14.2 INTRUSION DETECTION

Intrusion detection means to detect the vulnerabilities exploited against the computer system or against any application. Intrusion detection system helps in providing the information about such vulnerabilities to the network administrator and helps him in preparing some system to protect such attacks or deal with such vulnerabilities. It includes collection of information by monitoring the network traffic and the suspicious activities in the network. It also collects the information about these vulnerabilities from different sources and analyses the same. Many people think that firewall is sufficient to protect their network and can recognise the attacks on the network and block the intrusions. But the fact is that the firewall works just like a fence to our home. It restricts the access only to the designated points on the network, but the whole network cannot be secured using firewall. Firewall cannot detect the new attacks on the network. This detection of new attacks is done by IDS.

Intrusion detection provides the following functions:

1. Monitoring and analysing both the user and the system activities
2. Analysing system configurations and vulnerabilities
3. Assessing the integrity of system and files
4. Analysing the traffic pattern based on knowing attack patterns
5. Analysing abnormal activity patterns
6. Tracking the policy violations by the user
7. Doing audit of the operating system

Today, it is more difficult to provide 100% security to any network. This is because the technologies for attacks are very user-friendly and many free tools are easily available to perform such attack. No prior technical knowledge is required to attack any system. This helps a novice attacker in making the attack with more ease.

The intrusion detection system can be divided into following two types depending on the architecture:

1. ***Network intrusion detection system (NIDS):*** It works on the network and performs an analysis of all the traffic passing on the entire subnet. Every packet is monitored and if the attack is identified or some abnormal behaviour is observed, then the alert can be sent to the administrator.

2. ***Host intrusion detection system (HIDS):*** It works off the host, monitors the system events and audits the event logs. It then takes a snap shot of the existing system files and compares it with the previous snap shot available. If any of these files are found modified or deleted, then the alert is sent to the administrator.

14.3 INTRUSION DETECTION SYSTEM

An *intrusion detection system* (*IDS*) is a security system that monitors the network traffic and analyses the data for possible attacks from outside the network or from inside the network.

IDS can be categorised depending on the method of detection attacks. Following are the categories of IDS:

1. ***Misuse-based detection versus anomaly-based detection:*** The misuse-based intrusion detection systems (IDS) uses a database of previous attack patterns and known vulnerabilities as a reference. Each intrusion have some specific pattern. This pattern is called *signature*. This pattern or signature is used to identify the attacks on the computer system or on the network. So, this system is also called *signature-based IDS*. The drawback of misuse-based IDS is that there is a need of frequently updation of the database. If there are some unique attacks, this IDS may fail to identify such attacks.

In anomaly-based intrusion detection systems (IDS), a baseline or learned pattern of normal system activity is used as references to identify intrusion. Using this information, an alarm is to be triggered. The drawback of this method is that it has higher false alarm rate.

2. ***Network-based system versus host-based systems:*** Network-based intrusion detection system monitor the packets that flow over the network. These packets are compared with the reference data present and then analysed. Then, it is verified whether the said packet is malicious or benign. It is responsible to control the vulnerabilities in the networks, so, it is distributed IDS. Network-based IDS uses packet-sniffing technique to collect the packets along the network. The architecture for Network-based IDS is shown in Figure 14.1.

In a host-based system, the activity on each individual computer or host is examined by the IDS. It is installed on an individual computer to detect the attack on that computer. There are two drawbacks of this method. The first drawback is that the system compromises with security; therefore, the log files of the system are corrupt or inaccurate. The same corrupted or inaccurate files are reported by the IDS, which makes it unreliable. The second drawback is that in host-based IDS, the IDS has to be deployed on each computer, which increases the administrative overload.

3. Passive system versus active system: A passive IDS is configured to only monitor and analyse the network traffic and if vulnerability or attack is found, it sends an alert to the network administrator. It is not able to protect or correct any actions by itself. An active IDS is used to block the suspected attacks automatically. There is no intervention required from the network administrator. It is also known as *intrusion detection and prevention system*. The advantage of this method is that it takes real time corrective action.

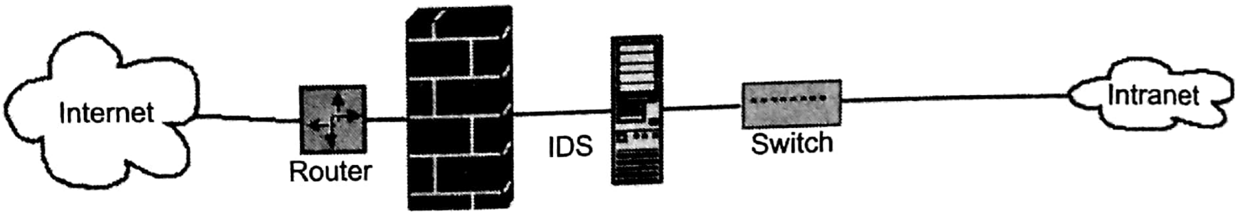

Figure 14.1 Network-based IDS.

14.3.1 Need for Intrusion Detection Systems

Out of the total security attacks that occur on a network, up to 85% attacks come from the users inside the network. These users may be authorised users of the system. The remaining attacks come from outside the network. It consists of mainly denial of service attacks or attacks to penetrate the infrastructure of the network. To protect the network from all these types of attacks, IDS is an integral part of the network or information security. It is helpful for complete supervision of the network. IDS is used to

1. Prevent problem like behaviours of the system
2. Detect various attacks and vulnerabilities in the network
3. Detect new attacks and identify its signature
4. Protect the network from internal as well as external users

Nowadays, due to the availability of tools for making attacks, it is very easy to make attack on any computer system or network. There are different methods to protect the system or network from these attacks. Firstly, develop a fully secure computer system or network. For this, the system is accessible only to the authenticated and authorised users. Secondly, use of cryptographic methods to protect the data applies tight access control. But in real life, all these solutions are feasible due to the following reasons:

1. In actual practice, to develop a completely secure system is not possible. Designing and implementing a totally secure system is an extremely difficult task.
2. Use of cryptographic methods to protect the information has its own limitations. The security of these methods depends on the secret key. If the attacker is able to capture this secret key, then he can read, change or modify the data and the entire system can be broken.
3. Many times, the protective measures are applied to prevent the external attacks. But as discussed above, approximately 85% of the total attacks are

from internal users. This happens because the internal legitimate users misuse their privileges and create the attacks internally.

4. If we tight the access control, the efficiency of the system reduces.

When an attack is detected, the IDS first alarms the network administrator. IDS works as a reactive system, instead of preventative one. It works as an informative system.

14.3.2 Intrusion Detection Method

Intrusion detection can be done using the following strategies:

1. Define the rules for the normal behaviour of the computer system or network and then search for the traffic, which is responsible for the change in behaviour of the system or computer.
2. Define the patterns of the attack and then search for the occurrence of an attack.

The first strategy is called *anomaly-based IDS* and the second strategy is called *misuse-based IDS*. We will now discuss about these methods in the subsequent sections.

Anomaly-based Detection

Anomaly-based detection techniques are based on the assumption that all intrusive activities are malicious. Therefore, we have to build a system, with a normal activity profile of the computer system and then wait for the anomalous activities to happen. That is, we identify the system states which have different behaviour from the normal established profile. Such activities are identified as intrusive activities and flagged as intrusion. However, if we assume that the rules for intrusive activities and the rules of anomalous activities are not exactly the same, but there are some matches among them, then there are chances like

1. Some activities, which are anomalous, but not intrusive activities, are also flagged as intrusion. This results in false positives.
2. Some activities are intrusive activities, but not anomalous. Such activities are not flagged and treated as normal activities. This results in false negatives.

False negative is a serious problem, as malicious packets are allowed to enter in the network or system as a normal packet. It may harm the system. This reduces the accuracy of the IDS and deteriorates the performance of the IDS. To reduce the false negatives in the system, generally the threshold is used. In anomaly-based IDS, there is a need to keep track of system profile and also updating of system profile is required. Therefore, this method is computationally expensive. The advantage of this method is that it is able to detect the new or unknown attacks.

A block diagram of anomaly-based detection system is shown in Figure 14.2.

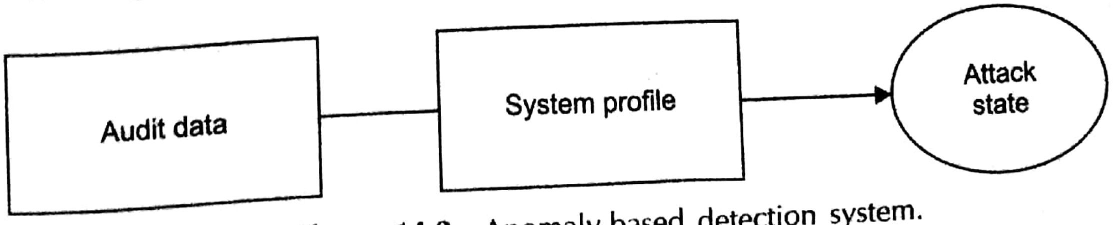

Figure 14.2 Anomaly-based detection system.

The main advantages of anamaly-based detection system are as follows:

1. It is possible to detect the new or unknown attacks.
2. Accuracy is more.
3. Internal attacks can be detected easily.

Disadvantages of anamaly-based detection system are given below:

1. False negatives are more.
2. It is expensive.
3. Accuracy is less.

Misuse-based Detection

In misuse-based detection method, the patterns or signatures are used to detect the attacks. If there are variations in the same attack, then it is possible to detect those attacks by using pattern or signature. Misuse-based detection systems use a database of information that has a number of patterns. The system collects audit data and compares this data with the stored patterns in its database. If any match is found, then the alarm is generated. If the match is not found, then it is considered as legitimate activity. The success of misuse-based detection method depends on the database of signatures or patterns. The database should include all possible patterns with the variations for different attacks and also for normal activities. How to generate these patterns or signatures is the main issue of this approach.

A block diagram of a misuse-based detection system is shown in Figure 14.3.

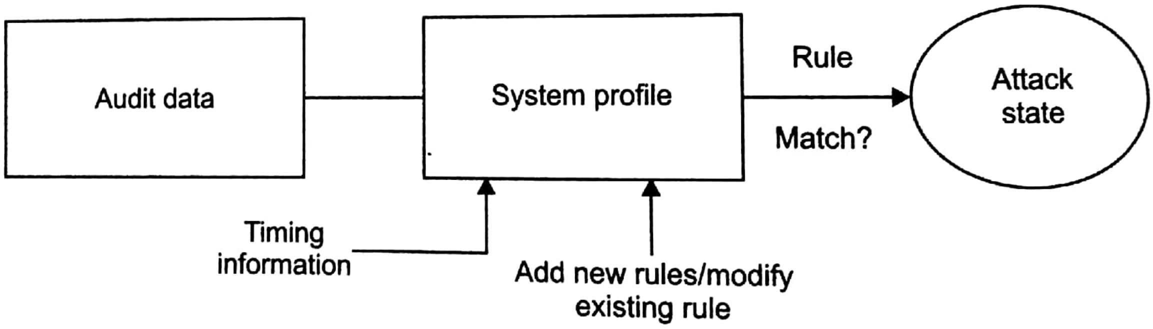

Figure 14.3 Misuse-based detection system.

The only advantages of misuse-based detection system is that it generally produces very few false positives.

Disadvantages of misuse-based detection system are as under:

1. A lot of effort is required for the generation of pattern or signature database.
2. It cannot detect new attacks.

14.4 ANOMALY-BASED INTRUSION DETECTION SYSTEMS

Anomaly-based intrusion detection systems have few major approaches to detect the intrusions. Some of these approaches are described here.

14.6 DISTRIBUTED INTRUSION DETECTION SYSTEM

With the widespread growth of internet, there is an increase in malicious activity against the network. Current IDS technology is sufficient to protect the global network infrastructure from attacks. So, there is a need of an IDS, which can support global network. Distributed IDS (dIDS) increases the identifying power and scope of single IDS by using an attack correlation with database obtained from geographically different networks. A distributed IDS consists of multiple intrusion detection systems over a large network. All these IDSs are communicated with each other, or with a central server. This allows them to monitor different advanced networks, help for analysis and find out the attack data. There are different agents which coordinate with each other and are distributed across a network. This gives the detailed pictures of different events that take place in the network to the network administrators. It allows maintaining the records related to attacks at the central place so that it is easily available to the analyst easily. There is a centralised analysis engine and on each system, there is an agent which monitors the network traffic. Current dIDS has the following limitations:

1. Observing a single site is not sufficient to detect the existence of attacks by the single attacker.

2. When a single attack is generated by a group of attackers, then to protect such attack, the global scope for assessment is required.
3. If there is a change in the system and attack behaviour, then false negatives are generated.
4. For prevention of attacks, the intention behind these attacks is required.
5. Due to advances in technology the attacks are automated. Also, these attacks are autonomous. To prevent these attacks, quick analysis and mitigation of these attacks are required.
6. The total volume of notifications about the attacks received by internet service providers (ISPs) and host systems is becoming overwhelming. If collective details about the attacks are provided to the responsible party, then the possibility of a positive response increases.

Thus, in nutshell, distributed intrusion detection system has a number of IDSs, which are spread over a global network (Internet). All these IDSs are interconnected and communicate with each other or with a central server. This allows it to monitor the network, help for analysis of the incident and find out the data related to attacks.

14.6.1 Overview

There are various components of dIDS. These components are discussed below:

Central Analysis Server

The core part of dIDS is central analysis server. It consists of a database, reporting engine and the web server. It collects the responses from the agents to permit attack correlation. It allows analysis to perform aggregation of attack, collect statistical information, recognise the pattern of attack and report the incident details.

Cooperative Agent Network

The most important components of the dIDS is the cooperative agent network. An *agent* is a software or a device which is responsible for collecting and inspecting the data. Agent might be a firewall, or host-based IDS or network-based IDS. Agent reports the information related to the attack on the central analysis server. There are multiple agents across a single network. It gives a broad view of the network than a single IDS.

Generally, these agents are located on separate network segments. They are also located on different geographical locations, as shown in Figure 14.4. The agents can also be distributed across multiple physical locations. Due to this, a single incident analysis team can view attack data across multiple corporate locations.

Attack Aggregation

Another important part of dIDS is attack aggregation. It is located in the central server. It is the method in which the information is gathered from the agent network. An example is collecting the information according to IP address of the attacker, putting together all attacks from an IP address, together with the other attacks from the same IP address. Another example is to collect the data of attacks according to destination port or put them by date and time.

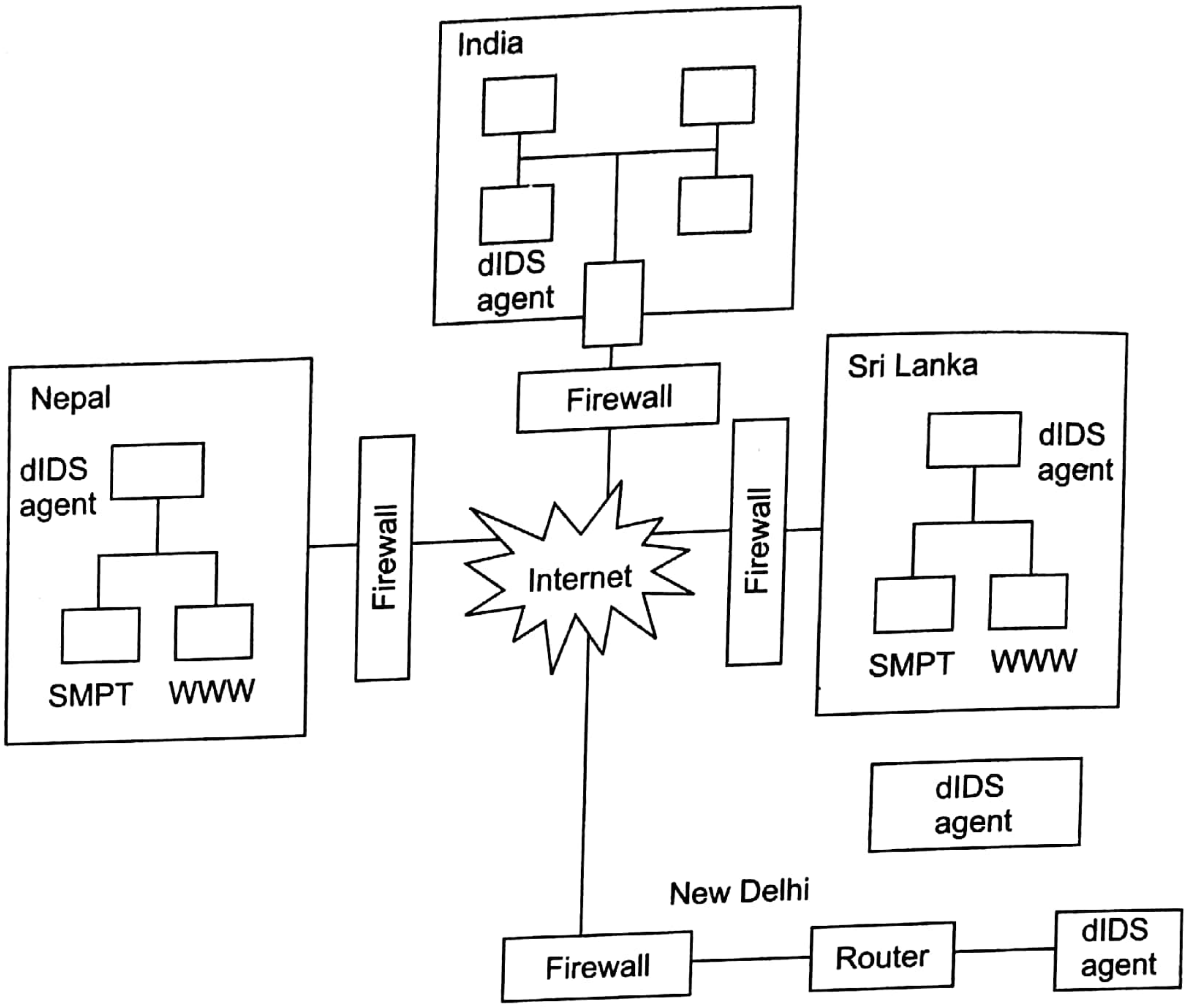

Figure 14.4 Agent network.

Data Sources

The agent reports about the internal network traffic to the perimeter or an organisation or both. This depends on where the agent resides. For dIDS, both the locations are useful because some malicious software behaves differently for inside the network than for outside the network. To get useful information about the internal attacks, the agent located inside the organisation is useful.

14.6.2 Advantages of a dIDS

The dIDS has many advantages over a single IDS. It can detect attack patterns across the entire network of the organisation, with physical locations having different time zones or even in different continents. Therefore, the attacks can be detected early and this protects the system from damage. The offending IPs are prohibited to access. Another advantage of dIDS is to allow early detection of Internet worm through the global network. The major advantage of dIDS is that a single team can analyse the attack information of places located at different places, whereas a single IDS system requires several analysis teams for the same. So, it reduces the cost of analysis. It also reduces the time required to collect the information from different places. Many times, the attacks are generated by people within the network. With the help of analysis server, the incident analyst is able to keep track of such attacks within the