Unit V

5 Firewall and Intrusion

Syllabus

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS: Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

Contents

5.1 Introduction

- An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Three classes of intruders are Masquerader, Misfeasor, and Clandestine user.
  1. **Masquerader** : An unauthorized user who penetrates a computer system's access control and gains access to user accounts.
  2. **Misfeasor** : A legitimate user who accesses resources he is not authorized to access. Who is authorized such access but misuses his privileges.
  3. **Clandestine user** : A user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Intrusion techniques

- **Objective :** An intruder wants to gain access to a system.
- Access is generally protected by passwords. System maintains a file that associates a password with each authorized user.
- Password file can be protected with : **One-way encryption and access control**
  1. **One way function :** A system stores passwords only in encrypted form. When 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 very few people.

Techniques for guessing passwords

1. Try default passwords. (Used with standard accounts that is shipped with systems.)
2. Try all short words, 1 to 3 characters long.
3. Try all the words in an electronic dictionary.
4. Collect information about the user's hobbies, family names, birthday, etc.
5. Try user's phone number, social security number, street address, etc.
6. Try all license plate numbers (AP 12 AA 4453).
7. Use a trojan horse.
8. Tap the line between a remote user and the host system.

5.2 Computer Intrusions

- Computer intrusions occur when someone tries to gain access to any part of your computer system.
- Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security.
- A computer intrusion is a set of actions that violate the security of a system. Such a situation must be detected and corrected in order to guarantee the integrity, confidentiality and/or availability of computing resources.
- There are two basic intrusion detection systems : misuse detection and anomaly detection. Misuse detection systems attempt to match computer activities with previously known attacks in their database.
- An important draw-back of this type of system is that it can only detect known attacks, so attacks that are not stored or variants of stored attacks will not be detected.
- Anomaly detection systems learn the normal activity of the system and attempt to detect any computer activity that deviates from normal patterns.

5.3 Firewall Introduction

- Information systems in an organization have changed vary rapidly over the years from centralized data processing, LANs, WANs and Internet connectivity.
- The Internet connectivity is essential for the organization enabling access to outside world. Also it is a threat to the organization if not secured from intrusions (unauthorized access/users).
- A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.
- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. 5.3.1.

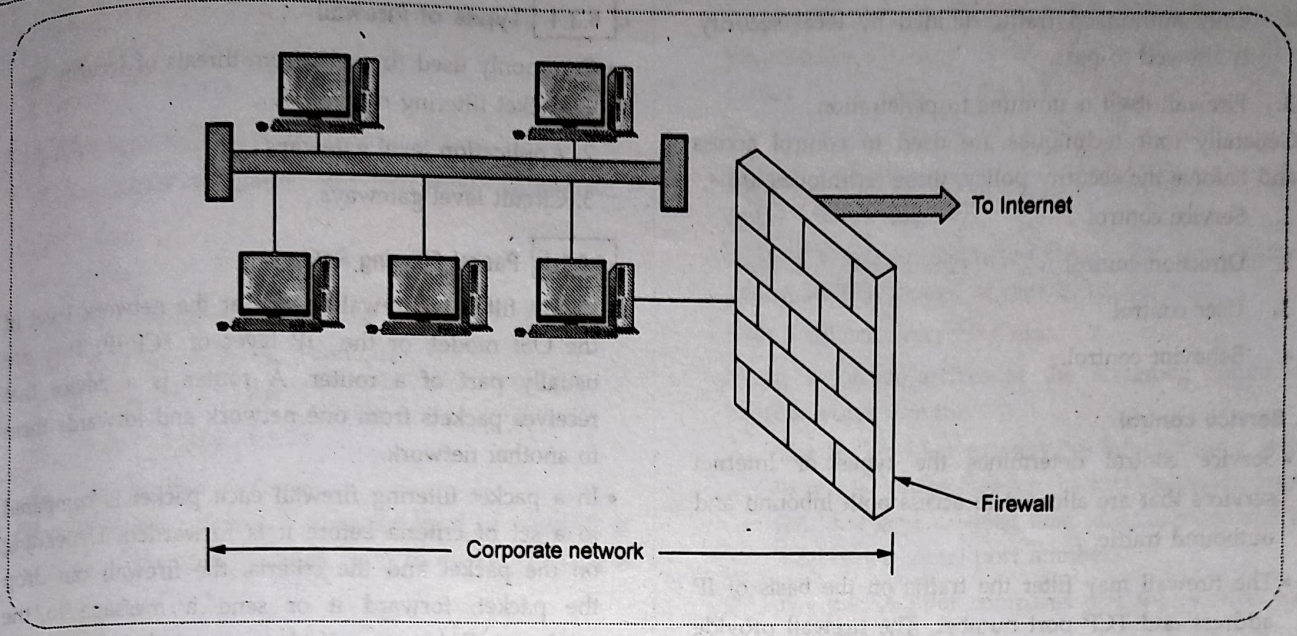

Fig. 5.3.1 Firewall

- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.
- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as **address filtering**.
- Firewalls can also filter specific types of network called **protocol filtering** because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP,FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state.

Limitations of firewall

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

Firewall technology

- Firewall technology generally falls into one of the two categories. Network level and application level.

1. Network level

This guards the entire network from unauthorised intrusion. An example of this technology is packet filtering, which simply reviews all information coming into a network and rejects the data that does not meet a predefined set of criteria.

2. Application level

This technology controls access on an application by application basis. For example, proxy servers can be set up to permit access to some application, such as HTTP, while blocking access to others, such as FTP.

Design goals

- Firewalls are very effective means for network based security threats. The design goals for firewall are as under

1. All the traffic must pass through firewall both from inside to outside and outside to inside.

2. Only authorized traffic defined by local security is allowed to pass.
3. Firewall itself is immune to penetration.

- Generally four techniques are used to control access and enforce the security policy, these techniques are -
  1. Service control
  2. Direction control
  3. User control
  4. Behavior control.

1. Service control

- Service control determines the types of Internet services that are allowed to access both inbound and outbound traffic.
- The firewall may filter the traffic on the basis of IP address and TCP port number. The firewall provide proxy software to receive and interpret each service request before passing it on.

2. Direction control

- Direction control determines the direction in which particular service requests may be initiated and is allowed to flow through the firewall.

3. User control

- User control gives access to a service according to which user is attempting to access it. This feature is usually applied for local user inside the firewall perimeter.

4. Behavior control

- Behavior control allows to control the use of any particular service. For example, the firewall may filter e-mails to eliminate spam.

5.3.1 Types of Firewall

- Commonly used firewalls from threats of security are
  1. Packet filtering router
  2. Application level gateways
  3. Circuit level gateways.

5.3.1.1 Packet Filtering Router

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network.
- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used.
- The advantage of packet filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer. This type of firewall only works at the network layer however and does not support sophisticated rule based models. Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit based filtering.
- Packet filtering router applies rule to each incoming and outgoing IP packet, according forward or discards it. Fig. 5.3.2 shows packet filtering router.

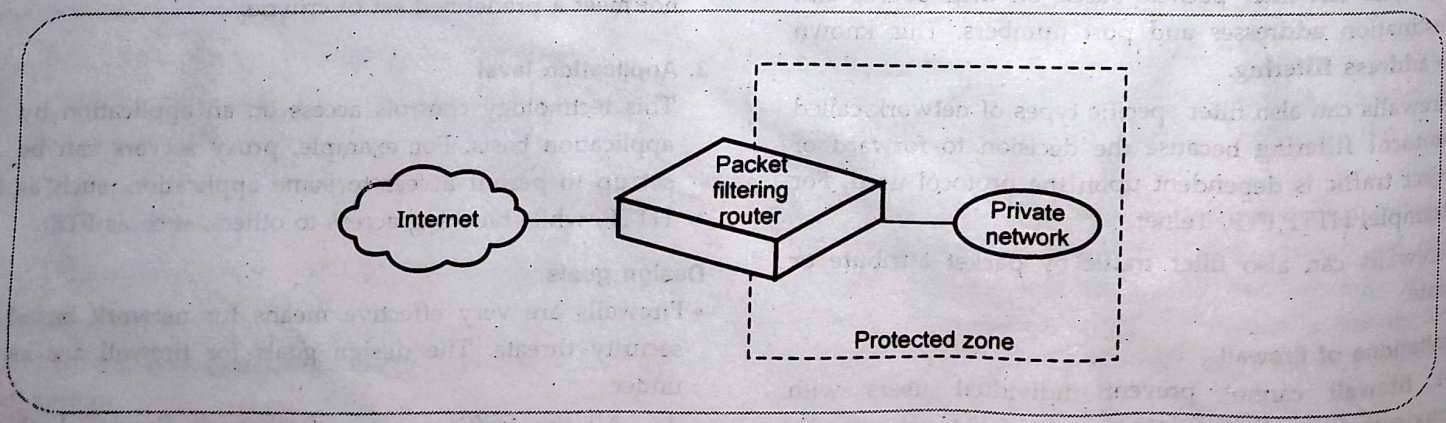

Fig. 5.3.2 Packet filtering router

- Filtering rules are based on information contained in the network packet such as
  i. Source IP address
  ii. Destination IP address
  iii. Source and destination transport level address.
  iv. IP field.
  v. Interface
- Attackers can try and break the security of the packet filter by using following techniques.
  i. IP address spoofing
  ii. Source routing attacks
  iii. Tiny fragment attacks
- Packet filtering provides a useful level of security at low cost. The type of router used in packet filtering is a screening router.

Screening router

- Each packet has two parts : The data that is part of the document and a header. If the packet is an envelope, then the data is the letter inside the envelope and the header is the address information on the outside.
- Here packet filter to refer to the technology or the process that is taking place and the screening router to refer to the thing that's doing it.
- Screening router can be a commercial router or a host-based router with some kind of packet filtering capability. Typical screening routers have the ability to block traffic between networks or specific hosts, on an IP port level. Some firewalls consist of nothing more than a screening router between a private network and the Internet.
- Screening routers operate by comparing the header information with a table of rules set by the network administrator to determine whether or not to send the packet on to its destination. If there is a rule that does not allow the packet to be sent on, the router simply discards it.

Working of packet filters

- Packet filters work by dropping packets based on their source and destination addresses or ports. Configuring a packet filter is a three step process. First of course, one must know what should and what should not be permitted. Next, the allowable types of packets must be specified, in terms of lofical expression on packet fileds. Finally the expression should be rewritten in whatever syntax your vendor supports.
- In general, for each packet, the router applies the rules sequentially, starting with the first one, until the packet fits or until it runs out of rules.
- For examples a router has 3 rules in its table.
- **Rule 1 :** Don't allow packets from a particular host, called TROUBLEHOST.
- **Rule 2 :** Let in connections into out mail gateway (using SMTP), located at port 25 on out host.
- **Rule 3 :** Block everything else.
- When a packet arrives at the screening router, the process works like this
  1. The packet filter extracts the information it needs from the packet header. In this example, it uses the local and external host identification and the local and external port numbers.
  2. The packet filter compares that information with the rules in the table.
  3. If the packet is from TROUBLEHOST, no matter what its destination, discard it.
  4. If the packet makes it past the first rule i.e. it's not from TROUBLEHOST, check to see if it's intended for port 25 on out SMTP-Mail host. If it is, send it on ; otherwise, discard it.
  5. If neither of the first two rules apply, the packet is rejected by rule three.
- Every packet has a set of headers containing certain information. The information is
  * IP source address.
  * IP destination address.
  * Protocol (whether the packet is a TCP, UDP or ICMP packet).
  * TCP or UDP source port.
  * TCP or UDP destination port.
  * TCP ack flag.

1. Inspection module

- If the header information listed above doesn't give you enough elements for setting up rules, you can use a packet filter that has an inspection module. An inspection module looks at more of the header information ; some can even look at the application data itself. For example, by inspecting the application data, the module can deny packets the contain certain application commands, such as the FTP put command or the SNMP set command.

2. State evaluation

- The header of a TCP packet contains an indicator called the ACK flag. When the ACK flag is set, it means that the incoming packet is a response to an earlier outgoing packet. If the flag is not set, the packet is not a response to an earlier outgoing packet, and therefore is suspect. It's common to set a screen rule to allow incoming packets that have the ACK flag set and reject those that don't. UDP doesn't use an ACK flag or any other similar indicator, so there's no way for the screening router to know whether an incoming packet was sent in response to an outgoing packet. The only safe thing to do in that situation is to reject the packet.
- That's where state evaluation comes in a screening router that has the state evaluation capability, "remembers" the original outgoing packet for a certain length of time (set by system administrator).

Advantages of packet filters

1. Low impact on network performance.
2. Packet filters are normally transparent to user.
3. Relatively inexpensive price.

Disadvantages of packet filtering firewall

1. They are vulnerable to attacks aimed at protocol higher than the network layer protocol.
2. They cannot hide the network topology.
3. Packet filtering firewall can not support all Internet applications.
4. These firewalls have very limited auditing capabilities.
5. Sometimes user level authentication do not supported by packet filtering firewall.

5.3.1.2 Application Level Gateways

- Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot access services for which there is no proxy. In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet or other traffic through. Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.
- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer.

Fig. 5.3.3 shows application level gateway.

Advantages

1. Application gateway provides high level of security than packet filters.
2. Easy to configure.
3. They can hide the private network topology.
4. It support user level authentication.
5. Capability to examine the all traffic in detail.

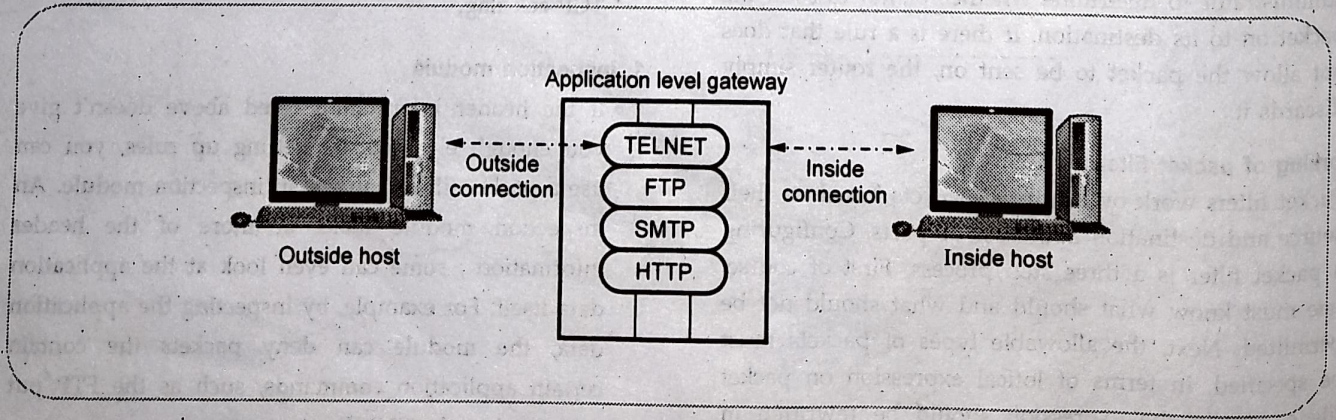

Fig. 5.3.3 Application gateway

Disadvantages

1. High impact on network performance.
2. Slower in operation because of processing overheads.
3. Not transparent to users.

5.3.1.3 Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

5.3.1.4 Comparison between Packet Filter and Proxies

Sr. No.	Packet filter	Proxy (Application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI, TCP layer of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level of security as compare to proxi.	High level of security.
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower than packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure than packet filtering.
8.	They cannot hide the private network topology.	They can hide the private network topology.

5.3.2 Firewall Location

1. DMZ network (Demilitarized Zone)
2. Virtual Private Network (VPN)
3. Distributed firewall

- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

1. DMZ Network (Demilitarized Zone)

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network, hosts in the DMZ may not connect to the internal network.
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.

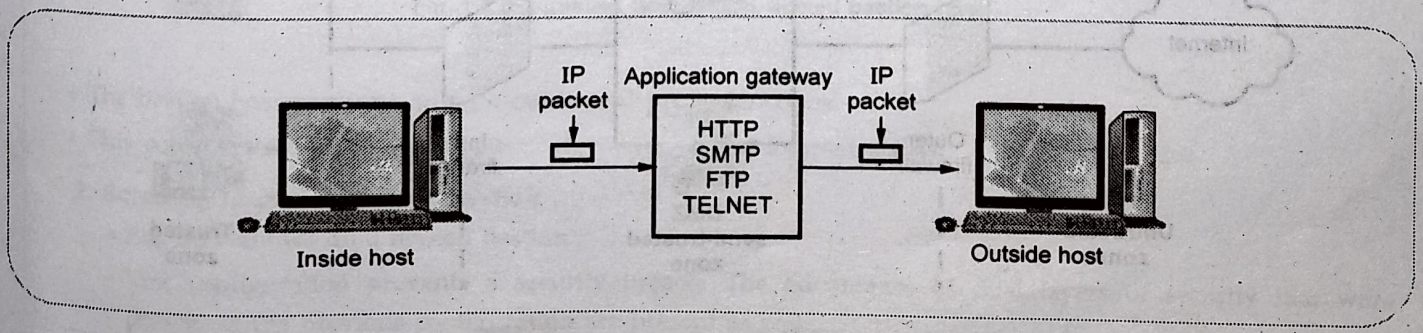

Fig. 5.3.4 Circuit gateway

- Fig. 5.3.5 shows DMZ network.
- Traffic from the Internet is filtered, but some of it is allowed to reach systems in the DMZ i.e. like web servers and mail servers. If an attacker succeeds in breaking into a system in your DMZ, they won't gain access to your internal network as traffic coming from the DMZ is filtered before being allowed into the internal network.
- To create a DMZ, you can use two firewalls. Our illustration shows an outer firewall that separates the DMZ from the Internet and an inner firewall that separates the DMZ from the internal network. The outer firewall controls the traffic from the Internet to the DMZ. The inner firewall controls traffic from the DMZ to the internal network.
- The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network.
- Internal firewalls serve three purposes :
  i. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
  ii. The internal firewall provides two-way protection with respect to the DMZ.
  iii. Multiple internal firewalls can be used to protect portions of the internal network from each other.

2. Virtual Private Networks (VPN)

- Virtual Private Networks (VPN) provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.
- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

3. Distributed Firewall

- A distributed firewall configuration involves stand-alone firewall devices plus host based firewalls working together under a central administrative control. Security policy is defined centrally and enforcement of policy is done by network endpoint(s).
- Administrators can configure host resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.

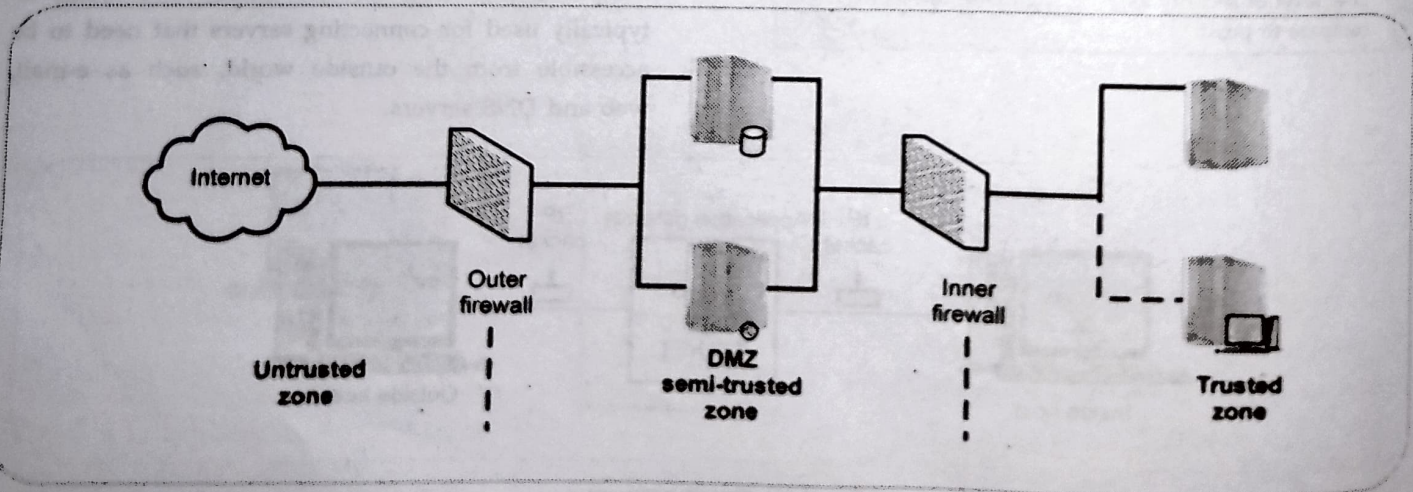

Fig. 5.3.5 DMZ network

- Tools let the network administrator set policies and monitor security across the entire network. These firewalls protect against internal attacks and provide protection tailored to specific machines and applications. Stand-alone firewalls provide global protection, including internal firewalls and an external firewall.

5.3.3 Firewall Configuration

- Firewall configuration are of three types :
  1. Screened host, single homed bastion host
  2. Screened host, dual homed bastion host
  3. Screened subnet.

1. Screened host, single homed bastion host

- In this system, firewall consists of two systems : A packet filtering router and a bastion host.
- The router is configured so that,
  1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
  2. For traffic from the internal network, only IP packets from the bastion host are allowed out.
- Fig. 5.3.6 shows screened host, single homed bastion host.

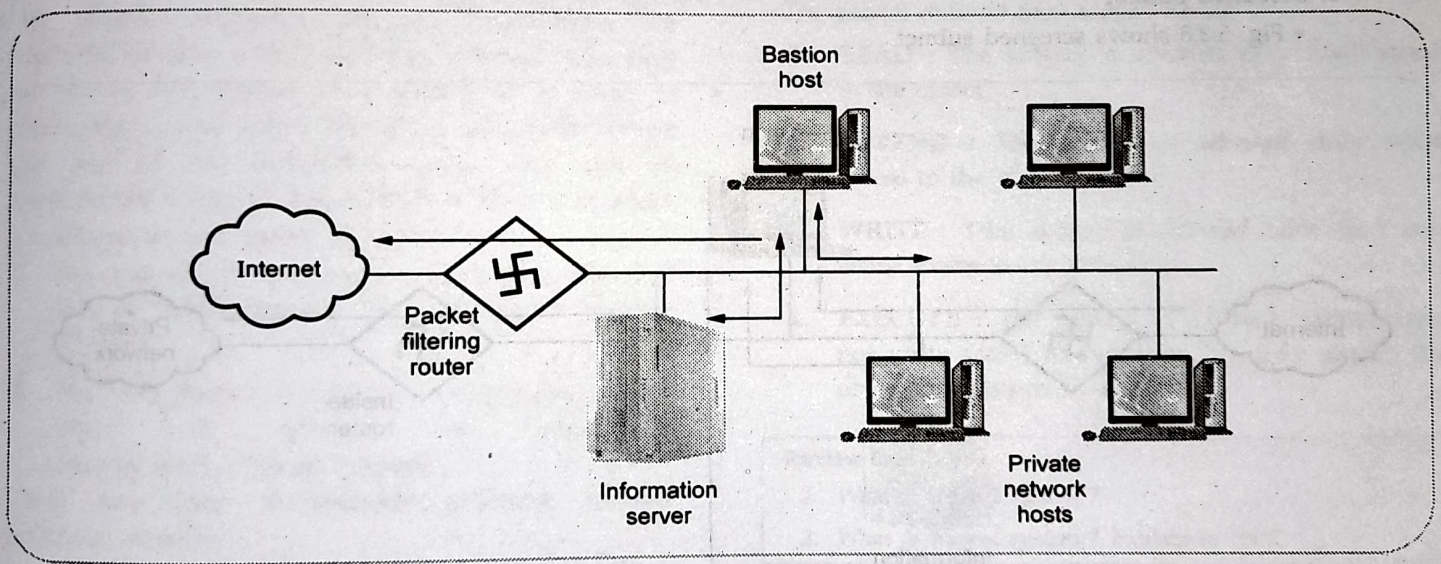

Fig. 5.3.6 Screened host, single homed bastion host

- The bastion host performs authentication and proxy functions.
- This configuration affords flexibility in providing direct internet access.

2. Screened host, dual homed bastion

- Fig. 5.3.7 shows dual homed bastion.
- This configuration prevents a security breach. The advantages of dual layers of security that were present in the previous configuration are present as well.

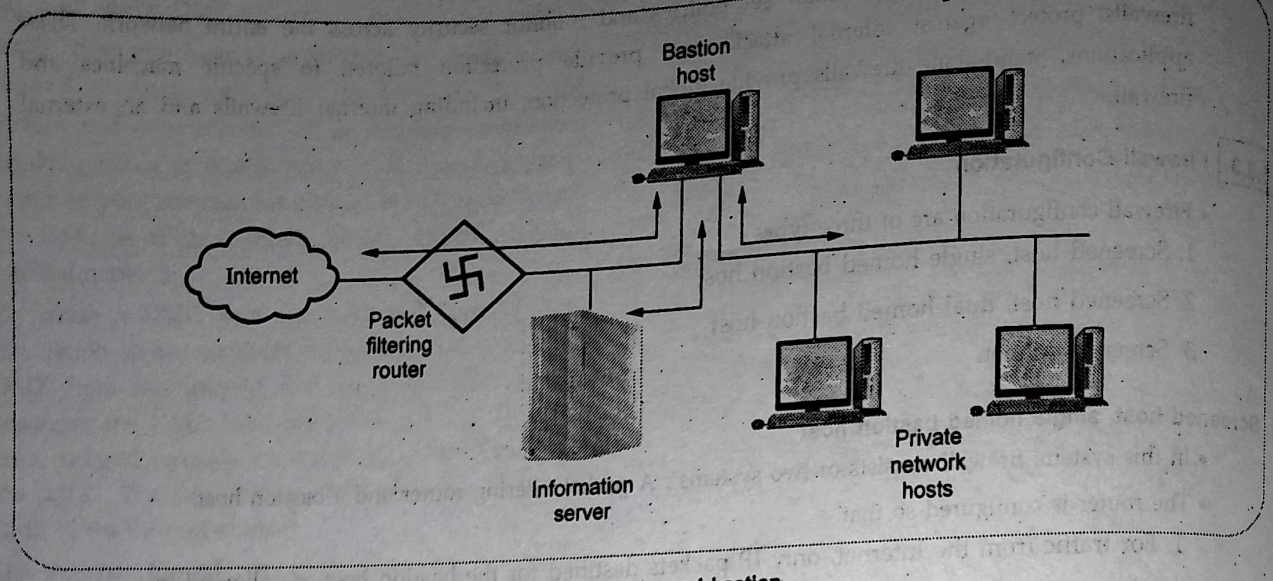

Fig. 5.3.7 Dual homed bastion

- An information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy.

3. Screened subnet

- Fig. 5.3.8 shows screened subnet

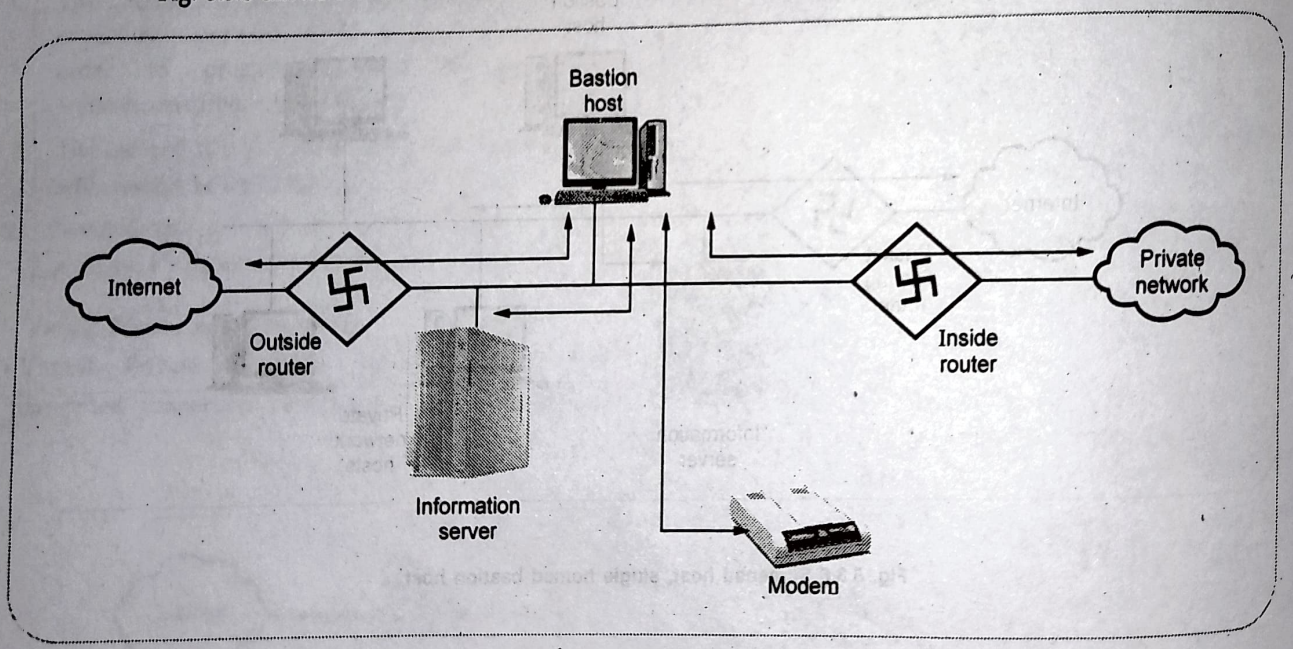

Fig. 5.3.8 Screened subnet

- This configuration creates an isolated subnetwork which may consists of simply the bastion host but may also include one or more information servers and modems for dial-up capability.

Advantages

1. There are now three levels of defense to thwart intruders.
2. Internal network is invisible to the Internet.
3. The systems on the inside network cannot construct direct routes to the internet.

Review Questions

1. *What are the various characteristics of firewall ?*
2. *Explain architecture of firewall.*
3. *Describe types of firewall in detail.*
4. *Describe screened subnet fire wall architecture.*
5. *Explain the firewall types with its operation.*
6. *Explain various types of firewall.*
7. *Describe operation of packet filtering firewall.*

5.4 Trusted Systems

- Another widely applicable requirement is to protect data or resources on the basis of levels of security, as is commonly found in the military where information is categorized as Unclassified (U), Confidential (C), Secret (S), Top Secret (TS) or Higher.
- Here subjects have varying rights of access to objects based on their classifications. This is known as multilevel security. A system that can be proved to enforce this is referred to as a **trusted system.**
- The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or incompatible level unless that flow accurately reflects the will of an authorized user. This can be implemented using the **Bell LaPadula Model,** in which a multilevel secure system must enforce :
  1. **No read up :** A subject can only read an object of less or equal security level - Simple Security Property.
  2. **No write down :** A subject can only write into an object of greater or equal security level - * (star) Property.
- These two rules, if properly enforced, provide multilevel security.

Bell LaPadula model

- The BLP model was developed in the 1970s as a formal model for access control. The model relied on the access control concept. In the model, each subject and each object is assigned a security class. In the simplest formulation, security classes form a strict hierarchy and are referred to as security levels. One example is the U.S. military classification scheme : *top secret > secret > confidential > restricted > unclassified.*
- It is possible to also add a set of categories or compartments to each security level, so that a subject must be assigned both the appropriate level and category to access an object.
- This concept is equally applicable in other areas, where information can be organized into gross levels and categories and users can be granted clearances to access certain categories of data. For example, the highest level of security might be for strategic corporate planning documents and data, accessible by only corporate officers and their staff; next might come sensitive financial and personnel data, accessible only by administration personnel, corporate officers and so on. This suggests a classification scheme such as *strategic > sensitive > confidential > public.*
- A subject is said to have a security clearance of a given level; an object is said to have a security classification of a given level. The security classes control the manner by which a subject may access an object.
- The model defined four access modes
  1. **READ :** The subject is allowed only read access to the object.
  2. **APPEND :** The subject is allowed only write access to the object.
  3. **WRITE :** Tthe subject is allowed both read and write access to the object.
  4. **EXECUTE :** The subject is allowed neither read nor write access to the object but may invoke the object for execution.

Review Questions

1. *What is trusted system ?*
2. *What is trusted system ? Explain in brief.*

5.5 Intrusion Detection

- ***Intrusion*** is the act of gaining unauthorized access to a system so as to cause loss.
- ***Intrusion detection*** is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.

- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Functions of intrusion detection systems

1. Monitoring and analysis of user and system activity
2. Auditing of system configurations and vulnerabilities
3. Assessing the integrity of critical system and data files
4. Recognition of activity patterns reflecting known attacks
5. Statistical analysis for abnormal activity patterns

Benefits of intrusion detection

1. Improving integrity of other parts of the information security infrastructure
2. Improved system monitoring
3. Tracing user activity from the point of entry to point of exit or impact
4. Recognizing and reporting alterations to data files
5. Spotting errors of system configuration and sometimes correcting them
6. Recognizing specific types of attack and alerting appropriate staff for defensive responses
7. Keeping system management personnel up to date on recent corrections to programs
8. Allowing non-expert staff to contribute to system security
9. Providing guidelines in establishing information security policies

Process model

- Many IDSs can be described in terms of following functional components :

1. **Information sources :** The different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.
2. **Analysis :** The part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.
3. **Response :** The set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

5.5.1 Prevention

- **Intrusion prevention** is the process of performing intrusion detection and then stopping the detected incidents.
- **An Intrusion Prevention System (IPS)** is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
- Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.
- Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

5.5.2 Detection

- Intrusion detection is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behaviour.
- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.
- IDS performs three tasks :
  a) An IDS monitors events of interests.
  b) An IDS generates significant data to systems administrators for analysis.
  c) An IDS creates alert for events when occurred.

5.5.3 Function and Strength of IDS

Intrusion detection systems perform the following functions well :

1. Monitoring and analysis of system events and user behaviors.
2. Testing the security states of system configurations.
3. Base lining the security state of a system, then tracking any changes to that baseline.
4. Recognizing patterns of system events that correspond to known attacks.
5. Recognizing patterns of activity that statistically vary from normal activity.
6. Managing operating system audit and logging mechanisms and the data they generate.
7. Alerting appropriate staff by appropriate means when attacks are detected.
8. Measuring enforcement of security policies encoded in the analysis engine.
9. Providing default information security policies.
10. Allowing non-security experts to perform important security monitoring function.

5.5.4 Types of IDS

5.5.4.1 Anomaly Detection

- An anomaly based intrusion detection system is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- It examines ongoing traffic, activity, transactions, and behaviour in order to identify intrusions by detecting anomalies.
- For instance, anomaly-based IDS will detect that an IP packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.
- The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation.
- Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation.
- The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.
- Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.
- The measures and techniques used in anomaly detection include : Threshold detection, statistical measures, and rule-based measures.

Advantages of anomaly detection

1. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
2. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of anomaly detection

1. Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
2. Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

5.5.4.2 Signature-based Detection

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware.
- A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first.
- New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.
- Also called misuse detection.

Advantages of signature-based detection

1. Signatures are easy to develop.
2. Understand if you know what network behavior you're trying to identify.

Disadvantages of signature-based detection

1. High false positive rate.
2. Largely ineffective at detecting previously unknown threats.
3. Signature database must be continually updated and maintained.

5.5.4.3 Comparison between Signature-based and Anomaly Detection

Parameters	Signature-based detection	Anomaly detection
Technique	Detect patterns of interest	Deviations from learned norms
Generalization	Problematic	Yes
Specific	Yes	No
Sensitivity	High	Moderate
False alarms	Low	Moderate
Adaptation	No	Yes

5.5.4.4 Network Based System

- A Network Intrusion Detection System (NIDS) is tries to detect malicious activity such as denial of service attacks; port scans or even attempts to crack into computers by network security monitoring of network traffic.
- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- The majority of commercial intrusion detection systems are network based.
- These IDSs detect attacks by capturing and analyzing network packets.
- Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.
- Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network.
- These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.
- As the sensors are limited to running the IDS, they can be more easily secured against attack.
- Many of these sensors are designed to run in stealth mode, in order to make it more difficult for an attacker to determine their presence and location.

Advantages of network-based IDSs

1. A few well-placed network-based IDSs can monitor a large network.
2. The deployment of network-based IDSs has little impact upon an existing network.
3. It can be made very secure against attack.

Disadvantages of network-based IDSs

1. Network-based IDSs may have difficulty processing all packets in a large or busy network.
2. Network-based IDSs cannot analyze encrypted information.
3. Most network-based IDSs cannot tell whether or not an attack was successful.
4. Some network-based IDSs have problems dealing with network-based attacks that involve fragmenting packets.

5.5.4.5 Host-based IDSs (HIDS)

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs.
- Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs.
- System logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend.

Advantages

1. With their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
2. It can often operate in an environment in which network traffic is encrypted.
3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.
5. When host-based IDSs use OS audit trails as an information source, the amount of information can be immense, requiring additional local storage on the system.

5.5.4.6 Differences between HIDS and NIDS

Sr. No.	NIDS	HIDS
1.	Broad in scope, (watching all network activities).	Narrow in scope (watching only specific host activities).
2.	Easier setup.	More complex setup.
3.	Better for detecting attacks from the outside.	Better for detecting attacks from the inside.
4.	Less expensive to implement.	More expensive to implement.
5.	Detection is based on what can be recorded on the entire network.	Detection is based on what any single host can record.
6.	Examines packet headers.	Does not see packet headers.
7.	Near real-time response.	Usually only responds after a suspicious log entry has been made.
8.	OS-independent.	OS-specific.
9.	Detects network attacks as payload is analyzed.	Detects local attacks before they hit the network.
10.	Detects unsuccessful attack attempts.	Verifies success or failure of attacks.

5.5.5 Limitations of IDS

Intrusion detection systems cannot perform the following functions :

1. Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
2. Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
3. Detecting newly published attacks or variants of existing attacks.
4. Effectively responding to attacks launched by sophisticated attackers.
5. Automatically investigating attacks without human intervention.
6. Resisting attacks that are intended to defeat or circumvent them.
7. Compensating for problems with the fidelity of information sources.
8. Dealing effectively with switched networks.

5.5.6 Difference between IDS and IPS

Sr. No.	IDS	IPS
1.	Installed on network segments (NIDS) and on host (HIDS).	Installed on network segments (NIPS) and on host (HIPS).
2.	Sits on network passively .	Sits inline (not passive).
3.	Cannot parse encrypted traffic.	Better at protecting applications.

4.	Central management control.	Central management control.
5.	Better at detecting hacking attacks.	Ideal for blocking web defacement.
6.	Alerting product (reactive).	Blocking product (proactive).

5.5.7 Intrusion Detection Techniques

- Intrusion detection techniques are as follows :

1. **Threshold detection :** It records each occurrence of suspicious events and compares it with a threshold number. Threshold detection involves counting no occurrences of a specific event type over an interval of time, if count surpasses a reasonable number, then intrusion is assumed establishing threshold number is difficult.
2. **Anomaly detection :** It requires little knowledge of the actual system beforehand. Usage patterns are established automatically by means of neural networks.
3. **Rule based detection :** Observe events on system and apply rules to decide if activity is suspicious or not. Analyze historical audit records to identify usage patterns and auto-generate rules for them. Then observe current behavior and match against rules to see if conforms. Like statistical anomaly detection does not require prior knowledge of security flaws.

5.5.8 Tools for Intrusion Detection

- Audit record is a fundamental tool for intrusion detecting. Two forms of audit records are used.

1. **Native audit records**

   In all multiuser operating system accounting software collects information about user activity.

2. **Detective specific audit records**

   A system that collects information need by intrusion detection system.

Audit record format

- Each audit record contains following field.

1. Subject
2. Action
3. Object
4. Exception - condition
5. Resource - usage
6. Time stamp.

Fig. 5.5.1 shows audit record format.

Subject	Action	Object	Exception condition	Resource-usage	Time-stamp

Fig. 5.5.1 Audit record format

5.5.9 Distributed IDS

- A distributed collection of hosts supported by a LAN or internetwork is called distributed intrusion detection system.

Components of distributed IDS

- The distributed IDS consists of three major components.

1. Host agent module
2. LAN monitor agent module
3. Central manager module.

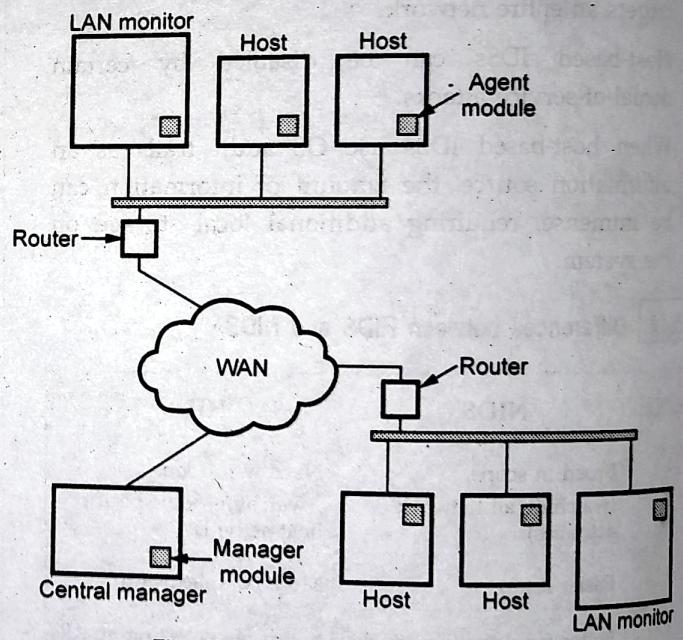

Fig. 5.5.2 Distributed ID architecture

Review Questions

1. *What are the challenges of intrusion detection ?*
2. *Explain anomaly-based intrusion detection system.*
3. *Explain types of Intrusion Detection System (IDS) ?*
4. *List and explain types of Intrusion Detection System (IDS).*
5. *Explain operation of anomaly based intrusion detection system in detail.*
6. *Explain the operaton of mis used - based intrusion detection system.*

5.6 Access Control

- Access control is an important tool of security to protect data and other resources.
- The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions
- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control

5.6.1 Discretionary Access Control (DAC)

- When user set an access control mechanism to allow or deny access to an object (system resource), such a mechanism is a Discretionary Access Control (DAC).
- The Discretionary Access Control (DAC) is also called as an Identity-Based Access Control (IBAC).
- A Discretionary Access Control (DAC) policy is a means of assigning access rights based on rules specified by users.
- The DAC policies include the file permissions model implemented by nearly all operating systems. In Unix, for example, a directory listing might yield "... rw, xr-xr-x ... file.txt", meaning that the owner of file.txt may read, write, or execute it, and that other users may read or execute the file but not write it. The set of access rights in this example is {read, write, execute}, and the operating system mediates all requests to perform any of these actions. Users may change the permissions on files they own, making this a discretionary policy.
- Discretionary Access Control List (DACL) determines which users and groups can access the object (system resource) for operations. It consists of a list of Access Control Entries (ACEs).

5.6.1.1 Drawbacks of DAC

- DAC system has two significant drawbacks :
1. It relies on decisions by the end user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject.
2. The subject's permissions will be inherited by any programs that the subject executes.

5.6.2 Mandatory Access Control (MAC)

- When a system mechanism controls access to an object and an individual user cannot alter that access, then such a control is called as Mandatory Access Control (MAC).
- Mandatory Access Control (MAC) is also called as rule-based access control.
- Mandatory access control is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
- Each security rule consists of a subject, which represents the party attempting to gain access, an object, referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.

5.6.2.1 Elements of MAC

- MAC has two key elements :

1. Labels :

- In a system using MAC, every entity is an object (laptops, files, projects, etc.) and is assigned a classification label.
- These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, etc.) are assigned a privilege label (sometimes called a clearance).

2. Levels :

- A hierarchy based on the labels is also used, both for objects and subjects.
- Top secret has a higher level than secret, which has a higher level than confidential.

5.6.2.2 MAC Implementations

- Major implementations of MAC are :
  1. **Lattice model :** Security levels for objects and subjects are ordered as a lattice.
  2. **Bell-LaPadula confidentiality model :** Advanced version of the lattice model (actually this uses a mix of MAC and DAC).

5.6.3 Role-Based Access Control (RBAC)

- A user is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- A role is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include "student," "alum," "faculty," "dean," "staff," and "contractor." In general, a user may have multiple roles.
  - Roles and their functions are often specified in the written documents of the organization.
  - The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g. hiring and resignation) and academic actions (e.g., admission and graduation).
- Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In RBAC, the rights and permissions are assigned to roles instead of individual users.
- RBAC is also called as Non-Discretionary Access Control (NDAC).
- This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.
- The RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances.
- RBAC is important because it provides customers a greater degree of control over cloud resource utilization with the added layer of system security.
- RBAC should be implemented in the following situations :

1. In an effort to minimize downtime and accidental changes to the cloud resources, the account owner would like to restrict access to the accounts to only a few people.
2. In an effort to synchronize cloud product access to the functions of an employee's job, the account owner would like to grant access to employees based on the nature of their position.
3. In an effort to help prevent unauthorized access to cloud products through the sharing of admin credentials, the account owner would like each user of the cloud accounts to have their own credentials.

5.6.3.1 Difference between DAC and RBAC

1. DAC is based on personal permissions, while RBAC is based on group-level permissions.
2. DAC is set by the data owner, while RBAC by the system owner/s (usually the developer defines the access given to each role, and the operational admin puts users into roles).
3. DAC definitions are typically attached to the data/resource, whereas RBAC is usually defined in two places : in code/configuration/metadata (the roles access), and on the user object (or table - the roles each user has).
4. DAC is administered "on the resource" (i.e. you administer each resource individually), whereas RBAC roles are centrally administered (who is associated with which roles).
5. DAC should be seen as enumerating "who has access to my data", and RBAC defines "what can this user do".
6. The definition of permissions per role is typically static in RBAC, and users are only granted roles; in DAC the permissions per resource are often changed at runtime.

5.6.4 Access Control Matrix

- A password scheme used to allow access to a user's computer account may be viewed as the simplest instance of an access control matrix : each resource has a list of identities associated with it (e.g. a computer account which authorized entities may access), and successful corroboration of an identity allows access to the authorized resources as listed for that entity.
- The simplest framework for describing a protection system is the access control matrix model.
- Two fundamental concepts in field authorization are :
  1. Access Control Lists (ACLs)
  2. Capabilities (C-lists)

5.6.4.1 ACLs and Capabilities Lists

- Access Control List (ACL) is a set of rules that define security policy. These ACLs contain one or more Access Control Entries (ACEs), which are the actual rule definitions themselves.
- These rules can restrict access by specific user, time of day, IP address, function (department, management level, etc.), or specific system from which a logon or access attempt is being made.
- The VPN secure connection can be easily cracked by Ophcrack.
- Session keys and encryption are poorly implemented and vulnerable to attacks.
- The control channel is open to snooping and denial of service.

Counter measures

- Discontinue IKE aggressive mode use, use token based authentication scheme.

VoIP hacking

- VoIP on an IP network rely on multiple protocols, one for signaling and one for transport of encoded voice traffic.
- Two most common protocols are H.323 and SIP.

Most common VoIP attacks

1. Denial of service.
2. Spoofing the CLID (caller ID).
3. Injecting data into established call.
4. Attacking through services linked to VoIP, such as -
   - Advanced voice mail
   - Instant messaging
   - Calender services
   - User management
5. Accessing repository of recorded calls.

Counter measures

- Network segment between voice and data LANs.
- Authentication and encryption for all SIP communication.
- Replay IDS/IPS.

Review Question

1. *What is access control security service ?*

❑❑❑