MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2013 Certified)

SUMMER – 19 EXAMINATION

Subject Name: Computer Security **Model Answer** **Subject Code: 17514**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills.
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

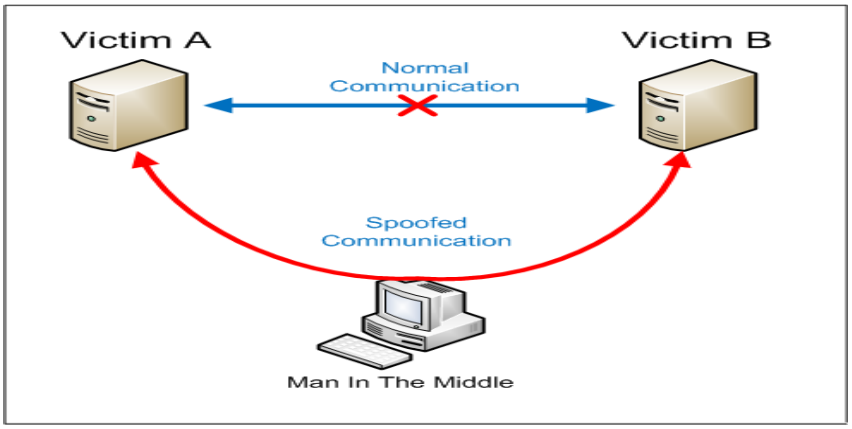
Q. No.	Sub Q. N.	Answer	Marking Scheme
1	A	**Attempt any THREE :**	**12 M**
	a	**Explain the term Intruders and Insiders.**	**4 M**
	Ans	**Intruders** • Keep trying attacks till success as they have the access and knowledge to cause immediate damage to organization. • Individual or a small group of attackers, they can be more in numbers. • Next level of this group is script writers, i.e. Elite hackers are of three types: Masquerader, Misfeasor, Clandestine user is misuse of access given by insiders directly or indirectly access the organization. • They may give remote access to the Organization Intruders are authorized or unauthorized users who are trying access the system or network. • They are hackers or crackers • Intruders are illegal users. • Less dangerous than insiders • They have to study or to gain knowledge about the security system • They do not have access to system.	Intruders: 2 M, Insiders: 2M **OR** Answer with Relevant Contents

		• Many security mechanisms are used to protect system from Intruders **Insiders** • More dangerous than outsiders As they have the access and knowledge to cause immediate damage to organization • They can be more in numbers who are directly or indirectly access the organization. • They may give remote access to the organization. • Insiders are authorized users who try to access system or network for which he is unauthorized. • Insiders are not hackers. • Insiders are legal users	
	b	**Explain piggybacking and Shoulder surfing**	**4 M**
	Ans	**Piggy backing:** •It is the simple process of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. •An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. i.e.: 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. •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. •It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others. The process of sending data along with the acknowledgment is called piggybacking. Piggybacking is distinct from war driving, which involves only the logging or mapping of the existence of access points. •It is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. •An attacker can thus gain access to the facility without having to	Piggybacking explanation: 2M, Shoulder surfing explanation: 2M **OR** Answer with Relevant Contents

		know the access code or having to acquire an access card. •Piggybacking, in a wireless communications context, is the unauthorized access of a wireless LAN. Piggybacking is sometimes referred to as "Wi-Fi squatting." •The usual purpose of piggybacking is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network. **Shoulder Surfing**: •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. •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. •To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand. •Both of these attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions. •Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information.	
	c	**Explain the terms:** **(i)Gryptography (ii) Gryptanalysis (iii) Gryptology (iv) Cipher text.**	**4 M**
	Ans	(i)**Cryptography**: Cryptography is art & science of achieving security by encoding messages to make them non-readable. (ii)**Cryptanalysis**: Cryptanalysis is the technique of decoding messages from a non-readable format without knowing how they were initially converted from readable format to non-readable format. (iii)**Cryptology**: It is the art and science of transforming the intelligent data into unintelligent data and unintelligent data back to intelligent data. Cryptology = Cryptography + Cryptanalysis (iv)**Cipher text**: It is an encrypted text. When plain text is converted using encryption, this encrypted text is called as cipher text.	each correct definition 1M **OR** Answer with Relevant Contents

	d	**Define virus and logic bomb**	**4 M**
	Ans	**Virus:** 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. Types of viruses: •Parasitic Viruses •Memory resident viruses •Non-resident viruses •Boot sector Viruses •Overwriting viruses •Stealth Virus •Macro Viruses **Logic bomb:** A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates.	Virus definition: 2M and Logic bomb definition: 2M **OR** Answer with Relevant Contents
	B	**Attempt any ONE :**	**6 M**
	a	**Explain the terms :(i) Assets (ii) Vulnerability (iii) Risks**	**6 M**
	Ans	**(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. **(ii)Vulnerability:** 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	Assets: 2M Vulnerability: 2M Risks: 2M **OR** Answer with Relevant Contents

		technology development, and as part of a technology selection process. **(iii)Risks:** 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; and 2.The likelihood of occurrence.	
	b	**Explain following terms of Intellectual property:** **(i)Copyright (ii) Patent (iii) Trademark.**	**6 M**
	Ans	**(i) Copyright:** Copyright is a form of IPR concerned with protecting works of human intellect. The domain of copyright is literary and artistic works, might that be writings, musicals and works of fine arts, such as paintings and sculptures, as well as technology-based works such as computer programs and electronic databases. **(ii)Patent:** Patent is an exclusive right granted by law to an inventor or assignee to prevent others from commercially benefiting from his/her patented invention without permission, for a limited period of time in exchange for detailed public disclosure of patented invention. **(iii) Trademark:** A trademark is a sign that individualizes the goods or services of a given enterprise and distinguishes them from those of competitors. To fall under law protection, a trademark must be distinctive, and not deceptive, illegal or immoral.	Copyright: 2 M, Patent: 2M, Trademark : 2 M **OR** Answer with Relevant Contents
2		**Attempt any TWO :**	**16 M**
	a	**Explain man-in-middle and TCP/IP Hacking attacks.**	**8 M**
	Ans	**Man-in-middle attack:** A man in the middle attack occurs when attackers are able to place themselves in the middle of two other hosts that are communicating in order to view or modify the traffic. This is done by making sure that all communication going to or from the target host is routed through the attacker‘s host. Then the attacker is able to observe all traffic before transmitting it and can actually modify or block traffic. To the target host, communication is occurring normally, since all expected replies are received.	Man-in-middle explanation: 2M diagram: 2M , TCP/IP Hacking attacks:



TCP/IP Hacking attacks:

- IP Address Spoofing

Source and destination address contained in the IP header are the only information needed for routing the packet. Anyone who has access to the IP layer can easily spoof the packet's IP source address and then masquerade it as from another host in the network. The IP address

spoofing is based upon maliciously creating TCP/IP packets using someone else's IP address as source address so as to either conceal own identity or impersonate the identity of the user of the spoofed IP address being used the packets are routed by the router to the destination.

Upon receipt the recipient uses the IP address of the source to reply to the packet. Since the source address is spoofed, the recipient will reply to the spoofed address and not to the original sender who had deliberately changed his IP address in the original packet. Since the address has been changed intentionally it will be difficult to trace back

to the attacker. Using this concept the following types of attacks are normally carried out.

- Denial of Services Attacks (DoS)

Using the above trick the attacker can send a large number of packets to the victim . As he will not receive any packet from the victim, all the replies will be directed towards the spoofed IP addresses and causes the victim to go out of services. Using DoS an attacker can disrupt the normal functioning of the network and carry out the following attacks:-

Storage Consumption Attacks – The attacker tries to consume all the available local storage space on the target machine to

4M
any 2
attacks
OR
Answer
with
Relevant
Contents

slowly bring it to a grinding halt. A simple trick of sending emails with very large attachments can be used for launching this type of DoS. Multiple large
DVD VOB files and uncompressed JPEG or BMP (bitmap) images of very high resolution are common file types used to accomplish such attacks.

Subnet Mask Corruption Attacks – The attacker may send a message which causes the target machine to reset its subnet mask and so disrupt the target's subnet routing.

Connection Resources Consumption Attacks
By sending very large numbers of erroneous requests for TCP session establishment an attacker can consume all of the target's available connection resources thereby resulting in the target being unable to service any new authentic connection requests.

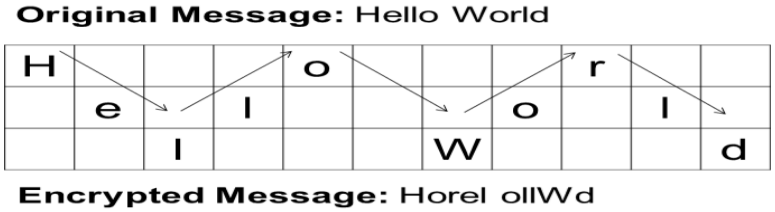
Buffer Overflow Attacks – A buffer overflow attack occurs when a process receives much more data than expected and if it has no programmed routine to deal with this excessive amount of data, it may act in unexpected ways that an attacker can exploit. There are numerous variations and forms of buffer overflow attack that have been formulated over the years, with the most common of all being the "Ping of Death".

Ping of Death Attacks - The Ping of Death attack is also referred to as the "Large Packet Ping Attack". The attacker initiates a "ping of death" attack by using network utility PING of Internet Control Message Protocol (ICMP) to "ping" the target with an illegally modified and very large IP datagram. This will result in overfilling of the target system's buffers causing the target to reboot or hang. PING can be configured to send the "illegal" IP datagram packets in bursts or as a continual stream. In the case of a continual stream the target will be immediately under attack once it reboots and will thus hang or reboot continually until something is done to stop it receiving the attacker's packets.

SYN Attacks - A SYN attack occurs when anattacker exploits the use of the buffer space during the Transmission Control Protocol (TCP) session initialization- three-way handshake. The receiving machine (usually a server) can maintain multiple concurrent conversations all established using the same small "in-process" buffer pool.

		Smurf Attacks – Here a combination of IP address Spoofing and ICMP flooding are used to saturate a target network with traffic so that the normal traffic is disrupted thereby causing a Denial of Service (DoS) attack. Smurf attacks consist of the source site, the bounce site and the target site. First the attacker selects a bounce site (usually a very large network). The attacker then modifies a PING packet so that it contains the address of the target site as the PING packet's source address.	
	b	**Explain access control policies.**	**8 M**
	Ans	**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. **Discretionary Access control (DAC):** Restricting access to objects based on the identity of subjects and or groups to which they belongs 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 **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. **Role Based Access Control (RBAC):** Each user can be assigned specific access permission for objects associated with computer or network. Set of roles Role in turn assigns access permissions which are necessary to perform role. Different User will be granted different permissions to do specific duties as per their classification.	Access control Definition: 2M, Each access control policy description: 2M **OR** Answer with Relevant Contents
	c	**Explain the rail fence techniques and simple columnar transposition technique. Solve the following example using rail fence technique. "COMPUTER SECURITY IS IMPORTANT"**	**8 M**
	Ans	**Rail Fence Technique**:	Explanatio

It is one of the easiest transposition techniques to create cipher text. When plain text message is codified using any suitable scheme, the resulting message is called Cipher text or Cipher.
Steps are: Plain text = Hello World
Assume No. of rows (rails)=3
Step 1:Write down Plain text as sequence of diagonal. Read Plain text written in



Original Message: Hello World

H				o				r		
	e		l				o		l	
		l				W				d

Encrypted Message: Horel ollWd

Step 1 as sequence of rows. As, Then concatenate these two sequences of text as one to create following

Cipher Text:
Horel ollWd

simple columnar transposition techniques:
The columnar transposition cipher is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher -text. It can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult
to break than either cipher on its own. The cipher uses a columnar transposition to greatly improve its security.
Algorithm:
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.
Example:
The key for the columnar transposition cipher is a keyword e.g. LEAVES. The row length that is used is the same as the length of the keyword. To encrypt a below plaintext COMPUTER PROGRAMMING

1	**2**	**3**	**4**	**5**
C	O	M	P	U
T	E	R	P	R
O	G	R	A	M
M	I	N	G	X

n of rail fence techniques :3M , Explanation of simple columnar transposition techniques :3M

Solving example using rail fence technique: 2M
OR
Answer with Relevant Contents

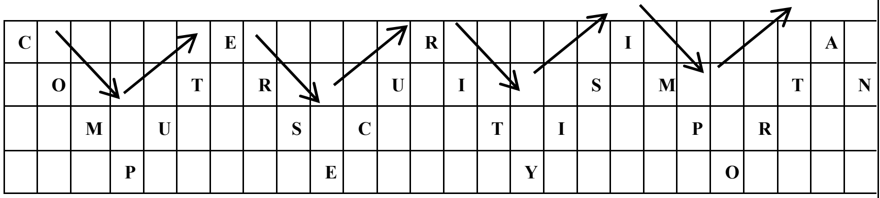
L(4)	E(2)	A(1)	V(5)	E(3)
P	O	C	U	M
P	E	T	R	R
A	G	O	M	R
G	I	M	X	N

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.

The Encrypted text or Cipher text is: PPAG OEGI CTOM URMX MRRN

Solve the following example using rail fence technique. "COMPUTER SECURITY IS IMPORTANT"

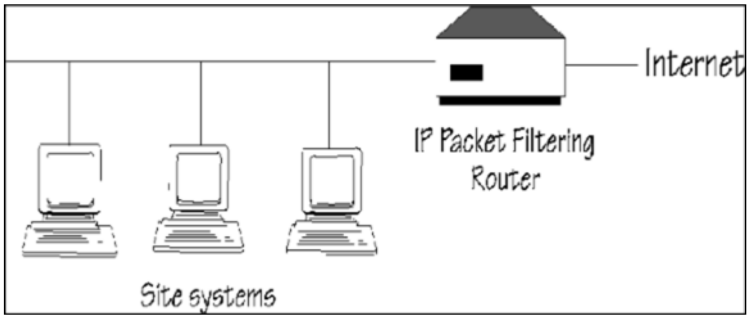
Assume no .of rows(rails):04



C						E						R						I						A	
	O				T		R				U		I				S		M				T		N
		M		U				S		C				T		I				P		R			
			P						E						Y						O				

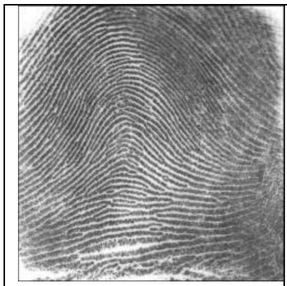
Cipher text: CERIA OTRUISMTN MUSCTIPRT PEYO

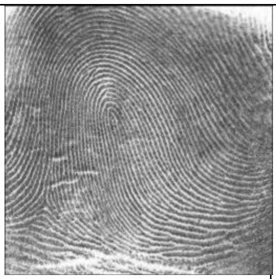
3		**Attempt any FOUR :**	**16 M**
	a	**List types of firewall. Explain packet filter with diagram.**	**4 M**
	Ans	Types of firewall • Packet filtering firewalls • Circuit level gateways • Application gateways • Stateful multilayer inspection firewall **Packet filtering firewall:**	List1M Explanation 2M Diagram1 M **OR**

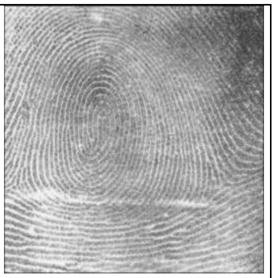
		- Packet filtering firewalls are functioning at the IP packet level. Packet filtering firewalls filters packets based on addresses and port number. - These firewalls work at the network layer of OSI model, or IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP addresses, source and destination port number and type of the protocol embedded in that packet. These firewalls often contain an ACL (Access Control List) to restrict who gains access to which computers and networks. 	Answer with Relevant Contents
	b	**Explain fingerprint and retina pattern in biometric.**	**4 M**
	Ans	**Fingerprint:** - The fingerprints of the user are matched with the database and matching is carried out using complex image processing algorithms. The user is authenticated, if match of satisfactory is level is obtained. - The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. **Fingerprint patterns:** - The three basic patterns of fingerprint ridges are the arch, loop, and whorl. - An arch is a pattern where the ridges enter from one side of	Explanation of fingerprint -2m Explanation of retina-2m **OR** Answer with Relevant Contents

the finger, rise in the center forming an arc, and then exit the other side of the finger.

- The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter.
- In the whorl pattern, ridges form circularly around a central point on the finger.
-


The Arch Pattern


The Loop Pattern


The Whorl Pattern

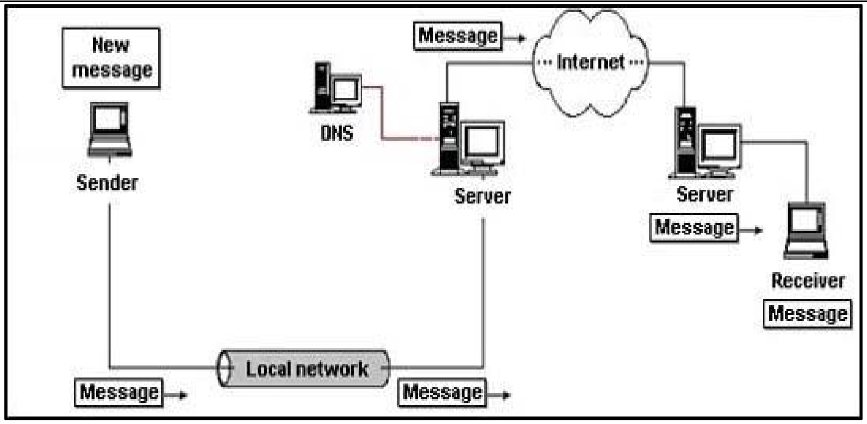
Retina pattern:

- A retinal scan is very difficult to fake because no technology exists that allows the forgery of a human retina, and the retina of a deceased person decays too fast to be used to fraudulently bypass a retinal scan.
- A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them. The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique.

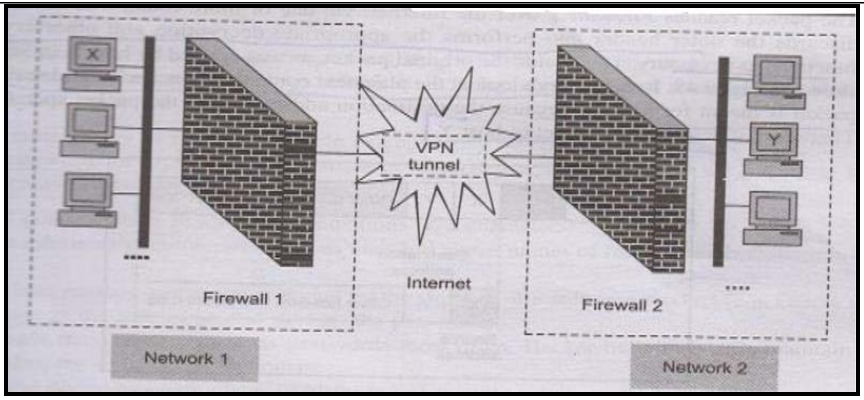
A biometric identifier known as a retinal scan is used to map the unique patterns of a person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person’s eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Because retinal blood vessels are more absorbent of this light than the rest of the eye, the amount of reflection varies during the scan. The pattern of variations is converted to computer code and stored in a database.

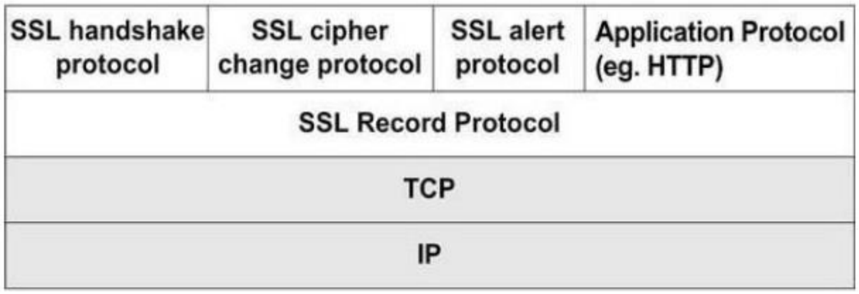
	c	**Explain steganography technique.**	**4 M**
	Ans	**Steganography:** • Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the	Term – 1M, Concept- 2M,

		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. **Steganography process:** **Cover-media + Hidden data + Stego-key = Stego-medium** 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. Stenography takes cryptography a step further by hiding an encrypted message so that no one suspects it exists. Ideally, anyone scanning your data will fail to know it contains encrypted data. Stenography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information. I.e. One can hide text, data, image, sound, and video, behind image.	Example 1M **OR** Answer with Relevant Contents
	d	**Explain working principle of SMTP.**	**4 M**
	Ans	• ***S**imple **M**ail **T**ransfer **P**rotocol,* a protocol for sending e-mail 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.	Explanation-2m Diagram-2m **OR** Answer with Relevant Contents

		 New message Sender DNS Message Internet Server Server Message Receiver Message Local network Message Message • A message (Notes or SMTP-based) is created on the client's local network. • The user sends the message via the Domino 6 server. • Lotus Domino executes a TCP/IP DNS (Domain Name System) resolution and finds the target server. The message is transferred to the target recipient's server, and then delivered to the recipient.	
	e	**Explain web security threats.**	**4 M**
	Ans	The main types of threats to web systems are listed below: ***Physical:*** Physical threats include loss or damage to equipment through fire, smoke, water & other fire suppressants, dust, theft and physical impact. Physical impact may be due to collision or the result of malicious or accidental damage by people. Power loss will affect the ability for servers and network equipment to operate depending upon the type of back-up power available and how robust it is. ***Malfunction:*** Both equipment and software malfunction threats can impact upon the operations of a website or web application. Malfunction of software is usually due to poor development practices where security has not been built into the software development life cycle. ***Malware:*** Malware, or malicious software, comes in many guises. Web servers are popular targets to aid distribution of such code and sites which have vulnerabilities that allow this are popular targets. ***Spoofing:*** Spoofing where a computer assumes the identity of another and masquerading where a user pretends to be another, usually with higher privileges, can be used to attack web systems to poison data deny service or damage systems. ***Scanning:*** Scanning of web systems are usually part of network or application fingerprinting prior to an attack, but also include brute force and dictionary attacks on username, passwords and	Explanation-4m **OR** Answer with Relevant Contents

		encryption keys. ***Eavesdropping:*** Monitoring of data (on the network, or on user's screens) may be used to uncover passwords or other sensitive data.	
4	A	**Attempt any THREE :**	**12 M**
	a	**Explain the concept of hacking.**	**4 M**
	Ans	- Hacking is one of the most well-known types of computer crime. - A hacker is someone who find out and exploits the weaknesses of computer systems or networks. - Hacking refers to unauthorized access of another's computer systems. - These intrusions are often conducted in order to launch malicious programs known as viruses, worms, and Trojan horses that can shut down hacking an entire computer network. - Hacking is also carried out as a way to talk credit card numbers, intent passwords, and other personal information. - By accessing commercial database, hackers are able to steal these types of items from millions of internet users all at once. There are different types of hackers: 1. White hat 2. Black hat 3. Grey hat 4. Elite hacker 5. Script hacker	Explnation -4m **OR** Answer with Relevant Contents
	b	**Explain the working of VPN.**	**4 M**
	Ans	A Virtual Private Network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider's servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and certified connections to provide you with a secure connection to private networks and to protect your identity. VPN connections technically give you all the benefits of a Local Area Network (LAN), which is similar to that found in many offices but without requiring a hard-wired connection. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.	Explanation-2m Diagram-2m **OR** Answer with Relevant Contents

		 X Y VPN tunnel Internet Firewall 1 Firewall 2 Network 1 Network 2	
	c	**Explain data recovery procedure.**	**4 M**
	Ans	**Data recovery:** All computer users need to be aware of backup and recovery procedures to protect their data. Data Protection can be taken seriously as its important for financial, legal or personal reasons. These are various formatted partition recovery tool available. Although every tool will have different GUI & method of recovery. **Steps of data recovery:** • Step1: If you cannot boot the computer, please use data recovery bootable disk. • Step 2: Select the file types you want to recover & volume where the formatted hard drive is. The tool will automatically scan the selected volume. • Step 3: Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive. **Data recovery procedures:** A computer data recovery procedure is an important part for any computer literate personality that cannot be neglected. Computer professional or computer forensic expert who uses data recovery should maintain the secrecy and privacy of the client. Any action or activity that leads to disclosure of privacy of the client should be avoided. The values such as integrity, accuracy & authenticity should be exercised in an ethical environment. The evidence that is produced before the court should be fairly examined & analyzed. There should not be any carelessness and ignorance regarding the handling of evidence. The case evidence should be examined in detail based upon validated principles.	Explnation -2m Procedure- 2m **OR** Answer with Relevant Contents
	d	**Explain secure socket layer.**	**4 M**
	Ans	• SSL is a commonly used internet protocol for managing the security of a message transmission between web	Explnation -2m

		browser and web server. • SSL is succeeded by transport layer security (TLS) and it is based on SSL. • SSL uses a program layer which is located between internet 's hypertext transfer protocol (http) and transport control protocol (TCP) layers. • SSL is included as part of both the Microsoft and Netscape browsers and most web server products. • SSL provides two levels of security services, authentication and confidentiality. • SSL is logically a pipe between web browser and web server.  SSL handshake protocol | SSL cipher change protocol | SSL alert protocol | Application Protocol (eg. HTTP) SSL Record Protocol TCP IP	Diagram-2m **OR** Answer with Relevant Contents
	B	**Attempt any ONE :**	**6 M**
	a	**Explain CIA model for security.**	**6 M**
	Ans	Confidentiality, Integrity and Authentication i.e. these three concepts are considered as backbone of security. These concepts represent the fundamental principles of security. **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. • Example of compromising the Confidentiality of a message is shown in fig • Here, the user of a computer A send a message to user of computer B. another user C gets access to this message, which is not desired and therefore, defeats the purpose of confidentiality. • This type of attack is also called as **Interception.**	2M for each concept of C,I and A **OR** Answer with Relevant Contents

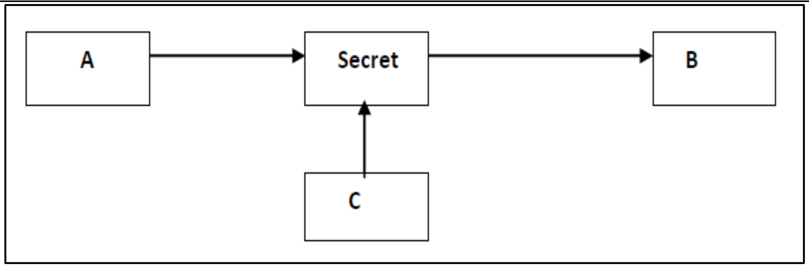


Fig. Loss of confidentiality

Authentication:

- Authentication helps to establish proof of identities.
- The Authentication process ensures that the origin of a message is correctly 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.

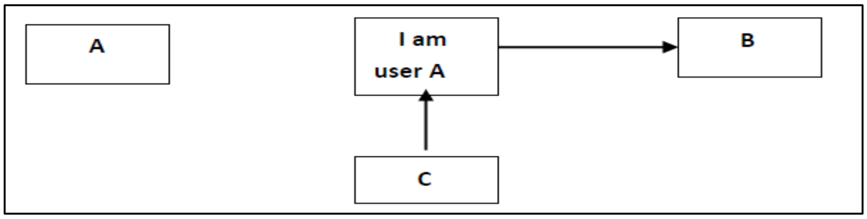
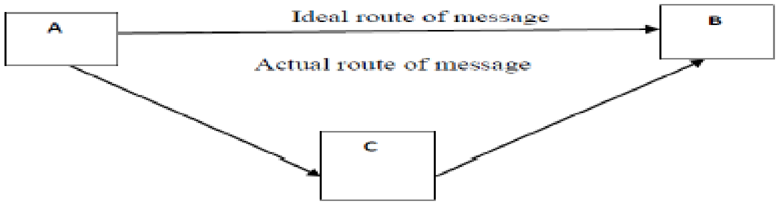


Fig. Absence of Authetication

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.
- For example, here user C tampers with a message originally sent by user A, which is actually destined for user B. user C somehow manages to access it, change its contents and send the changed message to user B. user B has no way of knowing that the contents of the message were changed after user A had sent it. User A also does not know about this change.
- This type of attack is called as **Modification**

		 A Ideal route of message B Actual route of message C **Fig. Loss of Integrity**	
	b	**Explain sniffing and spoofing attacks.**	**6 M**
	Ans	**Sniffing:** 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. **Spoofing:** Spoofing is nothing more than making data look like it has come from a different source. This is possible in TCP/ IP because of the friendly assumption behind the protocol. When the protocols were developed, it was assumed that individuals who had access to the network layer would be privileged users who could be trusted. When a packet is sent from one system to another, it includes not only the destination IP address ant port but the source IP address as well which is one of the forms of Spoofing. **Example of spoofing:** • e-mail spoofing • URL spoofing • IP address spoofing.	Sniffing-3M Spoofing-3M **OR** Answer with Relevant Contents
5		**Attempt any TWO :**	**16 M**
	a	**Explain role of people in security.**	**8 M**
	Ans	**Role of People in Security:** • Lock the door to your office or workspace. • Do not leave sensitive information inside your car unprotected. • Secure storage media containing sensitive information in a secure storage device. • Shred paper containing organizational information before	8 Points Each 1 M **OR** Answer with Relevant Contents

		discarding it. • Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it. • Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse about other employees or problems that are occurring at work.) • Protect laptops that contain sensitive or important organization information wherever the laptop may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop so that, should the equipment be lost or stolen, the information remains safe.) • Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information? • Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials. • Be aware of the correct procedures to report suspected or actual violations of security policies. Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defense.	
	b	**Explain proxy server and application level gateway.**	**8 M**
	Ans	Proxy server is an intermediary server between client and the internet. Proxy servers offers the following basic functionalities: • Firewall and network data filtering. • Network connection sharing • Data caching Purpose of Proxy Servers Following are the reasons to use proxy servers. • Monitoring and Filtering • Improving performance • Translation • Accessing services anonymously • Security **1. Monitoring and Filtering**	4 M for each explanation **OR** Answer with Relevant Contents

- Proxy servers allow us to do several kind of filtering such as:

- Content Filtering

2. Filtering encrypted data

- Bypass filters

- Logging and eavesdropping

- Improving performance

- It fastens the service by process of retrieving content from the cache which was saved when previous request was made by the client.

3. Translation

- It helps to customize the source site for local users by excluding source content or substituting

- Source content with original local content. In this the traffic from the global users is routed to the Source website through Translation proxy.

4. Accessing services anonymously

- In this the destination server receives the request from the anonymizing proxy server and thus does not receive information about the end user

5. Security

- Since the proxy server hides the identity of the user hence it protects from spam and the hacker attacks.

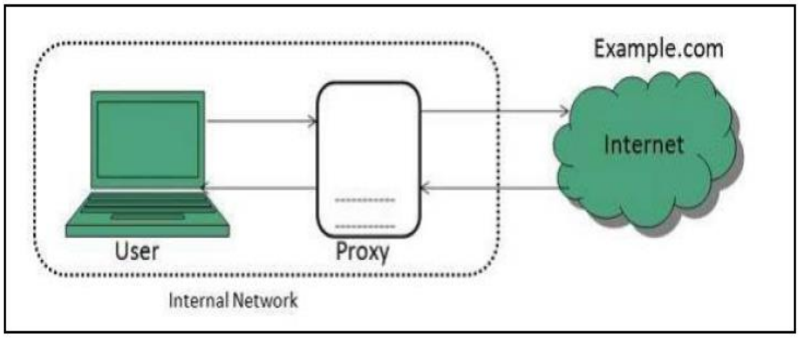


Fig. Proxy Server

Application level Gateway

A firewall that filters information at the application level blocks all IP traffic between the private network and the Internet. No IP packets from the clients or servers of the private network are allowed to enter or leave the Internet.

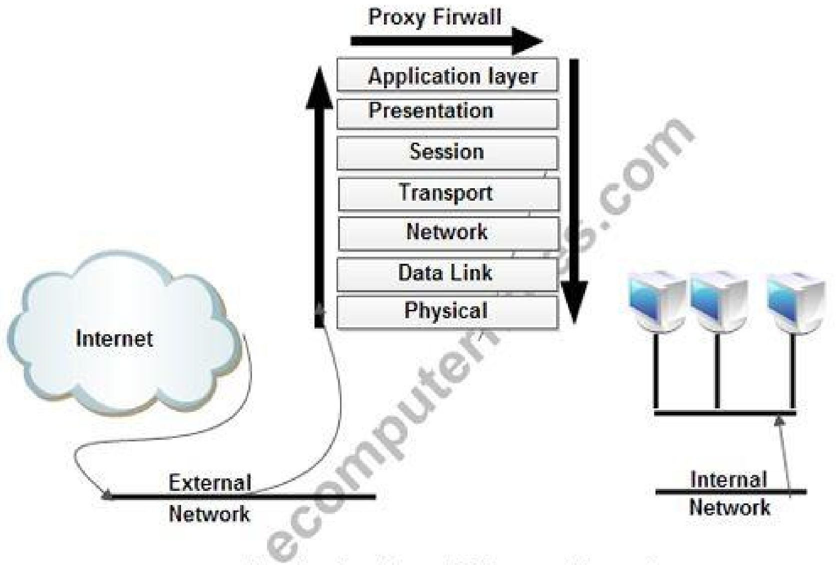
Instead, this type of firewall operates according to what is referred to as the proxy principle. This means that internal clients set up connections to the firewall and communicate with a proxy server. If the firewall decides that the internal client should be allowed to communicate, it sets up a connection with the external server and performs the operation on behalf of the client. This method solves many of the security problems associated with IP.

Each proxy server uses a particular application protocol, such as http-proxy or ftp-proxy. The proxy firewall uses a combination of different proxy servers which allows many different applications to be handled.

In addition to providing the best security, the proxy firewall can be used to fetch and store information from the Internet in a cache memory. The proxy firewall can achieve short response and download times because it "understands" the application programs and can see which URLs are most in demand.

Like a circuit level gateway, an application level gateway intercepts incoming and outgoing packets, acts as a proxy for applications, providing information exchange across the gateway. It also functions as a proxy server, preventing any direct connection between a trusted server or client and an untrusted host. The proxies that an application level gateway runs often differ in two important ways from the circuit level gateway:

The proxies are application specific
The proxies examine the entire packet and can filter packets at the application layer of the OSI model.



Application Level Gateway Firewall

Unlike the circuit gateway, the application level gateway accepts only packets generated by services. They are designed to copy, forward and filter. For example, only an HTTP proxy can copy, forward and filter HTTP traffic. If a network relies only on an application level gateway, incoming and outgoing packets cannot access services for which there is no proxy. For example, if an application level gateway ran ITP and HTTP proxies, only packets generated by these services could pass through the firewall. All other services would be blocked.

The application level gateway runs proxies that examine and filter individual packets, rather than simply copying them and recklessly forwarding them across the gateway. Application specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer (layer 7) of the OSI model. These proxies can filter on particular information or specific individual commands in the application protocols the proxies are designed to copy, forward and

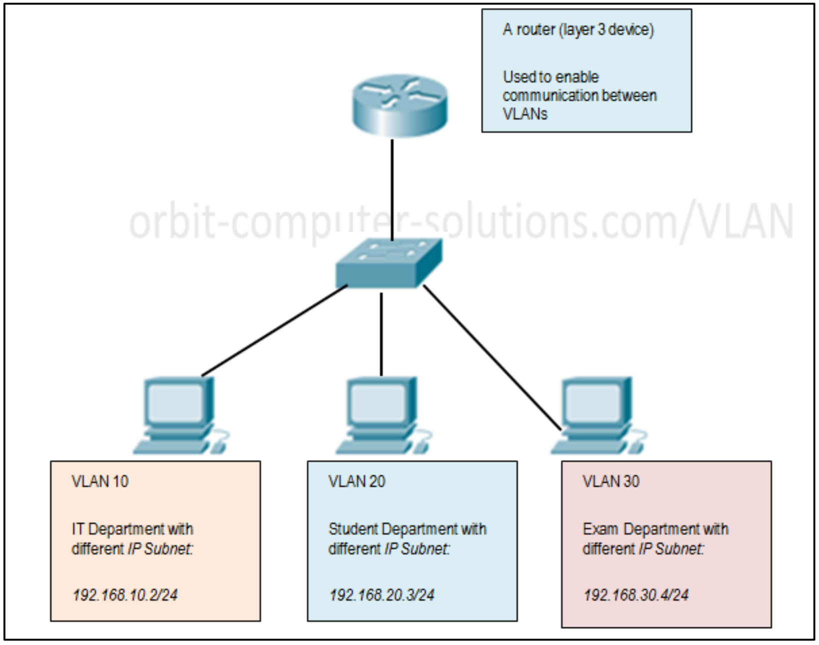
As an example, an application level proxy is able to block FTP put commands while permitting FTP get commands.

Current technology application level gateways are often referred to as strong application proxies. A strong application proxy extends the level of security afforded by the application level gateway. Instead of copying the entire datagram on behalf of the user, a strong application proxy actually creates a brand /I new empty datagram inside the firewall. Only those commands and data found acceptable to the strong application proxy are copied from the

		original datagram outside the firewall to the new datagram inside the firewall. Then, and only then, is this new datagram forwarded to the protected server behind the firewall. By employing this methodology the strong application proxy can mitigate the risk of an entire class of covert channel attacks. An application level gateway fitters information at a higher OSI layer than the common static or dynamic packet filter, and most automatically create any necessary packet filtering rules, usually making them easier to configure then traditional packet filters. **Benefits** Better logging handling of traffic (because all data between the client and the server is routed through the application proxy it is able to both control the session and provide detailed logging; This ability to log and control all incoming and outgoing traffic is one of the main advantages of application level gateway State aware of services (FTP, XII, etc.) Packet air gap like architecture, i.e. breaks direct connection to server behind firewall eliminating the risk of an entire class of covert channel attacks Strong application proxy that inspects protocol header lengths can eliminate an entire class of buffer overrun attacks Highest level of security. **Weaknesses** A poor implementation that relies on the underlying as Inetd daemon will suffer from a severe limitation to the number of allowed connections in today's demanding high simultaneous session environment. Complex setup of application firewall needs more and detailed attentions to the applications that use the gateway.	
	c	**Explain VLAN in detail.**	**8 M**
	Ans	A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to changes in network requirements and relocation of workstations and server nodes. Higher-end switches allow the functionality and implementation of	4 marks for explanation 4 marks for advantages and disadvantages **OR**

		VLANs. The purpose of implementing a VLAN is to improve the performance of a network or apply appropriate security features. VLAN (Virtual Local Network) is a logically separate IP subnet work_which allows multiple IP networks and subnets to exist on the same-switched network. VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a modern way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. By using VLAN, a network administrator will be able to group together stations by logical function, or by applications, without regard to physical location of the users. Each VLAN functions as a separate LAN and spans one or more switches. This allows host devices to behave as if they were on the same network segment. For traffic to move between VLANs, a layer 3 device (router) is required. VLAN has three major functions: **i.** Limits the size of broadcast domains **ii**.Improves network performance **ii.** Provides a level of security **How VLAN works.** Let's use this real-world scenario; Think about a small organization with different offices or departments, all in one building. Some years later, the organization expands and now spans across three buildings. The original network is still the same, but offices and departments computers are spread out across three buildings. The HR offices remain on the same floor and other departments' are on the other floors and buildings. However, the network administrator wants to ensure that all the office computers share the same security features and bandwidth controls. Creating a large LAN and wiring each department together will constitute a huge task and definitely won't be easy when it comes to managing the network. This where VLAN switching comes in, it will be easier to group offices and departments with the resources they use regardless of their location, and certainly easier to manage their specific security and bandwidth needs. Opting for a switched VLAN allows the network administrator to create groups of logically networked devices that act as if they are	Answer with Relevant Contents

on their own independent network (VLAN), even if they share a common infrastructure with other VLANs.
When you configure a VLAN, you can name it to describe the primary role of the users for that VLAN.


A router (layer 3 device)
Used to enable communication between VLANs
orbit-computer-solutions.com/VLAN
VLAN 10
IT Department with different IP Subnet:
192.168.10.2/24
VLAN 20
Student Department with different IP Subnet:
192.168.20.3/24
VLAN 30
Exam Department with different IP Subnet:
192.168.30.4/24

The key benefits of implementing VLANs include:

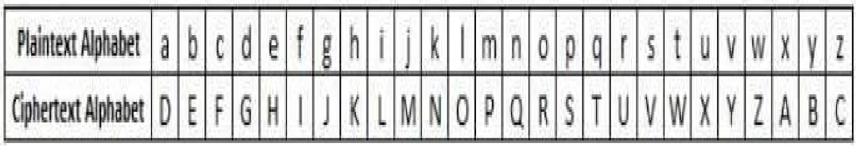
- Allowing network administrators to apply additional security to network communication
- Making expansion and relocation of a network or a network device easier
- Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations
- Decreasing the latency and traffic load on the network and the network devices, offering increased performance

VLANs also have some disadvantages and limitations as listed below:

- High risk of virus issues because one infected system may spread a virus through the whole logical network
- Equipment limitations in very large networks because additional routers might be needed to control the workload
- More effective at controlling latency than a WAN, but less efficient than a LAN.

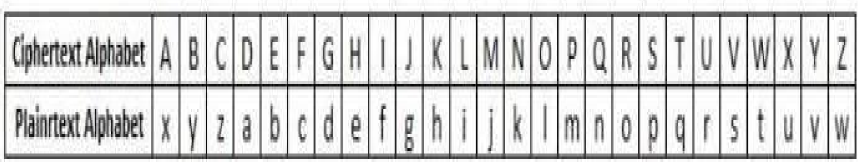
6		**Attempt any FOUR :**	**16 M**
	a	**Describe different Password selection criteria.**	**4 M**
	Ans	**Password selection criteria:** 1. **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords. This user education strategy is unlikely to succeed at most installations, particularly where there is a large user population or a lot of turn over. Many users will simply ignore the guidelines. Others may not be good judges of what is a strong password. For example, many users believe that reversing a word or capitalizing the last letter makes a password un-guessable. 2. **Computer-generated passwords**: Passwords are quite random in nature. Computer generated passwords also have problems. If the passwords are quite random in nature, users will not be able to remember them. Even if the password is pronounceable, the user may have difficulty remembering it and so be tempted to write it down. In general, computer-generated password schemes have a history of poor acceptance by users. FIPS PUB 181 defines one of the best-designed automated password generators. The standard includes not only a description of the approach but also a complete listing of the C source code of the algorithm. The algorithm generates words by forming pronounceable syllables and concatenating them to form a word. A random number generator produces a random stream of characters used to construct the syllables and words. 3. **Reactive password checking:** A reactive password checking strategy is one in which the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user. This tactic has a number of drawbacks. First it is resource intensive, if the job is done right. Because a determined opponent who is able to steal a password file can devote full CPU time to the task for hours or even days an effective reactive password checker is at a distinct disadvantage. Furthermore, any existing passwords remain vulnerable until the reactive password checker finds them. 4. **Proactive password checking:** The most promising approach to improved password security is a proactive	Marks each for any 4 points **OR** Answer with Relevant Contents

		password checker. In this scheme, a user is allowed to select his or her password. However, at the time of selection, the system checks to see if the password is allowable and if not, rejects it. Such checkers are based on the philosophy that with sufficient guidance from the system, users can select memorable passwords from a fairly large password space that are not likely to be guessed in a dictionary attack. The trick with a proactive password checker is to strike a balance between user acceptability and strength. If the system rejects too many passwords, users will complain that it is too hard to select a password. If the system uses some simple algorithm to define what is acceptable, this provides guidance to password crackers to refine their guessing technique. In the remainder of this subsection, we look at possible approaches to proactive password checking.	
	b	**Explain Caesar's cipher substitution technique with example.**	**4 M**
	Ans	Caesar Cipher It is a mono-alphabetic cipher wherein each letter of the plaintext is substituted by another letter to form the cipher text. It is a simplest form of substitution cipher scheme. This cryptosystem is generally referred to as the **Shift Cipher**. The concept is to replace each alphabet by another alphabet which is 'shifted' by some fixed number between 0 and 25. For this type of scheme, both sender and receiver agree on a 'secret shift number' for shifting the alphabet. This number which is between 0 and 25 becomes the key of encryption. The name 'Caesar Cipher' is occasionally used to describe the Shift Cipher when the 'shift of three' is used. **Process of Shift Cipher** • In order to encrypt a plaintext letter, the sender positions the sliding ruler underneath the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift. • The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath. The result of this process is depicted in the following illustration for an agreed shift of three positions. In this case, the plaintext 'tutorial' is encrypted to the ciphertext 'WXWRULDO'. Here is the ciphertext alphabet for a Shift of 3 −	Explanation : 2 M, Example: 2 M **OR** Answer with Relevant Contents



Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- On receiving the cipher text, the receiver who also knows the secret shift, positions his sliding ruler underneath the cipher text alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
- He then replaces the cipher text letter by the plaintext letter on the sliding ruler underneath. Hence the cipher text 'WXWRULDO' is decrypted to 'tutorial'. To decrypt a message encoded with a Shift of 3, generate the plaintext alphabet using a shift of '-3' as shown below −



Ciphertext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Plainrtext Alphabet	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Security Value

Caesar Cipher is **not a secure** cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

For example, here's the Caesar Cipher encryption of a full message, using a left shift of 3.

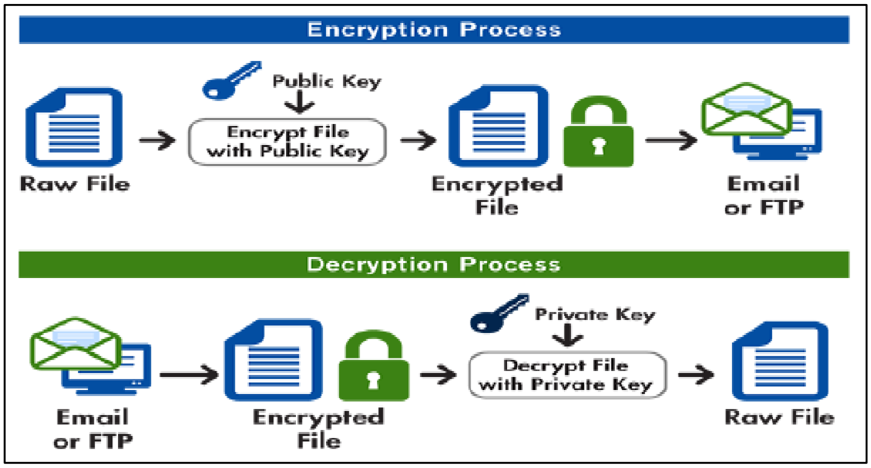
Plaintext:

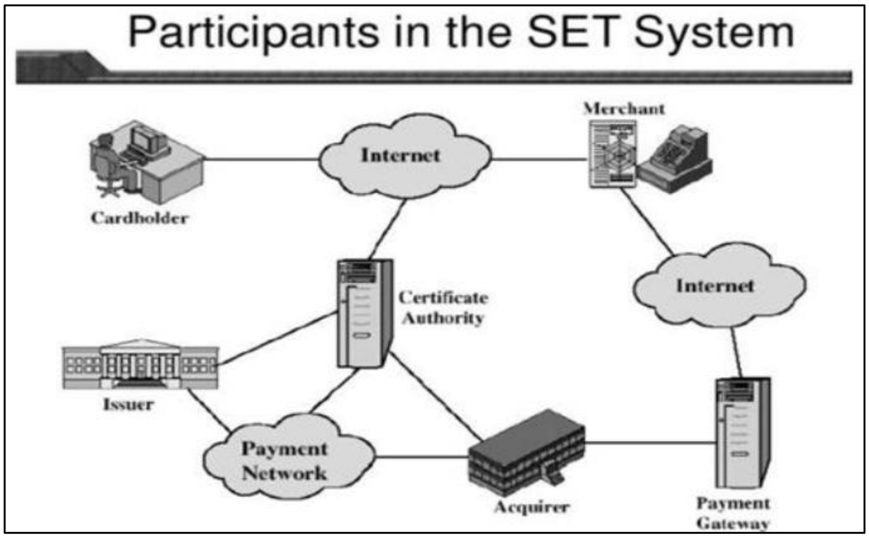
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Cipher text:

QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

	c	**Explain working principle of PGP.**	**4 M**
	Ans	**PGP is Pretty Good Privacy.** It is a popular program used to encrypt and decrypt email over the internet. It becomes a standard for email security. It is used to send encrypted code (digital signature) that lets the receiver verify the sender's identity and takes care that the route of message should not change. PGP can	PGP Definition: 2M, Steps in PGP: 2M

		be used to encrypt files being stored so that they are in unreadable form and not readable by users or intruders It is available in Low cost and Freeware version. It is most widely used privacy ensuring program used by individuals as well as many corporations.  Encryption Process Public Key Encrypt File with Public Key Raw File Encrypted File Email or FTP Decryption Process Private Key Decrypt File with Private Key Email or FTP Encrypted File Raw File **There are five steps as shown below:** **1. Digital signature:** it consists of the creation a message digest of the email message using SHA-1 algorithm. The resulting MD is then 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 are compressed together to reduce the size of final message that will be transmitted. For this the Lempel -Ziv algorithm is used. **3. Encryption:** The compressed output of step 2 (i.e. the compressed form of the original email and the digital signature together) are encrypted with a symmetric key. **4. Digital enveloping:** the symmetric key used for encryption in step 3 is now 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 input into printable character output. The binary input is processed in blocks of 3 octets (24-bits).these 24 bits are considered to be made up of 4 sets, each of 6 bits. Each such set of 6 bits is mapped into an 8-bit output character in this process.	**OR** Answer with Relevant Contents
	d	**Explain formatted partition recovery.**	**4 M**
	Ans	**Formatted partition recovery:** • Formatting refers to dividing the disk in accordance with	Explanation : 2

		certain principles, allowing computer to store and search files. • Formatting disk is to eliminate all files on disk. • There are various formatted partition recovery tool available. • Although every tool will have different GUI & method of recovery. • These tools usually operate as per following process steps: **Step1:** If you cannot boot the computer, please use data recovery bootable disk. **Step 2:** Select the file types you want to recover & volume where the formatted hard drive is. The tool will automatically scan the selected volume. **Step 3:** Then the founded data will be displayed on the screen & you can get a preview of it. Then select the file or directory that you want to recover & save them to a healthy drive.	marks, Steps: 4 marks **OR** Answer with Relevant Contents
	e	**Explain Secure Electronic Transaction**.	**4 M**
	Ans	**Secure Electronic Transaction** is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. It is a set of security protocols and formats that enable the users to employ the existing credit card payment infrastructure on the internet in a secure manner.  Participants in the SET System Merchant Internet Cardholder Certificate Authority Internet Issuer Payment Network Acquirer Payment Gateway **Components of SET:** 1) Cardholder 2) Merchant 3) Issuer	1 Mark- What is SET; 1Mark Enlisting any 4 components; 2 Marks- Explanation of any four components **OR** Answer with Relevant Contents

		4) Acquirer 5) Payment gateway 6) Certification Authority(CA) **1) Cardholder:** A cardholder is an authorized holder of a payment card such as MasterCard or Visa that has been issued by an Issuer. **2) Merchant:** Merchant is a person or an organization that wants to sell goods or services to cardholders. **3) Issuer:** The issuer is a financial institution that provides a payment card to a cardholder. **4) Acquirer:** This is a financial institution that has a relationship with merchants for processing payment card authorizations and payments. Also provides an assurance that a particular cardholder account is active and that the purchase amount does not exceed the credit limits. It provides electronic fund transfer to the merchant account. **5) Payment Gateway:** It processes the payment messages on behalf of the merchant. It connects to the acquirer's system using a dedicated network line. **6) Certification Authority (CA):** This is an authority that is trusted to provide public key certificates to cardholders, merchant, and Payment Gateway.	