Serial No.	Date	Title

First Sessional - May 2021

[SECTION - A]

[Answer - 1]

Information System - IS was derived from IT, but it is not just part of IT anymore.
Today, IS has provided highly productive results thus becoming more efficient.

Cyber Security - It is the protection of information & IS against the potential threats on the internet.

Goals of cyber Security

Protect the confidentiality of data.

Preserve the integrity of data

Promote the Availability of data for authorized users.

Secure information - Reducing the risk of data breaches & attacks in IT systems. Applying Security controls to prevent Unauthorized access to Sensitive information.
Ex DoS Attack

Db Security - It concerns the use of a broad range of Information Security controls to protect db against compromises of their integrity.

(e)

Hacking

* to use a computer to look at & change information that is stored on another computer without permission

Attacking

* To act upon or work against forcefully attack on enemy fortification.

[Section - B]

(a) **Access Control** - It is a mechanism that defines & controls access rights for individuals who can use specific resources in the OS.

Access control System include -

* File permission
* Program Permission
* Data right permission

important field for cyber Security

* identification V/S Authentication
* Authentication & Authorization
* mandatory Access Control
* Discretionary Access control
* Role based Access control.

(c) Database Security

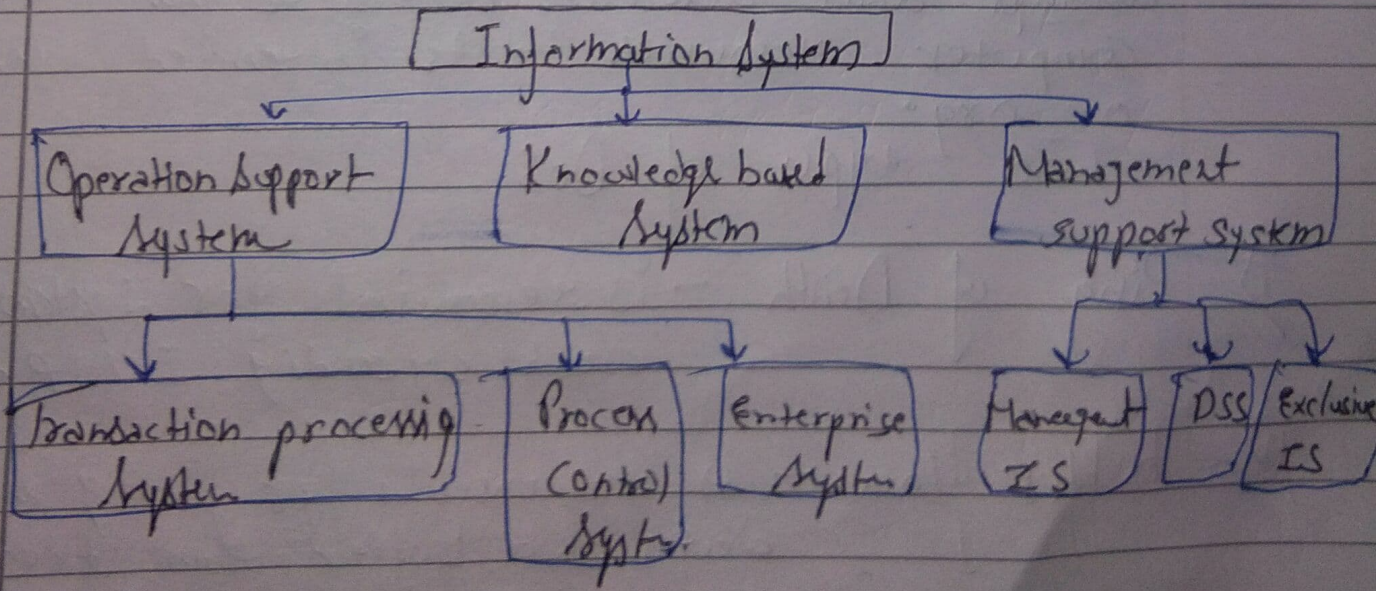
= DBS encompasses a range of security controls designed to protect the DBMS.
The types of DBS measures your business should use include protecting the underlying infrastructure that securely configuring the DBMS & the access to the data itself.

Why is DB Security important.

* Deployment failure.
* Excessive privileges
* Platform vulnerability
* Unmanaged sensitive data
* Backup data exposure
* Weak Authentication.

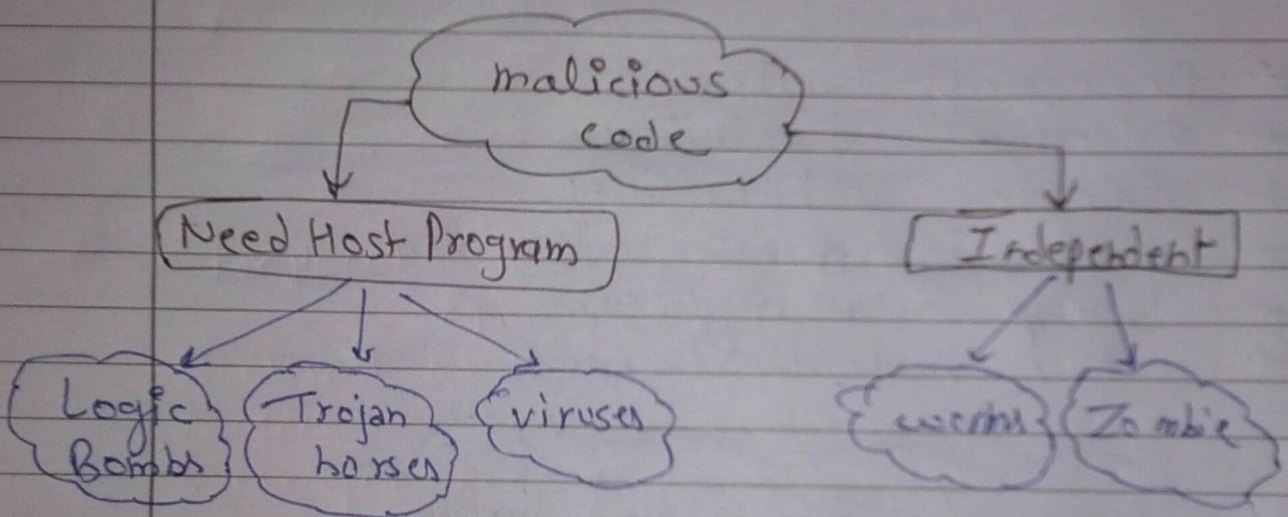
(d) Types of information System

IS supports all the different business operations in an org.



(e) i) Malicious Software

A computer program is a sequence of symbols and instructions used to achieve a desired functionality. It is termed malicious when the sequence of instructions is used to intentionality have adverse effects on the computer by malicious code.



ii) Denial of Service Attacks - DoS attack refers to as attempt that restricts access to the computer resources to its intended users or org.

Two types of DoS

i) Ping of Death - is responsible for system crash by sending ICMP.

ii) buffer flow - is responsible for putting more data on a buffer than it can hold.

[Section - C]

(a) **Security Threats** - There are numerous threats to Security of applications & data. with the increasing use of the internet & the advancing IT, applications are becoming increasingly vulnerable. threats that could be a malicious code, virus, worms etc.

* **Viruses** - virus refers to piece of s/w that is designed & developed with the purpose of infecting a computer system.

→ which a virus gets transmitted to a system -
by email
by cd & pendrive
by another software program

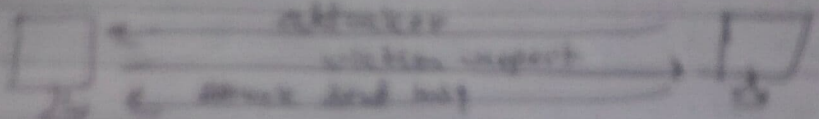
* **Worms** - worms can be defined as threats that are self sufficient to replicate themselves & do not need any host application to get transmitted. The worms used to reside in the RAM of a target computer.

by email
by TCP/IP
by internet services.

* **Trojan Horses** - It can be defined as programs that are transmitted to a system under disguise of any legitimate

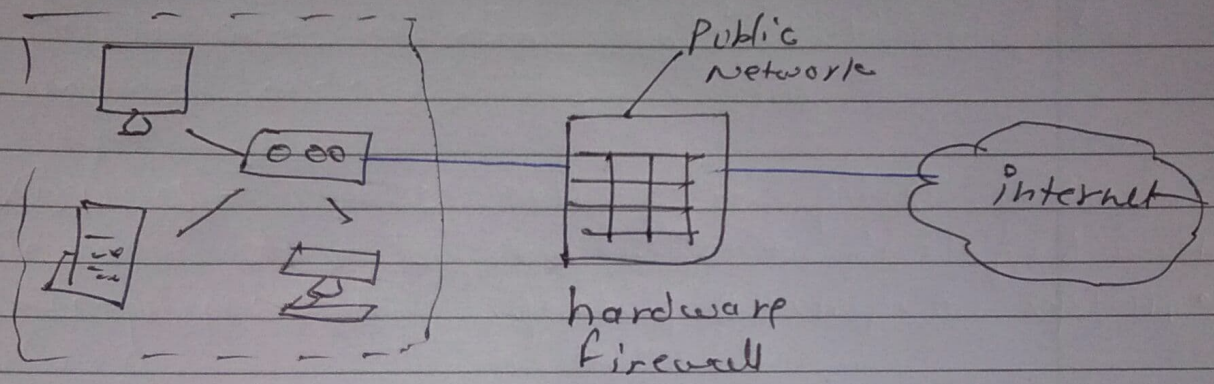
apps as programs, such as an attachment to a program or part of an installation process.

* **Logic bomber** - These logic bombers display a message to user & occurs at first when either the user is accessing the Internet or making use of a word processor application.



* **Trapdoor** - backdoor attacks which were also known as backdoor, have 2 different meanings.
backdoor attack defines troubleshooting of developer hacking into a system, the back door term is referred to as gaining access to a network.

6. **Firewall** - It is a part of computer system or network that is designed to inspect incoming & outgoing network traffic & alter the traffic flow by dropping or passing certain packets.



* **VPN** - It stands for Virtual Private Networks.
  * It is most secure remote method of connecting a computer to a private Network with the help of a public Network, such as the internet.

* VPN fingerprint
* username enumeration
* offline Password cracking.
* DoS Attacks
* Lack of account lockout.

* **Intrusion Detection System** - It has a sensor as its core element that is used to detect intrusions. The data received by these sensors is obtained from various source such as IDS knowledge db.