TED (10)-4079/5059 Reg. No...........................

(REVISION-2010) Signature.........................

FIFTH/SIXTH SEMESTER DIPLOMA EXAMINATION IN ENGINEERING/ TECHNOLOGY-OCTOBER,2012

# INFORMATION SECURITY

[*Time:* 3 hours

(Maximum marks: 100)

Marks

## PART –A

(Maximum marks:10)

I Answer the following questions in one or two sentences. Each question carries 2 marks

**1. List the requirements of a message to be authentic.**

**Confidentiality**

Data confidentiality: Assures that confidential information is not disclosed to unauthorized individuals

Privacy: Assures that individual control or influence what information may be collected and stored

**Integrity**

Data integrity: assures that information and programs are changed only in a specified and authorized manner

System integrity: Assures that a system performs its operations in unimpaired manner

**Availabilit**y: assure that systems works promptly and service is not denied to authorized users

**2. State subjects and objects in connection with access control**

**A subject** is an entity capable of accessing objects, usually a process. Any user or application actually gains access to an object by means of a process that represents it. A subject is typically held accountable for the actions they have initiated, and an audit trail may be used to associate with a subject and security-relevant actions performed on an object.

**An object** is any resource to which access is controlled. In general, and object is an entity used to contain and/or receive information. Examples include records, blocks, pages, segments, files, portions of files, directories, directory trees, mailboxes, messages, and programs. The number and types of objects to be protected by an access control system depends on the environment in which access control.

3. **Describe hackers**
   Hacker is an individual or system who attempts to acquire information that should have been protected. In some cases, this information is in the form of a user password. With knowledge of some other user's password, an intruder can log in to a system and exercise all the privileges accorded to the legitimate user.
4. **Outline flooding**
   The aim of this attack is to overwhelm the capacity of the network connection to the target organization. If the attacker has access to a system with a higher capacity network connection, then this system can likely generate a higher volume of traffic than the lower capacity target connection can handle.
5. **Describe Bastion host**
   A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an application-level or circuit-level gateway

## PART—B

(Maximum marks:30)

**II Answer *any five* of the following. Each question carries 6 marks.**

1. **List and explain the computer system resources to be protected**

   **Data :** It is the information about users,system, data base etc.

   **Software**: It contains the operating systems informations and contents,the varieties of application software etc
   **Hardware:**The hardware components that needed to configure the system.
   **Communication medium:**The communication facilities and network components that is LAN, bridges, Routers, etc
2. **Describe the DES algorithm and specify an application.**

   The most widely used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the NIST, as FIPS PUB 46. The algorithm itself is referred to as the Data Encryption Algorithm (DEA). DES takes a plaintext block of 64 bits and a key of 56 bits, to produce a cipher text block of 64 bits. Concerns about the strength of DES fall into two categories: concerns about the algorithm itself and concerns about the use of a 56-bit key. The first concern refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm. Over the years, there have been numerous attempts to find and exploit weaknesses in the algorithm, making DES the most-studied encryption algorithm in existence. A more serious concern is key length. With a key length of 56 bits, there are $2^{56}$ possible keys, which is approximately $7.2 \times 10^{16}$ keys. As noted on the previous slide, this can now be broken relatively easily.

**3. Describe smart token authentication protocol.**

Objects that a user possesses for the purpose of user authentication are called tokens. Now examine two types of tokens that are widely used, which are cards that have the appearance and size of bank cards

- Embossed - Raised characters only, on front, e.g. Old credit card
- Magnetic stripe - Magnetic bar on back, characters on front, e.g. Bank card
- Memory - has Electronic memory inside, e.g. Prepaid phone card
- Smartcard - has Electronic memory and processor inside, e.g. Biometric ID card

**4. Summarize the different access control policies.**

An access control policy, which is embodied in an authorization database, dictates what types of access are permitted, under what circumstances, and by whom. Access control policies are generally grouped into the following access control categories:

• Discretionary access control (DAC): based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

• Mandatory access control (MAC): based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources).

• Role-based access control (RBAC): based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

**5. Describe methods of signature detection in IDS.**

Signature techniques detect intrusion by observing events in the system and applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious. In very general terms, we can characterize all approaches as focusing on either anomaly detection or penetration identification, although there is some overlap in these approaches.

Rule-based anomaly detection is similar in terms of its approach and strengths to statistical anomaly detection. With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. Rules may represent past behavior patterns of users, programs, privileges, time slots, terminals, and so on. Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.

Rule-based penetration identification takes a very different approach to intrusion detection. The key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.

**6. Describe types of audit records maintained for IDS.**

A fundamental tool for intrusion detection is the audit record. Some record of ongoing activity by users must be maintained as input to an IDS. Basically, two plans are used:

• Native audit records: Virtually all multi-user operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.

• Detection-specific audit records: A collection facility can be implemented that generates audit records containing only that information required by the IDS. One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two

**7. Illustrate application proxy firewall.**

- Examines packets and their contents at the Application Layer
- Can cause delay due to additional processing
- May strip info on internal servers, server version on outgoing messages (e.g., email)
- May allow only certain types of sessions through:
  - FTP: May permit receives, no sends.  Or sends of specific files only.
  - Email:  Encrypts email between all of company's offices
  - HTTP: May filter PUT commands, URL names.  Can cache replies.
- Authentication:  Perform extra authentication for external access (via dialup or internet)

## PART—C

**(Maximum marks:60)**

(Answer *one* full question from each unit. Each question carries 15 marks.)

UNIT--I

**III (a) State security implementation and describe different techniques. 9**

- **Prevention:** For the effective implementation of the computer security, it is needed to provide a good prevention method to prevent the overwhelm of the attacks.

  - **Detection:** to identify the weakness of the system and identify the point in which the system affected**.**
  - **Response:** To the quick response for the attack, some attack response plan is needed
  - **Recovery:** recovery strategies are needed when attacks affect
  - the assets of a computer system can be categorized as hardware, software, data, and communication lines and networks. We briefly describe these four categories and relate these to the concepts of integrity, confidentiality, and availability, as illustrated here in Figure 1.3.
  - **Hardware -** A major threat = is the threat to availability. Hardware is the most vulnerable to attack and the least susceptible to automated controls. Threats include accidental and deliberate damage to equipment as well as theft. Theft of CDROMs and DVDs can lead to loss of confidentiality. Physical and administrative security measures are needed to deal with these threats.
  - **Software -** includes the operating system, utilities, and application programs. A key threat is an attack on availability. Software is often easy to delete. Software can also be altered or damaged to render it useless. Careful software configuration management can maintain high availability. A more difficult problem is software modification (e.g. from virus/worm) that results in a program that still functions but that behaves differently than before, which is a threat to integrity/authenticity.
  - **Data -** involves files and other forms of data controlled by individuals, groups, and business organizations. Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously. The obvious concern with secrecy is the unauthorized reading of data files or databases. A less obvious secrecy threat involves the analysis of data and manifests itself in the use of so-called statistical databases, which provide summary or aggregate information. Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous.

•

**(b) List the requirements of hash function**. 6

- applied to any size data
- H produces a fixed-length output.
- H(*x*) is relatively easy to compute for any given *x*
- one-way property
  - computationally infeasible to find *x* such that H(*x*) = *h*
- weak collision resistance
  - computationally infeasible to find *y* ≠ *x* such that H(*y*) = H(*x*)
- strong collision resistance
  - computationally infeasible to find any pair (*x*, *y*) such that H(*x*) = H(*y*)

**OR**

**IV (a) Describe any five challenges of computer security. 10**

**1**. Computer security is not as simple as it might first appear to the novice. The requirements seem to be straightforward, but the mechanisms used to meet those requirements can be quite complex and subtle.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks (often unexpected) on those security features.

3. Hence procedures used to provide particular services are often counterintuitive.

4. Having designed various security mechanisms, it is necessary to decide where to use them.

5. Security mechanisms typically involve more than a particular algorithm or protocol, but also require participants to have secret information, leading to issues of creation, distribution, and protection of that secret information.

**IV (b) List and explain the requirements for symmetric encryption 5**

- Plaintext: This is the original message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key: The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

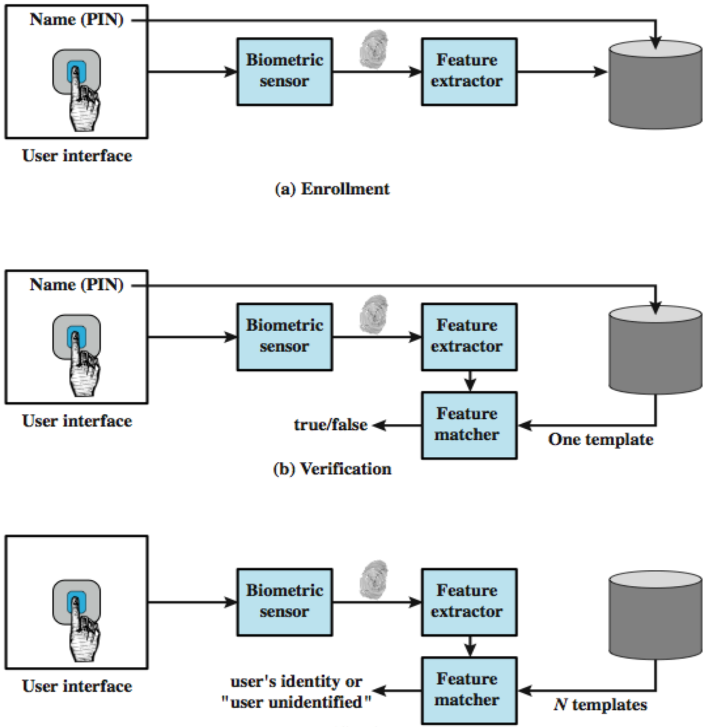
• Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm.
2. Sender and receiver must have secure obtained, & keep secure, the secret key.

## UNIT--II

**V Illustrate the user identification stage in a biometric authentication system. 15**



(a) Enrollment

(b) Verification

(c) Identification

Each individual who is to be included in the database of authorized users must first be enrolled in the system. This is analogous to assigning a password to a user .For a biometric system, the user presents a name and, typically, some type of password or PIN to the system. At the same time the system senses some biometric characteristic of this user (e.g. fingerprint of right index finger). The system digitizes the input and then extracts a set of features that can be stored as a number or set of numbers representing this unique biometric characteristic ;this set of numbers is referred to as the user's template. The user is now enrolled in the system, which maintains for the user a name (ID), perhaps a PIN or password, and the biometric value. Depending on application, user authentication on a biometric system involves either verification or identification. Verification is analogous to a user logging on to a system by using a memory card or smart card coupled with a password or PIN. For biometric verification, the user enters a PIN and also uses a biometric sensor. The system extracts the corresponding feature and compares that to the template stored for this user. If there is a match, then the system authenticates this user. For an identification system, the individual uses the biometric sensor but presents no additional information. The system then compares the presented template with the set of stored templates. If there is a match, then this user is identified. Otherwise, the user is rejected.

**OR**

**VI (a) Describe the discretionary access control.** **9**

For discretionary access control, a general approach to access control as exercised by an operating system or a database management system is that of an access matrix. One dimension of the matrix consists of identified subjects that may attempt data access. Typically, this list will consist of individual users or user groups, although access could be controlled for terminals, hosts, or applications instead of or in addition to users. The other dimension lists the objects that may be accessed. At the greatest level of detail, objects may be individual data fields. More aggregate groupings, such as records, files, or even the entire database, may also be objects in the matrix. Each entry in the matrix indicates the access rights of that subject for that object. In practice, an access matrix is usually sparse and is implemented by decomposition in one of two ways
The matrix may be decomposed by columns, yielding **access control lists** (ACLs);

- For each object, an ACL lists users and their permitted access rights. The ACL may contain a default, or public, entry. This allows users that are not explicitly listed as having special rights to have a default set of rights. Elements of the list may include individual users as well as groups of users. When it is desired to determine which subjects have which access rights to a particular resource, ACLs are convenient, because each ACL provides the information for a given resource. However, this data structure is not convenient for determining the access rights available to a specific user.

Decomposition by rows yields **capability tickets**, shown in Figure 4.3c. A capability ticket specifies authorized objects and operations for a user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists. In particular, the ticket must be unforgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets would have to be held in a region of memory inaccessible to users. The convenient and inconvenient aspects of capability tickets are the opposite of those for ACLs. It is easy to determine the set of access rights that a given user has, but more difficult to determine the list of users with specific access rights for a specific resource.

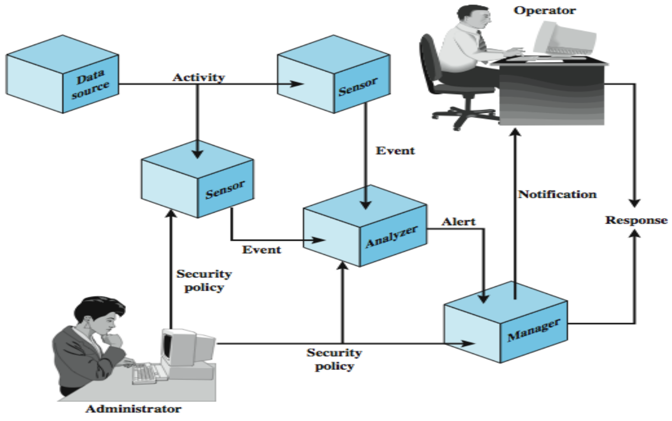
**VI (b) Describe the means of user authentication** **6**

There are four general means of authenticating a user's identity, which can be used alone or in combination:

• Something the individual knows: Examples includes a password, a personal identification number (PIN), or answers to a prearranged set of questions.
• Something the individual possesses: Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a *token*.
• Something the individual is (static biometrics): Examples include recognition by fingerprint, retina, and face.
• Something the individual does (dynamic biometrics): Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.
All of these methods, properly implemented and used, can provide secure user authentication. However, each method has problems. An adversary may be able to guess or steal a password. Similarly, an adversary may be able to forge or steal a token. A user may forget a password or lose a token. Further, there is a significant administrative overhead for managing password and token information on systems and securing such information on systems. With respect to biometric authenticators, there are a variety of problems, including dealing with false positives and false negatives, user acceptance, cost, and convenience.

## UNIT III

**VII(a) Describe the functional components of an intrusion detection message exchange** **9**



. This model does not correspond to any particular product or implementation, but its functional components are the key elements of any IDS. The specification defines formats for event and alter messages, message types, and exchange protocols for communication of intrusion detection information. The functional components are as follows:

- Data source: raw data an IDS uses to detect unauthorized or undesired activity
- Sensor: collects data from the data source & forwards events to the analyzer
- Analyzer: process analyzing data collected for unauthorized/undesired activity

- Administrator: human with overall responsibility for setting security policy of org
- Manager: process from which operator manages components of ID system
- Operator: human that is the primary user of the IDS manager

The sensor monitors data sources looking for suspicious activity. The sensor communicates suspicious activity to the analyzer as an event. If the analyzer determines that the event is of interest, it sends an alert to the manager component. The manager component issues a notification to the human operator. A response can be initiated automatically by the manager component or by the human operator. The security policy is the predefined, formally documented statement that defines what activities are allowed to take place.

**VII (b) List the Snort header elements. 6**

Snort uses a simple, flexible rule definition language that generates the rules used by the detection engine. Although the rules are simple and straightforward to write, they are powerful enough to detect a wide variety of hostile or suspicious traffic. Each rule consists of a fixed header and zero or more options. The header includes:

- Action: tells Snort what to do when it finds a packet that matches the rule criteria (alert, log, pass, activate, dynamic, drop, reject, drop)
- Protocol: if packet protocol matches this field then analysis proceeds
- Source IP address: source of packet
- Source port: for the specified protocol (e.g.,a TCP port).
- Direction: unidirectional (->) or bidirectional (<->).
- Destination IP address: destination of packet.
- Destination port

Following the rule header may be one or more rule options. Each option consists of an option keyword, which defines the option; followed by arguments, which specify the details of the option. Table 6.5 in the text gives examples of options in each category. The example shown of a Snort rule checks detects a type of attack at the TCP level known as a SYN-FIN attack. It has specified source and destination networks, and checks if the SYN and the FIN bits are set, ignoring reserved bit 1 and reserved bit 2 in the flags octet.

**OR**

**VIII (a) Describe Virus and explain its different phases. 9**

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. A virus can do anything that other programs do. The difference is that a virus attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs. Most viruses carry out their work in a manner that is specific to a particular operating system and, in some cases, specific to a particular hardware platform. Thus, they are designed to take advantage of the details and weaknesses of particular systems. During its lifetime, a typical virus goes through the following four phases:

• Dormant phase: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

• Propagation phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

• Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

• Execution phase: The function is performed, which may be harmless, e.g. a message on the screen, or damaging, e.g. the destruction of programs and data files

**VIII (b) Describe the operation of a behavior blocking software. 6**

Unlike heuristics or fingerprint-based scanners, behavior-blocking software integrates with the operating system of a host computer and monitors program behavior in real-time for malicious actions. The behavior blocking software then blocks potentially malicious actions before they can affect the system. Monitored behaviors can include

• Attempts to open, view, delete, and/or modify files;

• Attempts to format disk drives and other unrecoverable disk operations;

• Modifications to the logic of executable files or macros;

• Modification of critical system settings, such as start-up settings;

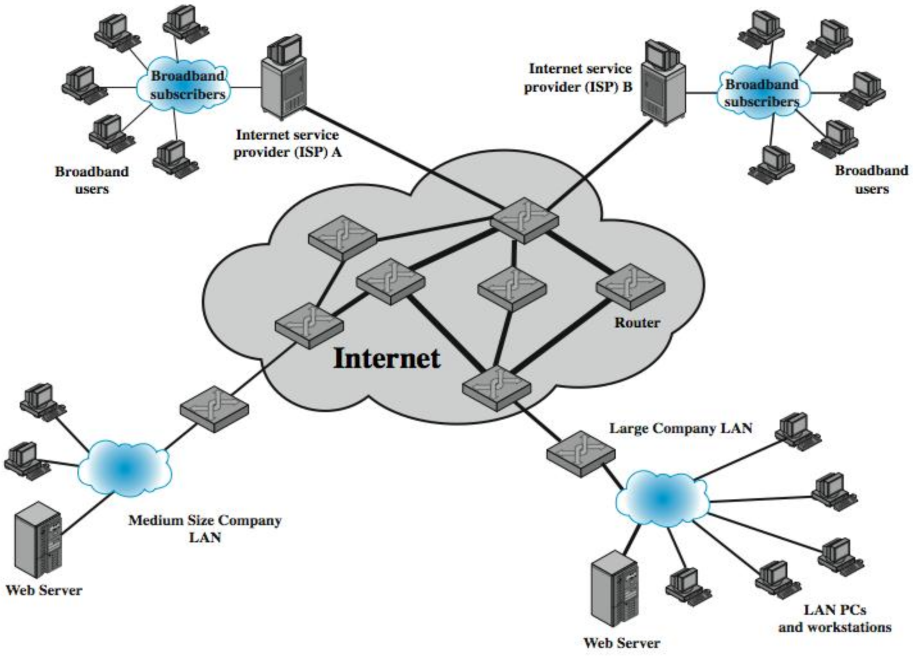
• Scripting of e-mail and instant messaging clients to send executable content; and

• Initiation of network communications.

Figure 7.5 illustrates its operation. Behavior-blocking software runs on server and desktop computers and is instructed through policies set by the network administrator to let benign actions take place but to intercede when unauthorized or suspicious actions occur. The module blocks any suspicious software from executing. A blocker isolates the code in a sandbox, which restricts the code's access to various OS resources and applications. The blocker then sends an alert. Because behavior blocker can block suspicious software in real-time, it has an advantage over such established antivirus detection techniques as fingerprinting or heuristics. Behavior blocking alone has limitations. Because the malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked.

## UNIT IV

**IX (a) Describe denial of service attack architecture 9**



**.** Denial of service is a form of attack on the availability of some service. In the context of computer and communications security, the focus is generally on network services that are attacked over their network connection. From this definition you can see that there are several categories of resources that could be attacked:

- network bandwidth - relates to the capacity of the network links connecting a server to the wider Internet
- system resources - typically aims to overload or crash its network handling software
- application resources - aim to overload the capabilities of a server and limit its ability to respond to requests from other users

Denial of Service attacks have been a problem for many years. The 2006 CSI/FBI Computer Crime and Security Survey states that 25% of respondents experienced some form of denial of service attack in the previous 12 months. This value has varied between 25% and 40% over the previous 8 years of surveys.

**IX(b) Describe the capabilities of firewalls 6**

The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management.
2. A firewall provides a location for monitoring security-related events.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator (NAT),, and a network management function that audits or logs Internet usage.

4. A firewall can act as the platform for IPSec to implement virtual private networks.

**OR**

**X (a) Describe the counter measures of DDoS attacks. 9**

There are a number of steps that can be taken to both limit the consequences of being the target of a denial of service attack, and also to limit the chance of your systems being compromised and then used to launch denial of service attacks. It is important to recognize that these attacks cannot be prevented entirely, as high traffic volumes may sometimes occurs by accident as a result of high publicity about a specific site, or due to extreme popularity of a site, e.g. a posting to the well-known “Slashdot” news aggregation site often results in overload of the referenced server system. Similarly, when popular sporting events like the Olympics or Soccer World Cup matches occur, sites reporting on them experience very high traffic levels. Also if an attacker can direct a large enough volume of legitimate traffic to your system, then there is a high chance this will overwhelm its network connection, and thus limit legitimate traffic requests from other users. There is very little that can be done to prevent this type of either accidental or deliberate overload, without also compromising network performance. The provision of significant excess network bandwidth and replicated distributed servers is the usual response, particularly when the overload is anticipated.

In general, there are three lines of defense against DDoS attacks:

- Attack prevention and preemption (before the attack): These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients.
- Attack detection and filtering (during the attack): These mechanisms attempt to detect the attack as it begins and respond immediately.

- Attack source traceback and identification (during and after the attack): This is an attempt to identify the source of the attack as a first step in preventing future **attacks.**

**X (b) Describe host-based firewall and personal firewall** **6**

- **Host-Based Firewalls**
- often used on servers
- used to secure individual host
- available in/add-on for many O/S
- filter packet flows
- advantages:
    - taylored filter rules for specific host needs
    - protection from both internal / external attacks
    - additional layer of protection to org firewall
    - **Personal Firewall**
    - controls traffic flow to/from PC/workstation
    - for both home or corporate use
    - may be software module on PC
    - or in home cable/DSL router/gateway
    - typically much less complex
    - primary role to deny unauthorized access
    - may also monitor outgoing traffic to detect/block worm/malware activity
    -