UNIT 3

Cryptographic Systems

Q. 1. Describe the model of Cryptographic systems.

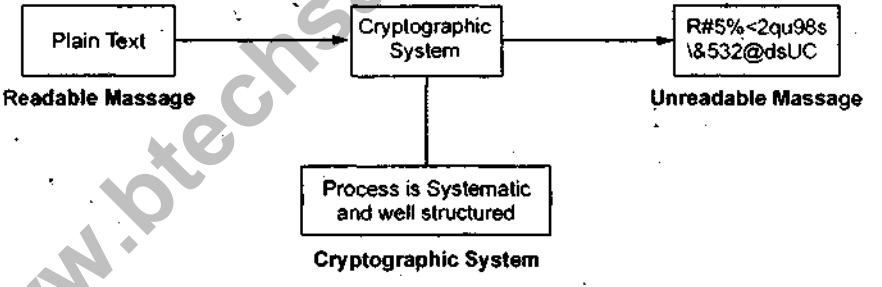
or

What is cryptography? Explain.

Ans. Cryptography is the art and science of secret communications. Cryptography is a technique used to achieve security by encoding messages to make them non-readable.

As the name cryptography suggests, the original purpose of cryptography was to hide something that had been written. Thus, cryptography is used to hide the meaning of information in any form. Such as data stored on a disc or a message in transit through a communication network. Cryptography can be applied to anything that can be digitally coded such as:

- Softwares
- Graphics
- Images
- Voice etc.

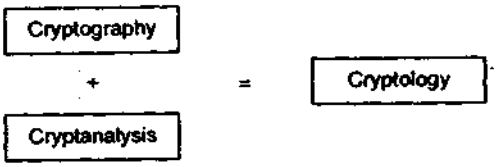


Q. 2. Discuss the following terms in short:

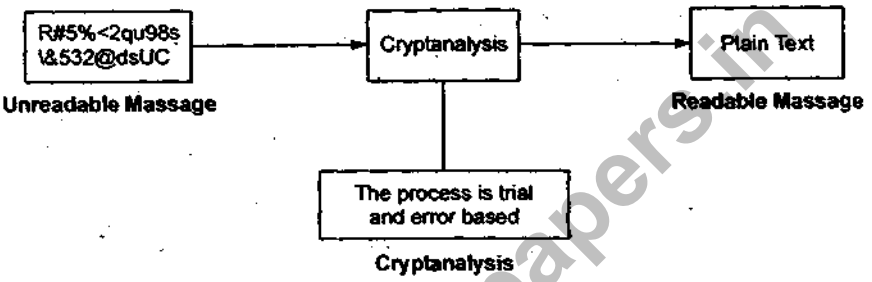
1. **Cryptology**
2. **Cryptanalysis**
3. **Cipher text**

Ans. 1. Cryptology: Cryptology is the science and art of secret communication. It is the combination of cryptography and cryptanalysis.

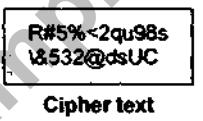
2. Cryptanalysis: Cryptanalysis is a set of methods used to break a cipher system, and/or forge coded signals so that they will be accepted as authentic. It is the technique of decoding messages from a non readable format back to readable format without knowing how they were initially converted from readable format to non readable format.



- Thus, it is a technique used to forge coded signals so that they can be accepted as authentic.



3. Cipher text: It is the result of the application of the cipher to the plain text. That is, it is the encoded text after application of cryptography to the plain text.



Q. 3. What are objective, requirement and threats in a cryptographic system? What do you mean by Non-repudiation in such systems? Discuss the issue of integrity and authentication of the documents.

Ans. Objective: the original purpose of cryptography was to hide something that had been written. Thus, cryptography is used to hide the meaning of information in any form. Such as data stored on a disc or a message in transit through a communication network. Cryptography can be applied to anything that can be digitally coded such as: Software, graphics or voice.

Requirement: From e-mail to cellular communication from secure web access to digital cash, cryptography is an essential part of information system. It helps provide accountability, fairness, accuracy and confidentiality. It can prevent fraud in e-commerce and assure the validity of financial transactions. It can be used to protect one's anonymity.

Threats: The threats to a cryptographic system are as follows:

1. Brute force attack (breaking the key)
2. Password hacking
3. Packet sniffing
4. Modification of the original document.

Non Repudiation: It is the method by which the sender of the message/ data is provided with a proof of the delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

Integrity: The concept of integrity ensures that:

1. Modifications are not made to data by unauthorized personnel or processes.

2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data are internally and externally consistent.

Authentication of Documents: This is the testing or reconciliation of evidence of document's ID. It establishes a document id and ensures that documents/ programs are those they say they are. It is a security measure designed to establish the validity of the transmission, message or originator or a means of verifying a document/ program's eligibility to do specific tasks.

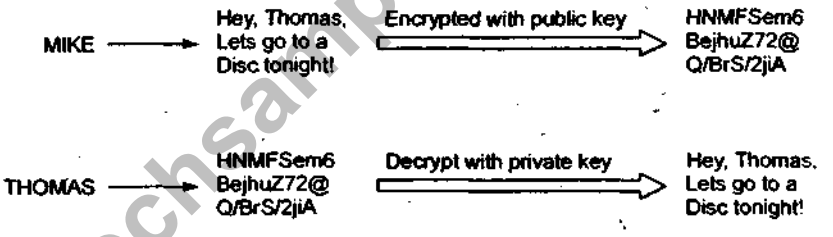
Q. 4. Why we use keys in cryptography? And explain the concept of public and private key.

Ans. Keys are used in cryptography to encrypt the information. Only a person with the appropriate key can make it readable again. Thus, it means that without an appropriate key, one cannot access the message or decode it to a readable form. Key plays an important role in cryptography, the presence of key thus, is used for locking of the encrypted message which can only be unlocked/decrypted using the correct combination of the key (Private Key) or the same key which was used for locking/ encrypting (Public key).

Public key: Public key are those keys which are made available to anyone who needs it and is used to encrypt the data.

Private key: Private Key is safe and is not available to anyone except the creator and is used to decrypt the data encrypted by public key.

Example: Mike sends a message to Thomas and encrypts it with Thomas's public key.



Advantages of public key cryptography:

1. Each user has a pair of key- a public key and a private key. The private key is kept a secret, while the public key may be distributed.
2. Messages are encrypted with recipient's public key and can only be decrypted with corresponding private key.
3. No need to exchange the keys among the users.
4. Public key cryptography prevents the sender of the information from claiming later that the information was never send.
5. It allows the recipient of the information to verify that it has not been modified in transit.

Q. 5. Compare and contrast between Cryptography and Steganography.

Ans. Cryptography and Steganography, both techniques are used to make the data secure over the transmission. The comparison is as follows:

Cryptography	Steganography
1. Cryptography is the art and science of achieving security by encoding messages to make them non readable.	1. Steganography is a technique that facilitates hiding of a message that is to be kept secret, inside other message.
2. The original message is changed in encrypted method.	2. The original message is never changed, only hidden.

Q. 6. Differentiate between symmetric key and asymmetric key cryptography.

OR

How symmetric key cryptography does differ from asymmetric key cryptography?

Ans. Symmetric key cryptography: In symmetric key cryptography same key is used for both encryption and decryption.

Asymmetric key cryptography: In asymmetric key cryptography different key is used for both encryption and decryption.

Symmetric key cryptography	Asymmetric key cryptography
Strengths:	**Strengths:**
1. Much faster than asymmetric system.	1. Better key distribution then symmetric system.
2. Hard to break with a large key size.	2. Better scalability than symmetric system
	3. Can provide authentication and non repudiation.
Weakness:	**Weakness:**
1. Requires secure delivery mechanism.	1. Works more slowly than symmetric key system.
2. Key management can become overwhelming.	2. Involves mathematical intensive tasks.
3. Does not provide authenticity or non-repudiation.	

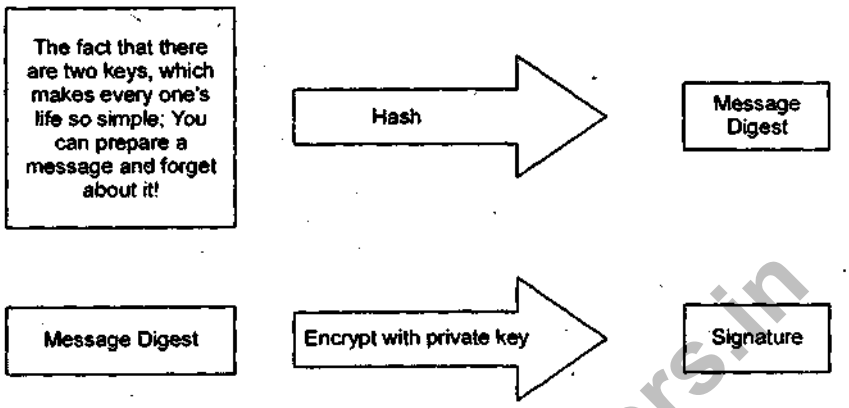
Q. 7. With a suitable illustration, explain the working of digital signatures.

or

What is a 'message digest'? Explain.

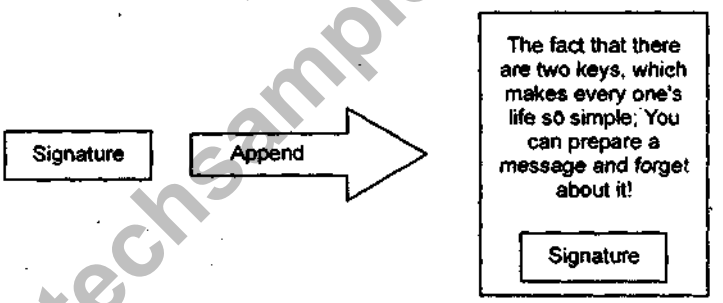
Ans. With private key and right software, a user can put digital signatures on documents and other data. A digital signature is a 'stamp' user places on the data that is unique to him/her and is very difficult to forge. In addition, the signature assures that any changes made to the data that have been signed cannot go undetected.

To sign a document, a person using the keys will use suitable software available to crunch down the data into just a few lines by a process called **'hashing'**.



Message Digest: A message digest is a product of a one way hash function applied on a message; it is a fingerprint or a unique summary that can uniquely identify the message. However, it is not possible to change a message digest back into the original data from which it was created.

The software then encrypts the message digest with the private key. The result is the digital signature.



Finally, the software appends the digital signature to the document. All of the data that were hashed have been signed.

Q. 8. What is the role of digital certificate in 'Message Authentication'?

Ans. A digital signature is a message digest used to cryptographically sign a message. Digital signatures rely on asymmetric or public key cryptography. We know that to create a digital signature, you sign the message with your private key. The digital signature then becomes the part of the message. This has two effects:

1. Any changes to the message can be detected, owing to the message digest algorithm.
2. You cannot deny signing the message, because it was signed with your private key.

These two features, message integrity and non repudiation make digital signature a very useful component in message authentication.

Q. 9. Discuss fingerprinting in brief.

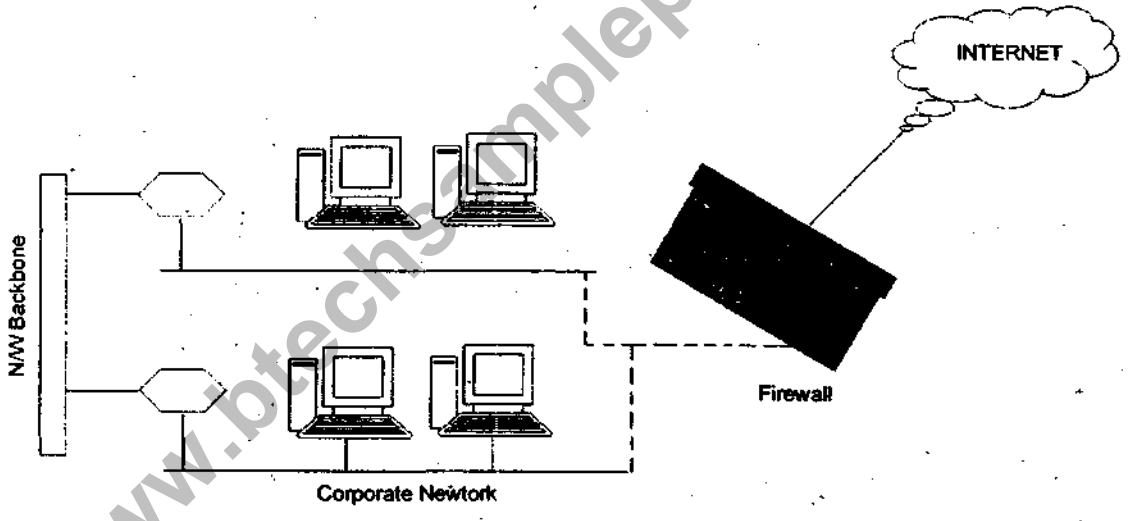
Ans. Fingerprint identification techniques fall in two categories:

1. Automated fingerprint identification systems (AFISs).

2. Fingerprint recognition systems (FRSs).
   - Fingerprint technique is a part of biometrics. Fingerprint recognition derives a unique template from the attribute of the fingerprint without storing the image itself or even allowing for its reconstruction.
   - Fingerprint recognition for identification acquires the initial image through a live scan of finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse.
   - Solid state sensors overcome the overcome the reduced sensitivity and reliability of optical scanners due to repeated use by using devices with electrical capacitance to sense the ridges of the fingerprint and create a compact digital image.

Q. 10. Explain, what are firewalls? And why are they needed?

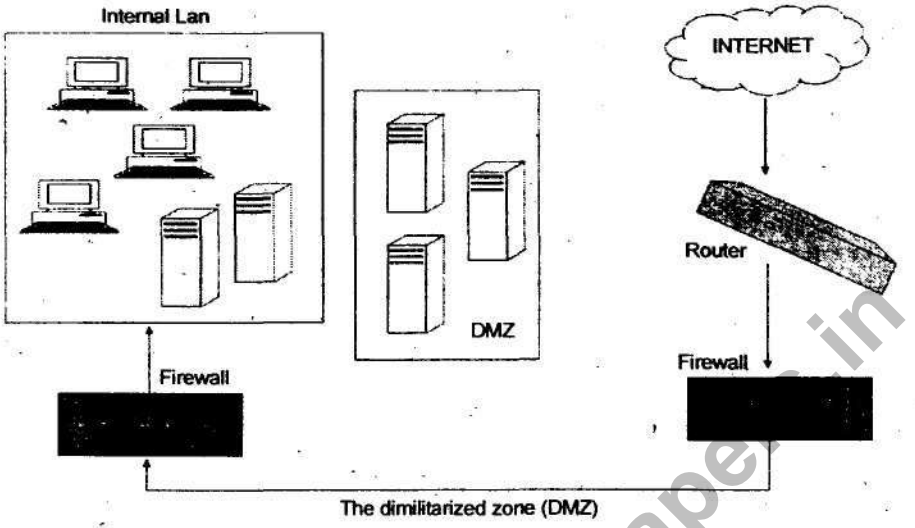
Ans. A firewall is a barrier to keep destructive forces away from your property/ assets. In fact, that is why it is called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to another. Firewalls protect the network from unauthorized use by attackers. Basically, any device that can control network traffic for security can be called a firewall.



Firewalls are used to restrict access from one network to another network. Most organizations use firewalls to restrict access into their network from internet users. Firewalls can be used internally to restrict one internal network segment from accessing another internal segment. Firewalls also log intruders attempt to access the computer network, providing important information such as: date/time, IP address of intruder and method of attack. Thus, computer firewalls (made of software and/or hardware) are there to protect computers against unauthorized access.

Q. 11. What is the concept of demilitarized zone (DMZ)?

Ans. The area separated between the two firewalls is called DMZ. Basically, a DMZ is a sub network that is located neither inside the internal network nor outside as part of the internet. Technically, a demilitarized area is any area where access is controlled, but not prevented by firewall technology. A DMZ can lie between two firewalls. Alternatively, a DMZ can also be off from a separate segment from one firewall. In either case, the types of access to and from DMZ servers are controlled and should be limited to a small group of peoples or network.

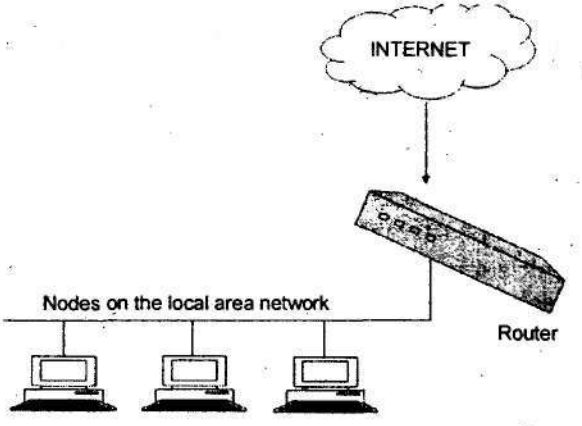


DMZ servers can provide multiple functionalities, such as electronic commerce (e-commerce) servers, web servers, file transfer protocol (FTP) servers, etc.

Q. 12. What are different types of firewalls?

Ans. Firewalls fall within three main categories. The most primary firewall devices are built using routers and they work on the lower layers of the network protocol stacks. These are called packet filtering routers or screening routers. These routers have the ability to filter IP packets. Proxy servers and application servers/ application level firewall operate at the upper level of the protocol stacks. The third type is the socks proxy that provides proxy services at the socket layer.

Packet-filtering firewall: Packet filtering firewalls are also called screening routers or filtering routers. This type of firewall system operates at the network layer or transport layer. Routers examine every packet coming in and going out of an intranet and decide where to send those packets so that they can be delivered to the proper address. They can control the type and direction of traffic permitted and essentially can also decide whether packets should even be delivered. In other words, they can block certain packets from coming in or going out of an intranet. When routers are used in this way- to protect an intranet by blocking certain packets- they are called filtering routers or screening routers.

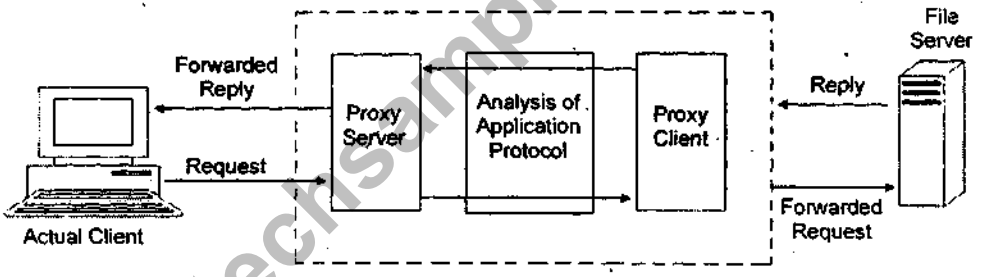


From security perspective, 'filtering' is a good concept. Filtering basically stops connections from or to the specified host or network. It can even block connections to a specific port. A packet-filtering firewall, thus, looks at the data packet to get information about the source and destination addresses of an incoming packet, the sessions communication protocol and the source and destination application ports for the desired service. A packet filtering router can filter IP packets based on some or all of the following criteria:

1. Source IP address
2. Destination IP address
3. Transmission control protocol (TCP)/ user datagram protocol (UDP) source port.
4. TCP/ UDP destination port.

Application- level firewall: Application layer firewall or application-level firewalls are also known as proxy firewalls. This type of firewall will have multiple interfaces, one for each network to which it is connected.

Thus, an application-level firewall is commonly a host computer that is running proxy server software, which makes it a proxy server. This type of firewall functions by transferring a copy of each accepted data packet from one network to another, there by masking the origin of the data. This way, services used by a workstation can be controlled. It also protects the network from outsiders who may try to get information about the network architecture.



An application-level firewall

Application gateways typically work as follows:

1. An internal user contacts the application gateway using a TCP/IP application, such as HTTP or TELNET.
2. The application gateway asks the user about remote host with which the user wants to set up a connection for actual communication.
3. The user provides information to the application gateway.
4. The application gateway now accesses the remote host on behalf of the user and passes the packets of the user to the remote host.
5. The application gateway now acts like a proxy of the actual end users and deliver packets from the user to the remote host and vice-versa.

Q. 13. Explain how network security matters in the modern digital world, in which today's extended enterprises operates.

or

Explain the basic concept of 'Network Security'.

Ans. Network security has become very complex today. Network security is fundamental defense to safeguard the collaborative enterprise. Network security involves some basic concept as follows:

1. **Computer Security:** The concepts of computer security are related to the security of the computers. Eventually, came on the scene in a big way and most of the information assets of the organizations become easier to use and more and more people got to access them with interactive sessions.
2. **Network Security:** New security problems occur when computers are networked together. Issues such as various types of networks, encryption standard, emission control, etc. came up in the domain of network security. Network security has three elements: Cryptography, secure network protocols and access control mechanisms.

On the basis of security, we can classify the networks in the following categories:

1. **Trusted networks:** Trusted networks are the networks inside network security perimeter. These networks are ones that organizations need to protect. A network administrator employed in an organization administers the computers that comprise these networks, and the organization, controls their security measures.
2. **Semi trusted networks:** These are the networks dedicated to the organization use, but not under organization's control (i.e. Internet). These are also referred to a demilitarized zone (DMZ). Under the scenario of semi trusted networks, access is allowed to some database material and electronic mail (e-mail).
3. **Un-trusted networks:** These are the networks that are known to be outside an organization's security perimeter. Essentially, they are any network where you do not know the routing of messages. They are un-trusted because they are outside an organization's control. There is no control over the administration or security policies for these sites. They are private, shared networks from which you are trying to protect your network.
4. **Unknown networks:** These networks are neither trusted nor un-trusted. By default, all non-trusted networks are considered unknown networks.

Q. 14. What are the network security dimensions?

Ans. There is always some risk given that not all internet users are involved in lawful activities. There are two key questions behind most security issues in a networked environment: the first one is how to protect confidential information from those who do not explicitly need to access it? and the other one is how the network and its resources can be protected from malicious users and accidents that originate outside the network.

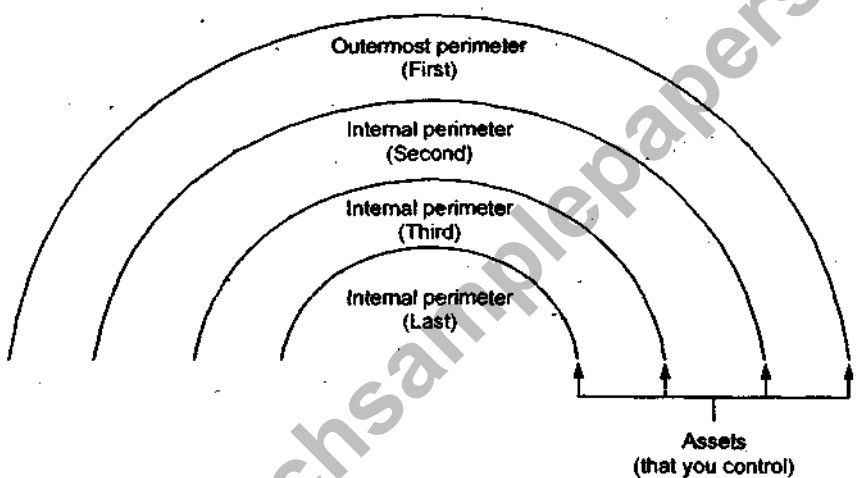
The pre occupation of network security professionals is protecting confidential information and protecting the corporate network to maintain internal network system integrity under the threat of attacks. Network intrusion is the most common security issue. The other issues for network security are:

1. Attacks against network assets, that is, information and physical assets accessible through the network.
2. Network perimeter threats.
3. Security of the network router.
4. Security of wireless networks.

5. Host security
6. World wide web security.
7. Intrusion detection systems (IDSs)
8. Operating systems (OSs) security.

Q. 15. Discuss, security perimeter for network protection.

Ans. The' perimeter' represents the point at which external traffic gains initial access to the network as well as the point through internal traffic will traverse the internet. The purpose of the perimeter security layers is to protect against hackers trying to penetrate the network, DOS and sophisticated attacks at the application level or the other hybrid methods of attacks. It is critical to deploy multiple security layers at the perimeter so that if an attack gets through the first layer, supporting layer will stop the attack.



Types of perimeter networks

There are three types of perimeter networks: the outer-most perimeter, internal perimeters and the inner-most perimeter. The outer-most perimeter network identifies the separation point between the asset that the organization controls and the asset that are not controlled. Usually, this point is the router, which is used to separate the network from other networks. Internal perimeter network represents perimeter boundaries where other security mechanisms are in place, such as internet firewalls and filtering routers.

In many cases, perimeter security represents the greatest assortment of security layers and may include VPN, DoS, firewall and intrusion protection.

Q. 16. Explain various methods of attacks on a network.

Ans. Intruders attempt to attack networks to get hold of the information resources on the network. Network intruders come in three forms- Masquerader, an individual who is authorized to use a computer; Misfeasor, a legitimate user who misuses his/her privileges and Clandestine user, an individual who seizes supervisory control of the system and uses it to suppress audit information. Conceptually network attacks can be classified as:

1. **Interruption:** Denying'services to the authorized users. These are attacks on system availability.

2. **Interception:** Unauthorized user obtaining access to a service. It is an attack on confidentiality.
3. **Modification:** Unauthorized access and tempering with data. This is an attack on integrity.
4. **Fabrication:** Counterfeit data. This is an attack on authenticity.

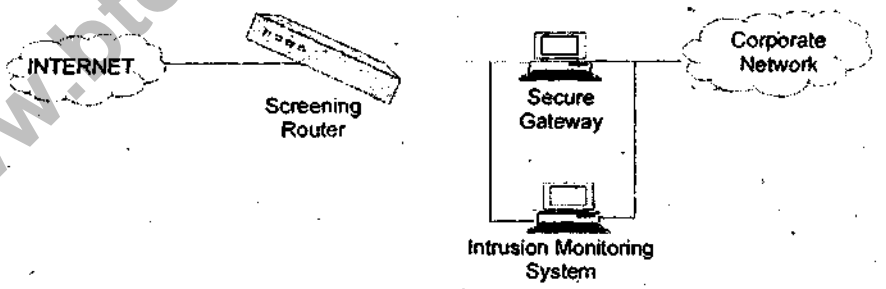
Technically, speaking following are four common methods of attacks that present opportunities to compromise the information on the network:

1. **Password Attack:** A user's password is stolen using any one of the following methods- Brute force attack, Key logger, Trojan, Sniffing, etc.
2. **Network Packet Sniffers:** Steals important information from the packets being transferred over the network.
3. **IP Spoofing:** Using someone else's IP address as your own without permission.
4. **DoS Attack:** Sending large no. of requests to the server at a time, which it cannot handle and ultimately crashes.

Q. 17. Explain the need for Intrusion monitoring and detection system.

Ans. The incorporation of monitoring and detection of possible threats to the networks provides the corporations with the ability to ensure the following:

1. **Protected information assets are not accessed by unauthorized entities:** Even if this does happen, there is a clear audit record. By installing IDS within the corporate network, one can offer protection to that information without the need for a secure gateway.
2. **The ability to monitor network tfaffic without impact to the network:** A secure gateway is intrusive. All the data packets must pass through it before they can be transmitted to the remote network. An intrusion monitoring system is passive in the sense that it "listens" on the network and takes appropriate action with the packets.
3. **Actively respond to attacks on system:** If implemented properly, intrusion monitoring systems have the ability to perform specific actions when an event takes place. Those actions range from notification to automatic reconfiguration of a device and blocking the connection at the network level.



Intrusion Monitoring System

4. **Security professionals are able to understand the attacks on the networks and build systems to resist these attacks:** Review the information captured by intrusion monitoring system, can assist in process to improve the level of infosec (information security) and decrease the risk of loss.

5. **Security metrics get generated:** As in many programs good quality metrics are required to report on the operational aspect of IT system. Good detection method helps generate metrics around attempts to penetrate the organizational network.

Q. 18. What is IDS? Explain its categories.

Ans. An IDS inspects all inbound and outbound network activities. It can be set up to identify any suspicious network activity patterns that may indicate a network or system attack. Unusual patterns that are known to generally attack networks can signify someone attempting to break into the network system or trying to compromise the system.

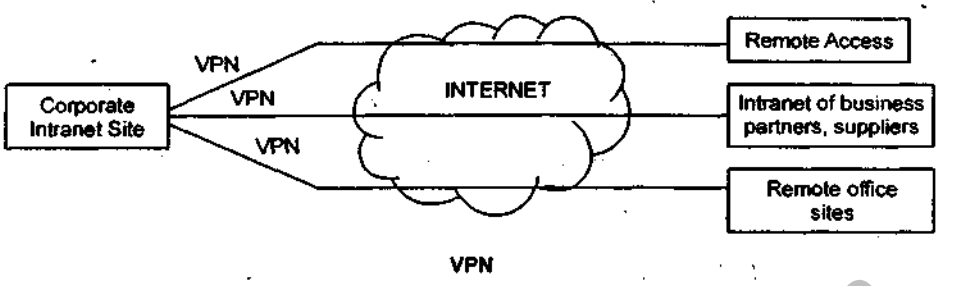
1. The IDS can be hardware or software based security service that monitors and analyses system events for the purpose of finding and providing real time or near-real time warning of events that are identified by the network configuration to be attempts to access system resources in an unauthorized manner.

There are many ways in which an IDS can be categorized as follows depending on its use:

1. **Misuse Detection:** The IDS analyses the information it gathers and compares it to the database of attack signatures. This type of IDS depends on attacks that have already been documented. Like virus detection systems, software for misuse detection is only as good as the databases of attack signatures.
2. **Anomaly Detection:** In this type of detection system, a baseline is established. It consists of things such as the network's traffic load state, breakdown, protocol and typical packet size.
3. **Network based IDS (NIDS):** NIDSs monitor network traffic and uncover possible attacks or suspicious activities. In an NIDS, the IDS sensors evaluate the individual packets that are flowing through the network.
4. **Host based IDS (HIDS):** HIDSs can be installed on individual workstations and or servers to watch for an appropriate or anomalous and insider attacks. They are usually used to make sure that the users do not accidentally delete system files, reconfigure important settings or put the system at risk in any other way.
5. **Passive IDS:** In a passive system, the IDS detect a potential security breach, log the information and signal an alert. i.e. no direct action is taken by the system.
6. **Reactive IDS:** In a reactive IDS, the IDS can respond in several ways to the suspicious activity such as by logging the user off the system, closing down the connection or even reprogramming the firewall to block network traffic from suspected malicious source.

Q. 19. Explain what virtual private networks are? And why do organizations need them?

Ans. Virtual private network (VPN) is a network of virtual circuits that carries private traffic through public or shared networks such as the internet or those provided by network service providers. VPNs allow a trusted network to communicate with another trusted network over un-trusted / public network such as internet. VPNs are used primarily to extend an enterprise's internal private network (intranet) across un-trusted public networks. They provide the capability to securely convey information across the public network into the corporate network.



NEED:

A well designed VPN can provide great benefits:

1. Extends geographic connectivity
2. Improves security
3. Reduces operational costs versus a traditional wide area network
4. Reduce transit time and transportation cost for remote users
5. Improves productivity
6. Simplifies network topology
7. Provides global networking opportunities
8. Provides a telecommuter support
9. Provides a broadband networking compatibility
10. Provides a faster return on investment (ROI) than a traditional WAN.

VPNs have several characteristics:

- Traffic is encrypted to prevent eaves dropping
- Remote site is authenticated
- Multiple protocols are supported
- Connection is point to point

Q. 20. How does tunneling protocol works for VPNs?

Ans. Tunneling is an important concept with response to VPNs. Tunneling is the transmission of data intended for use only in the private network through the public network in such a way that the routing nodes in the public network are unaware that transmission is the part of the private network.

A tunnel is a means of forwarding data across a network from one node to another, as if the two nodes were directly connected. This is achieved by encapsulating the data - an extra header is added to the data send by the transmitting end of the tunnel, and the data are forwarded by intermediate nodes based on this outer header without looking at the contents of the original packets.

Q. 21. Describe authentication mechanism in VPN.

Ans. A VPN involves two entities: the protected or 'inside' network, which provides physical and administrative security to protect the transmission, and a less trustworthy, that is 'untrusted' outside network or segment. A firewall sits between remote user's workstation or client and the host network or server. As the user's client establishes the communication with the firewall, the client may pass authentication data to an authentication service inside the perimeter.

For better security, many VPN client programs can be configured to require that, all IP traffic must pass through the tunnel while the VPN is active with an organization's internal networks that is protected from the outside internet by a firewall, people who share it may be simultaneously working for different employers over their respective VPN connections from the shared internal network. Each employer would therefore want to ensure that their proprietary data are kept safe and secure even if another computer in local gets infected with malware.

Q. 22. What are the security concerns in VPN?

Ans. Security concerns in VPN: Much of the security management for VPNs is an extension of the organization's overall security policies. Since VPN technologies extend the private network over the internet for companies to conduct business, several security concerns beyond these present in the private network needs to be addressed.

There are security risks and implementation issues that much be dealt with. One of the single biggest security issue with the use of remote access VPN by an employee is the simultaneous connection to other internet sites. Normally, the VPN software on the user's computer determines if the target should be sent to the organization via VPN. If the user computer has been compromised with a Trojan horse program, it may be possible for some external unauthorized users to use the employee's computer, to connect to the organization's internal network. Thus, VPN needs to be focused on the following:

1. The OSI model
2. Gateway security
3. Packet filter
4. Application and circuit proxies
5. Intrusion detection system (IDS)
6. Protection for information.