Unit V

CHAPTER 5

Intrusion and Firewall

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.

Syllabus Topic : Introduction, Firewall Introduction, Characteristics and Types, Benefits and Limitations, Firewall Architecture

5.1 Firewall Introduction

Q. 5.1.1 Write a short note on firewall. (Ref. Sec. 5.1)

Q. 5.1.2 What is firewall? (Ref. Sec. 5.1)

- Firewall is called as barrier place between inside and outside network to protect organization from inside and outside hackers. It also filters all traffic between intranet and extranet which runs through it.
- The main purpose of the firewall is to keep attackers outside the protected environment. For that policies are set in the firewall to decide what is allowed and what is not allowed.
- Moreover we can decide the allowed places, allowed users, allowed sites, can provide different access rights to different category of the users.
- **Example :** Cyber am through which only educational sites are allowed through college internet and non-educational sites like facebook, twitter can be blocked using firewall.

5.1.1 Firewall Characteristics

→ **(SPPU - May 16, Dec. 16, May 17)**

Q. 5.1.3 What are the various characteristics of firewall ? (Ref. Sec. 5.1.1)

May 16, Dec. 16, May 17, 5 Marks

- Following lists the characteristics as well as design goals for a firewall :
  1. All inside and outside traffic must pass through the firewall. This is possible only because of physically blocking of all access to the local network except via the firewall.
  2. The traffic defined by the local security policy will only allowed to pass through the network. Different types of firewall are used to define the policies as per the norms decided.
  3. The firewall itself is immune to penetration. Different techniques are used to control access and enforce the site's security policy.
- **Service control :** This policy helps to determine which type of internet services that can be accessed inbound and outbound. Firewall can filter traffic on the basis of IP address and TCP port number. It also act as proxy server that receives and interprets each service request before passing it on.

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

User control : This technique is used to controls access to a service according to which user is attempting to access it.

Behaviour control : Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam.

1.2 Limitations of Firewalls

Q. 5.1.4 What are the disadvantages of firewalls? (Ref. Sec. 5.1.2)

A firewall may be apivotal component of securing your rganize and is planned to address the issues of information ntegrity or activity verification (through stateful packet spection) and secrecy of your inner network (through AT). Your network picks up these benefits from a firewall accepting all transmitted activity through the firewall. our network picks up these benefits from a firewall by ceiving all transmitted activity through the firewall.

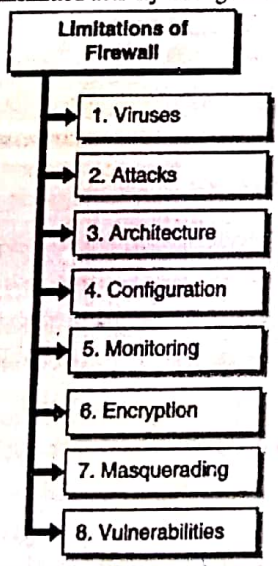

Fig. 5.1.1 : Limitations of Firewall

owing are the limitations of firewall :

1. **Viruses**

Not all firewalls have full protection against computer viruses because virus uses different encoding techniques to encode files and transfer them over Internet.

2. **Attacks**

A firewall cannot prevent users or attackers with modems from entering in to or out of the internal network, thus bypassing the firewall and its protection completely.

3. **Architecture**

Firewall architecture depends upon single security mechanism failure. If that security mechanism has a single point of failure, affects on entire firewall programs which opens the loop falls for intruders.

4. **Configuration**

Firewall doesn't have mechanism to tell administrator about incorrect configuration. Only trained professionals in the field of network security can configure firewall properly.

5. **Monitoring**

Firewall doesn't give notification about hacking. It will notify only about threat occurrences. The reason is, organization demands additional hardware, software and different networking tools as per there requirement hence there is no control on it.

6. **Encryption**

Firewall and Virtual Private Networks (VPNs) don't encrypt confidential documents and E-mail messages sent within the organization or to outsiders. Dignified procedures and tools are needed to provide protection against confidential documents.

7. **Masquerading**

Firewalls can't stop hacker those who steal login id and password of authentic user to gain access to a secure network. Once attacker gains full access of the entire network, attacker can delete or change the network policies of organization.

8. Vulnerabilities

Firewall can't tell other venerability that might allow a hacker access to your internal network.

5.1.3 Firewall Architecture and Types

(SPPU - Dec. 14, May 15, May 16, Dec. 16, May 17)

Q. 5.1.5 What is packet filtering? Differentiate packet filtering router and stateful inspection firewall. (Ref. Sec. 5.1.3) **Dec. 14, 8 Marks**

Q. 5.1.6 Enlist and explain firewall design principles in short. (Ref. Sec. 5.1.3) **May 15, 8 Marks**

Q. 5.1.7 Explain Architecture of firewall. (Ref. Sec. 5.1.3) **May 16, 6 Marks**

Q. 5.1.8 Describe types of firewall in detail. (Ref. Sec. 5.1.3) **Dec. 16, May 17, 6 Marks**

A firewall is a kind of reference monitor. All network traffic passes through firewall. That's why it is always in invoked condition. A firewall is kept isolated and cannot be modified by anybody other than administrator. Generally it is implemented on a separate computer through which intranet and extranets are connected.

Following are the common architectural implementations of firewalls :

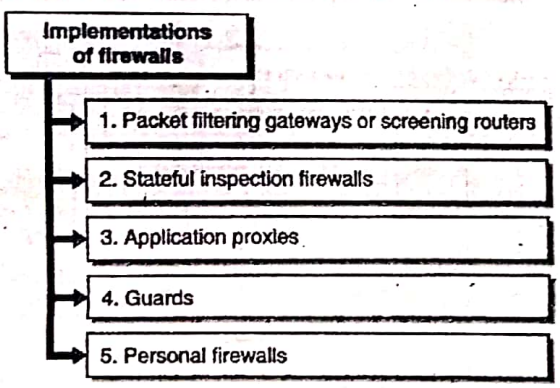

Fig. 5.1.2 : Implementations of firewalls

1. Packet Filtering Gateway

- It is the most simple and easy to implement firewall. Packet filtering is done on the basis of packets source or destination address or based on some protocol type like HTTP or HTTPs.
- If the firewall is placed just behind the router then the traffic can be analyzed easily. In the Fig. 5.1.3 it is shown that how packet filtering gateway can block traffic from network 1 and allow traffic from network 2.
- Also the traffic using telnet protocol is blocked. Packet filters do not analyze the contents of the packet rather they just check IP address of the packets as shown in Fig. 5.1.3.
- The biggest disadvantage of the packet filtering gateway is that it requires lot of detailing to set policies.

Example

- If port 80 is blocked. If some applications essentially need use of port 80 then in this case we have to provide all the details of those applications for which port 80 is needed.

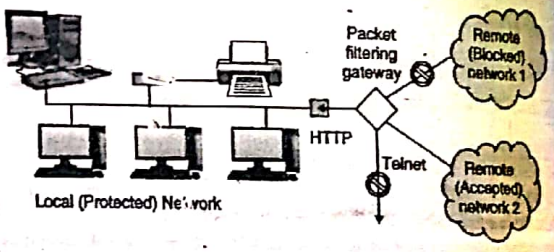

Fig. 5.1.3 : Packet Filter Blocking Addresses and Protocols

2. Stateful Inspection Firewall

- Packet filtering is done one packet at time. Sometimes attacker may use this technique for their attack. Attacker can split the script of attack into different packets so that the complete script of attack cannot be identified by packet filtering firewall.
- To avoid this stateful inspection firewall keeps record of states of the packets from one packet to another. Thus sequence of packets and conditions within the packets can be identified easily.

3. Application Proxies

- Packet filters cannot see inside the packets. From the packet headers they just get IP addresses for filtering.

Application proxy is also known as a bastion host. Fig. 5.1.4 shows firewall proxies.

Example

A college wants to publish a list of selected students. Then they just want students to read that list. No student can change that list. Moreover students cannot access more data than the list.

Application proxy helps us in this regard. Here it helps us to check only list is displayed on the screen and not more than that. That list should not have any modified contents.

Proxies on the firewall can be customized as per the requirements.

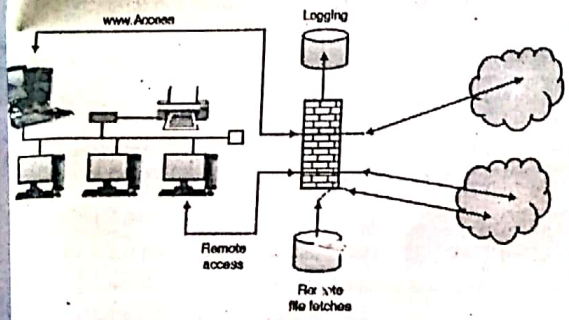

Fig. 5.1.4 : Firewall Proxies

4. Guard

A guard is kind of complex firewall. It works similar to proxy firewall. Only difference is that guard can decide what to do on behalf of the user by using available knowledge.

It can use knowledge of outside users identity, can refer previous interactions, blocked list etc.

ample

In order to increase the speed of the internet a school can set download limit for the students.

A student can download only 20mb data per day etc.

5. Personal Firewalls

8.1.9 What is personal firewalls?
(Ref. Sec. 5.1.3(5))

- For a personal use to keep separate firewall on a separate machine is quite difficult and costly. So personal users need a firewall capability on lower cost.
- An application program which can have capabilities of a firewall can solve this problem.
- It can screen incoming and outgoing traffic on a single host.
- Symantec, McAfee, Zone alarm are the examples of personal firewalls. Personal firewalls can be combined with antivirus systems.

5.1.4 Firewall Configurations

➔ (SPPU - Dec. 13)

Q. 5.1.10 How firewalls are configured and managed? (Ref. Sec. 5.1.4) Dec. 13, 4 Marks

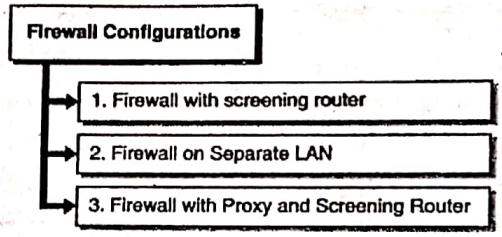

Fig. 5.1.5 : Firewall Configurations

➔ **1. Firewall with screening router**

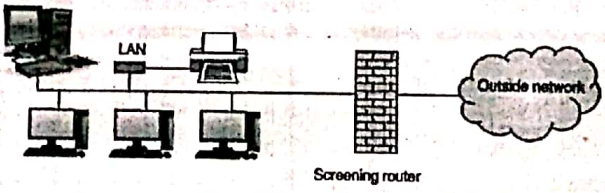

Fig. 5.1.6

The screening router is placed in between intranet and extranet. Another name for screening router firewall is network level or packet-filter firewall. Protocol attributes are used for performing the screening of incoming packets. The attributes like source or destination address, type of protocol, source or destination port, or some other protocol-specific attributes plays a vital role. A screening router performs packet-filtering and is utilized as a firewall. In a few cases a screening router may be utilized as perimeter assurance for the internal network or as the whole firewall solution.

2. Firewall on Separate LAN

Unauthorized internet users from accessing private networks connected to the internet are prevented by firewall, especially intranets. All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security constraint.

To overcome the problem of the exposure of LAN, a proxy firewall can be installed on its own LAN.

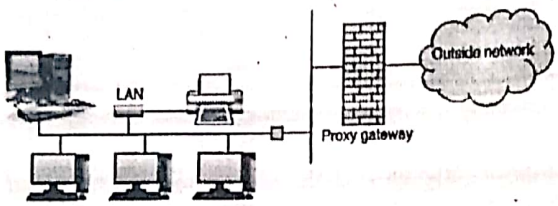

Fig. 5.1.7

3. Firewall with Proxy and Screening Router

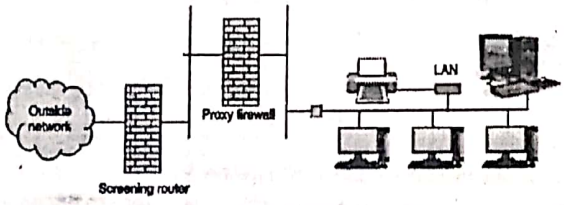

Fig. 5.1.8

If screening router is installed behind the proxy firewall, then it ensures the correct address to proxy firewall. In other words it is a double guard protection. If anyone fails LAN is not exposed.

Syllabus Topic : Trusted Systems

5.2 Trusted Systems

(SPPU - May 16, May 17)

Q. 5.2.1 What is Trusted System ? (Ref. Sec. 5.2) May 16, May 17, 5 Marks

Trusted system is level base security system where protection is provided and handled according to the different levels. This is commonly found in military, where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS), or beyond.

This concept is equally applicable in other areas, where information can be organized into categories and users can be granted clearances to access certain categories of data. When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security.**

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 non-comparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated. A multilevel secure system must enforce the following :

- **No read-up :** A subject can only read an object of less or equal security level. This is referred to in the literature as the **simple security property**
- **No write-down :** A subject can write into an object of greater or equal security level. This is referred to as the ***-property** (pronounced star property)

These two rules, if properly enforced, provide multilevel security. For a data processing system, the approach that has been taken, and has been the object of much research and development, is based on the **reference monitor** concept. The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object. The reference monitor has access to a file, known as the security kernel database that lists the access privilege (security clearance) of each subject and the protection attributes (classification level) of each object. The reference monitor enforces the security rules (no read-up, no write-down) and has the following properties:

- **Complete mediation :** The security rules are enforced on every access, not just, for example, when a file is opened (requires high performance overhead).
- **Isolation :** The reference monitor and database are protected from unauthorized modification (requires impossibility for attacker to change database).
- **Verifiability :** The reference monitor's correctness must be provable. That is, it must be possible to

demonstrate mathematically that the reference monitor enforces the security rules and provided complete mediation and isolation. If provided, system is referred to as a trusted system. These are stiff requirements.

Important security events, such as detected security violations and authorized changes to the security database, are stored in the audit file.

These are the systems whose failure may break a specified security policy. The base of the trusted system is as follows :

- It combines software and hardware portions with respect to security.
- It can act as a mediator.
- It is tamperproof.
- It is validated.

Syllabus Topic : Access Control

5.3 Access Control

➔ (SPPU - Dec. 16)

Q. 5.3.1 What is Access control security service? (Ref. Sec. 5.3) Dec. 16. 5 Marks

Access Control is the ability to limit and control the access to the host systems. It prevents unauthorized use of a resource. The service used to prevent unauthorized use of a resources i.e. complete control over who can access to resources, under what conditions access can occur and what are different accessing methodology.

For example

It controls the access of resources which is to be made available only to legitimate user. Secondly it looks to the conditions of accessing the resource or network and what is allowed to be done to the resources.

Database administrator decides what should be stored in a database and to whom access rights can be given based on the needs of different users. Database administrator takes these decisions on the basis of access policies.

Following are the factors that the DBMS may consider for deciding access policies :

1. **Availability of Data :** While updating proper blocking and locking should be used so that other processes cannot interfere and can get correct data also.
2. **Acceptability of Access :** DBMS must protect sensitive data from unauthorized users.
3. **Assurance of Authenticity :** Sometimes database may permit some users to access sensitive data.

   Example : During auditing of a failure database may give permission to auditor/administrator also to access the sensitive data in order to resolve the problem after looking at the severity of the things.

Syllabus Topic : Intrusion Detection

5.4 Introduction to Intrusion Detection

- With the rapid expansion of Internet during recent years, security has becomes an essential issue for computer networks and computer systems.
- As defined earlier the main aim of a security system is to protect the most valuable assets (data/secret information) of an organizations like banks, companies, universities and many others, because these organizations have data or secret information in some form, and their security policies are keen for protecting the privacy, integrity, and availability of these valuable information or data.
- As these organizations will have different security policies and requirements depending on their vision and missions.
- Many efforts have been carried out to accomplish this task are security policies, firewalls, anti-virus software even *Intrusion Detection Systems* (IDSs) to configure different services in operating systems and computer networks.
- But still detecting different attacks (like denial service attacks, IP spoofing, ping of death, network scanning etc.) against computer networks is becoming a crucial

problem to solve in the field of cryptography and network security.

- To overcome all above problems researcher in the field of computer security came with existing but different solution called Intrusion Detection System (IDS). Before discussing on IDS let us understand some key points like what is intrusion? What is intrusion detection and then what is intrusion detection system?

5.4.1 Intrusion Detection

Q. 5.4.1 What are the strengths and limitations of Intrusion Detection System? (Ref. Sec. 5.4.1)

Q. 5.4.2 What is intruder and intrusion detection system? (Ref. Sec. 5.4.1)

- Before defining Intrusion Detection first understand what is an Intruder?
- An *Intruder* is a person who intercepts system availability, confidentiality and data integrity. Intruder's gains unauthorized access to a system with criminal intensions. Intruder may damage that system or disturbs data.
- When an attacker or intruder attempts to break into an information system or performs an illegal action such as denial of service attacks, scanning a networks, ping scan, sending many request for connection setup using fake IP address, etc. which is legally not allowed, that is called as an *intrusion*.
- *Intrusion detection* is an important technology that monitors network traffic, events and identifies network intrusions such as abnormal network behaviours, unauthorized network access and malicious attacks to computer systems.
- The general example of intrusion detection is when we suffer from some disease and asking doctor what happen to me. Doctor suggests for blood checking and sends blood sample to laboratory for detection.
- The blood report given by pathologies is just detection of disease (number of platelets count, WBC, RBC, haemoglobin, etc.) then after checking the entire history of blood report doctor suggests medicine to cure the disease.
- Here blood report is intrusion detection where as medicine given by the doctor after checking blood report is called intrusion detection system. Finally how fast patient get relief depends upon the doctor's education, experience and knowledge, joke apart let us move towards technical definition of IDS.

Syllabus Topic : Intrusion Detection System - Need, Methods

5.5 Intrusion Detection System : Need, Methods, Types of IDS

→ **(SPPU - Dec. 13, Dec. 14, May 15, May 16, May 17)**

Q. 5.5.1 What is Intrusion Detection System (IDS)? Explain different reasons for using IDS and different terminologies associated with IDS. (Ref. Sec. 5.5) **Dec. 13. 8 Marks**

Q. 5.5.2 What is IDS? Differentiate statistical Anomaly detection and rule base intrusion detection. (Ref. Sec. 5.5) **Dec. 14. 8 Marks**

Q. 5.5.3 What is intrusion detection system? Enlist and explain different types of IDS. (Ref. Sec. 5.5) **May 15. 8 Marks**

Q. 5.5.4 What are the challenges of intrusion detection? (Ref. Sec. 5.5) **May 16, May 17. 6 Marks**

- Intrusion Detection system has some policies or mechanisms to protect computer systems from many attacks. As the use of data transmission and receiving over the internet increases the need to protect the data of these connected systems also increases. Many scientists have different definition of IDS but as per our point of view IDS can be defined as below point.
- "An Intrusion Detection System is software that monitors the events occur in a computer systems or networks, analyzing what happens during an execution and tries to find out indications that the computer has

been misused in order to achieve confidentiality, integrity and availability of a resource or data".

The IDS will continuously run on our system in the background, and only generate the alert when it detects something suspicious as per its own rules and regulation or attack signature present into it and taking some immediate action to prevent damage.

Intrusion detection

- System examines or monitors system or network activity to find possible attacks on the system or network. Signs of violation of system security policies, standard security practices are analyzed.
- Intrusion Prevention is the process of detecting intruders and preventing them from intrusive effort to system.

Challenges of intrusion Detection

In order to better understand intrusion detection systems, it is important to realize that threats to networked computer systems come in a number of forms. According to the source of threats, potential intruders can be roughly classified into two categories :

1. **Outside Intruders :** The attack is launched by an unauthorized computer user. The attacker will stole or broken passwords, using system vulnerabilities or improper configurations, human engineering techniques, to gain access to computers.
2. **Inside Intruders :** Internal intruders, who have permission to access the system with some restrictions, In this case, the intruder already has legitimate access to a computer system, but utilizes any of the previously mentioned techniques to gain additional privileges and misuse the computer system. Sometimes inside intruders are more harmful than outside intruders. It is observed that 80% of intrusions and attacks come from within organizations.

Following are the possible type of attacks that intrusion detection needs to face :

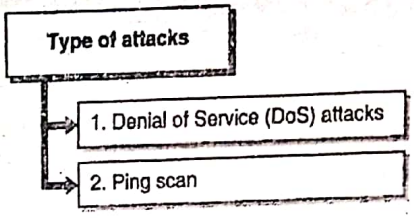

Fig. 5.5.1 : Type of attacks

⇒ 1. Denial of Service (DoS) attacks

- These attacks attempt to *"shut down a network, computer, or process; or otherwise deny the use of resources or services to authorized users"*.
- There are two types of DoSattacks :
  - (i) Operating system attacks, which target bugs in specific operating systems and can be fixed with patches;
  - (ii) Networking attacks, which exploit inherent limitations of networking protocols and infrastructures.
- An example of operating system attack is teardrop,in which an attacker exploits a vulnerability of the TCP/IP fragmentation re-assembly code that do not properly handle overlapping IP fragments by sending a series of overlapping packets that are fragmented. Typical example of networking DoS attack is a "SYN flood" attack, which takes advantage of three-way handshake for establishing a connection. In this attack, attacker establishes a large number of "half-open" connections using IP spoofing. The attacker first sends SYN packets with the spoofed (faked) IP address to the victim in order to establish a connection.
- The victim creates a record in a data structure and responds with SYN/ACK message to the spoofed IP address, but it never receives the final acknowledgment message ACK for establishing the connection, since the spoofed IP addresses are unreachable or unable to respond to the SYN/ACK messages.

- Although the record from the data structure is freed after a time out period, the attacker attempts to generate sufficiently large number of "half-open" connections to overflow the data structure that may lead to a segmentation fault or locking up the computer.

➡ 2. Ping scan

- The simplest form of scan, an attacker sends an ICMP echo request packet to every candidate machine (which is the same way the *ping* tool works).
- Any addresses that respond are noted as active.

(1) **TCP Connect ( ) scan :** Another simple scan, an attacker attempts to open a standard TCP connection to a typical port on the candidate machine (such as the HTTP port 80). Any machine where such a connection succeeds is noted as active. Since many systems log any connection attempts, this type of scan is relatively easy to recognize from standard audit data.

(2) **UDP scans :** This scan consists of sending UDP packets to likely ports on candidate machines at worst, scanning for any open UDP ports. Since UDP is connectionless, such attempts are harder to control using filtering firewalls, and may be capable of finding unprotected services and hosts. Many variations on these scanning techniques exists – including scans using fragmented packets, and scans spread across a long period or a number of source machines. In practice, completely blocking scans is probably infeasible – but may give an administrator early warning of an impending attack.

(3) **Rlogin:**The RLOGIN attack is characterized by a high rate of connections from one node to another, often within a small period of time. In this attack, the intruder is attempting to gain access to the system.

☞ **Need of IDS**

Intrusion Detection has its primary goal the detection of abuses of computer systems also it performs a variety of functions like :

- Monitoring and analyzing user and system activity.
- Auditing system configurations and vulnerabilities.
- Assessing the integrity of critical system and data files.
- Recognition of activity patterns reflecting known attacks.
- Statistical analysis for abnormal activity patterns.
- Operating-system audit-trail management, with recognition of user activity reflecting policy violations.
- IDS should offer reports of attacks in real time, ideally as the intrusion is in progress allowing security personnel to take corrective action.
- IDS should cooperate with other security mechanisms, increasing the overall security of systems. Ideally, IDS should be capable of detecting failures or attacks on other security mechanisms, forming a second level of defence.
- IDS should be capable of responding to intrusive behaviour: by increasing its monitoring in the relevant sections, or by excluding or restricting intrusive behaviour.
- IDS should protect itself against attacks, ensuring that the integrity of the greater system, and audit information up to the point of compromise remains intact, and ensuring that a compromised or hostile component cannot adversely affect the functioning of the system as a whole.

Other than monitoring network intruder and policy violations, the IDS can be useful in many other ways:

- To identify problem based on security policies.
- To maintain the logs of all the threat those are detected by IDS.
- As users are monitored continuously in network, making them analyze so that less violations cannot be committed.
- Using some preventive measures so that violation cannot be occur like terminating the network connections, user session or block access to the targets or the accounts that are likely to be violated.

The IDPS (Intrusion Detection and Prevention System) can acts like proxy, which helps in un-packaging the payload of the request and remove header. This helps to invalidate the intruder attacks.

The IDPS can sometimes change the security environment to prevent it from attacks.

5.5.1 Intrusion Detection Methods/ Techniques

→ (SPPU - Dec. 16)

Q. 5.5.5 Explain methods for intrusion detection system (IDS).(Ref. Sec. 5.5.1) **Dec. 16. 6 Marks**

The categorization of Detection methodologies are : ignature Based, anomaly based, stateful protocol analysis. lost of the IDPS uses these techniques to reduce or make etwork error free.

5.5.1(A) Signature Based Detection

It is a process of comparing the signatures of known threat with the events that are been observed. Here the current packet is been matched with log entry of the signatures in the network.

Signature is defined as the pattern (structure) that we search inside a data packet. The data packet may contain source address, destination address, protocol, port number etc.

If an attacker adds any malicious code into these data packet he is generating attack pattern or signature.

Signature based IDS create databases of such attack pattern for detecting the known or documented attacks. Single signature is used to detect one or more types of attacks which are present in different parts of a data packet.

Signature based IDS used to monitor the events occurred in the network and match those events against a database of attack signatures to detect intrusions.

It also uses a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks.

- For example, we may get signatures in the IP header, transport layer header (TCP or UDP header) and application layer header or payload. Signature based intrusion detection system sometimes also called misuse detection techniques. It checks for the attack pattern with the existing stored database pattern and if match is found then generates the alert.
- Signature based IDSs are unable to detect unknown and newly generated attacks because it requires manual updating of each new type of attacks into to the existing database. The most well known example of signature - based IDS is SNORT IDS freely available for attack detection and study purpose.

Advantages

- An advantage of misuse-detection IDS is that it is not only useful to detect intrusions, but it will also detect intrusion attempts.
- Effective at detecting known attack without too many false alerts as compare to anomaly detection technique.
- Most of the current network intrusion detection system uses misuse detection technique for finding the attack pattern and detect them according to the rules and regulation used.
- Furthermore, the misuse detection IDS could detect port - scans and other events that possibly precede an intrusion.

Disadvantages

- Detecting only known attacks therefore it cannot identify new attacks efficiently.
- If there is single variation into attack signature it invalidates the attack signature or unable to detect it.
- Constant updating of attack pattern is required.

5.5.1(B) Anomaly Based Detection

→ (SPPU - May 16, May 17)

Q. 5.5.6 Explain Anomaly-based Instruction Detection System. (Ref. Sec. 5.5.1(B)) **May 16. May 17. 6 Marks**

- It is the process of comparing activities which are supposed to be normal against observed events to identify deviation.
- An IDPS uses Anomaly based detection techniques, which has profiles that represent normal activities of user, host, connections or applications.
- **For example :** Web activities are a normal activity done in a network. Anomaly based IDS works on the notation that "attack behavior" enough differ from "normal behavior" (IDS developer may define normal behavior).
- Normal or acceptable behaviours of the system (e.g. CPU usage, job execution time etc.) if the system behaviour looks abnormal i.e. increasing CPU speed, too many job execution at a time then it is assumed that the systems is out of normal activity. Anomaly based detection is based on the abnormal behaviour of a host or network.
- Database for such type of IDS is the events generated by user, host and network, and the "normal" behaviour of the systems. These events (historical data) are collected from the research laboratories which continuously work on normal and abnormal behaviour systems over a period of time.
- Anomaly based IDS checks ongoing traffic, host activities, transactions and behaviour in order to identify intrusions by detecting anomalies. Host - based IDS generally uses anomaly based techniques.
- This can be done in two ways:

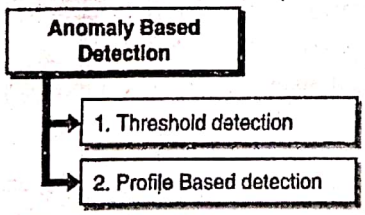

Fig. 5.5.2 : Anomaly based detection

➜ **1. Threshold detection**

Threshold is defined for all users for all groups and frequency of all events is measured comparing with threshold.

➜ **2. Profile Based detection**

Profiles of individuals are created and they are matched against the collected statistics for checking the irregular patterns.

☞ **Advantages**

An anomaly detection system observes and checks the deviation of normal network. If it observes any changes or suspicious in the network from normal deviations it will immediately inform and alert about the unknown attack.

☞ **Disadvantages**

- Anomaly detection techniques generate large number of false alarms due to the unpredictable behaviours of users and networks.
- It also requires extensive "training data set" of system events, records in order to characterize normal behaviour patterns.
- In addition, because a user's normal behaviour usually changes over time (for example, a user's behaviour may change when he moves from one host to another host), it is very difficult to collect the historical data of normal and abnormal behaviour.

5.5.1(C) Stateful Protocol Analysis

Unlike anomaly based detection which uses host and network specific profiles, the stateful protocol analysis relies on Vendor developed universal profiles. The stateful protocol analysis means the IDPS is able of checking the network, applications, and protocols that are pre defined in them. It can identify unexpected sequence of threats in form of commands.

☞ **Disadvantage of stateful protocol analysis**

- Stateful protocol analysis are extensively resource demanding.
- These methods don't capture threats or attacks that don't hamper the general accepted protocol in network.

Syllabus Topic : Types of IDS

5.2 Types of IDS

→ (SPPU - Dec. 16)

5.5.7 Explain types of Intrusion detection systems (IDS). (Ref. Sec. 5.5.2) **Dec. 16. 6 Marks.**

5.5.8 Describe the different types of IDS and their limitations. (Ref Sec. 5.5.2)

The types of IDS are differentiated mainly by the types of event they monitor or scrutinize. There are four types of IDS.

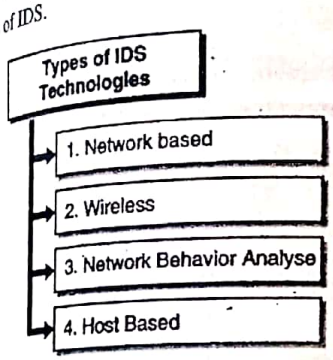

Fig. 5.5.3 : Types of IDS

1. Network based

The IDS monitors network traffic. It analyzes the network activities and protocol activities to identify suspicious activity of the network.

→ **2. Wireless**

The IDS monitors the wireless network traffic. It analyzes the network activities and protocol activities of wireless network.

→ **3. Network Behaviour Analyse**

These network behavior analyze identify the treats that create unusual traffic overflow, DDOS (Distributed Denial of Service) attacks, malwares, and policy violations.

→ **4. Host Based**

- These IDS monitors the host and the event occurs within that host.
- Among above four types of IDS two are important and most commonly used to monitor the networks and hosts.

5.5.2(A) Network based IDS (NIDS)

- As the usage and popularity of Internet is increasing tremendously, the attacks to the network are increasing for example TCP hijacking, DOS, IP Spoofing etc.

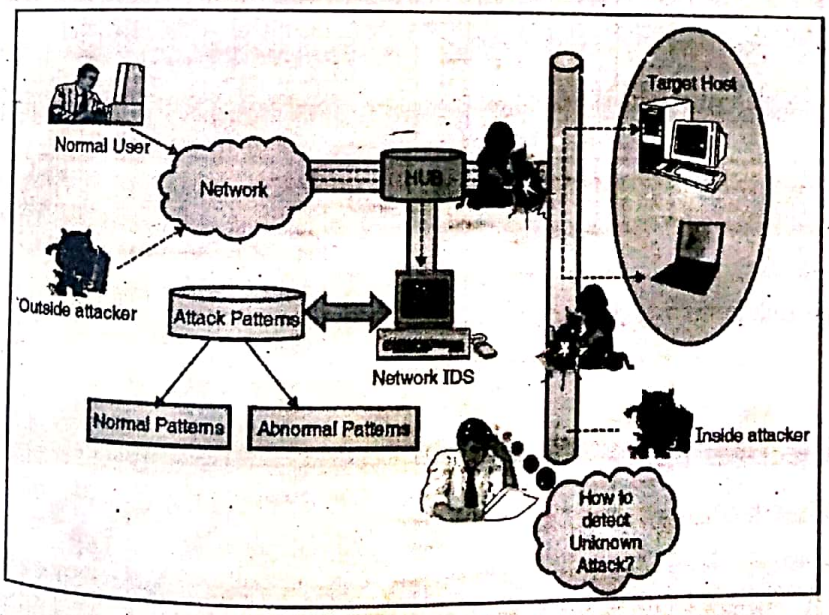

Fig. 5.5.4 : NIDS architecture

- These network attacks cannot be detected by host based IDS It need Network based IDS to detect the attack and resolve it. General architecture of NIDS is shown in Fig. 5.5.4.
- NIDS detects attacks by monitoring, capturing and analyzing packets or network traffic and tries to give indication that computer has been misused. It detects malicious data present into packets by monitoring network traffic.
- NIDS continually monitors network traffic and discovers that if hacker/ intruder are attempting to break into a system.
- When NIDS installed on main server which consist of multiple hosts in a single network, it detects attacks present in the multiple hosts by checking incoming packets that looks unordinary.
- NIDS uses raw network packets as the training dataset for offline detection collected from well known research laboratory such as Defence Advance Research Project Agency (DARPA).
- As defined earlier it can be installed on servers, workstations, personal computers or machines dedicated to monitor incoming network packets from switches, routers and probes for intrusions.

Advantages of NIDS

- A well placed network - Based IDS can monitor a large network.
- NIDS just listen to the network; it does not interfere in the network.
- NIDS can be made very secure against attack and made invisible to many attackers.
- Network-based IDS use live network traffic for real time attack detection and also operating system independent.

Disadvantages of NIDS

- It becomes difficult for NIDS to recognize the attack in large or busy network due to high traffic is there in network. It will be difficult for NIDS to analyze.
- NIDS cannot analyze the network if communication is in encrypted format.
- Difficult to detect the whole process of attack, usually detect only the initial level of attack.
- We have seen a different type of IDS but we must know how these IDS detect whether given packet is malicious and the system behaviour is abnormal. There are two main types of detection techniques for analyzing events generation, system logs, audit trails, and malicious packet activities namely:anomaly detection and misuse detection also called signature based IDS.
- (NIDS) usually consists of a network sensor with a Network Interface Card (NIC) or LAN card operating in casual mode. The IDS is placed along a network segment or boundary and it monitors all traffic on that network segment.

5.5.2(B) Host Based IDS (HIDS)

HIDS usually collects information from the operating system audit trails, and system logs. (An audit trail is a series of records of computer events, about an operating system, an application, or user activities generated by an auditing system that monitors system activity). HIDS generally installed on individual host which is connected to the internet.

Features of HIDS

- HIDS focus monitoring and analyzing the computer system they are installed on.
- It continuously monitors the state of system. It check content of RAM and the file system to check that their content do not look suspicious.
- It generally looks for the real time malicious, suspicious activity of system log.

Advantages of HIDS

- As defined earlier Host-based IDS operate on OS audit trails; they can help detect Trojan horse or other attacks that creates the software integrity violation.

HIDS analyze most of the encrypted network traffic, which usually encrypted or decrypted by the sender and/or receiver.

It is able to monitor and detect attack, which is sometimes not possible for Network IDS.

Disadvantages of HIDS

Host-based IDS are difficult to manage, because they generally installed on individual host. Monitoring to individual host is difficult because of different system configuration and log generation.

When host-based IDS use operating system logs as an information source the amount of data can be increase, requiring additional local storage on the system.

Host - based IDS are not suitable for detecting network denial of service and network scan attacks because it only checks only those packets received by individual host.

Syllabus Topic : Password Management, Limitations and Challenges

5.6 Password Management

→ **(SPPU - May 16, Dec. 16, May 17)**

Q. 5.6.1 List and explain any two password management practices. (Ref. Sec. 5.6)

May 16, Dec. 16, May 17, 6 Marks

In password management system the passwords can be created and stored very effectively. As many different users are using system all require their passwords for functioning in order to protect their data from each other.

Another important aspect of password management is to disclose the passwords by a safe, secure and appropriate way.

Password manager is important software available for password management. With the help of it passwords can be stored and organized. It stores passwords in an encrypted format.

Public Key Infrastructure

- Public Key Infrastructure (PKI) is a technology that uses mathematical algorithms and processes to facilitate secure transactions by providing data confidentiality, data integrity and authentication. PKI makes use of digital certificates to provide proof of identity for the individual.
- A digital certificate is a kind of digital document that binds a public key to a person for authentication, rather like a personal identity card. A trusted Certificate Authority (CA) creates the certificate and digitally signs it using the CA's private key, thereby authenticating the identity of the requestor.
- A person can use his or her certificate for authentication with different applications, and the applications then check the user's identity by verifying the digital signature with the issuing CA. PKI is particularly useful for user authentication in on-line transaction and public applications, because there is no advance pre-registration process required for each application. Users only need to apply for a certificate from a trusted CA to authenticate themselves with various applications.

Deploying PKI requires some worth noting security considerations as follows :

1. The private key must be protected and stored in a safe place, such as in a security token or smart card secured by a Pin.
2. Relevant password restrictions should be imposed on the PIN of the security token / smart card to prevent unauthorized access to the private key inside.
3. There should be proper procedures in place to handle key life-cycle management, issuing and revoking of certificates, storing and retrieving certificates and CRLs (Certificate Revocation Lists).
4. For private key backup, the key must be copied and stored in an encrypted form and protected at a level not lower than that of the original private key.
5. As not all applications support the use of PKI, there may be interoperability issues.

Single Sign-On

With the use of Single Sign-On (SSO) technology, users are able to identify themselves with the authentication server only once to access a variety of applications, including both internal and external systems. Users can enjoy the benefit of choosing one password to access multiple applications, instead of memorizing many different passwords

However, compromise of one authentication event could result in the compromise of all resources that the user has access rights to. Implementing SSO requires the following worth noting security considerations:

1. As one single authentication controls access to all resources, it is important that the authentication process is secure enough to protect those resources. This protection should satisfy the requirements of the most critical application. The single authentication process should not be weaker than the original authentication method used by the various applications, otherwise, the result is a downgrade in security level.
2. A second factor of authentication, such as a security token and smart card, can be used to strengthen the authentication process.
3. Relevant password restrictions, such as the minimum password length, the password complexity, the maximum number of trial attempts and the minimum time for renewal, and so on, should be imposed.
4. As the authentication server may become an attractive target for attack, it should be well protected so that intruders cannot access authentication information which could then be used for unauthorized access to all the systems.
5. Auditing and logging functions should be used to facilitate the detection and tracing of suspicious unsuccessful login attempts.
6. Encryption should be used to protect against authentication credentials transmitted across the network.

One-Time-Password Token

Another technology that may be used to facilitate password management is the one-time password token. Users authenticate themselves with two unique factors, something they have (the token) and something they know (the PIN).

Users do not need to choose or memorize passwords. The token will generate a unique, one-time-use password for each authentication process, based on the PIN and other factors, granting access to protected resources.

The following are some considerations when implementing one-time-password tokens :

1. A token is needed for each user of the authentication process, which implies additional investment.
2. Users must carry the token at all times, and they will not be able to access the system if they lose the token or forget to bring it with them. Unlike software based access control systems, which only require a password reset, users may not be able to use the system for hours or days if the token is lost.
3. Users should be aware of the physical security of the token and ensure that the token is properly protected at all times.
4. Most of the current one-time-password authentication schemes only authenticate the initial connection. Connections thereafter are assumed to be authenticated, and these connections are susceptible to being hijacked.
5. Security tokens may not support all applications or servers.

Best Practices

How to choose a good password of bad passwords? The following are examples of badly chosen passwords that can be easily guessed or cracked using password crackers freely available on the Internet.

- "password" - the most easily guessed password
- "administrator" - a login name
- "cisco" - a vendor"s name
- "peter chan" - a person"s name

"aaaaaaaa" - repeating the same letter

"abcdefgh" - consecutive letters

"23456789" - consecutive numbers

"qwertyui" - adjacent keys on the keyboard

"computer" - a dictionary word

"computer12" - simple variation of a dictionary word

"c0mput3r" - simple variation of a dictionary word with "o" substituted by "0" and "e" substituted by "3"

To avoid falling prey to attackers, there are a number of simple rules that can be followed when creating a password : Password Management.

Don'ts

Do not use your login name in any form (as-is, reversed, capitalized, doubled, etc.).

Do not use your first, middle or last name in any form.

Do not use your spouse's or child's name.

Do not use other information easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, and the name of the street you live on, so on.

Do not use a password that contains all digits, or all the same letters.

Do not use consecutive letters or numbers like "abcdefgh" or "23456789".

Do not use adjacent keys on the keyboard like "qwertyui".

Do not use a word that can be found in an English or foreign language dictionary.

Do not use a word in reverse that can be found in an English or foreign language dictionary.

Do not use a well-known abbreviation e.g. HKSAR, HKMA, MTR.

Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols, or substituting characters, like 3 for E, $ for S, and 0 for O.

Do not reuse recently used passwords.

13. Do not use the same password for everything; have one password for non-critical activities and another for sensitive or critical activities.

☞ Do's

1. Use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.
2. Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
3. Use a password that you can type quickly, without having to look at the keyboard, thereby preventing passers-by seeing what you are typing.

☞ Things to note when handling passwords

(A) Don'ts

1. Do not write down your password, particularly anywhere near your computer or file it in a box file with the word "password" written on it.
2. Do not tell or give out your passwords to other people, even for a very good reason.
3. Do not display your password on the monitor.
4. Do not send your password unencrypted, especially via email.
5. Avoid using the "remember your password" feature associated with some websites, and disable this feature in your browser software.
6. Do not store your password on any media unless it is protected from unauthorized access (e.g. encrypted with an approved encryption method).

(B) Do's

1. Change your password frequently, at least every 90 days.
2. Change the default or initial password the first time you login.
3. Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up action.

Syllabus Topic : Computer Intrusion

5.7 Computer Intrusion

- Unauthorized access to your computer/service/or data is called intrusion.
- Access could be physical or logical.
- Think of physical access as someone break-in to your house and access your computer using the username and password you have it on the posted notes next to the computer.
- Logical access is where attacker can access your computer/service or data over the network. He/she doesn't have to be physically on to your machine.
- Complete compromise is when you have root or administrator access to the computer, partial access is when you are able to log in as a user with limited rights or permission.

Chapter Ends...

❑❑❑