Q8 What is VPN? What are its various types? Explain with the help of diagram?

Ans 1) VPN is a technology for using the internet or another intermediate network to connect computers to isolated remote computers network that would otherwise be inaccessible.

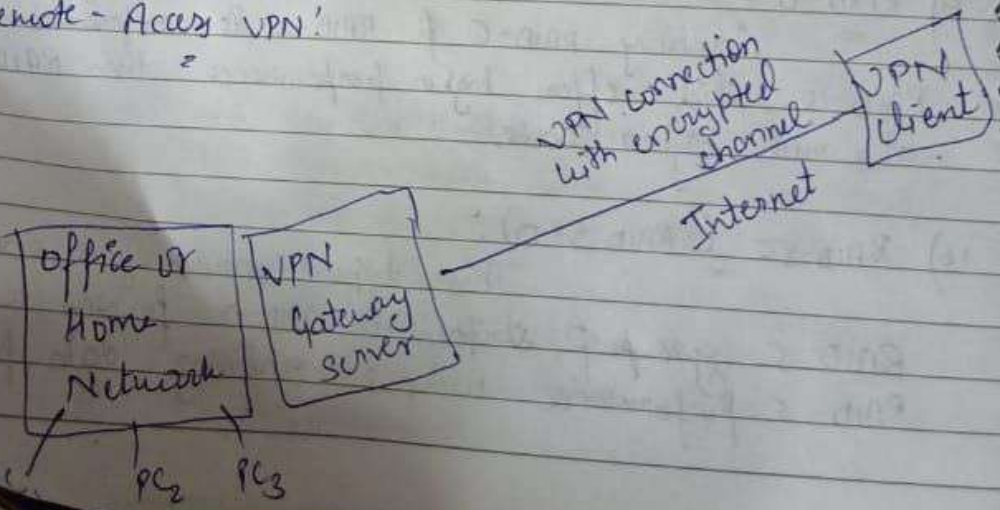
2) VPN is a technology that lets people access their office computer network over the internet while at home or travelling. Accessing a network in this way is referred to as remote ~~access~~ access.

3) VPN can be ~~contrasted~~ contrasted with an expensive system of owned or leased lines that can only be used by one organisation.

Types of VPN:

1) Remote-Access VPN
2) Site-to-Site VPN

1) Remote-Access VPN:



packets to pass through the firewall unless they match the established rule set. It is of 2 types:-

1) Stateful firewalls
2) Stateless firewalls.

Stateful firewalls maintain context about active sessions and use that "state information" to speed packet processing.

Stateless firewall require less memory & can be faster for simple filters that require less time to filter than to look up a session.

2) Application layer:
= This type of firewall operates at application layer. It uses various proxy servers to proxy the traffic instead of routing it on network.

3) Personal firewalls:
If the computer is not protected when the user connects to the internet, hackers can gain access to personal information from the computer. They can install code on the computer that destroys files or causes malfunctions. A firewall helps to screen out many kinds of malicious internet traffic before it reaches to the user's system.

DATE
PAGE

Types of Virus:

1) Trojan Horse:
It is an appearance having a useful & desired function. It neither replicates and nor copies itself. But damage the security of computer. The trojan horse must be sent by someone by another program and may arrive in the form fake program.

2) Worms:
The Worm is a program that makes distribution of copies itself. They also utilize large amount of bandwidth & memory, so effected server & networks.

3) Boot-Sector Virus:
It affect the boot sector of harddisk ['C' disk].
This type is also called master boot sector virus or master boot record. Virus boot sector exist on storage ~~area~~ area i.e. HDD, floppy disk, CD-DVD. During the booting process the boot sector program is automatic located by the hardware & then located.

4) Direct Action Virus:
This type of virus only come into exchange banned life containing virus is also executed when specific condition is met. The virus will be go into action & directory & folder that

DATE
PAGE

3) Skimming:

It is a method used by identity thieves to capture information from a cardholder. Several approaches can be used by fraudsters to procure card information with the most advanced approach involving a small device called a skimmer.

4) Digital Signature:

Digital Signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message. This binding can be independently verified by receiver as well as any third party.

Q5 What is Virus? Explain its various components in detail?

Ans Virus:

A Virus is an executable program depending upon the nature of virus. It may cause damage of your harddisk. A virus can be introduce to a computer system along with any software. It can attack itself too or sometimes even replace an existing program. When the user run the program, the virus is also executed.

compress algorithm

Authenticate :

= First, the server & client authenticate themselves to the other site. Server is authenticate using ~~xor~~ host key, X.509 certificate can be used as a ~~key~~ host key. Client authentication is done by

1) Public key authentication
2) Password "
3) Host based "
4) keyboard "

Data Exchange is performed if authentication was successful. For data exchange the client & server create & manage a logical connection.

Q4 Short Note

1) Digital Signature
2) Cyber Ethics
3) Skimming

2) Cyber Ethics :

= Ethics are principles or standards of human conduct. Cyberethics is a code of behaviour on the internet. Based on common sense of good judgement, cyberethics also includes obeying laws that apply to online behaviour. When ever we practice cyberethics, we are more likely to have a safer & enjoyable internet experience.

Ransomware:
- It is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.

Q8 Limitations of firewall?

Ans 1) Firewalls cannot protect you from poor decisions.

2) They cannot protect you when your security policy is too liberal.

3) Firewalls are ineffective against nontechnical security risks such as social engineering.

4) Firewalls cannot stop internal users from accessing websites with malicious code, making user education critical.

Q9 What is virus scanners & heuristic scanner?

Ans Virus Scanner:
- A virus scan is a process of using anti-virus software to scan & identify viruses in a computing device.

Heuristic Scanner:
- It is a method of detecting viruses by examining code for suspicious properties.

DATE
PAGE

Q10 ~~Ans~~ what do you mean by cyber assets?

Ans Assets generally include hardware, software & confidential information. It should be protected from illicit access, use, disclosure, alteration, destruction & resulting in loss to the organisation.

Having two key allow initiating secure communication through public unprotected channel without the need to pass the private key to the otherside. It can be used in following ways:

(1) Any sender uses widely known public key to encrypt the message. Only receiver also knows the private key can decrypt it.

(2) Sender uses the private key can encrypt the hash code of the message. And attached it as a public electronic signature.

(3) A guard say a challenge that the passing person must written encoded with the private key.

Q5 Define clustering? What are its various advantages?

Ans Connecting two or more computers together in such a way that they behave like a single computer. Clustering is used for parallel processing, load balancing & fault tolerance.

Advantage:

1) If one of these computer fails, another computer in the cluster can then assume the workload of the failed computer.
2) Support for a greater number of users.
3) Performance increased

DATE
PAGE

MD5:

- Message Digest Algorithm - 5
- Cryptography has function created by RON Rivest for the MIT laboratory from Computer Science in 1992.
- It produce a 128 bit fingerprint or message digest of the i/o.
- It was created to be a digital signature for application where large file can be verified by checking MD5 hash o/p.

Purpose of MD5:

- NOMADS use the data file as i/p to create a MD or signature for a specific file.
- MD5 checksum i.e created can be used as a compact digital fingerprints for the associated file.
- This sign can be used to verify the file by using a piece of software like MD5 sum.

RSA algorithm:

It is widely used asymetric encryption algorithm. That when properly implemented cannot be cracked in acceptable time. RSA can be used for user authentication, data encryption & digital data signing. It uses 2 keys:

1) Public
2) Private

Q6 Difference b/w HTTP & HTTPS?

Parameter	HTTP	HTTPS
1) Stand for	Hypertext transfer protocol	Hypertext transfer protocol with security.
2) Security	Data is vulnerable to hacker, security is low.	It is designed to prevent from hacking
3) Port	By default Port no is 80	By default Port no is 443.
4) Start with	URL begins with ~~https://~~ http://	URL begins with https://
5) Domain Name Validation	It has no need of SSL	It requires SSL certificate

Q7 What is Zombie & Ransomware?

Ans Zombie:

It is a computer connected to the internet that has been compromised by a hacker, computer virus or trojan horse program & can be used to perform malicious tasks of one sort or another under remote direction.

DATE
PAGE

Decrypting is the act of translating a message written with secret characters into a readable message, the unencrypted message.

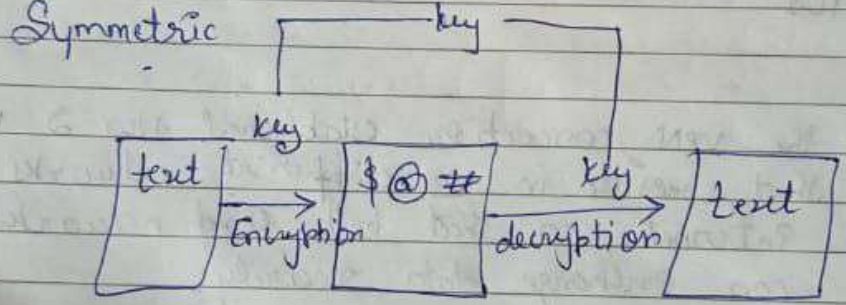
Symmetric & Asymmetric Algorithms:

Symmetric Algorithm:

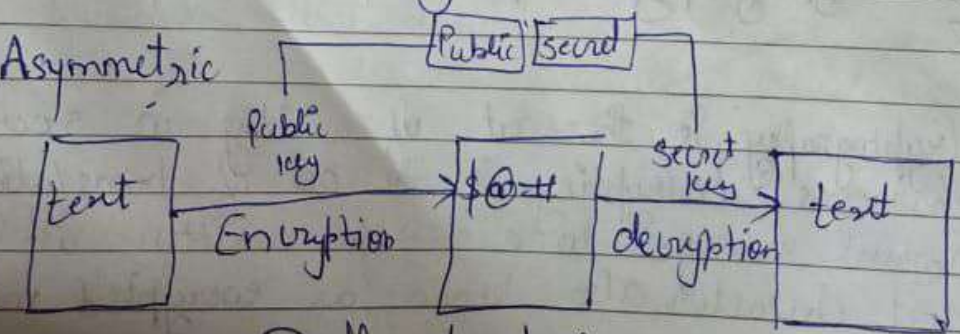
This is the simplest kind of encryption that involves only one secret key to cipher & decipher information.

Asymmetric Algorithm:

It is also known as public key cryptography, which is a relatively new method compared to symmetric encryption.



Same key all time



Different keys

DATE
PAGE

(4)

Q1 List types of attacks on network?

Ans
1) Data Modification
2) Spoofing
3) DOS Attack
4) Compromised key Attack
5) Sniffer Attack

Q2 Describe hashing?

Ans Hashing is generating values or values from a string or text using a mathematical function. It is one way to enable security during the process of message transmission when the message is intended for a particular recipient only.

Q3 What is digital Signature & digital certificate?

Ans Digital Signature is a technique which is used to validate the authenticity & integrity of the message. The basic idea behind the digital signature is to sign a document.

Digital certificate is an electronic password that allows a person, organization to exchange data securely over the internet using the public key infrastructures.

Q4 Explain RSA algorithm with diagram? Explain MD5 with its properties?

5) RAID-4:
- This type uses large stripes, which means you can read records from any single drive. This allows you to take advantage of overlaped I/O for read operations.

6) RAID-5:
- This type includes a rotating parity array, thus addressing the write limitation in RAID-4.

7) RAID-6:
- This type is similar to RAID-5 but includes a second parity scheme that is distributed across different drives & thus offers extremely high fault & drive failure tolerance.

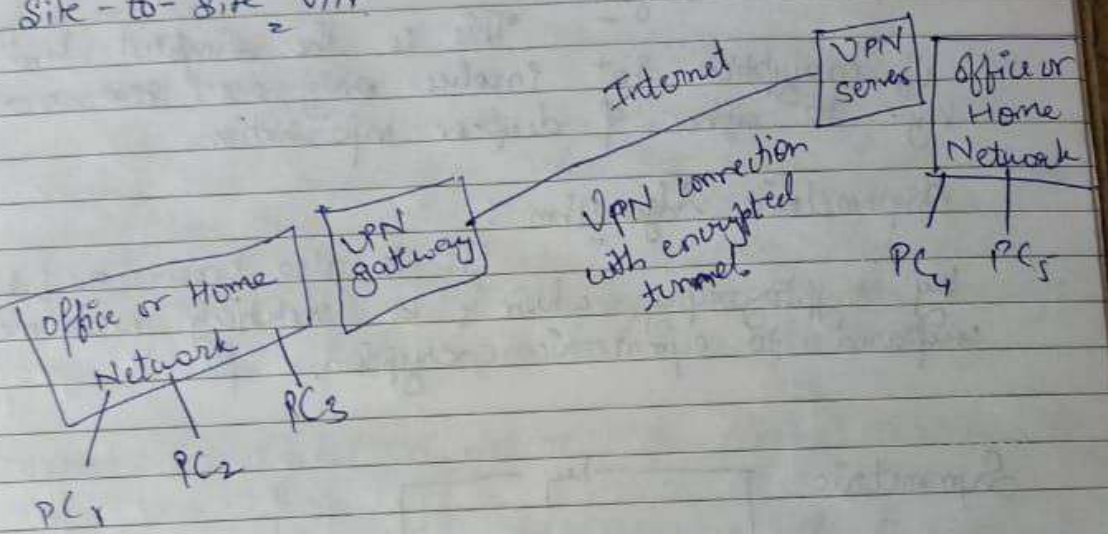
8) RAID-7:
- This type includes a real-time embedded OS as a controller, caching via a high-speed bus & other characteristics of a stand alone computer.

9) RAID-10:
= Combining RAID-0 & RAID-1 is referred to as RAID-10, which offers higher performance than RAID-1 but at much higher costs.

10) RAID-50 (RAID 5+0):
= This type consists of a series of RAID-5 groups & striped in RAID-0 fashion to improve RAID-5 performance without reducing data protection.

It is very common VPN service that can be set up in office or home network. It can be implemented by setting up a VPN gateway or server & you can connect to it by using VPN client from other location.

e) Site-to-Site VPN:



It is the VPN connection established b/w 2 VPN server that reside in 2 different networks over the Internet, so that both networks computers can exchange data securely.

Q. Explain Cryptography? Explain symmetric & asymetric key?

Ans Cryptography is the art of writing in secret characters. Encrypting is the act of translating a normal message to a message written with secret characters also known as encrypted message.

Specified in the exec, but file path.

5) File infector Virus:

The virus overright the file. The most common type of virus is file factor virus first take boot.

Q6 What is firewall? Explain its types?

Ans Firewalls are software programs or hardware devices that filter the traffic that flows into our PC or our network through a internet connection.

A firewall can offer the security that makes us less vulnerable & also protect our data from being compromised or our computers being taken hostage.

Types of firewalls:

1) Network layer
2) Application layer
3) Personal firewalls

1) Network layer

They are also called packet filters & they operate at a relatively low level of the TCP/IP protocol stack, not allowing

Q.7 What do you mean RAID? Explain its various components in detail.

Any RAID stands for Redundant Array of Inexpensive Disks. It is a way of storing the same data in different places on multiple hard disks. By placing data on multiple disks, I/O operations can overlap in a balanced way, improving performance. A RAID appears to the operating system to be a single logical hard disk.

Various levels of RAID.

1) RAID-0:
   - This technique has stripping but no redundancy of data. It offers the best performance but no fault tolerance.

2) RAID-1:
   - This type is also known as disk mirroring & consists of at least two drives that duplicate the storage of data. There is no stripping.

3) RAID-3:
   This type uses stripping and dedicates one drive to storing parity information. The ECC (embedded error checking) information is used to detect errors.

4) RAID-2:
   This type uses stripping across disks with some disk storing ECC information.

iii) Preserving the internal & external consistency.

Internal consistency:
Ensures that internal data is consistent.

External consistency:
Ensures that the data stored in the database is consistent with the real world.

3) Availability:
It assures that a system's authorized users have timely & uninterrupted access to the information in the system & to the network.

Other important terms:

1) Identification:
The act of a user professing an identity to the system, such as login ID.

2) Authentication:
- Verification that the user's claimed identity is valid.

3) Accountability:
- Determination of the actions and behaviour of a single individual within a system & holding the individual responsible for his/her actions.

DATE
PAGE

Q3 Explain the basics of SSH?

Ans SSH (Secure Shell):

It is a set of protocol commonly referred to as SSH for secure transfer from the internet such as TCP. It was initially designed as a secure replacement of UNIX remote shell application. SSH protocol designed & implemented which is mentioned as below.

1) SSH accept the client to always authenticate to the server.
2) SSH is quite efficient when very small chunk of data (1-4 byte) are send.
3) It allow to organise tunels.
4) It is easy to understand & use.

Also SSH key most commonly used of SSH authentication are stored in different incompatible format.

SSH consist of 3 ways:

1) Handshake
2) Authentication
3) Data Exchange

During handshake phase, the slide exchange information about SSH protocol version & use cipher suite are the combination of asymetric, symmetric, hash &

DATE
PAGE

Q: What is need for cyber law? (10)

Ans Cyber Crime :

It may be difined as "Unlawful" acts wherein the computer is both a tool & target. Cyber criminal is a person who commits an illegal act with a guilty intention a crime in content to cyber crime.

Some Kinds of Cyber Criminals:

1) Crackers
2) Hackers
3) Pranksters
4) Career Criminals
5) Cyber bulls

Cyber law - Indian Perspective (IT Act 2000 & amended 2008)

The IT Act 2000 provides legal recognition to the transaction done via electronic exchange of data & other electronic commerce transactions.

Objectives of the Act:

1) Give legal recognition to digital signatures for the authentication of any information requiring legal authentication.

2) Facilitate the electronic storage of data.
3) Give legal sanction & also facilitate the electronic transfer of funds b/w banks & financial institution.
4) Facilitate the electronic ~~fating~~ filling of document with government agencies & also department.

Q2 What are the principles of security? (10)

Ans There are three principles of network security:-
1) Confidentially
2) Integrity
3) Availability

1) Confidentially:
It is concurned with preventing unauthorized disclosure of sensitive information. This disclosure could be intentional, such as breaking a cipher & reading the information, or it could be unintentional due to the carelessness or incompetence of individuals handling the information.

2) Integrity:
There are 3 goals of integrity:-
i) Preventing the modification of information by unauthorized users.
ii) Preventing the unauthorized or unintentional modification of information by unauthorized users.