E</td></tr><tr><td>C</td><td>O</td><td>M</td><td>P</td><td>U</td><td>T</td></tr><tr><td>E</td><td>R</td><td>P</td><td>R</td><td>O</td><td>G</td></tr><tr><td>R</td><td>A</td><td>M</td><td>M</td><td>I</td><td>N</td></tr><tr><td>G</td><td>L</td><td>E</td><td>X</td><td>X</td><td>M</td></tr></table> <p>In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.</p>	O	R	A	N	G	E	C	O	M	P	U	T	E	R	P	R	O	G	R	A	M	M	I	N	G	L	E	X	X	M	<p>W-22</p>	<p>4M</p>
O	R	A	N	G	E																												
C	O	M	P	U	T																												
E	R	P	R	O	G																												
R	A	M	M	I	N																												
G	L	E	X	X	M																												

	<table><tr><td>5</td><td>6</td><td>1</td><td>4</td><td>3</td><td>2</td></tr><tr><td>O</td><td>R</td><td>A</td><td>N</td><td>G</td><td>E</td></tr><tr><td>C</td><td>O</td><td>M</td><td>P</td><td>U</td><td>T</td></tr><tr><td>E</td><td>R</td><td>P</td><td>R</td><td>O</td><td>G</td></tr><tr><td>R</td><td>A</td><td>M</td><td>M</td><td>I</td><td>N</td></tr><tr><td>G</td><td>L</td><td>E</td><td>X</td><td>X</td><td>M</td></tr></table> <p>The Encrypted text or Cipher text is:</p> <p>MPMETGNMUOIXPRXCERGORAL</p>	5	6	1	4	3	2	O	R	A	N	G	E	C	O	M	P	U	T	E	R	P	R	O	G	R	A	M	M	I	N	G	L	E	X	X	M		
5	6	1	4	3	2																																		
O	R	A	N	G	E																																		
C	O	M	P	U	T																																		
E	R	P	R	O	G																																		
R	A	M	M	I	N																																		
G	L	E	X	X	M																																		
09	<p>Write a short note on steganography.</p> <p><u>OR</u></p> <p>Explain steganography technique with suitable example.</p>	<p>W-22</p> <p>S-23</p> <p>W-23</p> <p>W-24</p>	<p>4M</p> <p>4M</p> <p>2M</p> <p>3M</p>																																				
Answer:	<p>Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, html or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text or even images. In modern steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant data that is part of a particular file format such as a JPEG image.</p> <div><pre>graph LR; subgraph Sender; Cover-image --> EP[Embedding Process]; EM[Embedded message] --> EP; SK1[Stego-key] --> EP; end; EP -- "Stego-image" --> EX[Extracting Process]; subgraph Receiver; EX --> EM2[Embedded message]; SK2[Stego-key] --> EX; end;</pre></div>																																						

	<p>Steganography process: Cover-media + Hidden data + Stego-key = Stego-medium</p> <p>Cover media is the file in which we will hide the hidden data, which may also be encrypted using stego-key. The resultant file is stego-medium. Cover-media can be image or audio file.</p> <p>Advantages:</p> <ol style="list-style-type: none"> 1. With the help of steganography we can hide secret message within graphics image. 2. In modern Steganography, data is encrypted first and then inserted using special algorithm so that no one suspects its existence. <p>Drawbacks:</p> <ol style="list-style-type: none"> 1. It requires lot of overhead to hide a relatively few bits of information. 2. Once the system is discovered, it becomes virtually worthless. 		
<p>10</p> <p>Answer:</p>	<p>Explain creation and verification of digital signature.</p> <p>Working of digital signature Generation and Verification:</p> <p>1. Key Generation: Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.</p> <p>2. Signature Verification: Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.</p>	W-22	4M

	<p>Generation and Verification of digital signatures:</p> <pre> graph TD subgraph "Generation of MD" M1[Message] --> MD1[Message digest] end subgraph "Encryption" MD1 --> EMD[Encrypted message digest using private key] end subgraph "Generation of digital signatures by the sender" M1 --> MD2[Message digest] EMD --> MD2 end subgraph "Verification of digital signatures by the receiver" EMD --> MD3[Message digest] MD2 --> MD3 end MD2 --> MD3 MD3 --> MD3 </pre>		
<p>11</p> <p>Define following terms: (i) Cryptography (ii) Cryptology</p> <p>Answer:</p>	<p>(i) Cryptography is art & science of achieving security by encoding messages to make them non-readable.</p> <pre> graph LR ID[Intelligible data] --> C[Cryptography] --> UID[Un-Intelligible data] </pre> <p>(ii) Cryptology: It is the art and science of transforming the intelligence data into unintelligent data and unintelligent data back to intel data.</p> $\text{Cryptology} = \text{Cryptography} + \text{Cryptanalysis}$	S-23	2M
<p>12</p> <p>Construct digital signature using cryptool.</p> <p>Answer:</p>	<p>Step 1: Open Cryptool application. Step 2: Open the file and enter message to create digital signature Step 3: Select menu Digital signature-> Sign Document Step 4: Select any Hash function and choose private key. Step 5: Enter PIN number and Click on Sign button to gen digital Signature.</p>	S-23	2M

13	<p>Convert plain text into cipher text by using Simple columnar technique of the following sentence: "Maharashtra State Board of Technical Education"</p>	S-23	4M																																																								
Answer:	<p>"Maharashtra State board of Technical Education "</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr><tr><td>M</td><td>A</td><td>H</td><td>A</td><td>R</td></tr><tr><td>A</td><td>S</td><td>H</td><td>T</td><td>R</td></tr><tr><td>A</td><td>S</td><td>T</td><td>A</td><td>T</td></tr><tr><td>E</td><td>B</td><td>O</td><td>A</td><td>R</td></tr><tr><td>D</td><td>O</td><td>F</td><td>T</td><td>E</td></tr><tr><td>C</td><td>H</td><td>N</td><td>I</td><td>C</td></tr><tr><td>A</td><td>L</td><td>E</td><td>D</td><td>U</td></tr><tr><td>C</td><td>A</td><td>T</td><td>I</td><td>O</td></tr><tr><td>N</td><td>X</td><td>X</td><td>X</td><td>X</td></tr></table> <p>PLAIN TEXT: MAHARASTRA STATE BOARD OF TECHNICAL EDUCATION</p> <p>LET ORDER BE: 4,5,3,2,1</p> <p>CIPHER TEXT: ATAATIDIXRRRTRECUOXHHTOFNETXASSBOHLAXMAAEDCACN</p>	1	2	3	4	5	M	A	H	A	R	A	S	H	T	R	A	S	T	A	T	E	B	O	A	R	D	O	F	T	E	C	H	N	I	C	A	L	E	D	U	C	A	T	I	O	N	X	X	X	X								
1	2	3	4	5																																																							
M	A	H	A	R																																																							
A	S	H	T	R																																																							
A	S	T	A	T																																																							
E	B	O	A	R																																																							
D	O	F	T	E																																																							
C	H	N	I	C																																																							
A	L	E	D	U																																																							
C	A	T	I	O																																																							
N	X	X	X	X																																																							
14	<p>Convert the given plain text, encrypt it with the help of Caesar's cipher technique. "Network and Information Security".</p>	S-23	4M																																																								
Answer:	<p>"Network and Information Security".</p> <table><tr><td>Plain text</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>Cipher text</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td></tr></table> <table><tr><td>Plain text</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>Cipher text</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr></table>	Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M	Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P	Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C		
Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M																																														
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P																																														
Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																														
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C																																														

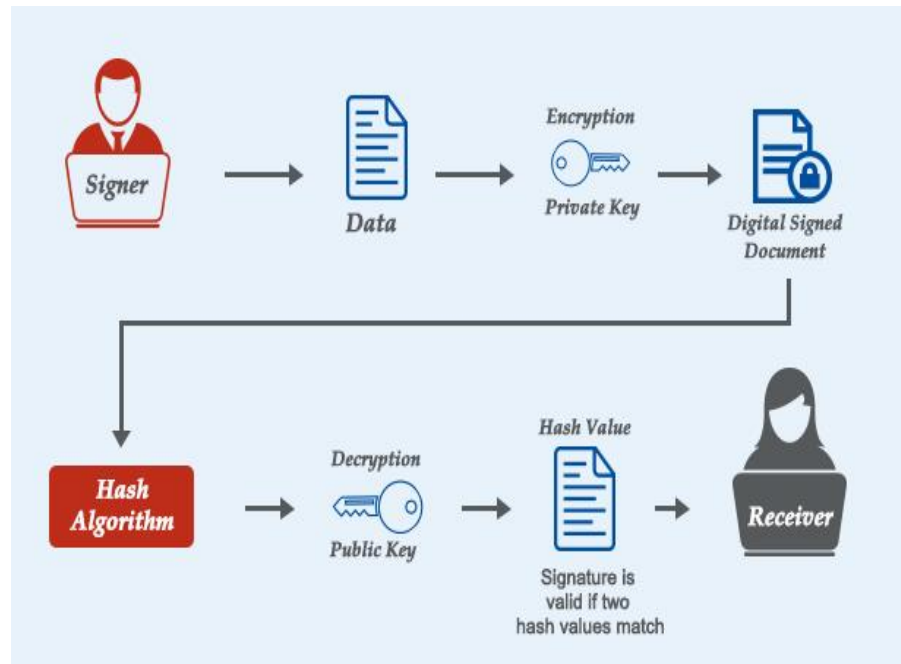
	PLAIN TEXT: NETWORK AND INFORMATION SECURITY CIPHER TEXT: QHWZRUNDQGLQIRUPDWLRQVHFXULWB		
15 Answer:	<p>Define the following terms: (i) Cryptography (ii) Cryptanalysis</p> <p>(i) Cryptography is art & science of achieving security by encoding messages to make them non-readable.</p> <div style="text-align: center;">  <pre> graph LR A[Readable message] --> B[Cryptography System] B --> C[Unreadable message] A --- D[Plaintext] C --- E[Cipher text] </pre> </div> <p>(ii) Cryptanalysis is the study of analyzing and breaking cryptographic systems with the goal of deciphering encrypted information without possessing the proper key or authentication credentials.</p> <div style="text-align: center;">  <pre> graph LR A["&\$#*%@-"] --> B[Cryptanalysis System] B --> C[Welcome] A --- D[Cipher text] C --- E[Plaintext] </pre> </div>	S-23 W-23 W-24	4M 2M 2M
16 Answer:	<p>Describe digital signature technique using message digest. <u>OR</u> Illustrate digital signature & explain it with neat diagram.</p> <p>Digital Signature:</p> <ol style="list-style-type: none"> Digital signature is a strong method of authentication in an electronic form. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols. Digital Signature is used for authentication of the message and the sender to verify the integrity of the message. Digital Signature may be in the form of text, symbol, image or audio. In today's world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster. 	S-23 S-24	4M 3M

6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature.
7. Digital signature algorithms are divided into two parts.
 - a. Signing part: It allows the sender to create his digital signature.
 - b. Verification part: It is used by the receiver for verifying the signature after receiving the message.

Generation and Verification of digital signatures:

Working:

1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.
2. The message digest is encrypted using users private key.
3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.
4. The receiver calculates the message digest from the plain text or message he received.
5. Receiver decrypts the encrypted message digest using the senders public key. If both the MDs are not same then the plaintext or message is modified after signing.



	Advantages of Digital Signatures <ul style="list-style-type: none"> • Speed: Businesses no longer have to wait for paper documents to be sent by courier. Contracts are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically. • Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents. • Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit. • Authenticity: An electronic document signed with a digital signature can stand up in court just as well as any other signed paper document. • Non-Repudiation: Signing an electronic document digitally identifies you as the signatory and that cannot be later denied. • Time-Stamp: By time-stamping your digital signatures, you will clearly know when the document was signed. 		
17	Consider plain text "CERTIFICATE" and convert it into cipher text using Caesar Cipher with a shift of position 4. Write steps for encryption.	W-23	4M
Answer:	<p>Caesar cipher technique is proposed by Julius Caesar. It is one of the simplest and most widely known encryption techniques. It is a type of substitution technique in which each letter in the plain text is replaced by a letter some fixed number of position down the alphabet. The Caesar cipher involves replacing each letter of the alphabet with the letter three places further down the alphabet.</p> <p>For example, with a shift of 3, A would be replaced by D, B would become E, and so on as shown in the table below</p>		

	<table><tr><td>Plain text</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td></tr><tr><td>Cipher text</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td></tr></table> <table><tr><td>Plain text</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td>Cipher text</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr></table> <p>PLAIN TEXT – CERTIFICATE CIPHER TEXT– FHUWLILFDWH</p> <p>Algorithm to break Caesar cipher:</p> <ol style="list-style-type: none">1. Read each alphabet in the cipher text message, and search for it in the second row of the table above.2. When a match in found, replace that alphabet in the cipher text message with the corresponding alphabet in the same column but the first row of the table. (For example, if the alphabet cipher text is J, replace it with G).3. Repeat the process for all alphabets in the cipher text message.	Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M	Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P	Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C		
Plain text	A	B	C	D	E	F	G	H	I	J	K	L	M																																														
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P																																														
Plain text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																														
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C																																														
<p>18</p> <p>Answer:</p>	<p>Convert the given plain text into cipher text using simple columnar technique using the following data: Plain text: NETWORK SECURITY Number columns: 06 Encryption key: 632514</p> <p>Simple columnar transposition technique: Algorithm:</p> <ol style="list-style-type: none">1. The message is written out in rows of a fixed length.2. Read out again column by column according to given order or in random order.3. According to order write cipher text. <p>Example The key for the columnar transposition cipher is a keyword e.g., 632514. The row length that is used is the same as the length of the keyword. To encrypt a below plaintext: NETWORK SECURITY.</p>	<p>W-23</p>	<p>4M</p>																																																								

	<table><tr><td>6</td><td>3</td><td>2</td><td>5</td><td>1</td><td>4</td></tr><tr><td>N</td><td>E</td><td>T</td><td>W</td><td>O</td><td>R</td></tr><tr><td>K</td><td>S</td><td>E</td><td>C</td><td>U</td><td>R</td></tr><tr><td>I</td><td>T</td><td>Y</td><td>X</td><td>X</td><td>X</td></tr></table> <p>In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.</p> <table><tr><td>6</td><td>3</td><td>2</td><td>5</td><td>1</td><td>4</td></tr><tr><td>N</td><td>E</td><td>T</td><td>W</td><td>O</td><td>R</td></tr><tr><td>K</td><td>S</td><td>E</td><td>C</td><td>U</td><td>R</td></tr><tr><td>I</td><td>T</td><td>Y</td><td>X</td><td>X</td><td>X</td></tr></table> <p>The Encrypted text or Cipher text is: OUXTEYESTRRXWCXNKI</p>	6	3	2	5	1	4	N	E	T	W	O	R	K	S	E	C	U	R	I	T	Y	X	X	X	6	3	2	5	1	4	N	E	T	W	O	R	K	S	E	C	U	R	I	T	Y	X	X	X		
6	3	2	5	1	4																																														
N	E	T	W	O	R																																														
K	S	E	C	U	R																																														
I	T	Y	X	X	X																																														
6	3	2	5	1	4																																														
N	E	T	W	O	R																																														
K	S	E	C	U	R																																														
I	T	Y	X	X	X																																														
<p>19</p> <p>Answer:</p>	<p>State the use of Digital Certificates. Describe the steps for digital certificate creation.</p> <p>A Digital Certificate is a cryptographic tool used to verify the identity of an entity and facilitate secure communication in a network. It acts as a trusted "electronic passport" that confirms the identity of an organization, individual, or device.</p> <p>Primary Uses of Digital Certificates:</p> <ol style="list-style-type: none">1. Authentication: Digital certificates help verify the identity of users, websites, or devices, ensuring that communication is happening with the correct entity.2. Data Encryption: Digital certificates, especially in Public Key Infrastructure (PKI) systems, are used for encrypting data, ensuring that it remains confidential during transmission.	<p>W-23</p>	<p>4M</p>																																																

	<p>3. Digital Signatures: They are used for signing digital documents or messages, providing proof of origin, integrity, and non-repudiation.</p> <p>4. Secure Communication: Digital certificates enable secure protocols like SSL/TLS for encrypting web traffic (e.g., HTTPS), ensuring the confidentiality and integrity of communication over the internet.</p> <p>5. Non-Repudiation: They ensure that the sender cannot deny the authenticity of the message, as the certificate is linked to their identity.</p> <p>Steps for Digital Certificate Creation. The process of creating a digital certificate involves several steps, mainly revolving around public key cryptography. Here's an overview of the general process for creating a Digital Certificate:</p> <p>Step 1: Generate a Key Pair</p> <ul style="list-style-type: none"> • Private Key: The entity that needs the certificate (e.g., a website or user) generates a private key. This key is kept secret and is used for decryption or digital signing. • Public Key: The corresponding public key is generated, which can be shared openly. The public key is used for encrypting • messages that only the private key can decrypt, or for verifying a digital signature. <p>Step 2: Create a Certificate Signing Request (CSR)</p> <ul style="list-style-type: none"> • The entity creates a CSR, which is a request to the Certificate Authority (CA) to issue a digital certificate. The CSR includes: <ul style="list-style-type: none"> ○ The public key generated in Step 1. ○ Distinguished Name (DN) information, including: <ul style="list-style-type: none"> ▪ Common Name (e.g., domain name for SSL certificates) <ul style="list-style-type: none"> ▪ Organization Name ▪ Organizational Unit (e.g., department) ▪ Country ▪ Locality and State ○ The signature of the entity's private key, ensuring that the request is authentic. 		
--	--	--	--

	<p>Step 3: Submit the CSR to a Certificate Authority (CA)</p> <ul style="list-style-type: none"> • The entity submits the CSR to a Certificate Authority (CA), a trusted organization responsible for verifying the entity's identity and issuing certificates. • The CA may perform various checks, including verifying the domain ownership (for SSL certificates) or checking the identity of the individual or organization requesting the certificate. <p>Step 4: Certificate Authority Verifies the Identity</p> <ul style="list-style-type: none"> • The CA verifies the identity of the requester, often through a combination of automated and manual methods. This could involve validating domain ownership (in the case of SSL certificates) or reviewing business documents for an organization. <p>Step 5: CA Issues the Digital Certificate</p> <ul style="list-style-type: none"> • Once the identity is verified, the CA generates the digital certificate. The certificate contains: <ul style="list-style-type: none"> ◦ The public key from the CSR. ◦ The Distinguished Name (DN) of the certificate holder. ◦ The Certificate Authority's digital signature. ◦ The Validity Period, specifying the start and expiration dates. ◦ The Serial Number and other relevant metadata. • The CA signs the certificate with its private key, providing a way to verify the authenticity of the certificate. <p>Step 6: Install the Digital Certificate</p> <ul style="list-style-type: none"> • The digital certificate is sent back to the requester, who can now install it on their server or device. • The private key remains securely stored by the entity, while the public key is embedded in the certificate. <p>Step 7: Public Key Infrastructure (PKI) Trust Chain</p> <ul style="list-style-type: none"> • When the digital certificate is installed, it is used to establish secure communication (e.g., through HTTPS). The certificate is verified by clients (browsers or other systems) using the CA's 		
--	---	--	--

	<p>Step 5: Convert to Hexadecimal</p> <p>Now, we convert this output back into hexadecimal:</p> <p>1000 0010 0000 0010 0000 0000 0000 0000 0000 0010 0000 0000 0000 0000 0000 0000 = 0x8002000000000000</p> <p>Final Output:</p> <p>The output of the Initial Permutation (IP) for the input 0x0000008000000002 is: 0x8002000000000000</p> <p>This is the resulting value after applying the DES Initial Permutation (IP) to the provided 64-bit input.</p>																																																														
21	<p>Convert plain text into cipher text by using simple columnar technique of the following sentence: ALL IS WELL FOR YOUR EXAM.</p> <p>Simple columnar transposition technique: Algorithm:</p> <p>1. The message is written out in rows of a fixed length. 2. Read out again column by column according to given order or in random order. 3. According to order write cipher text.</p> <p>Example To encrypt a below plaintext: ALL IS WELL FOR YOUR EXAM</p> <table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>A</td><td>L</td><td>L</td><td>I</td><td>S</td><td>W</td></tr><tr><td>E</td><td>L</td><td>L</td><td>F</td><td>O</td><td>R</td></tr><tr><td>Y</td><td>O</td><td>U</td><td>R</td><td>E</td><td>X</td></tr><tr><td>A</td><td>M</td><td></td><td></td><td></td><td></td></tr></table> <p>In the above example, the plaintext has been padded so that it neatly fits in a rectangle. The columns are now reordered Randomly</p> <table><tr><td>5</td><td>6</td><td>1</td><td>4</td><td>3</td><td>2</td></tr><tr><td>S</td><td>W</td><td>A</td><td>I</td><td>L</td><td>L</td></tr><tr><td>O</td><td>R</td><td>E</td><td>F</td><td>L</td><td>L</td></tr><tr><td>E</td><td>X</td><td>Y</td><td>R</td><td>U</td><td>O</td></tr><tr><td></td><td></td><td>A</td><td></td><td></td><td>M</td></tr></table> <p>The Encrypted text or Cipher text is: SOEWRXAEYAIFRLLULLOM</p>	1	2	3	4	5	6	A	L	L	I	S	W	E	L	L	F	O	R	Y	O	U	R	E	X	A	M					5	6	1	4	3	2	S	W	A	I	L	L	O	R	E	F	L	L	E	X	Y	R	U	O			A			M	S-24	4M
1	2	3	4	5	6																																																										
A	L	L	I	S	W																																																										
E	L	L	F	O	R																																																										
Y	O	U	R	E	X																																																										
A	M																																																														
5	6	1	4	3	2																																																										
S	W	A	I	L	L																																																										
O	R	E	F	L	L																																																										
E	X	Y	R	U	O																																																										
		A			M																																																										

22	Differentiate between substitution & transposition techniques?	S-24	4M																		
Answer:	<table><tr><th>Features</th><th>Substitution Technique</th><th>Transposition Technique</th></tr><tr><td>Definition</td><td>It replaces the plaintext characters with other numbers, characters, and symbols.</td><td>It scrambles the character's position in the plaintext.</td></tr><tr><td>Alterations</td><td>The character's identity is changed, while its position does not change.</td><td>The character's identity is changed instead of its identity.</td></tr><tr><td>Forms</td><td>It utilizes the monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher.</td><td>It utilizes the keyed and keyless transpositional ciphers.</td></tr><tr><td>Detection</td><td>The low-frequency letter may easily identify the plaintext.</td><td>The keys close to the right key lead to the discovery of the plaintext.</td></tr><tr><td>Examples</td><td>Caesar Cipher</td><td>Reil Fence Cipher</td></tr></table>	Features	Substitution Technique	Transposition Technique	Definition	It replaces the plaintext characters with other numbers, characters, and symbols.	It scrambles the character's position in the plaintext.	Alterations	The character's identity is changed, while its position does not change.	The character's identity is changed instead of its identity.	Forms	It utilizes the monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher.	It utilizes the keyed and keyless transpositional ciphers.	Detection	The low-frequency letter may easily identify the plaintext.	The keys close to the right key lead to the discovery of the plaintext.	Examples	Caesar Cipher	Reil Fence Cipher		
Features	Substitution Technique	Transposition Technique																			
Definition	It replaces the plaintext characters with other numbers, characters, and symbols.	It scrambles the character's position in the plaintext.																			
Alterations	The character's identity is changed, while its position does not change.	The character's identity is changed instead of its identity.																			
Forms	It utilizes the monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher.	It utilizes the keyed and keyless transpositional ciphers.																			
Detection	The low-frequency letter may easily identify the plaintext.	The keys close to the right key lead to the discovery of the plaintext.																			
Examples	Caesar Cipher	Reil Fence Cipher																			



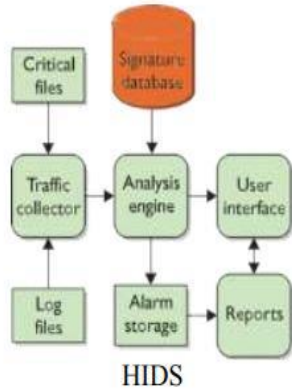
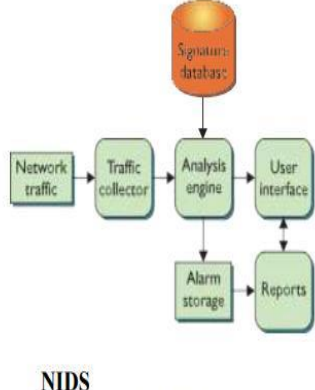
JSPM's
**RAJARSHI SHAHU COLLEGE OF ENGINEERING,
 POLYTECHNIC**
Department of Computer Engineering
 Academic Year: 2024-25



UNIT-IV (18 Marks)

MSBTE Question bank & Answer

Q.No	Question	Year	Marking									
01.	Define firewall. Enlist types of firewalls	S-22	2M									
Answer:	Definition Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers. Types of Firewall : 1 .Packet Filter 2. Circuit level Gateway 3. Application Gateway 4. Software 5. Hardware 6. Hybrid 7. Stateful multilayer Inspection Firewall	W-23	2M									
		W-24	2M									
02.	Differentiate between host-based & network based IDS.	S-22	4M									
Answer:	<table><tr><th>Sr.No.</th><th>Host Based Ids</th><th>Network Based Ids</th></tr><tr><td>1</td><td>Examines activity on an individual system, such as a mail server, web server, or individual PC.</td><td>Examines activity on the network itself</td></tr><tr><td>2</td><td>It is concerned only with an Individual system and usually has no visibility into the activity on the network or systems around it</td><td>It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.</td></tr></table>			Sr.No.	Host Based Ids	Network Based Ids	1	Examines activity on an individual system, such as a mail server, web server, or individual PC.	Examines activity on the network itself	2	It is concerned only with an Individual system and usually has no visibility into the activity on the network or systems around it	It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.
	Sr.No.	Host Based Ids	Network Based Ids									
	1	Examines activity on an individual system, such as a mail server, web server, or individual PC.	Examines activity on the network itself									
2	It is concerned only with an Individual system and usually has no visibility into the activity on the network or systems around it	It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems.										

	<p>3</p> <p>HIDS is looking for certain activities that typify hostile actions or misuse, such as the following:</p> <ul style="list-style-type: none"> • Logins at odd hours • Login authentication failures • Additions of new user accounts • Modification or access of critical system files 	<p>NIDSs look for certain activities that typify hostile actions or misuse, such as the following:</p> <ul style="list-style-type: none"> • Denial-of-service attacks • Port scans or sweeps • Malicious content in the data payload of a packet or packets • Vulnerability scanning • Trojans, viruses, or worms • Tunneling • Brute-force attacks 		
	<p>4</p>  <p style="text-align: center;">HIDS</p>	 <p style="text-align: center;">NIDS</p>		
	5	It is host dependent	It is host independent	
	6	It has low false positive rate	It has high false positive rate	
	7	It senses local attack.	It senses network attack	
	8	It slow down the host that have IDS client installed	It slow down the network that have IDS client installed	

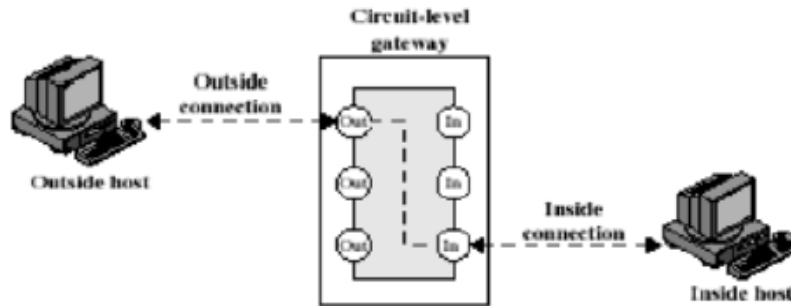
03.	<p>Explain DMZ.</p> <p style="text-align: center;">OR</p> <p>Describe DMZ with suitable example.</p>	S-22	4M
		W-22	4M
		S-23	4M
<p>Answer:</p>	<p>DMZ (Demilitarized Zone):-</p> <ul style="list-style-type: none"> It is a computer host or small network inserted as a “neutral zone” in a company’s private network and the outside public network. It avoids outside users from getting direct access to a company’s data server. A DMZ is an optional but more secure approach to a firewall. It can effectively acts as a proxy server. The typical DMZ configuration has a separate computer or host in network which receives requests from users within the private network to access a web sites or public network. Then DMZ host initiates sessions for such requests on the public network but it is not able to initiate a session back into the private network. It can only forward packets which have been requested by a host. 	W-23	4M
		W-24	4M
		S-24	6M
		W-24	4M

DMZ (Demilitarized Zone)



Advantage: The main benefit of a DMZ is to provide an internal network with an additional security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization's private network.

04.	<p>Differentiate between firewall & IDS</p> <p>OR</p> <p>State any four difference between Firewall and Intrusion Detection System.</p>	S-22	4M																		
Answer:	<table> <tr> <th>Sr.No.</th> <th>Firewall</th> <th>IDS</th> </tr> <tr> <td>1</td> <td>Firewall is hardware or software that stands between a local network and the Internet and filters traffic that might be harmful based on Pre-determined rules.</td> <td>An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.</td> </tr> <tr> <td>2</td> <td>Firewall does not inspect content of permitted traffic</td> <td>IDS inspects overall network traffic</td> </tr> <tr> <td>3</td> <td>A firewall can block an unauthorized access to network</td> <td>An IDS can only report an intrusion .It cannot block it.</td> </tr> <tr> <td>4</td> <td>Firewalls Block traffic based on rules the</td> <td>IDS gives Alerts/alarms on detection of anomaly</td> </tr> <tr> <td>5</td> <td>It filters traffic based on IP address and port numbers</td> <td>It detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts</td> </tr> </table>	Sr.No.	Firewall	IDS	1	Firewall is hardware or software that stands between a local network and the Internet and filters traffic that might be harmful based on Pre-determined rules.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.	2	Firewall does not inspect content of permitted traffic	IDS inspects overall network traffic	3	A firewall can block an unauthorized access to network	An IDS can only report an intrusion .It cannot block it.	4	Firewalls Block traffic based on rules the	IDS gives Alerts/alarms on detection of anomaly	5	It filters traffic based on IP address and port numbers	It detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts	S-23	4M
Sr.No.	Firewall	IDS																			
1	Firewall is hardware or software that stands between a local network and the Internet and filters traffic that might be harmful based on Pre-determined rules.	An intrusion detection system (IDS) is a device or software application that monitors a traffic for malicious activity or policy violations and sends alert on detection.																			
2	Firewall does not inspect content of permitted traffic	IDS inspects overall network traffic																			
3	A firewall can block an unauthorized access to network	An IDS can only report an intrusion .It cannot block it.																			
4	Firewalls Block traffic based on rules the	IDS gives Alerts/alarms on detection of anomaly																			
5	It filters traffic based on IP address and port numbers	It detects real time traffic and looks for traffic patterns or signatures of attack and them generates alerts																			
05.	<p>Define & explain :</p> <p>(i) Circuit Gateway (ii) Honey Pots (iii) Application Gateway</p>	S-22	6M																		
Answer:	<p>i) Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed. A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.</p>																				

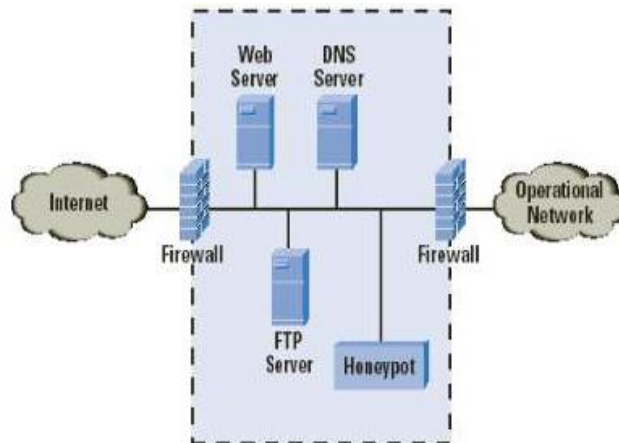


ii) Honey Pots

A relatively recent innovation in intrusion detection technology is the honey pot. Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. Honey pots are designed to:

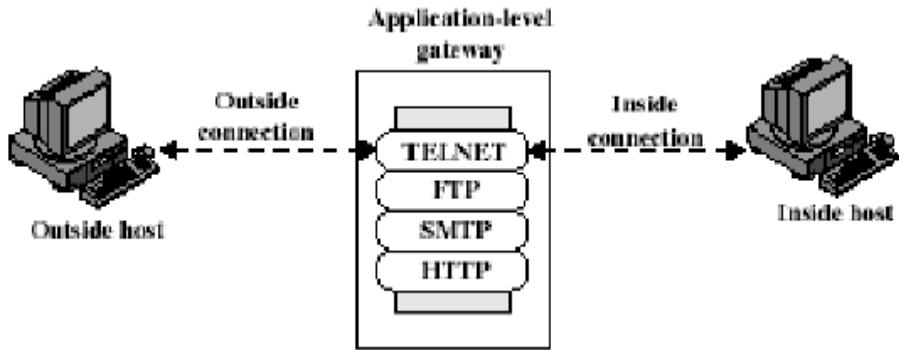
- divert an attacker from accessing critical systems
- collect information about the attacker's activity

It encourages the attacker to stay on the system long enough for administrators to respond. These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honey pot is suspect.



iii) Application Gateway

An Application level gateway, also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. Application level gateways tend to be more secure than packet filters. It is easy to log

	<p>and audit all incoming traffic at the application level. A prime disadvantage is the additional processing overhead on each connection.</p> 		
<p>06.</p> <p>Answer:</p>	<p>Explain Policies, configuration & limitations of Firewall.</p> <p>Policies of firewall: All traffic from inside to outside and vice versa must pass through the firewall. To achieve this all access to local network must first be physically blocked and access only via the firewall should be permitted. As per local security policy traffic should be permitted. The firewall itself must be strong enough so as to render attacks on it useless.</p> <p>Configuration of firewall There are 3 common firewall configurations.</p> <ol style="list-style-type: none"> 1. Screened host firewall, single-homed bastion configuration 2. Screened host firewall, dual homed bastion configuration 3. Screened subnet firewall configuration <p>1. Screened host firewall, single-homed bastion configuration</p> <p>In this type of configuration a firewall consists of following parts.</p> <p>(i) A packet filtering router (ii) An application gateway.</p> <p>The main purpose of this type is as follows:</p> <ul style="list-style-type: none"> • Packet filter is used to ensure that incoming data is allowed only if it is destined for application gateway, by verifying the destination address field of incoming IP packet. It also performs the same task on outgoing data by checking the source address field of outgoing IP packet. • Application gateway is used to perform authentication and proxy function. Here Internal users are connected to both application gateway as well as to packet filters therefore if packet filter is successfully 	<p>S-22 S-24</p>	<p>6M 6M</p>

attacked then the whole Internal Network is opened to the attacker

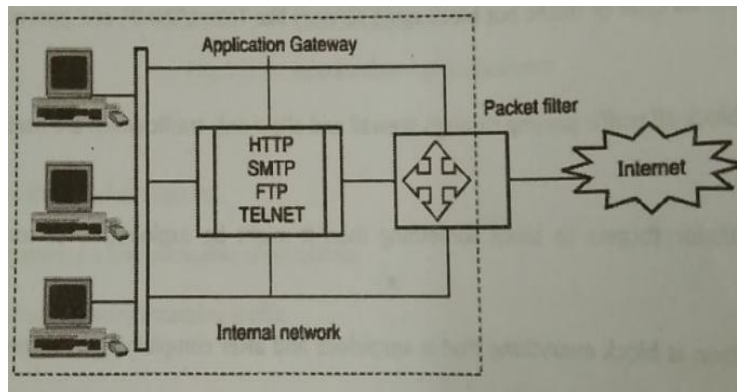


Fig single homed bastion configuration

2. Screened host firewall, dual homed bastion configuration

To overcome the disadvantage of a screened host firewall, single homed bastion configuration, another configuration is available known as screened host firewall, Dual homed bastion. In this, direct connections between internal hosts and packet filter are avoided. As it provides connection between packet filter and application gateway, which has separate connection with the internal hosts. Now if the packet filter is successfully attacked. Only application gateway is visible to attacker. It will provide security to internal hosts.

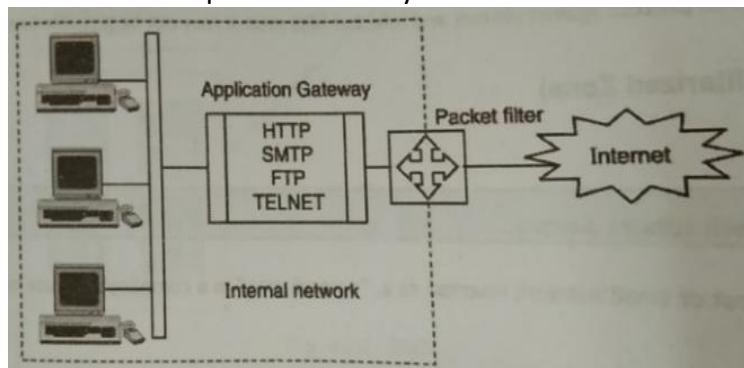


Fig dual homed bastion configuration

3. Screened subnet firewall configuration

It provides the highest security among all firewall configurations. It is an improved version over all the available schemes of firewall configuration. It uses two packet filters, one between the internet and application gateway and another between the application gateway and the internal network. Thus this configuration achieves 3 levels of security for an attacker to break into.

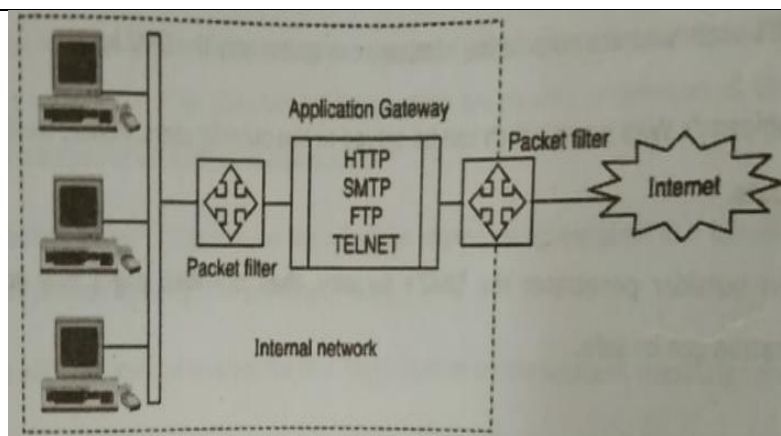
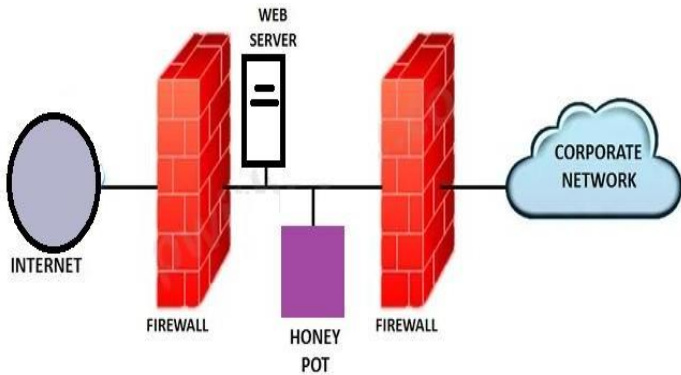
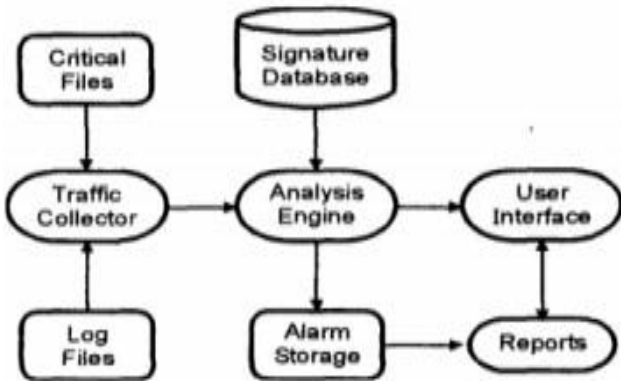


Fig Screened subnet firewall configuration

Limitations: (one mark)

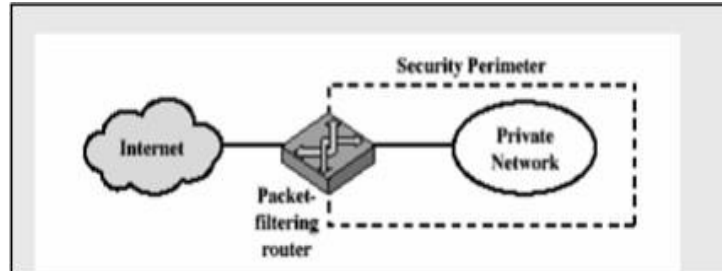
1. Firewall do not protect against inside threats.
 2. Packet filter firewall does not provide any content based filtering.
 3. Protocol tunneling, i.e. sending data from one protocol to another protocol which negates the purpose of firewall.
- Encrypted traffic cannot be examine and filter.

07.	Explain need for firewall.	W-22	2M
Answer:	<ul style="list-style-type: none"> • A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. • Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers. • Firewalls can be an effective means of protecting a local system or network of systems from network-based security threats while at the same time affording access to the outside world via wide area networks and the Internet. 		
08.	Explain Honey pots.	W-22	4M
Answer:	<p>Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet. The honeypots are designed to do the following:</p> <ol style="list-style-type: none"> 1. Divert the attention of potential attacker. 2. Collect information about the intruder's action. 3. Provide encouragement to the attacker so as to stay for some time, 		

	<p>allowing the administrations to detect this and swiftly act on this. Honeypots are designed for 2 important goals</p> <ol style="list-style-type: none"> 1. Make them look-like full real-life systems. 2. Do not allow legitimate users to know about or access them. 		
<p>9.</p> <p>Answer:</p>	<p>Explain Host based IDS.</p> <p>(Host Intrusion Detection System (HIDS))</p> <p>Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.</p> 	<p>W-22</p> <p>W-23</p> <p>S-24</p> <p>W-24</p>	<p>4M</p> <p>4M</p> <p>4M</p> <p>4M</p>

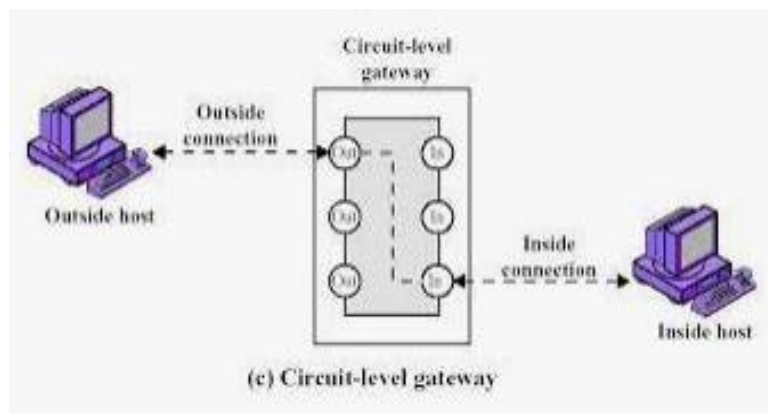
	<p>Basic Components HIDS:</p> <ul style="list-style-type: none"> • Traffic collector: This component collects activity or events from the IDS to examine. On Host-based IDS, this can be log files, audit logs, or traffic coming to or leaving a specific system • Analysis Engine: This component examines the collected network traffic & compares it to known patterns of suspicious or malicious activity stored in the signature database. The analysis engine acts like a brain of the IDS. • Signature database: It is a collection of patterns & definitions of known suspicious or malicious activity. • User Interface & Reporting: This is the component that interfaces with the human element, providing alerts & giving the user a means to interact with & operate the IDS. <p>Advantages:</p> <ul style="list-style-type: none"> - Analyze what an application does. - Detects the attacks excluded from the network <p>Disadvantages:</p> <ul style="list-style-type: none"> - Excluded from the network - Needs to be installed on every host spot - Passive in nature, so it just informs about the attack without doing anything about it. 		
10.	<p>List types of firewall and explain any one of them</p> <p>Answer: List of firewall are:</p> <ol style="list-style-type: none"> 1. Packet filter as a firewall 2. Circuit level gateway firewall 3. Application level gateway firewall 4. Proxy server as a firewall 5. Stateful multilayer Inspection Firewall <p>1. Packet filter as a firewall : As per the diagram given below Firewall will act according to the table given for example source IP 150.150.0.0 is the IP address of a network , all the packets which are coming from this network will be blocked by the firewall in this way it is acting as a firewall. Table also having port 80, IP Address 200.75.10.8 & port 23 firewall will act in the similar fashion. Port 23 is for Telnet remote login in this case</p>	W-22	6M

firewall won't allow to login onto this server. IP Address 200.75.10.8 is the IP address of individual Host, all the packet having this IP address as a destination Address will be denied. Port 80 no HTTP request allowed by firewall

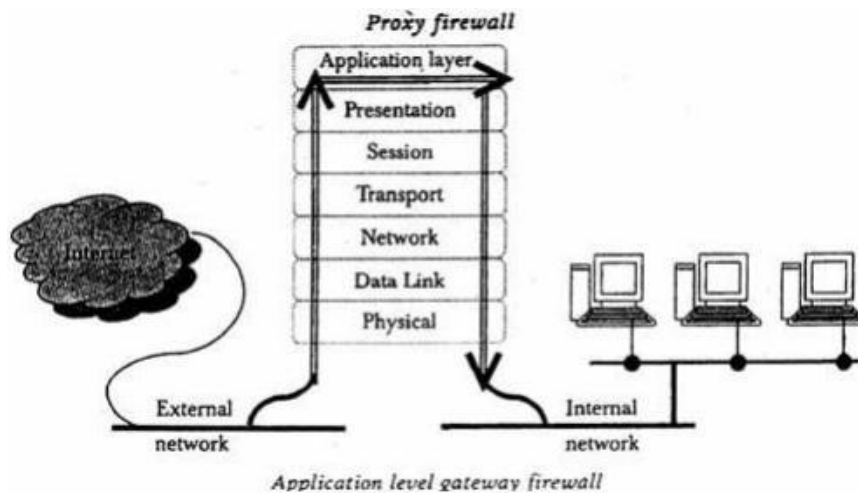


Packet Filtering

2. Circuit level gateway Firewalls: The circuit level gateway firewalls work at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate. And the information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. So, there is no way for a remote computer or a host to determine the internal private ip addresses of an organization, for example. This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet). This way, the packets are tagged with only the Public IP address (Firewall level) and the internal private IP addresses are not exposed to potential intruders

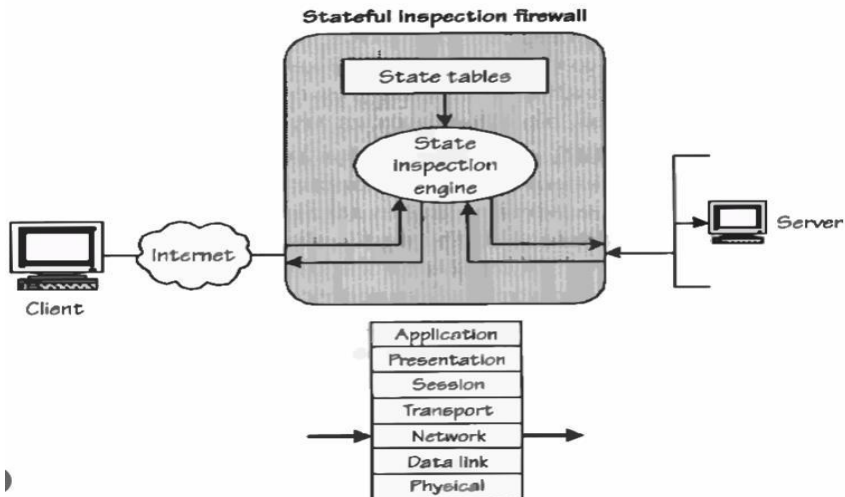
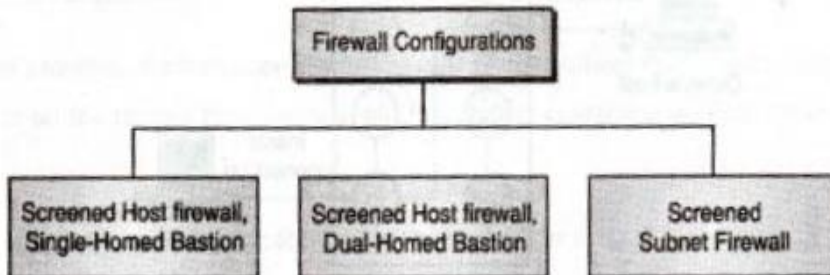


3. Application level gateway Firewalls: Application level firewalls decide whether to drop a packet or send them through based on the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. So, any suspicious data or connections are dropped by these proxies. Application level firewalls ensure protocol conformance. For example, attacks over http that violates the protocol policies like sending Non-ASCII data in the header fields or overly long string along with Non ASCII characters in the host field would be dropped because they have been tampered with, by the intruders.



5. Stateful multilayer Inspection Firewall (SMLI)

The Stateful multi-layer inspection (SMLI) firewall uses a sophisticated form of packet-filtering that examines all seven layers of the Open System Interconnection (OSI) model. Each packet is examined and compared against known states of friendly packets. While screening router firewalls only examine the packet header, SMLI firewalls examine the entire packet including the data. SMLI is a mechanism that uses a sophisticated form of packet-filtering, examining all major layers of the OSI model. In other words, this type of filter examines packets on the network, transmission, and application levels, comparing them to known trusted packets. SMLI checks the entire packet and only allows it to pass through each layer individually. Such firewalls inspect packets to assess the state of communication in order to ensure that all facilitated communication only takes place with trusted sources. To be more specific, an SMLI firewall is not necessarily a single firewall implementation. Rather, it is a series of firewalls that work in concert to secure traffic at different levels of the OSI model. It may be a

	<p>composition of a stateless packet filter, a state ful firewall, as well as an application- level proxy. SMLI.</p> 		
<p>11.</p> <p>Write a brief note on firewall configurations. OR State and explain 3 types of firewall configurations with a neat diagram.</p> <p>Answer:</p>	<p>A firewall is combination of packet filter and application level gateway, Base on these there are three types of configurations</p>  <p>1. Screened Host firewall, Single-Homed Bastion</p> <p>a) Here , the firewall configuration consist of two parts a packet filter router and application level gateway</p> <p>b) A packet filter router will insure that the income traffic will allowed only if it is intended for the application gateway, by examining the destination address field of each incoming IP Packet</p> <p>c) It will also insure that outgoing traffic is allowed only if it is originated from application level gateway, by examining the source address field of every outgoing IP packet.</p> <p>d) An application level gateway performs authentication as well as</p>	<p>W-22</p> <p>S-23</p> <p>W-23</p> <p>W-24</p>	<p>6M</p> <p>4M</p> <p>6M</p> <p>4M</p>

proxy function

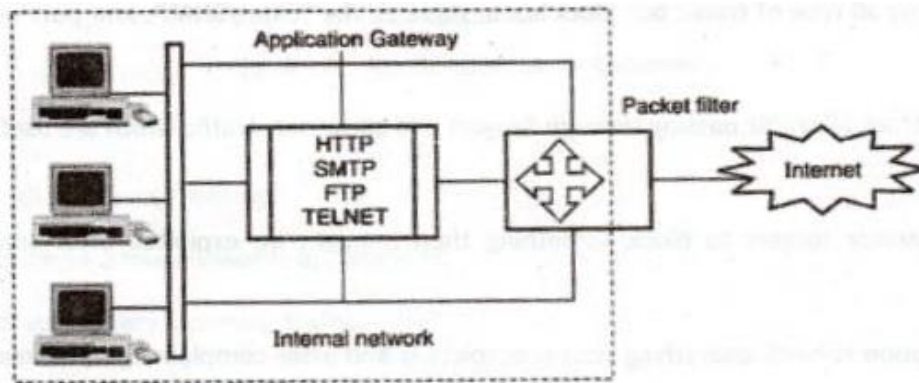


Fig: Single Homed Bastion

Advantages: It improve security of network by performing checks at both levels- that is packet and application level. It provide flexibility flexibility to the network administrator to define more secure policies.

Disadvantages: Internal users are connected to the application gateway as well as packet filter router, So if any how packet filter is attacked, then the whole internal network is exposed to the attacker.

1. Screened Host Firewall, Duel Homed Bastion: In this type of Configuration the direct connection between internal host and packet filter are avoided. Here the packet filter connection only to the application gateway, which is turned as separate connection with the internal host. Hence, Packet filter is successfully attacked, and then only application gateway is visible to the attacker.

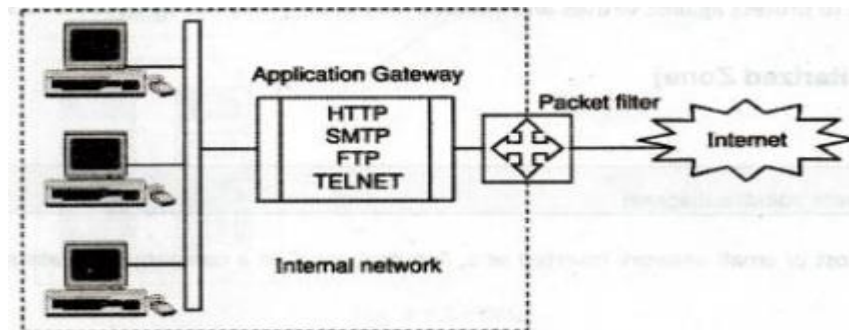
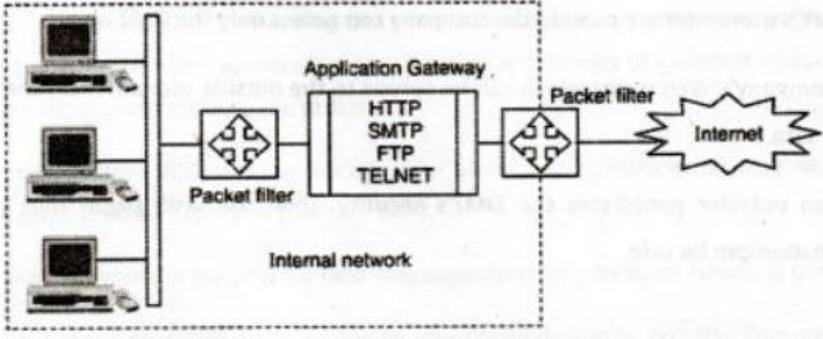
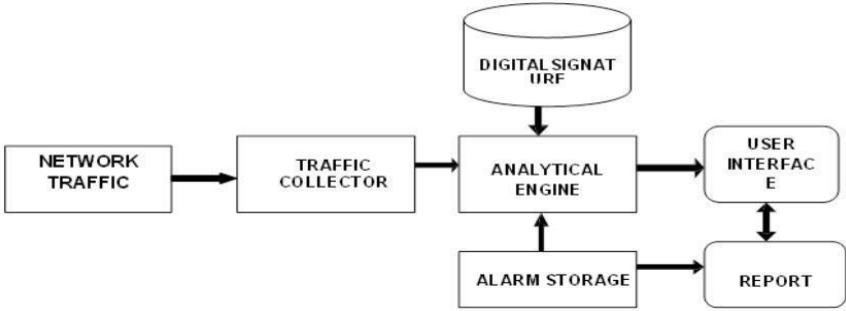


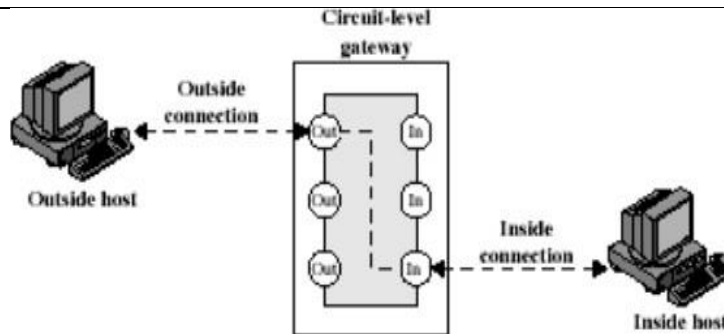
Fig: Dule Homed Bastion

3 Screened Subnet Firewall This type of configuration offer highest security among the possible configurations In this type two packet filters are used , one between internet and application gateway and other in

	<p>between application gateway and internal network This configuration achieve 3 level of security of an attacker to break into.</p>  <p>Fig: Screened Subnet Firewall</p>		
<p>12.</p> <p>Answer:</p>	<p>State any two policies of the firewall.</p> <p>a) All traffic from inside to outside and vice versa must pass through the firewall. To achieve this all access to local network must first be physically blocked and access only via the firewall should be permitted.</p> <p>b) As per local security policy traffic should be permitted. The firewall itself must be strong enough so as to render attacks on it useless.</p>	S-23	2M
<p>13.</p> <p>Answer:</p>	<p>Describe network based IDS with suitable diagram.</p> <p>Network Intrusion Detection System (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. Network based intrusion detection system sensors collect information from the network itself. Once, an abnormal behavior on network is observed, the alert can be sent to the administrator. NIDS is shown in fig. below.</p> <p>Network-based Intrusion Detection Systems:</p>  <p>Traffic collection: Collects activity as events from IDS to examine. On Host-based IDS, this can be log files, Audit logs or traffic coming to or leaving a system. On network based IDS, this is typically a mechanism for</p>	<p>S-23</p> <p>W-23</p> <p>W-24</p>	<p>6M</p> <p>4M</p> <p>4M</p>

	<p>copying traffic of network link.</p> <p>Analysis Engine: Examines collected network traffic & compares it to known patterns of suspicious or malicious activity stored in digital signature. The analysis engine act like a brain of IDS.</p> <p>Signature database: A collection of patterns & definitions" of known suspicious or malicious activity.</p> <p>User Interface & Reporting: interfaces with human element, providing alerts when suitable & giving the user a means to interact with & operate the IDS.</p> <p>Advantages of Network-based Intrusion Detection Systems : The deployment of network-based IDSs is usually easy with minimal effort. Network-based IDSs can be made very secure and is often invisible to most attackers. They can monitor a heterogeneous set of hosts and operating systems simultaneously, due to the fact that standard network protocols (e.g. TCP, UDP and IP) are supported and used by most major operating systems.</p> <p>Disadvantages of Network-based Intrusion Detection Systems : Network-based IDSs cannot analyses encrypted information. This problem is increasing as more organizations and attackers use virtual private networks, which normally utilize encrypted information. The processing load in a large or busy network may cause significant difficulties to the analysis engine part of the IDS. This condition (high processing load) can seriously limit an IDS's ability to detect attacks when the network load is above a specific amount of network traffic. Although some vendors have adopted hardware- based solutions for IDSs, to increase the speed of their processing capability (and the cost of implementation), the limitation still remains. The need to analyses packets as fast as possible, force developers to detect fewer attacks. Thus, the detection effectiveness is often compromised for the sake of cost effectiveness.</p>		
14.	<p>Describe following terms: (i) Packet filter Firewall (ii) Application gateway (iii) Circuit gateway</p> <p style="text-align: center;">OR</p> <p>State the working principle of application gateways. Describe circuit gateway operation.</p>	S-23	6M
Answer:	<p>(i). Packet Filter Firewall : A packet filtering router firewall applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. Such a firewall implementation involves a router,</p>	W-23	4M

	<p>which is configured to filter packets going in either direction i.e. from the local network to the outside world and vice versa. Packet filter performs the following functions :</p> <p>Receive each packet as it arrives. Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rule, decides whether to accept or discard the packet based on that rule.</p> <p>If there is no match with any rule, take the default action. It can be discard all packets or accept all packets.</p> <p>Advantages : simplicity, transparency to the users, high speed</p> <p>Disadvantages: difficult to set up packet filtering rules, lack of authentication.</p> <div data-bbox="516 770 1102 1060" data-label="Diagram"> <pre> graph LR A([Internal(private) network]) --- B[] B --- C((internet)) style B fill:#333,color:#fff,stroke:#fff,stroke-width:2px </pre> </div> <p>(ii) Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed. A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.</p>		
--	--	--	--

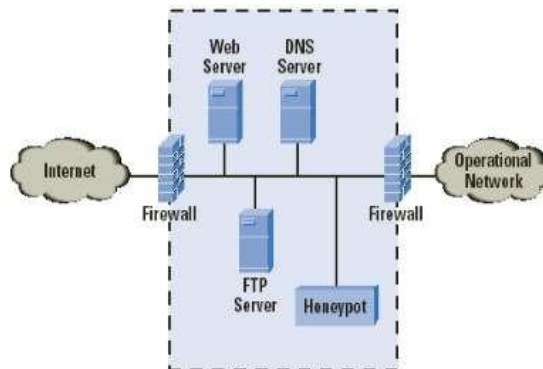


Honey Pots

A relatively recent innovation in intrusion detection technology is the honey pot. Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. Honey pots are designed to:

- divert an attacker from accessing critical systems
- collect information about the attacker's activity

It encourages the attacker to stay on the system long enough for administrators to respond. These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honey pot is suspect.



(iv)Application Gateway An Application level gateway, also called a proxy server, acts as a relay of application level traffic. The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed. When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints. Application level gateways tend to be more secure than packet filters. It is easy to log and audit all incoming traffic at the application level. A prime disadvantage is the additional processing overhead on each connection.

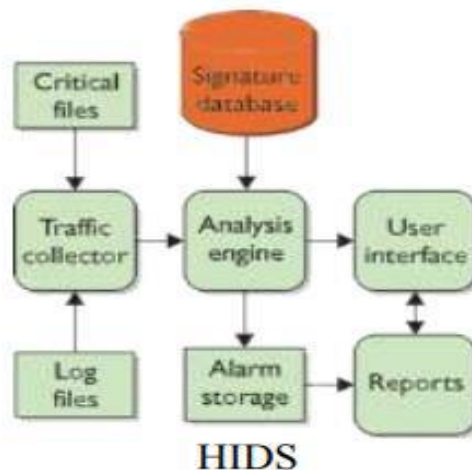
15.	<p>State the use of packet filters. Explain its operation.</p>	W-23	4M
Answer:	<p>Packet filters are a fundamental component of network security and are commonly used in firewalls to control and monitor the flow of network traffic. Their primary uses include:</p> <ol style="list-style-type: none"> 1. Access Control: Restricting or allowing traffic based on specified rules (e.g., IP addresses, ports, and protocols). 2. Traffic Monitoring: Analyzing and logging data packets to monitor network activity. 3. Network Segmentation: Enforcing boundaries between different network segments to reduce risks. 4. Mitigating Threats: Blocking unwanted or malicious traffic, such as IP spoofing or Denial of Service (DoS) attacks. <p>Operation of Packet Filters</p> <p>Packet filters work by inspecting packets at the network layer (Layer 3) and sometimes at the transport layer (Layer 4) of the OSI model. They determine whether to allow or block a packet based on a set of predefined rules.</p> <p>Steps in Packet Filtering Operation</p> <ol style="list-style-type: none"> 1. Inspection of Packet Headers: The packet filter examines the headers of incoming and outgoing packets. Key fields include: <ul style="list-style-type: none"> Source IP Address: The IP address of the sender. Destination IP Address: The intended recipient's IP address. Protocol Type: Determines whether it is TCP, UDP, ICMP, etc. Port Number: Indicates the specific application or service (e.g., HTTP uses port 80). 2. Rule Matching: Each packet is compared against a list of filtering rules defined by the administrator. A rule might specify: Allow traffic from a specific IP range on port 443 (HTTPS). Block all incoming traffic except for specific ports like 22 (SSH) or 80 (HTTP). 3. Action Enforcement: Based on the match, the packet filter performs one of two actions: Allow (Pass): The packet is forwarded to its 		

	<p>destination. Deny (Drop): The packet is discarded, and no further action is taken.</p> <p>Advantages of Packet Filters</p> <ul style="list-style-type: none"> -Fast and efficient due to simple header inspection. -Low resource requirements compared to more advanced firewalls. <p>Limitations of Packet Filters</p> <ul style="list-style-type: none"> -Cannot inspect packet payloads or higher-layer data (e.g., application content). -Vulnerable to IP spoofing if not configured properly. Lacks dynamic rule adaptation or advanced decision-making capabilities. 		
<p>16.</p> <p>Answer:</p>	<p>State the features of the following IDS:</p> <p>(i) Network based IDS (ii) Host based IDS (iii) Honey pots</p> <p>(i) Network based IDS: Examines activity on the network itself. It has visibility only into the traffic crossing the network link it is monitoring and typically has no idea of what is happening on individual systems. NIDSs look for certain activities that typify hostile actions or misuse, such as the following:</p> <ul style="list-style-type: none"> • Denial-of-service attacks • Port scans or sweeps • Malicious content in the data payload of a packet or packets • Vulnerability scanning • Trojans, viruses, or worms • Tunneling • Brute-force attacks <div data-bbox="565 1331 1023 1703" data-label="Diagram"> <pre> graph LR NT[Network traffic] --> TC[Traffic collector] TC --> AE[Analysis engine] SD[(Signature database)] --> AE AE --> UI[User interface] AE --> AS[Alarm storage] AS --> R[Reports] UI <--> R </pre> </div> <p>NIDS</p> <p>It is host independent, It has high false positive rate, it senses network attack. It slows down the network that has IDS client installed.</p>	W-23	6M

(ii) Host based IDS: Examines activity on an individual system, such as a mail server, web server, or individual PC. It is concerned only with an individual system and usually has no visibility into the activity on the network

or systems around it HIDS is looking for certain activities that typify hostile actions or misuse, such as the following:

- Logins at odd hours
- Login authentication failures
- Additions of new user accounts
- Modification or access of critical system files



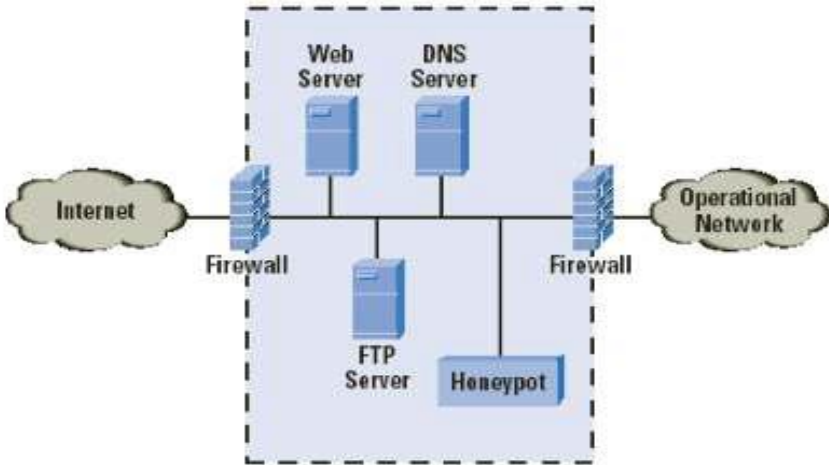
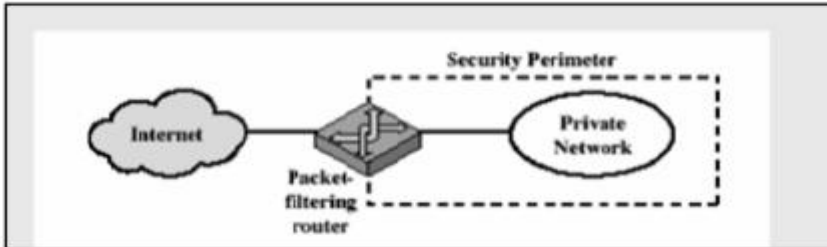
It is host dependent, It has low false positive rate, and It senses local attack. It slow down the host that have IDS client installed.

iii) Honey Pots

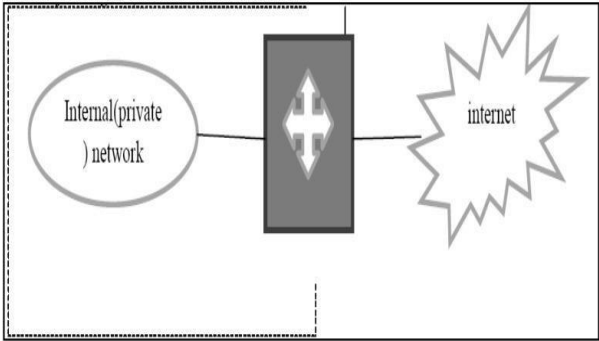
A relatively recent innovation in intrusion detection technology is the honey pot. Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. Honey pots are designed to:

- divert an attacker from accessing critical systems
- collect information about the attacker's activity

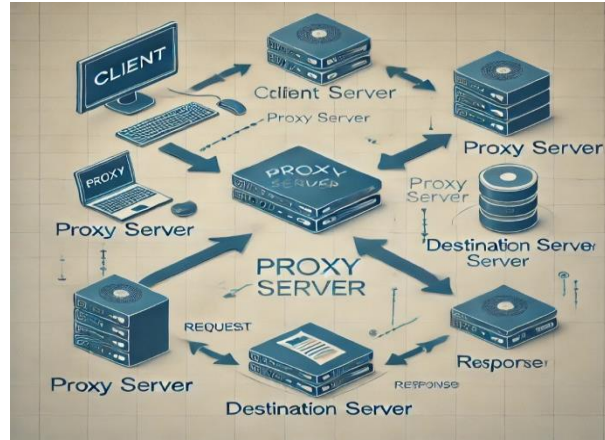
It encourages the attacker to stay on the system long enough for administrators to respond. These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honey pot is suspect

			
<p>17.</p> <p>Answer:</p>	<p>State any four limitations of firewall.</p> <ol style="list-style-type: none"> 1. Firewall do not protect against inside threats. 2. Packet filter firewall does not provide any content based filtering. 3. Protocol tunneling, i.e. sending data from one protocol to another protocol which negates the purpose of firewall. 4. Encrypted traffic cannot be examining and filter. 5. Firewall can be bypassed by hackers using techniques like port redirection or IP spoofing 6. Firewall can create compatibility issues when switching vendors 7. Continuous updating required. 8. High cost. 	S-24	2M
<p>18.</p> <p>Answer:</p>	<p>Describe packet filter router firewall with neat diagram.</p> <p>A packet filtering firewall is a network security device that filters incoming and outgoing network packets based on a predefined set of rules. Rules are typically based on IP addresses, port numbers, and protocols. By inspecting packet headers, the firewall decides if it matches an allowed rule; if not, it blocks the packet. The process helps protect networks and manage traffic, but it does not inspect packet contents for potential threats.</p>  <p style="text-align: center;">Packet Filtering</p>	S-24 W-24	4M 3M

	<p>This type of firewall operates at a fundamental level by applying a set of predetermined rules to each network packet that attempts to enter or leave the network. These rules are defined by the network administrator and are critical in maintaining the integrity and security of the network. Packet filtering firewalls use two main components within each data packet to determine their legitimacy: the header and the payload. The packet header includes the source and destination IP address, revealing the packet's origin and intended endpoint. Protocols such as TCP, UDP, and ICMP define rules of engagement for the packet's journey. Additionally, the firewall examines source and destination port numbers, which are similar to doors through which the data travels. Certain flags within the TCP header, like a connection request signal, are also inspected. The direction of the traffic (incoming or outgoing) and the specific network interface (NIC) the data is traversing, are factored into the firewall's decision making process. Packet filtering firewalls can be configured to manage both inbound and outbound traffic, providing a bidirectional security mechanism. This ensures unauthorized access is prevented from external sources attempting to access the internal network, and internal threats trying to communicate outwards.</p>		
<p>19.</p> <p>Answer:</p>	<p>Explain the features of IDS technique.</p> <ol style="list-style-type: none"> 1) IDS keeps an eye on the functions of routers, firewalls, key management servers, and files. 2) IDS provides continuous support to the users. 3) IDS arranges the various audit trails and other logs. 4) IDS generates an alarm when security breaches are detected. 5) IDS can detect any suspicious activities and alert the system administrator before any significant damage is done. 6) IDS can identify any performance issues on the network, which can be addressed to improve network performance. 7) IDS can help in meeting compliance requirements by monitoring network activity and generating reports. 8) IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security. 	S-24	4M
<p>20.</p> <p>Answer:</p>	<p>Define the term Honeypots.</p> <p>A Honeypot is a security mechanism designed to detect, deflect, or counteract unauthorized access or cyber-attacks. It is typically a decoy system, network, or application deliberately set up to mimic a legitimate target and lure attackers, thereby diverting them from real asset.</p>	W-24	2M

21. Answer:	Enlist two Intrusion Detection System. 1. Host-Based intrusion detection system 2. Network-based intrusion detection system	W-24	2M
22. Answer:	Draw & explain following terms: (i) Packet Filter Firewall (ii) Proxy Server (i) Packet Filter Firewall: A packet filtering router firewall applies a set of rules to each packet and based on outcome, decides to either forward or discard the packet. Such a firewall implementation involves a router, which is configured to filter packets going in either direction i.e. from the local network to the outside world and vice versa. Packet filter performs the following functions : Receive each packet as it arrives. Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rule, decides whether to accept or discard the packet based on that rule. If there is no match with any rule, take the default action. It can be discard all packets or accept all packets. Advantages : simplicity, transparency to the users, high speed Disadvantages: difficult to set up packet filtering rules, lack of authentication. 	W-24	6M

(ii) Proxy Server



A **proxy server** acts as an intermediary between a client (e.g., a user's device) and the internet or another server. It processes requests from clients seeking resources from other servers, forwarding those requests on behalf of the client and often modifying or filtering them for various purposes. The image illustrates the operation of a **proxy server** within a network. Here's how it works:

1. **Client:** The user's device (e.g., computer or smartphone) sends a request to access resources, such as a website or data from a server.
2. **Proxy Server:** The request first reaches the proxy server, which acts as an intermediary. The proxy can:
 - Filter or modify the request.
 - Mask the client's identity.
 - Cache the resource if it has been accessed before.
3. **Destination Server:** The proxy forwards the request to the actual server (e.g., a web server hosting the desired resource).
4. **Response:** The destination server processes the request and sends the response back to the proxy server, which forwards it to the client. This setup improves **privacy, security, performance, and access control** in a network environment.



JSPM's
**RAJARSHI SHAHU COLLEGE OF ENGINEERING,
 POLYTECHNIC**
Department of Computer Engineering
 Academic Year: 2024-25

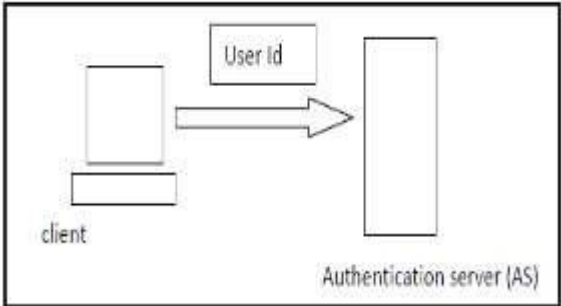
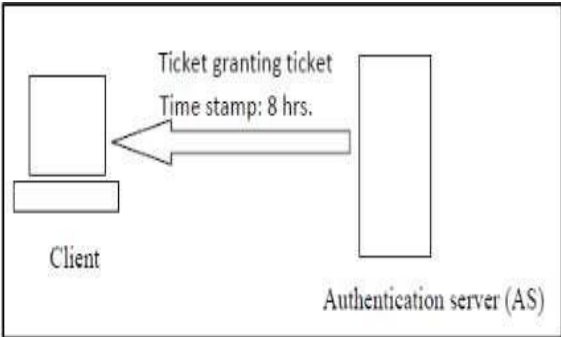


UNIT-V (14 Marks)

MSBTE Question bank & Answer

01.	<p>Classify following cybercrimes :</p> <p>(i) Cyber stalking</p> <p>(ii) Email harassment</p>	S-22	2M
Answer:	<p>i) Cyber stalking: Cyber Stalking means following some ones activity over internet. This can be done with the help of many protocols available such as e- mail, chat rooms, and user net groups.</p> <p style="text-align: center;"><u>OR</u></p> <p>Cyber stalking: Cyber stalking/ Harassment refers to the use of the internet and other technologies to harass or stalk another person online, and is potentially a crime in the India under IT act-2000. This online harassment, which is an extension of cyberbullying and in- person stalking, can take the form of e-mails, text messages, social media posts, and more and is often methodical, deliberate, and persistent.</p> <p>ii) Email harassment: Email harassment is usually understood to be a form of stalking in which one or more people send consistent, unwanted, and often threatening electronic messages to someone else</p> <p>Email harassment: Cybercrime against individual.</p>		
02.	<p>Define AH & ESP with respect to IP security</p>	S-22	2M
Answer:	<p>Authentication Header(AH):</p> <ol style="list-style-type: none"> 1. The AH provides support for data integrity and authentication of IP packets. The data integrity service ensures that data inside IP packet is not altered during the transit. 2. The authentication service enables an end user or computer system to authenticate the user or the application at the other end and decide to accept or reject packets accordingly <p>Encapsulation Header (ESP):</p> <ol style="list-style-type: none"> 1. Used to provide confidentiality, data origin authentication, data integrity. 2. It is based on symmetric key cryptography technique. 3. ESP can be used in isolation or it can be combined with AH. 		

03.	Explain Email security in SMTP.	S-22	4M
Answer:	<p>Email Security Email is emerging as one of the most valuable services on the internet today. Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver side.</p> <ol style="list-style-type: none"> 1. SMTP (simple mail transfer protocol) 2. PEM (Privacy Enhance Mail) 3. PGP (Pretty Good Privacy) <p>SMTP (Simple Mail Transfer Protocol)</p> <p>Simple Mail Transfer Protocol, a protocol for sending email messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application. SMTP usually is implemented to operate over Internet port 25. An alternative to SMTP that is widely used in Europe is X.400. Many mail servers now support Extended Simple Mail Transfer Protocol (ESMTP), which allows multimedia files to be delivered as e-mail. The basic phases of an email communication consists of the following steps :-</p> <ol style="list-style-type: none"> 1. At sender's end an SMTP server takes the message sent by uses computer 2. The SMTP server at the sender's end then transfer the message to the SMTP server of the receiver. <p>The receiver's computer then pulls the email message from the SMTP server at the receiver's end, using the other mail protocol such as Post Office Protocol (POP) or IMAP (Internet mail access protocol).</p>	W-24	4M

04.	Explain the working of Kerberos.	S-22	6M
Answer:	<p>Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.</p> <p>The entire process takes a total of eight steps, as shown below.</p> <p>1. The authentication service, or AS, receives the request by the client and verifies that the Client is indeed the computer it claims to be. This is usually just a simple database lookup of the users ID.</p>  <p>2. Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours. The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless. (This is used to make sure a hacker doesn't intercept the data, and try to crack the key. Almost all keys are able to be cracked, but it will take a lot longer than 8 hours to do so).</p>  <p>3. The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference. The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.</p>	W-22	6M
		S-23	6M
		W-23	6M
		S-24	2M
		W-24	6M

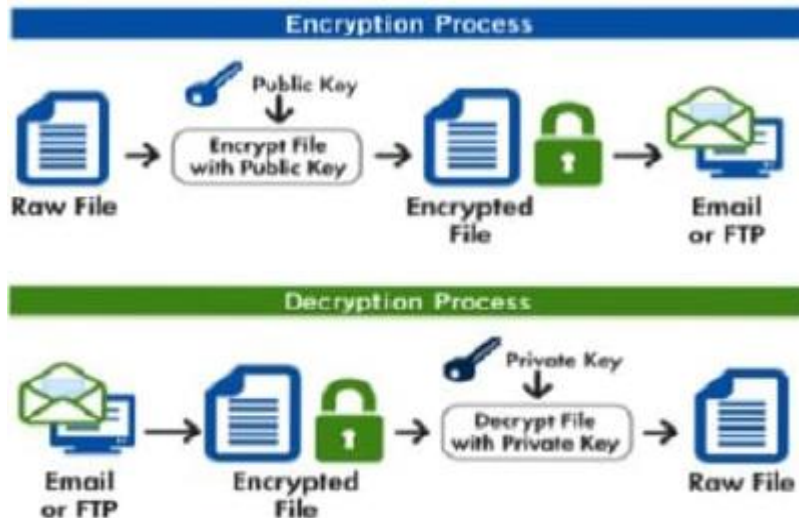
	<div data-bbox="527 195 1141 543" data-label="Diagram"> <p>client</p> <p>TGT Ticket Time stamp 8hrs</p> <p>Authentication server (AS)</p> <p>Ticket Granting Server (TGS)</p> </div> <p data-bbox="362 562 1235 632">5. The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.</p> <div data-bbox="522 644 1110 961" data-label="Diagram"> <p>Client</p> <p>Encrypted key Time stamp 8 hrs</p> <p>Authentication server (AS)</p> <p>Ticket Granting Server (TGS)</p> </div> <p data-bbox="362 978 1213 1050">6. The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service server.</p> <div data-bbox="527 1102 1107 1438" data-label="Diagram"> <p>client</p> <p>Encrypted key Time stamp 8hrs Ticket Granting Server (TGS)</p> <p>Authentication server (AS)</p> <p>Service server</p> </div> <p data-bbox="362 1455 1268 1640">7. The service server decrypts the key, and makes sure the timestamp is still valid. If it is, the service contacts the key distribution center to receive a session that is returned to the client. The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.</p>		
<p data-bbox="240 1682 285 1709">05.</p> <p data-bbox="203 1759 318 1787">Answer:</p>	<p data-bbox="345 1682 951 1709">Explain Public Key Infrastructure with example</p> <p data-bbox="362 1759 1276 1860">A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.</p>	<p data-bbox="1325 1682 1385 1709">S-22</p>	<p data-bbox="1458 1682 1503 1709">6M</p>

	<p>The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. PKI is the governing body behind issuing digital certificates. It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications. The public key infrastructure uses a pair of keys: the public key and the private key to achieve security. The public keys are prone to attacks and thus an intact infrastructure is needed to maintain them. PKI identifies a public key along with its purpose. It usually consists of the following components:</p> <ul style="list-style-type: none"> • A digital certificate also called a public key certificate • Private Key tokens • Registration authority • Certification authority • CMS or Certification management system <p>Working on a PKI: PKI and Encryption: The root of PKI involves the use of cryptography and encryption techniques. Both symmetric and asymmetric encryption uses a public key. There is always a risk of MITM (Man in the middle). This issue is resolved by a PKI using digital certificates. It gives identities to keys in order to make the verification of owners easy and accurate. Public Key Certificate or Digital Certificate: Digital certificates are issued to people and electronic systems to uniquely identify them in the digital world. The Certification Authority (CA) stores the public key of a user along with other information about the client in the digital certificate. The information is signed and a digital signature is also included in the certificate. The affirmation for the public key then thus be retrieved by validating the signature using the public key of the Certification Authority.</p>		
06.	Explain use of PC DSS.	W-22	2M
Answer:	<p>The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept process, store or transmit credit card information maintain a secure environment. PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data. It presents common sense steps that mirror best security practices.</p>		

07.	Describe working principle of SMTP.	W-22	4M
Answer:	<p>1. Composition of Mail: A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.</p> <p>2. Submission of Mail: After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.</p> <p>3. Delivery of Mail: E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name. If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.</p> <p>4. Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.</p> <p>5. Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.</p>		

08.	Explain IP sec security with help of diagram.	W-22	6M
Answer:	<div data-bbox="501 291 1062 919" data-label="Diagram"> <p>It encrypts and seal the transport and application layer data during transmission. It also offers integrity protection for internet layer. It sits between transport and internet layer of conventional TCP/IP protocol</p> <ol style="list-style-type: none"> 1. Secure remote internet access: Using IPsec make a local call to our internet services provider (ISP) so as to connect to organization network in a secure fashion from our house or hotel from there; to access the corporate network facilities or access remote desktop/servers. 2. Secure branch office connectivity: Rather than subscribing to an expensive leased line for connecting its branches across cities, an organization can setup an IPsec enabled network for security. 3. Setup communication with other organization: Just as IPsec allow connectivity between various branches of an organization, it can also be used to connect the network of different organization together in a secure & inexpensive fashion. Basic Concept of IPsec Protocol: IP packet consist two position IP header & actual data IPsec feature are implemented in the form of additional headers called as extension header to the standard, default IP header. IPsec offers two main services authentication & confidentiality. Each of these requires its own extension header. Therefore, to support these two main services, IPsec defines two IP extension header one for authentication & another for confidentiality. </div>		

	<p>It consists of two main protocols:</p> <p>Authentication header (AH): Authentication header is an IP Packet (AH) protocol provides authentication, integrity & an optional anti-reply service. The IPsec AH is a header in an IP packet. The AH is simply inserted between IP header & any subsequent packet contents no changes are required to data contents of packet. Security resides completing in content of AH.</p> <p>Encapsulation Header (ESP): Used to provide confidentiality, data origin authentication, data integrity. It is based on symmetric key cryptography technique. ESP can be used in isolation or it can be combined with AH.</p>		
<p>09.</p> <p>Answer:</p>	<p>List any four types of cybercrimes.</p> <p>Types of cybercrime</p> <ol style="list-style-type: none"> 1. Hacking types 1/2M 2. Digital Forgery 3. Cyber Stalking / Harassment 4. Cyber Pornography 5. Identity Theft and Fraud 6. Cyber Terrorism 7. Cyber Defamation 	S-23	2M
<p>10.</p> <p>Answer:</p>	<p>Describe PGP with suitable diagram.</p> <p>PGP is Pretty Good Privacy. It is a popular program used to encrypt and decrypt email over the internet. It becomes a standard for security. It is used to send encrypted code {digital signature} that the receiver verify the sender's identity and takes care that the route of message should not change. PGP can be used to encrypt file stored so that they are in unreadable form and not readable by u or intruders It is available in Low cost and Freeware version. It is most way use privacy ensuring program used by individuals well as many corporations.</p>	S-23	4M



There are five steps as shown below:

1. **Digital signature:** it consists of the creation a message digest email message using SHA-1 algorithm. The resulting MD is encrypted with the sender's private key. The result is the sender's digital signature.
2. **Compression:** The input message as well as p digital signature compressed together to reduce the size of final message that transmitted. For this the Lempel -Ziv algorithm is used.
3. **Encryption:** The compressed output of step 2 (i.e. the comp form of the original email and the digital signature together encrypted with a symmetric key.
4. **Digital enveloping:** the symmetric key used for encryption ins is nov encrypted with the receiver's public key. The output of step 3 and 4 together form a digital envelope.
5. **Base -64 encoding:** this process transforms arbitrary binary into printable character output The binary input is process blocks of 3 octets (24-bits) .these 24 bits are considered to be of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into bit output character in this process.

11.	Find the output of the initial permutation box when the input is given in hexadecimal as 0X0003 0000 0000 0001	S-23	4M																																																																																																																																																																				
Answer:	<table><tr><td>0</td><td>0</td><td>0</td><td>3</td><td>Hexadecimal</td></tr><tr><td>0000</td><td>0000</td><td>0000</td><td>0011</td><td>Binary</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>Hexadecimal</td></tr><tr><td>0000</td><td>0000</td><td>0000</td><td>0000</td><td>Binary</td></tr><tr><td>0</td><td>0</td><td>0</td><td>0</td><td>Hexadecimal</td></tr><tr><td>0000</td><td>0000</td><td>0000</td><td>0000</td><td>Binary</td></tr><tr><td>0</td><td>0</td><td>0</td><td>1</td><td>Hexadecimal</td></tr><tr><td>0000</td><td>0000</td><td>0000</td><td>0001</td><td>Binary</td></tr></table> <p>Input:</p> <table><tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>2</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>3</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>4</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>6</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>7</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>8</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table> <p>Permutation table</p> <table><tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>1</td><td>58</td><td>50</td><td>42</td><td>34</td><td>26</td><td>18</td></tr><tr><td>2</td><td>60</td><td>52</td><td>44</td><td>36</td><td>28</td><td>20</td></tr><tr><td>3</td><td>62</td><td>54</td><td>46</td><td>38</td><td>30</td><td>22</td></tr><tr><td>4</td><td>64</td><td>56</td><td>48</td><td>40</td><td>32</td><td>24</td></tr><tr><td>5</td><td>57</td><td>49</td><td>41</td><td>33</td><td>25</td><td>17</td></tr><tr><td>6</td><td>59</td><td>51</td><td>43</td><td>35</td><td>27</td><td>19</td></tr><tr><td>7</td><td>61</td><td>53</td><td>45</td><td>37</td><td>29</td><td>21</td></tr><tr><td>8</td><td>63</td><td>55</td><td>47</td><td>39</td><td>31</td><td>23</td></tr></table>	0	0	0	3	Hexadecimal	0000	0000	0000	0011	Binary	0	0	0	0	Hexadecimal	0000	0000	0000	0000	Binary	0	0	0	0	Hexadecimal	0000	0000	0000	0000	Binary	0	0	0	1	Hexadecimal	0000	0000	0000	0001	Binary		1	2	3	4	5	6	1	0	0	0	0	0	0	2	0	0	0	0	0	0	3	0	0	0	0	0	0	4	0	0	0	0	0	0	5	0	0	0	0	0	0	6	0	0	0	0	0	0	7	0	0	0	0	0	0	8	0	0	0	0	0	0		1	2	3	4	5	6	1	58	50	42	34	26	18	2	60	52	44	36	28	20	3	62	54	46	38	30	22	4	64	56	48	40	32	24	5	57	49	41	33	25	17	6	59	51	43	35	27	19	7	61	53	45	37	29	21	8	63	55	47	39	31	23
0	0	0	3	Hexadecimal																																																																																																																																																																			
0000	0000	0000	0011	Binary																																																																																																																																																																			
0	0	0	0	Hexadecimal																																																																																																																																																																			
0000	0000	0000	0000	Binary																																																																																																																																																																			
0	0	0	0	Hexadecimal																																																																																																																																																																			
0000	0000	0000	0000	Binary																																																																																																																																																																			
0	0	0	1	Hexadecimal																																																																																																																																																																			
0000	0000	0000	0001	Binary																																																																																																																																																																			
	1	2	3	4	5	6																																																																																																																																																																	
1	0	0	0	0	0	0																																																																																																																																																																	
2	0	0	0	0	0	0																																																																																																																																																																	
3	0	0	0	0	0	0																																																																																																																																																																	
4	0	0	0	0	0	0																																																																																																																																																																	
5	0	0	0	0	0	0																																																																																																																																																																	
6	0	0	0	0	0	0																																																																																																																																																																	
7	0	0	0	0	0	0																																																																																																																																																																	
8	0	0	0	0	0	0																																																																																																																																																																	
	1	2	3	4	5	6																																																																																																																																																																	
1	58	50	42	34	26	18																																																																																																																																																																	
2	60	52	44	36	28	20																																																																																																																																																																	
3	62	54	46	38	30	22																																																																																																																																																																	
4	64	56	48	40	32	24																																																																																																																																																																	
5	57	49	41	33	25	17																																																																																																																																																																	
6	59	51	43	35	27	19																																																																																																																																																																	
7	61	53	45	37	29	21																																																																																																																																																																	
8	63	55	47	39	31	23																																																																																																																																																																	

	<div>Output</div> <table><tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></tr><tr><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>2</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>3</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>4</td><td>1</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>5</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>6</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>7</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr><tr><td>8</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table> <div>Hexadecimal 0000 0082 0000 0002 Note: Any other relevant logic shall be considered.</div>		1	2	3	4	5	6	1	0	0	0	0	0	0	2	0	0	0	0	0	0	3	0	0	0	0	0	0	4	1	0	0	0	0	0	5	0	0	0	0	0	0	6	0	0	0	0	0	0	7	0	0	0	0	0	0	8	0	0	0	0	0	0		
	1	2	3	4	5	6																																																												
1	0	0	0	0	0	0																																																												
2	0	0	0	0	0	0																																																												
3	0	0	0	0	0	0																																																												
4	1	0	0	0	0	0																																																												
5	0	0	0	0	0	0																																																												
6	0	0	0	0	0	0																																																												
7	0	0	0	0	0	0																																																												
8	0	0	0	0	0	0																																																												
<div>12.</div> <div>Answer:</div>	<div>Describe COBIT framework with neat diagram.</div> <div><pre>graph TD; BR[Business Requirements] --> DI((Drive the investments in)); DI --> IR[IT resources]; IR --> TU((That are used by)); TU --> IP[IT processes]; IP --> TD((To deliver)); TD --> EI[Enterprise Information]; EI --> WR((Which respond to)); WR --> BR; COBIT[/COBIT/];</pre><p>COBIT Structure</p><p>COBIT stands for "Control Objectives for Info1mation and related Technology", it is a framework that was developed by ISACA (Information System Audit and Control Association). It is as guidance material for IT governance to manage their requirement technical issues, and business risks.</p></div>	<div>S-23 S-24</div>	<div>6M 6M</div>																																																															

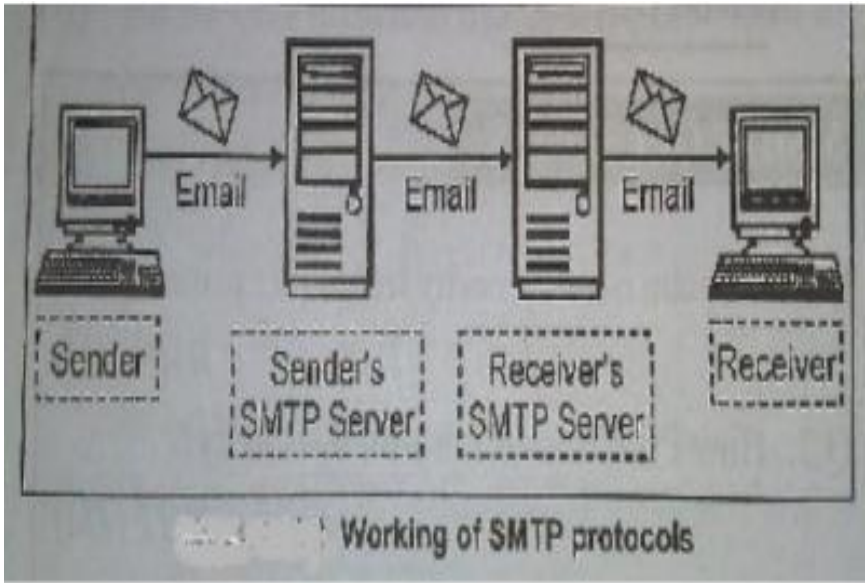
	<p>COBIT connects IT initiatives with business requirements, monitor and improves IT management practices, and ensures quality and reliability of information systems in an organization.</p> <ul style="list-style-type: none"> • Plan and Organize: This domain addresses direction to solution Information architecture, managing IT investments, asset risks, quality, and project • Acquire and Implement This domain acquires and main application software and technology infrastructure, development well as maintains procedures and manages changes, desired solutions and passes them to be turned into service • Deliver and Support This domain defines and manages levels, ensures the security of the system, educates or train advises users. It receives solutions and makes them usable Users. • Monitor and Evaluate: This domain monitors the process, as: internal control capability, finds independent assurance, provides independent audit Principle of COBIT: • Providing service of delivering information that an organized, requires. • Undesired events will be prevented, detected, and corrected. • Managing and controlling IT resources using a structured I processes. Fulfilling client's requirements. 		
<p>13.</p> <p>Answer:</p>	<p>List two protocols in IP Sec. State its function.</p> <p>1. Authentication Header (AH)</p> <p>Function: It Provides data integrity, authentication, and anti-replay protection for IP packets. Ensures that the data has not been tampered with during transit and that it originates from a legitimate source. AH does not provide encryption, so the payload remains visible.</p> <p>2. Encapsulating Security Payload (ESP)</p> <p>Function: Provides data confidentiality through encryption, as well as optional data integrity, authentication, and anti-replay protection. Ensures that the payload (data) is encrypted and protected from unauthorized access during transmission. Often used in combination with AH for comprehensive security.</p>	W-23	2M

<p>14.</p> <p>Answer:</p>	<p>Classify the following cybercrime:</p> <p>(i) Cyber terrorism against a government organization (it) Cyber-Stalking (iii) Copyright infringement (iv) Email harassment</p> <p>i) Cyber terrorism against a government organization: Cyber terrorism involves the use of cyber-attacks by malicious actors (e.g., terrorist groups or individuals) to disrupt critical government operations, instill fear, or achieve political, ideological, or social objectives.</p> <p>ii) Cyber stalking: Cyber Stalking means following some ones activity over internet. This can be done with the help of many protocols available such as e- mail, chat rooms, and user net groups.</p> <p>iii) Copyright infringement: Copyright infringement occurs when someone uses, reproduces, distributes, displays, or performs copyrighted material without the permission of the copyright owner, violating their exclusive rights under copyright law.</p> <p>iv) Email harassment: Email harassment is usually understood to be a form of stalking in which one or more people send consistent, unwanted, and often threatening electronic messages to someone else.</p>	<p>W-23</p>	<p>2M</p>
<p>15.</p> <p>Answer:</p>	<p>Describe ITIL framework with different stages of life cycle.</p> <p>The ITIL (Information Technology Infrastructure Library) framework is a set of best practices for delivering IT services. It provides a systematic approach to IT service management (ITSM) to ensure that IT services are aligned with business needs and delivered effectively and efficiently. ITIL is widely adopted across organizations to improve service delivery, reduce costs, enhance customer satisfaction, and manage risks in IT service operations.</p> <p>ITIL Service Lifecycle: The ITIL framework organizes service management into five stages in the service lifecycle. Each stage focuses on specific aspects of service management and has its own set of processes and best practices.</p> <p>1. Service Strategy Purpose: Defines the approach to create and deliver IT services that align with the organization's objectives and customer needs. Key Objectives:</p> <ul style="list-style-type: none"> Understand customer needs and the value IT services provide. 	<p>W-23</p>	<p>6M</p>

	<ul style="list-style-type: none"> • Define service portfolios and prioritize services based on business outcomes. • Manage demand, risk, and costs associated with IT services. <p>Processes:</p> <ul style="list-style-type: none"> • Service Portfolio Management • Financial Management for IT Services • Demand Management • Business Relationship Management <p>2. Service Design</p> <p>Purpose: Focuses on designing IT services and processes to meet the objectives defined in the Service Strategy stage.</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> • Design new or modified services to meet business requirements. • Ensure services are efficient, scalable, and resilient. • Document and manage service level agreements (SLAs). <p>Processes:</p> <ul style="list-style-type: none"> • Service Catalog Management • Service Level Management • Capacity Management • Availability Management • IT Service Continuity Management • Information Security Management • Supplier Management <p>3. Service Transition</p> <p>Purpose: Facilitates the transition of new or changed services into the operational environment, ensuring minimal disruption to business operations.</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> • Plan and manage service changes efficiently. • Test and validate services to meet design specifications. • Ensure stakeholders are informed and prepared for service deployment. <p>Processes:</p> <ul style="list-style-type: none"> • Change Management • Release and Deployment Management • Service Validation and Testing • Configuration Management 		
--	---	--	--

	<ul style="list-style-type: none"> • Knowledge Management <p>4. Service Operation Purpose: Focuses on managing and delivering IT services to ensure they meet agreed service levels and deliver value to the business.</p> <p>Key Objectives: -Maintain stability and availability of IT services. -Resolve incidents and service requests promptly. -Ensure user satisfaction and operational excellence.</p> <p>Processes:</p> <ul style="list-style-type: none"> • Incident Management • Problem Management • Event Management • Request Fulfillment • Access Management <p>5. Continual Service Improvement (CSI) Purpose: Continuously improve the effectiveness and efficiency of IT services and processes.</p> <p>Key Objectives: -Identify opportunities for improvement in services, processes, and infrastructure. -Measure and analyze performance metrics against SLAs and business goals. -Implement changes to enhance value delivery.</p> <p>Processes:</p> <ul style="list-style-type: none"> • Service Measurement and Reporting • Service Review and Assessment • Improvement Initiatives <p>Benefits of ITIL Framework</p> <ol style="list-style-type: none"> 1. Enhanced Customer Satisfaction: ITIL ensures services meet customer needs, improving satisfaction and trust. 2. Improved Service Quality: Standardized processes result in reliable and consistent service delivery. 3. Cost Optimization: Efficient use of resources reduces unnecessary expenditures and improves ROI. 		
--	---	--	--

	<p>4. Risk Management: Proactive risk identification and mitigation ensure business continuity.</p> <p>5. Alignment with Business Goals: IT services are closely aligned with organizational objectives.</p> <p>The ITIL framework provides a structured approach to IT service management, with its lifecycle stages ensuring end-to-end service excellence. Each stage plays a vital role in delivering value, from strategy and design to operation and continual improvement, making ITIL a cornerstone for modern IT organizations.</p>		
16.	<p>Define term cybercrime.</p> <p>Answer: Cybercrime /Computer crime, make the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. OR Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cyber criminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.</p>	S-24	2M
17.	<p>Explain working principle of SMTP in detail.</p> <p>Answer:</p> <ol style="list-style-type: none"> Composition of Mail: A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. Submission of Mail: After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25. Delivery of Mail: If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it. 	S-24	6M

	<p>5. Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.</p> 		
<p>18.</p> <p>Answer:</p>	<p>Explain following terms of intellectual property right: (i) Copyright (ii) Patent (iii) Trademark</p> <p>(i) Copyright</p> <ul style="list-style-type: none"> • Definition: Copyright protects the original works of authorship such as literature, music, art, software, and films. • Purpose: It grants the creator exclusive rights to reproduce, distribute, display, and perform their work or create derivative works. • Duration: Typically lasts for the life of the creator plus a specified number of years (e.g., 70 years in many jurisdictions). • Example: A novelist's book, a musician's song, or a software developer's code. <p>(ii) Patent</p> <ul style="list-style-type: none"> • Definition: A patent provides legal protection for new inventions, granting the inventor exclusive rights to make, use, or sell the invention for a specified period. • Purpose: It encourages innovation by ensuring inventors can profit from their inventions. 	W-24	6M

	<ul style="list-style-type: none"> • Duration: Generally 20 years from the filing date, depending on the type of patent and jurisdiction. • Example: A pharmaceutical company's formula for a new drug or a tech company's design for a new device. <p>(iii) Trademark</p> <ul style="list-style-type: none"> • Definition: A trademark is a symbol, logo, word, phrase, or design that identifies and distinguishes goods or services of one entity from others. • Purpose: It protects brand identity and prevents others from using similar identifiers that could confuse consumers. • Duration: Can last indefinitely as long as it is actively used and renewed. • Example: The Nike "swoosh" logo or the phrase "Just Do It." 		
19.	Describe cybercrime and cyber laws in details	W-24	4M
Answer:	<p>Cybercrime refers to criminal activities conducted using computers, networks, or other digital devices. It encompasses a broad range of illegal activities that exploit the vulnerabilities of technology to harm individuals, organizations, or even governments. Cybercrime is generally categorized into three main types:</p> <ol style="list-style-type: none"> 1. Crimes Against Individuals: These crimes target private individuals and can include: <ul style="list-style-type: none"> ○ Identity Theft: Unauthorized access to personal information to commit fraud. ○ Phishing: Fraudulent attempts to obtain sensitive data, such as login credentials and financial information. ○ Cyber stalking: Using online platforms to harass or intimidate individuals. ○ Distribution of Malicious Software: Installing viruses, spyware, or ransom are on personal devices. 2. Crimes Against Organizations: These crimes target businesses, institutions, or other entities and include: <ul style="list-style-type: none"> ○ Hacking: Unauthorized access to networks or systems to steal, alter, or destroy data. ○ Denial of Service (DoS) Attacks: Overloading a system to make it unavailable to legitimate users. 		

	<ul style="list-style-type: none"> ○ Corporate Espionage: Stealing trade secrets or proprietary data for competitive advantage. <p>3. Crimes Against Governments: Also known as cyber terrorism, these involve attacking government systems to disrupt operations, steal classified data, or spread political propaganda. Examples include:</p> <ul style="list-style-type: none"> ○ State-Sponsored Hacking: Attacks conducted by or on behalf of governments. ○ Election Interference: Hacking election systems to manipulate results or spread disinformation. <p>Examples of Cybercrime</p> <ul style="list-style-type: none"> • Online financial fraud and scams. • Data breaches exposing sensitive information. • Spread of child pornography. • Crypto jacking (unauthorized use of devices to mine crypto currency). <p>Cyber Laws refer to the legal frameworks designed to address and combat cybercrime, regulate online activities, and ensure the security and privacy of digital interactions. These laws vary by country but generally cover the following areas:</p> <p>1. Protection of Information</p> <ul style="list-style-type: none"> • Data Privacy Laws: Regulate the collection, storage, and use of personal data. Examples include the GDPR (General Data Protection Regulation) in the European Union. • Cyber security Laws: Mandate security measures for protecting digital systems and networks. <p>2. Prevention of Cybercrime</p> <ul style="list-style-type: none"> • Laws criminalizing hacking, identity theft, and distribution of malware. • Penalties for online fraud, cyber stalking, and harassment. • Measures to combat intellectual property theft, including software piracy and copyright infringement. 		
--	--	--	--

	<p>3. Regulation of E-Commerce</p> <ul style="list-style-type: none"> • Frameworks for secure online transactions. • Legal recognition of digital signatures and contracts. • Consumer protection laws for e-commerce fraud. <p>4. Intellectual Property Rights</p> <ul style="list-style-type: none"> • Laws protecting digital content, such as trademarks, patents, and copyrights. • Preventing unauthorized duplication or distribution of digital media. <p>5. Digital Evidence and Law Enforcement</p> <ul style="list-style-type: none"> • Guidelines for collecting, preserving, and presenting digital evidence in courts. • Jurisdictional laws for addressing cybercrime across international borders. 		
--	--	--	--



JSPM's
**JARSHI SHAHU COLLEGE OF ENGINEERING,
POLYTECHNIC**
Department of Computer Engineering
Academic Year: 2024-25



MSBTE QUESTION PAPER

22620

21222

3 Hours / 70 Marks

Seat No.

--	--	--	--	--	--	--	--

15 minutes extra for each hour

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Answer each next main Question on a new page.
 - (3) Illustrate your answers with neat sketches wherever necessary.
 - (4) Figures to the right indicate full marks.
 - (5) Assume suitable data, if necessary.
 - (6) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

Marks**1. Attempt any FIVE of the following :****10**

- (a) Define following terms :
 - (i) Confidentiality
 - (ii) Accountability
- (b) Explain the terms :
 - (i) Shoulder surfing
 - (ii) Piggybacking
- (c) Define term cryptography.
- (d) Classify following cyber crimes :
 - (i) Cyber stalking
 - (ii) Email harassment

- (e) Differentiate between viruses & worms (Any two).
- (f) Define firewall. Enlist types of firewalls.
- (g) Define AH & ESP with respect to IP security.

2. Attempt any THREE of the following :

12

- (a) Define following terms :
 - (i) Operating System Security
 - (ii) Hot fix
 - (iii) Patch
 - (iv) Service pack
- (b) Explain the mechanism of fingerprint & voice pattern in Biometrics.
- (c) Differentiate between symmetric & asymmetric key cryptography.
- (d) Write & explain DES algorithm.

3. Attempt any THREE of the following :

12

- (a) Describe the features of DAC access control policy.
- (b) Consider plain text “COMPUTER ENGINEERING” & convert given plain text into cipher text using ‘Caesar Cipher’ with shift of position three - write down steps in encryption.
- (c) Differentiate between host-based & network based IDS.
- (d) Define access control & explain authentication mechanism for access control.

- 4. Attempt any THREE of the following : 12**
- (a) Enlist substitution techniques & explain any one.
 - (b) Explain DMZ.
 - (c) Differentiate between firewall & IDS.
 - (d) Explain Email security in SMTP.
 - (e) Explain Digital Signature in Cryptography.
- 5. Attempt any TWO of the following : 12**
- (a) Define Information. Explain basic principle of information security.
 - (b) Define & explain :
 - (i) Circuit Gateway
 - (ii) Honey Pots
 - (iii) Application Gateway
 - (c) Explain the working of Kerberos.
- 6. Attempt any TWO of the following : 12**
- (a) Explain DOS with neat diagram.
 - (b) Explain Public Key Infrastructure with example.
 - (c) Explain Policies, configuration & limitations of Firewall.
-



22620

12223

3 Hours / 70 Marks

Seat No.

--	--	--	--	--	--	--	--

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Illustrate your answers with neat sketches wherever necessary.
 - (3) Figures to the right indicate full marks.

Marks**1. Attempt any FIVE of the following :****10**

- (a) Define computer security and state it's need.
- (b) Explain shoulder surfing attack.
- (c) Explain the term cryptography.
- (d) State the meaning of hacking.
- (e) Describe sniffing attack.
- (f) Explain need for firewall.
- (g) Explain use of PCI DSS.

2. Attempt any THREE of the following :**12**

- (a) Define Risk. Describe qualitative and quantitative risk analysis.
- (b) Explain working of biometric access control with any type of example.
- (c) Explain Ceaser's Cipher substitution technique with suitable example.
- (d) Describe DES algorithm with suitable example.



- 3. Attempt any THREE of the following : 12**
- (a) Explain the term Authorization and Authentication with respect to security.
 - (b) Write an algorithm for simple columnar transposition technique and explain with example.
 - (c) Describe DMZ with suitable example.
 - (d) Write short note on DAC & MAC.
- 4. Attempt any THREE of the following : 12**
- (a) Write a short note on steganography.
 - (b) Explain Honey pots.
 - (c) Explain Host based IDS.
 - (d) Describe working principle of SMTP.
 - (e) Explain creation and verification of digital signature.
- 5. Attempt any TWO of the following : 12**
- (a) Explain any three criteria for classification of information.
 - (b) List types of firewall and explain any one of them.
 - (c) Explain IP sec security with help of diagram.
- 6. Attempt any TWO of the following : 12**
- (a) Define virus and describe the phases of virus.
 - (b) Explain Kerberos with help of suitable diagram.
 - (c) Write a brief note on firewall configurations.
-



22620

22232

3 Hours / 70 Marks

Seat No.

--	--	--	--	--	--	--	--

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Illustrate your answers with neat sketches wherever necessary.
 - (3) Figures to the right indicate full marks.
 - (4) Assume suitable data, if necessary.

Marks**1. Attempt any FIVE of the following :****10**

- (a) Compare virus and logic bomb. (any two points).
- (b) Identify any four individual user responsibilities in computer security.
- (c) Define following terms :
 - (i) Cryptography
 - (ii) Cryptology
- (d) Construct digital signature using cryptool.
- (e) List any two types of active and passive attacks.
- (f) State any two policies of the firewall.
- (g) List any four types of cybercrimes.

2. Attempt any THREE of the following :**12**

- (a) Describe CIA model with suitable diagram.



- (b) Define following with suitable example :
 - (i) DAC
 - (ii) MAC
- (c) Differentiate between symmetric and asymmetric key cryptography. (any four points)
- (d) Explain steganography technique with suitable example.

3. Attempt any THREE of the following :

12

- (a) Describe piggy backing and shoulder surfing.
- (b) Convert plain text into cipher text by using Simple columnar technique of the following sentence :
“Maharashtra State Board of Technical Education”
- (c) State any four difference between Firewall and Intrusion Detection System.
- (d) Describe any four password selection criteria.

4. Attempt any THREE of the following :

12

- (a) Convert the given plain text, encrypt it with the help of Caesar's cipher technique.
“Network and Information Security”.
- (b) Demonstrate configuration of Firewall setting windows operating system.
- (c) Describe DMZ with suitable diagram.
- (d) Describe PGP with suitable diagram.
- (e) Find the output of the initial permutation box when the input is given in hexadecimal as

0 × 0003 0000 0000 0001

5. Attempt any TWO of the following : 12

- (a) Describe the following terms :
 - (i) Assels
 - (ii) Vulnerability
 - (iii) Risks
- (b) Describe network based IDS with suitable diagram.
- (c) Describe COBIT framework with neat diagram.

6. Attempt any TWO of the following : 12

- (a) Describe any three phases of virus with suitable example.
 - (b) Describe 'Kerberos' protocol with suitable diagram.
 - (c) Describe following terms :
 - (i) Packet filter Firewall
 - (ii) Application gateway
 - (iii) Circuit gateway
-

22620

23124

3 Hours / 70 Marks

Seat No.

--	--	--	--	--	--	--	--

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Answer each next main Question on a new page.
 - (3) Illustrate your answers with neat sketches wherever necessary.
 - (4) Figures to the right indicate full marks.
 - (5) Assume suitable data, if necessary.
 - (6) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

Marks**1. Attempt any FIVE of the following :****10**

- (a) List any four virus categories.
- (b) List any four biometric mechanisms.
- (c) Define the following terms :
 - (i) Cryptography
 - (ii) Cryptanalysis
- (d) Give examples of Active & Passive Attacks (two each).
- (e) State the two types of firewall with its use.
- (f) List two protocols in IP Sec. State its function.
- (g) Classify the following cyber crime :
 - (i) Cyber terrorism against a government organization
 - (ii) Cyber – Stalking
 - (iii) Copyright infringement
 - (iv) Email harassment



- 2. Attempt any THREE of the following : 12**
- (a) Explain basic principles of information security.
 - (b) Explain any two password attacks.
 - (c) Describe digital signature technique using message digest.
 - (d) Explain steganography technique with an example.
- 3. Attempt any THREE of the following : 12**
- (a) Describe :
 - (i) Piggybacking
 - (ii) Dumpster diving
 - (b) Consider plain text “CERTIFICATE” and convert it into cipher text using Caesar Cipher with a shift of position 4. Write steps for encryption.
 - (c) State the use of packet filters. Explain its operation.
 - (d) State the features of (i) DAC (ii) MAC.
- 4. Attempt any THREE of the following : 12**
- (a) Convert the given plain text into cipher text using simple columnar technique using the following data :
 - Plain text : NETWORK SECURITY
 - Number columns : 06
 - Encryption key : 632514
 - (b) State the working principle of application gateways. Describe circuit gateway operation.
 - (c) Describe DMZ with an example.
 - (d) State the use of Digital Certificates. Describe the steps for digital certificate creation.
 - (e) Considering DES, find the output of the initial permutation box when the input is given in hexadecimal as, 0×0000 0080 0000 0002

5. Attempt any TWO of the following : 12

- (a) State the criteria for information classification. Explain information classification.
- (b) State the features of the following IDS :
 - (i) Network based IDS
 - (ii) Host based IDS
 - (iii) Honey pots
- (c) Explain step-by-step procedure of Kerberos with diagrams.

6. Attempt any TWO of the following : 12

- (a) Explain the following attacks using an example :
 - (i) Sniffing (ii) Spoofing (iii) Phishing
 - (b) Describe ITIL framework with different stages of life cycle.
 - (c) State and explain 3 types of firewall configurations with a neat diagram.
-

S-24

Summer-2024

22620

23242

3 Hours / 70 Marks

Seat No.

		2	7	1	6	8	7
--	--	---	---	---	---	---	---

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Illustrate your answers with neat sketches wherever necessary.
 - (3) Figures to the right indicate full marks.
 - (4) Assume suitable data, if necessary.

1620

Marks**1. Attempt any FIVE of the following :****10**

- (a) Differentiate between viruses & worms.
- (b) State any four advantages of Biometrics.
- (c) Explain the term cryptanalysis.
- (d) Define term cyber crime.
- (e) Explain the term assets.
- (f) State any four limitations of firewall.
- (g) Explain working of Kerberos in short.

2. Attempt any THREE of the following :**12**

- (a) Enlist types of Biometrics & explain any one Biometrics type in detail.
- (b) Explain DOS with neat diagram.
- (c) Differentiate between symmetric and asymmetric cryptography.
- (d) Illustrate digital signature and explain it with neat diagram.



3. Attempt any THREE of the following :**12**

- (a) Define the following terms :
 - (i) Authentication
 - (ii) Authorization
- (b) Convert plain text into cipher text by using simple columnar technique of the following sentence :
ALL IS WELL FOR YOUR EXAM.
- (c) Describe packet filter router firewall with neat diagram.
- (d) Explain working of fingerprint mechanism and its limitations.

4. Attempt any THREE of the following :**12**

- (a) Explain Caesar's cipher substitution technique with example.
- (b) Describe host based IDS with its advantages and disadvantages.
- (c) Define Hacking. Explain different types of Hackers.
- (d) Explain the features of IDS technique.
- (e) Differentiate between substitution and transposition techniques ?

5. Attempt any TWO of the following :**12**

- (a) Explain active attack and passive attack with suitable example.
- (b) Describe the DMZ with suitable example.
- (c) Explain working principle of SMTP in detail.

6. Attempt any TWO of the following :**12**

- (a) Explain any three criteria for classification of information.
 - (b) Describe COBIT framework with neat sketch.
 - (c) Explain policies, configuration & limitations of firewall in detail.
-

12425

3 Hours / 70 Marks

Seat No.

2	6	8	0	+	1		
---	---	---	---	---	---	--	--

- Instructions :**
- (1) All Questions are *compulsory*.
 - (2) Answer each next main Question on a new page.
 - (3) Illustrate your answers with neat sketches wherever necessary.
 - (4) Figures to the right indicate full marks.
 - (5) Assume suitable data, if necessary.
 - (6) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

Marks

1. Attempt any **FIVE** of the following :

10

- ~~(a)~~ Define CIA model of Security Basic.
- ~~(b)~~ Enlist the types of Firewalls.
- ~~(c)~~ Differentiate between Virus & Worm (any two).
- ~~(d)~~ Explain the term Cryptography.
- (e) Define the term Honeypots.
- (f) Enlist two Intrusion Detection System.
- ~~(g)~~ Enlist two Active & Passive attack each.

2. Attempt any **THREE** of the following :

12

- ~~(a)~~ Explain criterias for information classification.
- ~~(b)~~ Describe the dumpster diving with its prevention mechanism.



22620

[2 of 4]

- (c) Draw and explain Host-Based intrusion detection system.
- (d) Explain Data Encryption Standard.

3. Attempt any THREE of the following :

12

- (a) Define following terms :
 - (i) Operating system security
 - (ii) Hot fix
 - (iii) Patch
 - (iv) Service Pack
- (b) Define password selection strategies.
- (c) Explain Caesar's Cipher substitute technique with suitable example.
- (d) Explain Email Security in SMTP.

4. Attempt any THREE of the following :

12

- (a) Differentiate between Symmetric and Asymmetric key cryptography.
- (b) Draw and explain DMZ.
- (c) Describe cyber crime and cyber laws in detail.
- (d) Write a brief note on Firewall configuration and state its limitations.
- (e) Draw and explain network-based intrusion detection system.

Attempt any TWO of the following :

12

- (a) Draw and explain DOS & DDOS attack in detail.
- (b) Write short note on :
 - (i) Digital signature
 - (ii) Steganography
- (c) Explain Kerberos with the help of suitable diagram.

22620

[3 of 4]

6. Attempt any TWO of the following :

- (a) Describe following terms w.r.t. biometric :
 - (i) Finger Print Analysis
 - (ii) Retina Scan
 - (iii) Keystroke
- (b) Draw and explain following terms :
 - (i) Packet Filter Firewall
 - (ii) Proxy Server
- (c) Explain following terms of intellectual property right :
 - (i) Copyright
 - (ii) Patent
 - (iii) Trademark



Jaywant Shikshan Prasarak Mandal's
RAJARSHI SHAHU COLLEGE OF ENGINEERING's
POLYTECHNIC



S.No.80, Pune-Mumbai Bypass Highway, Tathawade Campus, Pune.

Approved By AICTE & Govt. of Maharashtra, Affiliated to MSBTE

NBA ACCREDITED

ALL THE BEST

DEPARTMENT OF COMPUTER ENGINEERING