UNIT – 6
System Security

★ Intruders :–

→ An intruder is a person who attempts to gain unauthorised access to a system, to damage that system, or to disturb data on that system.

→ In summary, this person attempts to violate security by interfering with system availability, data integrity or data confidentiality.

→ One of the two most publicised threats to security is the intruder (the other viruses) generally referred to as a hacker or cracker. In an important early study of Intrusion Anderson (ANDE80) identified three classes of intruders –

1. Masquerader
2. Misfeasor
3. Clandestine user

1- Masquerader – An individual who is not authorised to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

2- Misfeasor – A legitimate user who accesses data, programs or resources for which such access is not authorised or who is authorised for such access but misuses his or her privilages.

3- Clandestine user – An individual who seizes supervisary control of the user/system. This control is used to evade auditing and access controls or

to suppress audit collection.

The Masquarader is likely to be an outsider, the misfeaser is generally is an insider and the clandestine user can be either an outsider or an insider.

★ Intrusion Techniques :-

The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. In some cases, this can be protected in one of two ways —

1- One-way Function — The system stores only the value of a function based on the user's password when the user presents a password, the system transforms that password and compares it with the stored value.

2- Access Control — Access to the password file is limited to one or a very few accounts. On the basis of a survey of the literature and interviews with a number of password crackers, reports the following techniques have been fixed for learning passwords —

(a) Try default passwords used with standard accounts that are shipped with the system.
(b) Exhaustively try all short passwords (those of one to three characters).
(c) Try words in the system's online dictionary or a list of likely passwords.
(d) Collect information about users, such as their

full names, the names of their spouse and children, picture in their office and books in their office that are related to hobbies.

(e) Try user's phone numbers, social security numbers and room numbers.

(f) Try all legitimate licence plate numbers for this state.

(g) Use a trojan horse to bypass restrictional access. Tap the line between a remote user and the host system.

→ The first six methods are various ways of guessing a password, if an intruder has to verify the guess by attempting to log in. It is a tedious and easily countered means of attack.

★ Intrusion Detection System (IDS) :—

→ IDS is used to detect where the intrusion occur.

→ IDS can be hardware or software based security service that monitors and analyses system events that may indicate a network system attack.

→ Following factors motivate efforts on intrusion detection-

(a) The sooner it is able to detect an intrusion, the quicker we can act. The hope of recovering from attacks and losses is directly propotional to how quickly we are able to detect an intrusion.

(b) Intrusion detection can help collect more information about intrusions, strengthening the intrusion prevention methods.

(c) Intrusion detection system can act as good deterrents prevention to intruders.

★ Categories of IDS :-

1. Misuse detection
2. Anomaly detection
3. Network based IDS (NIDS)
4. Host based IDS (HIDS)
5. Passive IDS
6. Reactive IDS

1- Misuse Detection — Here, the IDS analyses the information it gathers and compares it to the database of attack signatures.

2- Anomaly Detection — In this IDS, a baseline is maintained such as traffic load state, breakdown protocol and packet size, which is compared with the present network segments to identify analysis. If baseline is choosen protocol, then this is called protocol IDS.

3- Network Based IDS (NIDS) — NIDS monitor network traffic and analyze the individual packets that are flowing through the network.
It detects malicious packets that are designed by an attacker to be overlooked by the simplistic filtering rule of many firewalls.

4- Host Based IDS (HIDS) — HIDS can be installed on individual workstations or servers to examine the activity on each individual computer mode or host.

It evaluates modifications to important system files, abnormal or excessive central processing

unit (CPU) activity and misuse of root or administrative rights.

5- Passive IDS— Here, the IDS detects a potential security breach, logs the information, and signal and alerts. Here, no direct action is taken by the system.

6- Reactive IDS— Here IDS can respond in several ways to the suspicious activity such as by loging a user off the system, closing the connection or even reprogramming firewall to block network traffic from the suspected malicious source.

* Approaches of IDS :—

1- Knowledge Based IDS— Knowledge Based IDS uses a database of previous attacks and known system vulnerabilities to look for current attempts to exploit their vulnerabilities is found.

2- Behaviour Based IDS— It uses dynamic approach in the sense that they detect deviations from the learned patterns of user behaviour.

An alarm is triggered when any activity that is considered outside of normal system use takes place.

3- Statistical Anomaly IDS— It involves the collection of data relating to the behaviour of legitimate users over a period of time. Then statistical

tests are applied to observe behaviour of determine with a high level of confidence whether that behaviour is not legitimate user behaviour.

It fall into two categories —

(a) Threshold detection

(b) Profile-based anomaly detection

(a) Threshold Detection — This approach involves defining thresholds, independent of users for the frequency of occurance of various events.

(b) Profile-Based anomaly detection — A profile of the activity of each user is developed and used to detect changes in the behaviour of individual accounts.

4- Rule Based IDS — Rule-based techniques detect intrusion by detecting (observing) events in the system and applying a set of rules that lead a decision regarding whether a given pattern of activity is or is not suspicious.

It involves an attempt to define a set of rules that can be used to decide that a given behaviour is that of an intruder.

5- Rule-Based Penetration Identification IDS —

→ It takes a very different approach to intrusion detection, one based on expert system technology.

→ The key feature of such system is the use of rules for identifying known penetrations that would exploit know ~~so~~ weakness.

→ The penetration identification scheme used in IDES

is representative of the strategy followed.

→ Audit records are examined as they are generated and they are matched against the rule base. If a match is found then the user's suspicious rating is increased.

→ If enough rules are matched, then the rating will pass a thresholds that results in the reporting of an anomaly.

6- Distributed IDS — It needs to defend a distributed collection of hosts supported by a LAN or internetwork. Porras points out the following major issues in the design of a distributed intrusion detection system.

→ A distributed IDS may need to deal with different audit record formates.

→ One or more nodes in the network will serve as collection and analysis points for the data from the system on the network.

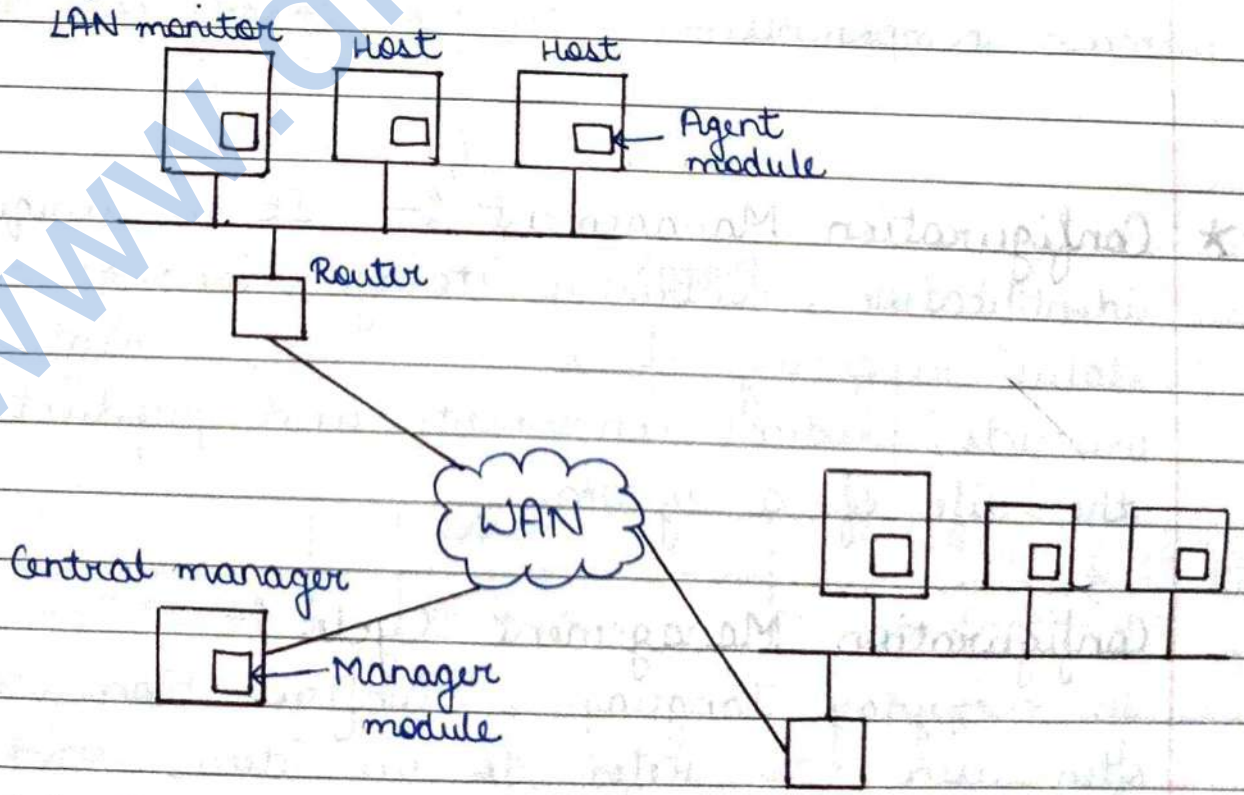


fig (a)- Architecture for distributed intrusion detection

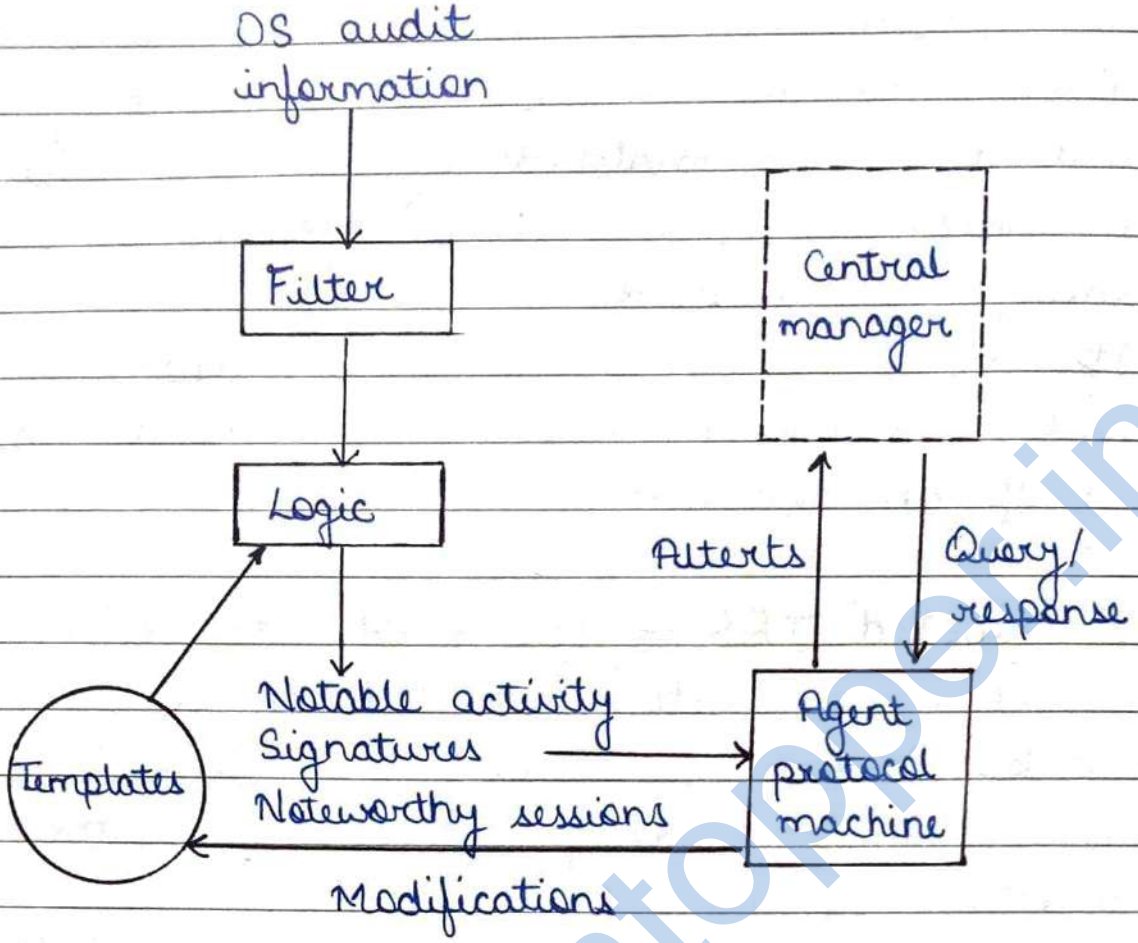


fig (b) Agent architecture

Either a centralised architecture can be used. Figure shows the overall architecture, which consist of three main components —

★ Configuration Management :— It is unique identification, controlled storage, change control and status reporting of selected intermediate work products, product components and product during the life of a system.

Configuration Management Cycle :-
In everyday language, "Configuration item" is often used to refer to an item, which is then said to be produced in several versions. This is

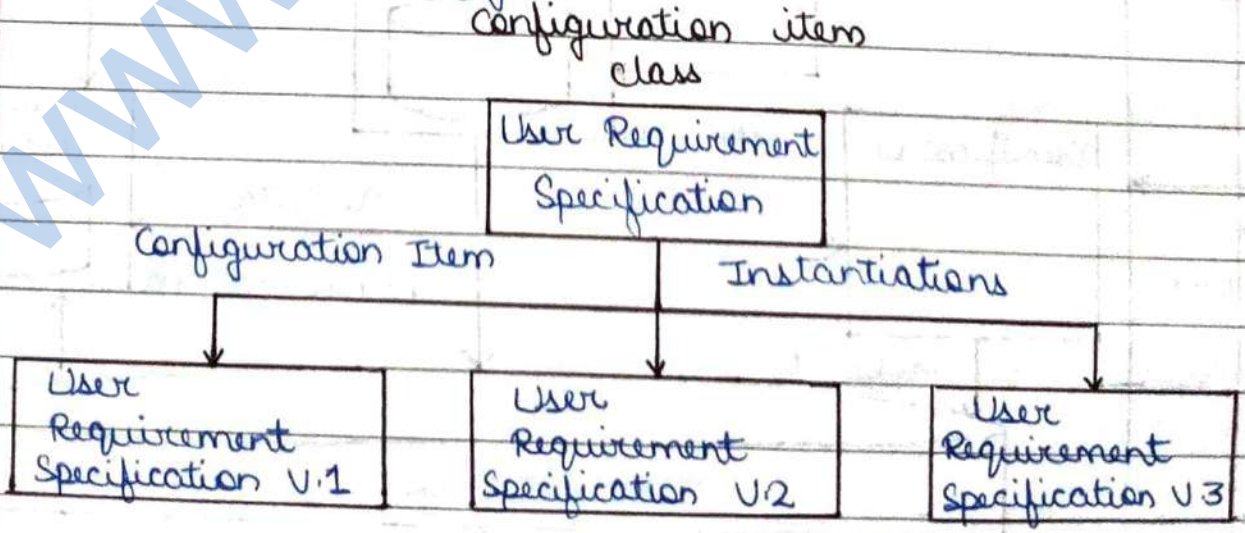
not strictly correct but it's acceptable as long as the reference is clearly understood by all involved. In fact, each new version of a configuration item is a new configuration item in its own right.

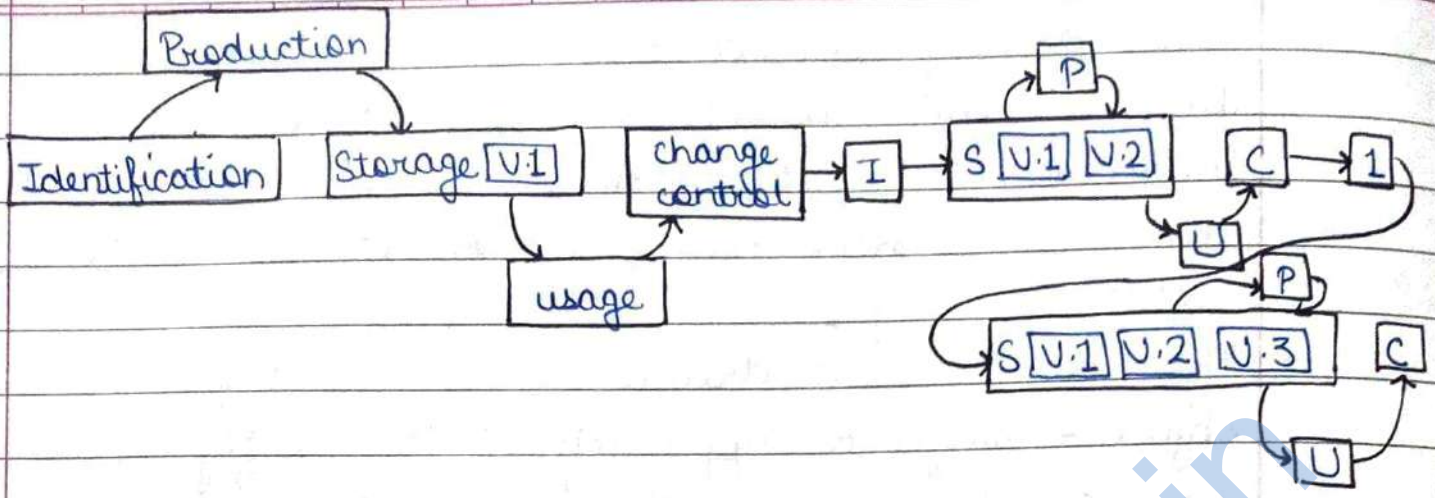
→ This can be illustrated by an analogy to an object - oriented approach. "The configuration item" may be seen as a class and the versions as instantiations of the class as shown in fig.

→ Version chains of configuration item i.e., versions 1, 2, 3 and so on may be formed by indicating which configuration item a given configuration item is derived from or based on.

→ Configuration management activities may be viewed as cyclic for each item class placed under configur-ation management. This means that a configuration item class continuously goes "through the mile."

→ The first cycle is initiated by a (planned) need for a configuration item, and later the driving force is change request (and only this!). This is illustrated in fig —





→ Configuration items are that are different versions of the same original item are obviously strongly related but each one is an individual item, which will be identified and may be extracted and used independ-ently. This is one of the main points of configurati-on management to be revert to an earlier version of an item class.

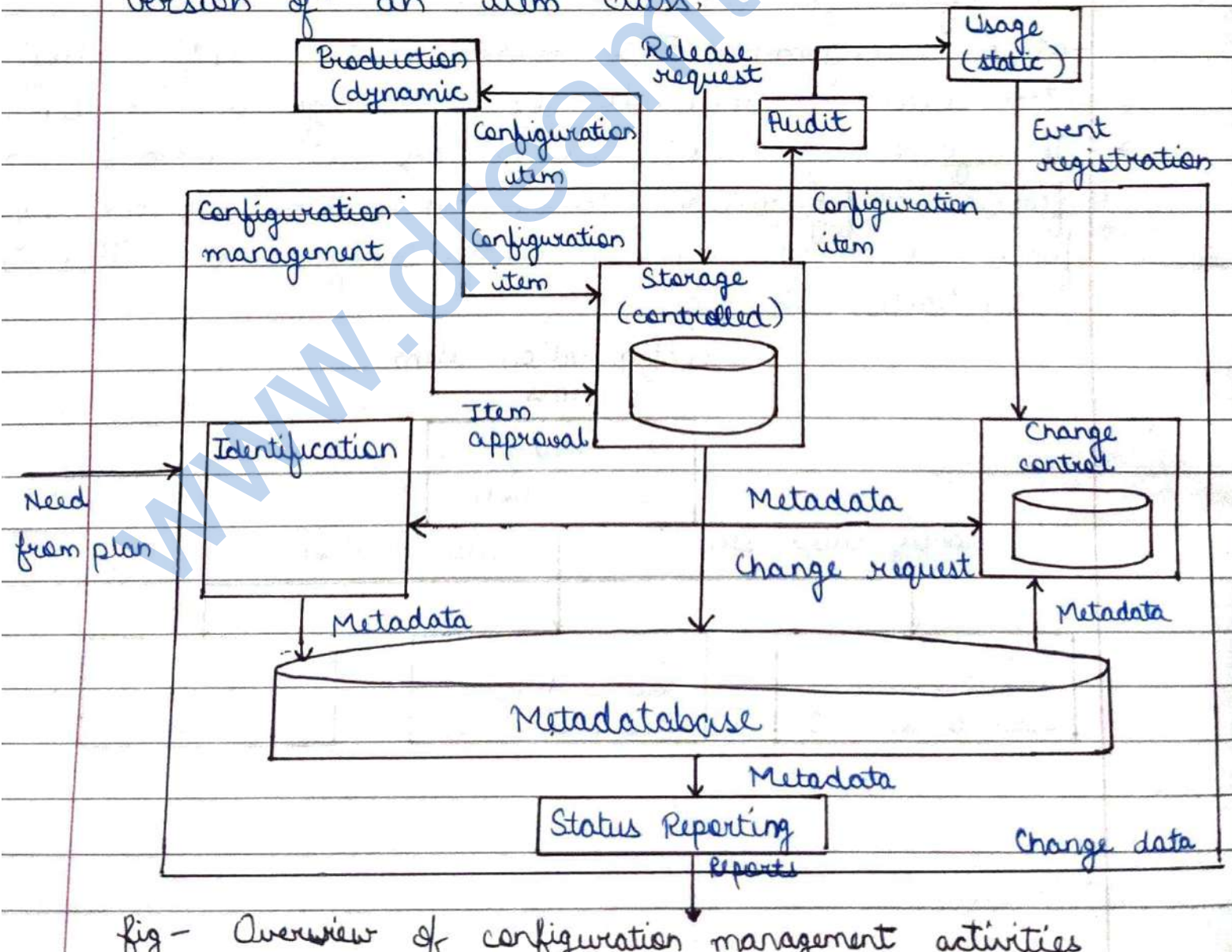


fig- Overview of configuration management activities

★ Virus :-

→ A virus is a piece of program code that attaches itself to legitimate program code and runs when the legitimate program runs. It can then infect other programs in that computer or in another computer in a same network.

→ Usually viruses cause damage to computer and network systems to the extent that it can be repaired assuming that the organisation deploys good backup and recovery procedures.

→ During its lifetime, a virus goes through four phases :-

(a) Dormant phase — Here, the virus is idle. It gets activated based on certain action or event. This is optional phase.

(b) Propagation phase — In this phase, a virus copies itself and each copy starts creating more copies of itself, thus propagating the virus.

(c) Triggering phase — A dormant virus moves into this phase when the action / event for which it was waiting is initiated.

(d) Execution phase — This is the actual work of the virus, which could be harmless or destructive.

★ Categories of Viruses :-

1- Parasitic virus — Such virus attaches itself to executable files and keeps replicating whenever files

the infected file is executed, the virus looks for other executable files to attach itself and spread.

2- Memory - Resident Virus — The virus first attach itself to an area of the main memory and then infects every executable program.

3- Boot Sector Virus — This virus infects the master boot record of disk and spread on the disk when operating system starts booting the computer.

4- Stealth Virus — This virus has intelligence built-in, which prevent anti-virus software program from detecting it.

5- Polymorphic Virus — A virus that keeps its signature on every execution, changing making it very difficult to detect.

6- Metamorphic Virus — In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

Q- What do you mean by firewalls? Discuss the need of firewall in VPN along with its types.

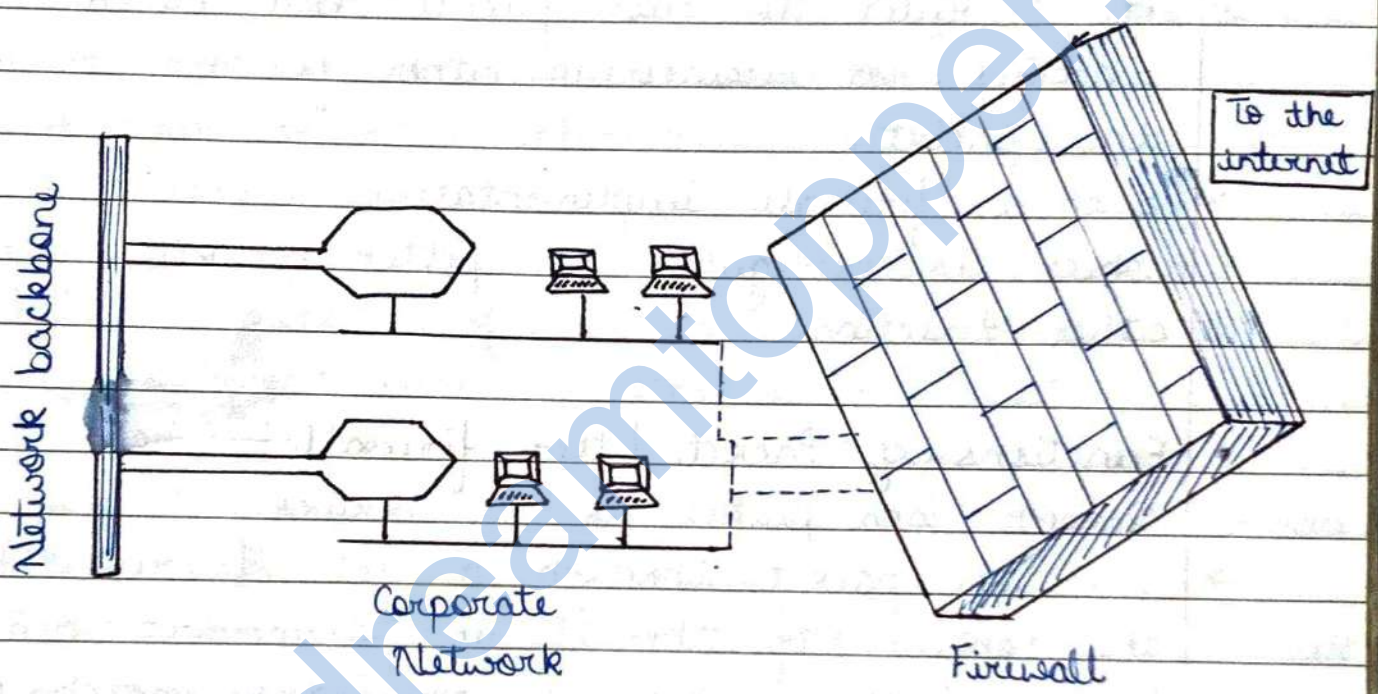
★ Firewall :-

→ A firewall acts like a sentry for a corporate network. Firewall stands between corporate network and the outside world and prevent the network from outsider's attack.

→ All the traffic between the network and the internet in either direction must pass through the firewall.

→ The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.

→ Technically, a firewall is a specialized version of router. Apart from a basic routing function and rules, a router can be configured to perform the firewall functionality with the help of additional software resources.



Characteristics of a good firewall :-

All traffic from inside to outside and vice-versa must pass through the firewall. To achieve this, all the access to the local network must first be physically blocked and access only via the firewall should be permitted.

→ Only the traffic, authorized as per the local security policy should be allowed to pass through.

→ The firewall itself must be strong enough so as to render attacks on it useless.
prevent

- Types of Firewall :- Depending on criteria used for filtering traffic, firewall are generally classified into two types -

(1.) Packet filter firewall
(2.) Application gateways firewall

1- Packet Filter Firewall — Packet filter also known as screening router or screening filter, applies a set of rules to each packet and based on the outcomes, it decides to either forward or discard the packet.

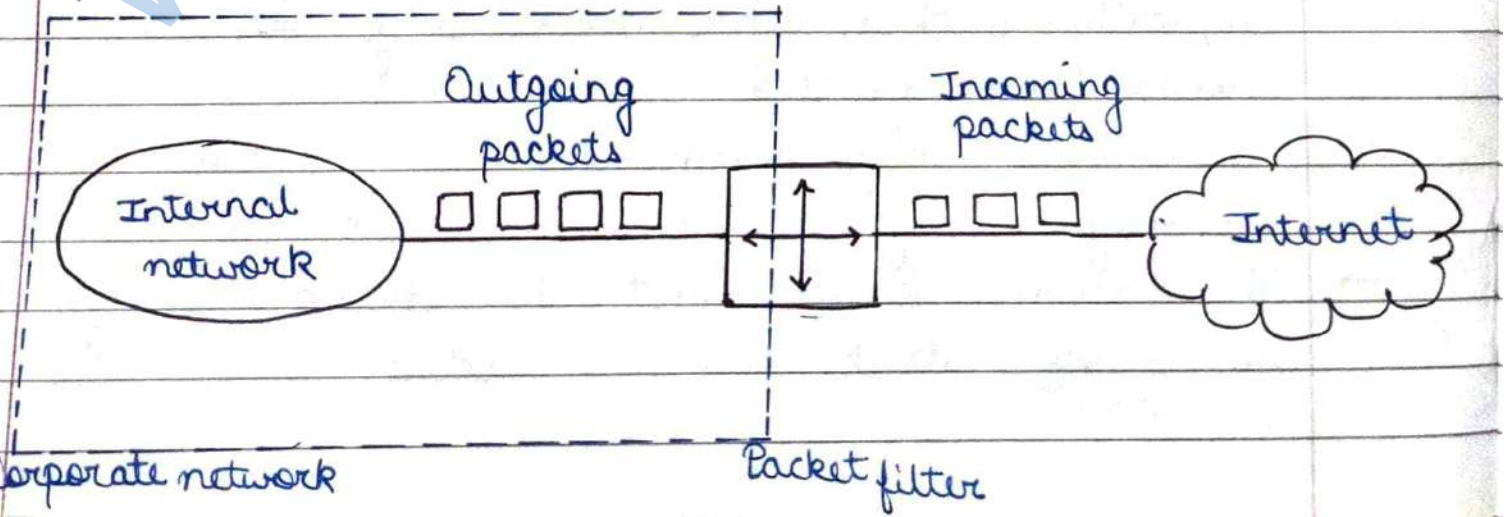
→ Such a firewall implementation involves a router, which is configured to filter packets going in either direction.

- Functions of Packet filter firewall —

→ Receive each packet as it arrives.

→ Pass the packet through a set of rules based on the contents of the IP and transport header fields of the packet. If there is match with one of the set of rules, decide whether to accept or discard the packet based on that rule.

→ If there is no match with any role, take the default action. The default action can discard all packets or accept all packets.



2- Application Gateways Firewall —

→ An application gateway is also called as a proxy server. This is because it acts like a proxy and decides about the flow of application level traffic.

→ An internal user contacts the application gateway using a TCP/IP application such as HTTP or TELNET.

→ The application gateway asks the user about remote host with which the user wants to set up a connection for actual communication.

→ The user provides information to the application gateway.

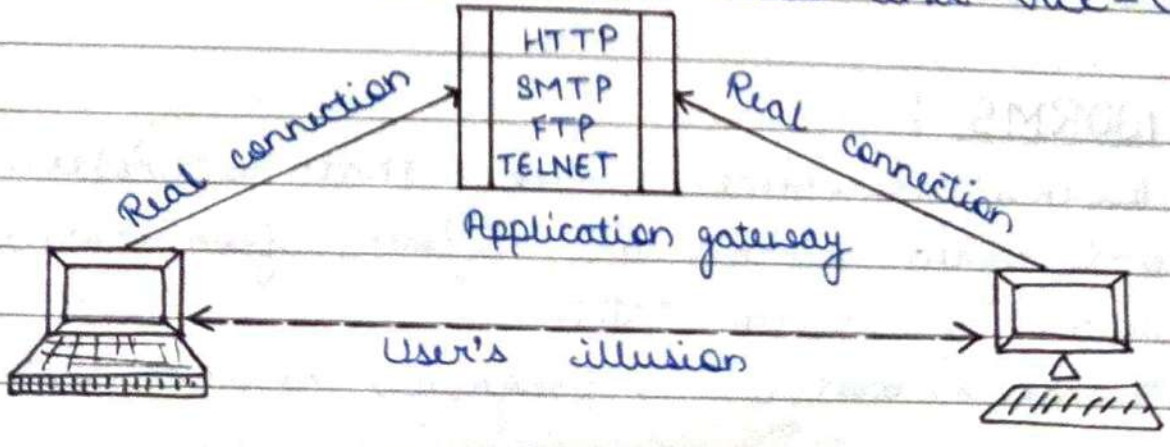
→ The application gateway now accesses the remote host on behalf of the user and passes the packets of the user to the remote host.

→ A variation of application gateway is called "circuit gateway", creates a new connection between itself and the remote host.

→ The circuit gateway changes the source IP address in the packets from the end user's IP address to its own.

→ This way, the IP addresses of computers of the internal users are hidden from outside world.

→ The application gateway acts like a proxy of the actual end-user and delivers packets from the user to the remote host and vice-versa.



★ Hardware Firewall :-

→ Hardware firewall is a stand alone product such as a broadband router.

→ It uses packet filtering as the method to transfer data. It compares the header of the packets and determines the destination and source address.

→ A hardware firewall is a device placed in between server computer and the internet. They are harder to configure than software firewalls.

→ Hardware firewall still protect the computer when the operating system crashes.

→ Hardware firewall does not consume CPU time and memory of server.

★ Software firewall :-

→ Software firewall are program based applications that run on a computer.

→ They work by monitoring all open ports on a computer and checking all the information that is received on them.

→ Software firewall is cheaper than a hardware firewall and easier to configure than hardware firewalls.

→ This firewalls consumes lot of memory and CPU time. It is not possible to protect whole network on single firewall.

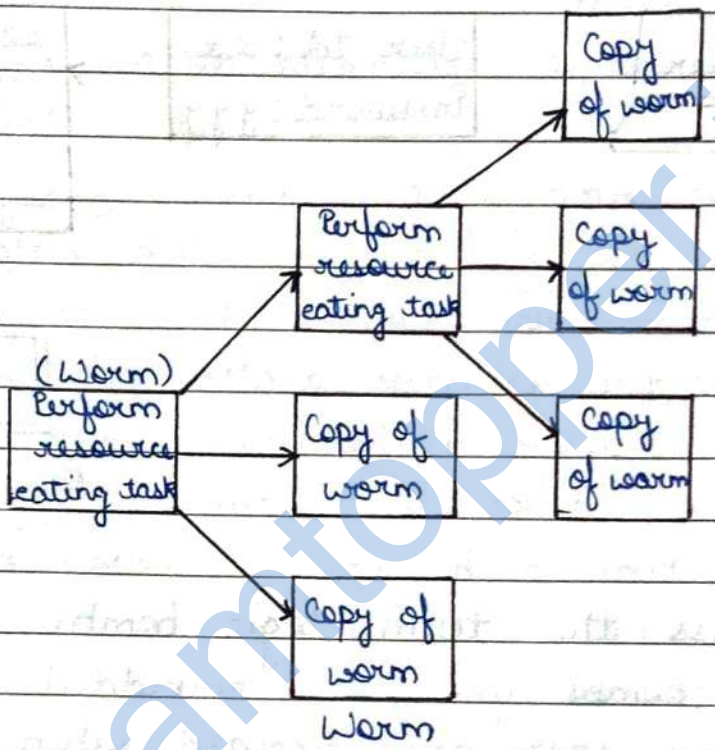
★ WORMS :-

1- Worms are piece of code that replicates itself again and again. Worms are different from viruses in terms of implementation.

2. A virus modifies a program, however a worm does

not modify a program.

3- A worm replicates so much itself that ultimately the computer or the network on which the worm resides become very slow, finally coming to a halt



4- Thus, the basic purpose of worm is different from virus. Virus used for destructive actions whereas worm does not perform any destructive action, only consumes system resources to make system unusable.

Ques – What is trojan horse?

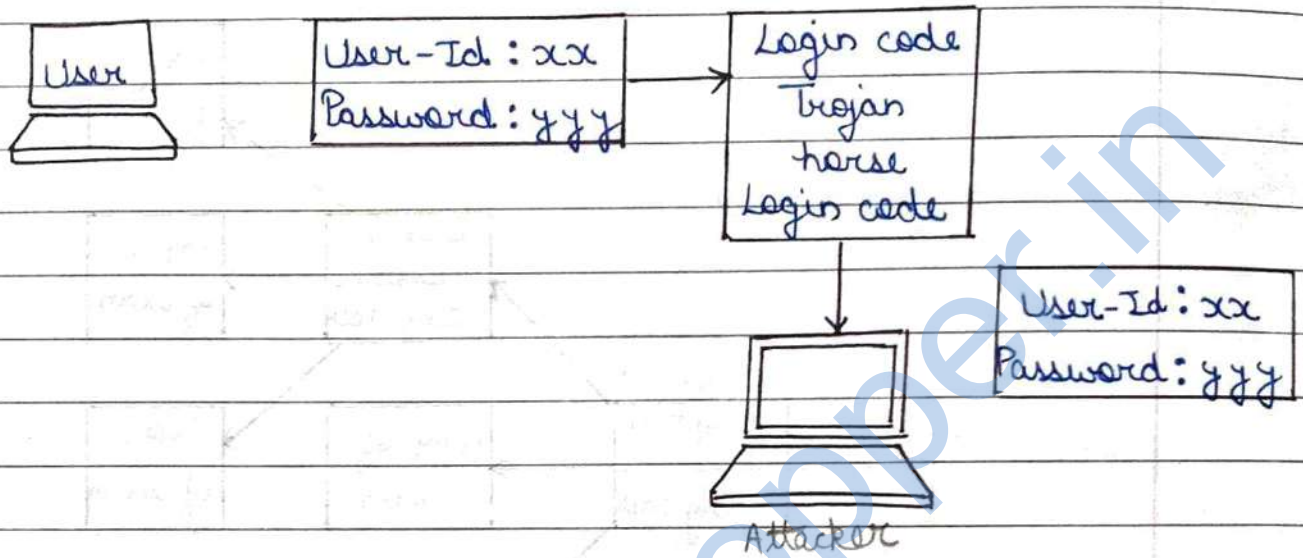
Ans – Trojan Horse :–

1- A trojan horse is a hidden piece of code, which allows attacker to obtain or reveal some confidential information about a computer or a network.

2- The name trojan horse is due to Greek soldiers, who hide inside a large hollow horse, which was pulled by Troy citizens and opened gates for rest of Greek soldiers.

3- In a similar way, trojan horse could attack to the

code of login screen. When user enters user id and password, the trojan could capture these details and send this information to attacker. Then attacker can use this information to gain access to the system.



Que- Discuss the term logic bomb.

Ans- Logic bombs are codes embedded in some legitimate program that are executed when a predefined event occurs.

2. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date or a particular user running the application.
3. These bombs display a message to the user and occur at time when either the user is accessing the internet or making use of a word processor application.
4. Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.
5. The logic bomb initiation is a four-step process-

(a) Attacker implants the logic bomb.
(b) Victim reports the installation.
(c) Attacker sends the attack message.

Ques- What is e-mail virus ?

Ans- 1- An e-mail virus is computer code sent as an e-mail note attachment which if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on hard disk and causing the attachment to be re-mailed to everyone in address book.

2- Although not the only kind of computer virus, e-mail viruses are the best known and undoubtedly cause the greatest loss of time and money overall.

3- The best two defenses against e-mail viruses for the individual user are—

(a) A policy of never opening (eg. double clicking on) an e-mail attachment unless you know who sent it and what the attachment contains.

(b) Installing and using antivirus software to scan any attachment before opening it.

Ques- What is macro virus ?

Ans- 1- A macro virus is a computer virus written in the same macro language used for software applications like word processors. It effects is to release a chain of events in conjunction with the application.

2- Microsoft word is an example of an application susceptible to macro viruses, this explains why it is a bad idea to open suspicious or unknown attachment even if they may appear legitimate.

3- Because macro programs embedded in these document run automatically when the document is opened, it is a likely mechanism to spread viruses.

4- Once triggered, the macro virus can embed itself in other documents including any future

documents created after the virus attack. as well as conceivably download software to the target computer.

5- Because a macro virus works using the application rather than an operating system, it can infect non windows computers as well.

6- Macro viruses are also known as script viruses and can also be embedded within web pages. The best defense against being infected by a macro virus, besides being very careful of what e-mail attachments you open, is having a quality updated antivirus.

Ques - What is malicious software or malware?

OR

Explain characteristics of malicious software (malware)

Ans- 1- Malicious software (malware) is any software that gives partial to full control of computer to do whatever the malware creator wants. Malware can be virus, worm, trojan etc.

2- Most malware requires the user to initiate its operation. Some vectors of attack include attachments in e-mails, browsing a malicious website that installs software after the user clicks OK on pop-up and from vulnerabilities in the operating system or programs.

Characteristics of malwares —

1- Self replicating malware actively attempts to propagate by creating new copies, or instances of itself. Malware may also be propagated passively by a user copying it accidentally, but this is not self

replication

2- The population growth of malware describes the overall change in the number of malware instance due to self replication.

3- Malware that does not self replicate will always have a zero population growth, but malware with a zero population growth may self replicate.

4- Parasitic malware requires some other executable code in order to exist. "Executable" in this context should be taken very broadly to include anything that can be executed such as boot block code on a disk, binary code.