1) Explain security technoology (Intrusion detection, prevention & other security tools).

## Intrusion detection system (IDS)

<u>Intruder</u>: he is person who is trying to gain an unauthorized access to a system/a network.

He trys to steal information update information, make system unusable etc.. (miss use of a system).

Intruder
↓
Intrusion
↓
Intrusion detection system (IDS).

<u>Instrusion</u>: The process/damage done by the intruder is called Intrusion.

<u>Intrusion detection system</u>:

It is security management system for computers & networks. It make sure that all data is safe with out any dangerous info.

→ To detect attack aganist computer system & networks

→ To detect attempts by legitimate user of the information system.

→ To document the existing thread to an organization.

→ To provide information about intrusions.

Types of IDPS: (Intrusion detection & prevention systems)

host based IDPS

network based IDPS

i) Network based IDPS:

→ It is completely network based

→ Analyzies/matches traffic to the library of known attacks

→ monitors, captures & analyze network traffic.

→ Detect malicious data present in packets.

→ NIDS Analysis very difficult in buys network

ii) Host Based IDPS :-

→ Host Based

→ installed on individual host or device or network

→ It monitors data packets from the device only and will alert the admin if suspicicious activity is detected

→ Snapshots

Existing system ⇌ Previous system

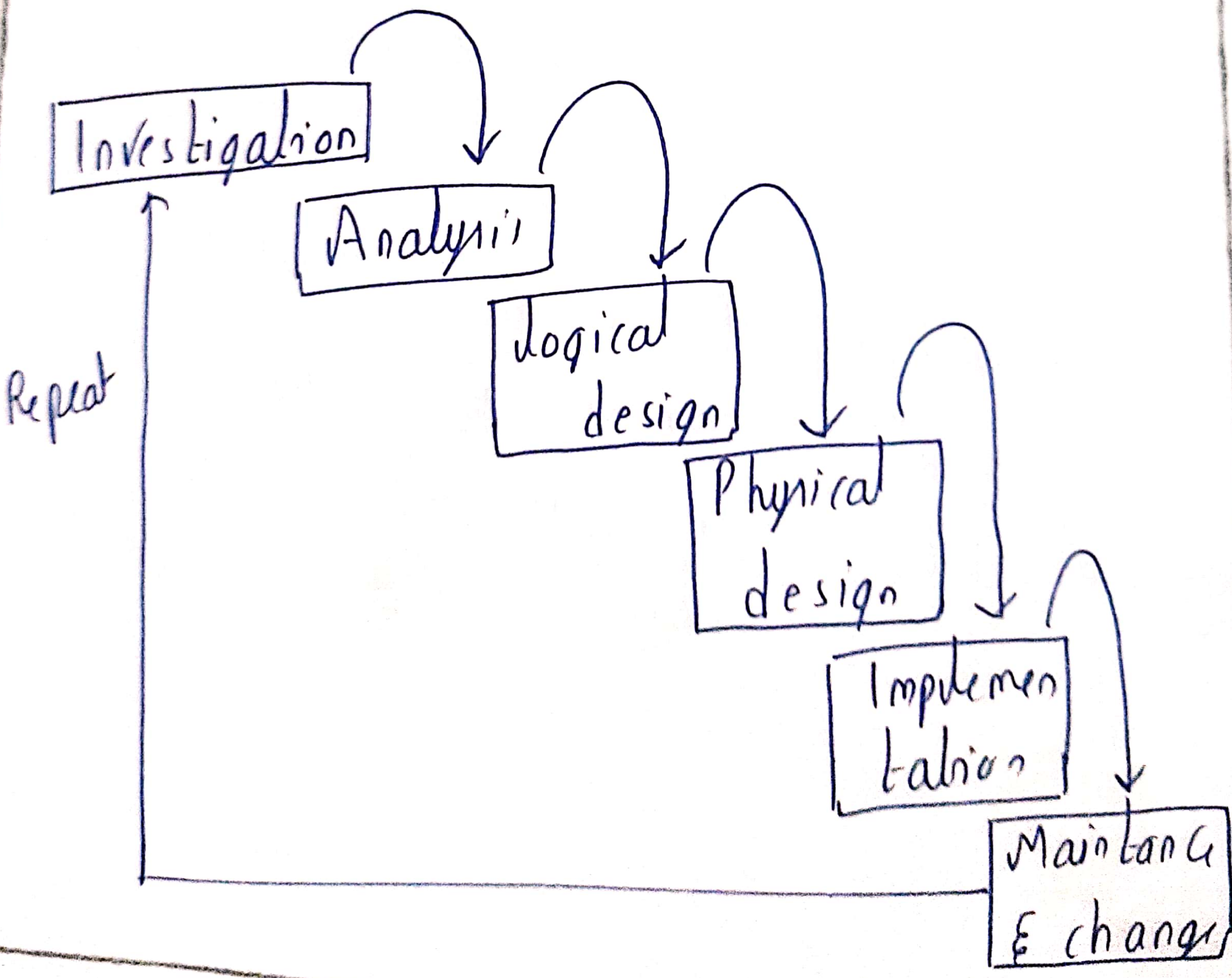
→ Files deleted or modification.

→ Secure System Development life Cycle:

→ The same phases used in traditional SDLC may be adapted to support specialized implementation of an Information security projects.

→ Here the identification of specific threads and creating controuls to counter them.

→ in short form it is called SecSDLC.



System Investigation: (what it can potentially do)

→ This process is started by officials/directives working at the top level management in organization.

→ the main goal is to know what problem is the system being developed to solve.

→ all the objectives, constrains & scope of project are specified

System Analysis: (understanding system properties checking for threats).

→ In this phase detailed document analysis of the document from the system Investigation phase are done

→ Previously existing security polocies, applications & software are analysed in order to check faults & Vulnerabilities in the system.

Logical Design: (planning for idea which could solve threats)

→ ~~Main~~ In the logical design phase, the information from the analysis phase is used to begin creating the solution.

→ The maid goal here is to make a logical blueprint that involves all the requirements

Physical Design: (designing a blueprint).

→ The technical team acquires the tools & blueprint & start implementing the software & by applying the security aspects (new).

Implementation: (Final product or software is made here. with testing).

→ here the final product or software is made or purchased

→ all the main stages like ordering, receiving testing are done here.

→ here an aggressive testing is done here & Final system documentation are written

Maintenance:

→ This is one of the longest & most expensive phase

→ after the implementation of the security program it must be insured that it is functioning properly & managed according.

→ Frequently this process is repeatedly for the better security.

→ When any kind of bugs or threats reported again the whole process starts & the issues are resolved

→ Secure SDLC is nothing but SDLC with security (from threats).