4.1 INTRUSION CONCEPTS

As the number of cyber-attacks and intrusions continues to rise, monitoring and securing a company's network is very important. To protect the data and business from these threats, we need a comprehensive cyber security setup. One vital piece to solve the above issue is an Intrusion Detection System.

4.1.1 Intruders

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. In summary, intrudes attempts to violate Security by interfering with system Availability, data Integrity or data Confidentiality

4.1.2 Types of Intruders

Intruders are divided into three categories

• **Masquerader**: The category of individuals that are not authorized to use the system but still exploit user's privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, their aim is to attack unethically to steal data/ information.

Misfeasor: The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are Individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data / information.

Clandestine User: The category of individuals those have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine User. AC Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/information.

4.1.3 Different ways adopted by intruders for cracking passwords for stealing confidential information

- Regressively try all short passwords that may open the system for them.
- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.
- Try unlocking the system by personal information of the user such as their name, family member names, address, phone number in different combinations.
- Making use of Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, locality info.

4.1.4 What is an Intrusion Detection System?

An Intrusion Detection System (IDS) is a technology solution that monitors inbound and outbound traffic in the network for suspicious activity and policy breaches. As the name suggests, the primary purpose of an IDS is to detect and prevent intrusions within IT infrastructure, then alert the relevant people. These solutions can be either hardware devices or software applications.

Typically, an IDS will be part of a larger Security Information and Event Management (SIEM) system. When implemented as part of a holistic system.

Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (ie, a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

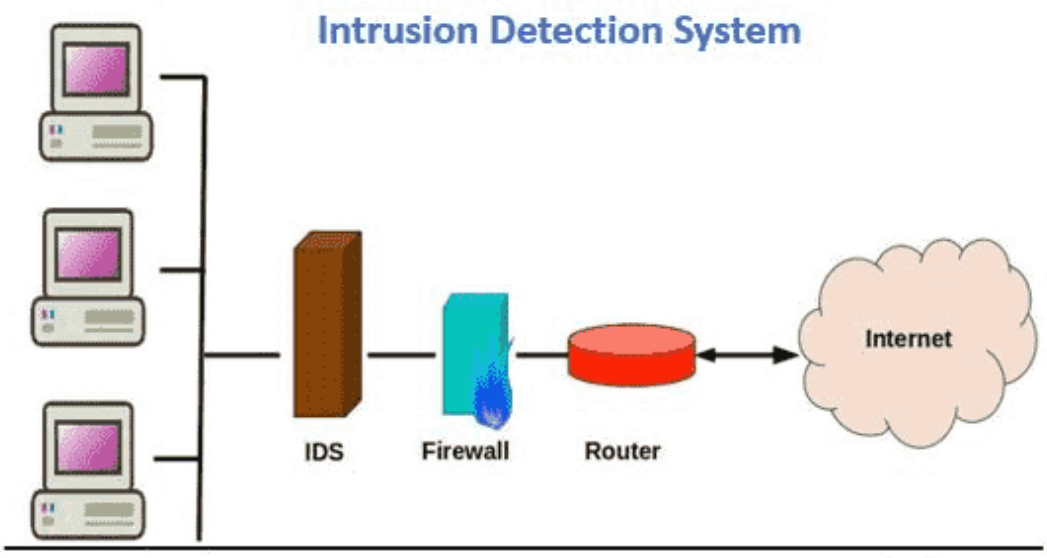

Figure 4.1: Intrusion Detection System

In short, an Intrusion Detection System (IDS) plays the role of a scout or security guard in the network, watching for suspicious attempts and notifying user as needed. However, there are several kinds of IDS solutions on the market today.

Generally, intrusion is categorized as follows:

Security intrusion: A security event, or a collection of related security events, that together make up a security incident and involve unauthorized access to a system (or system resource) by an intruder.

Intrusion Detection: A security service that keeps an eye on and examines system events in order to spot and warn of unauthorized attempts to access system resources in real-time or almost real-time

Three logical components of IDS:

Sensors: Data collection is done using sensors. Network packets, log files, and system call traces are examples of the inputs that a sensor can receive. Sensors gather this data and send it to the An analyzer

Analyzer: One or more sensors or data from other analyzers are input sources for analyzers. The analyzer is in charge of figuring out whether an intrusion has taken place. This component's output

serves as a notification of an intrusion What steps to take in response to the intrusion may be suggested by the analyzer? The sensor inputs could also be saved for later inspection and analysis

User Interface: An IDS's user interface enables a user to monitor system output or modify the system's behavior. The user interface in some systems could be comparable to a manager, director, or console component

A single sensor and analyzer may be used by an IDS, such as a traditional HIDS on a host or NIDS in a firewall device. In a distributed design, more advanced IDSs can relay data from many sensors across a variety se of host and network devices to a centralized analyst and user interface

IDSs are frequently categorized as follows:

Host-based IDS (HIDS): Looks for signs of suspicious behavior by keeping an eye on a single host's characteristics and the activities taking place on that host, such as process identifiers and system calls.

Network-based IDS (NIDS): Detects suspicious behavior by monitoring network traffic for specific network segments or devices and by analyzing network, transport, and application protocols.

Distributed or Hybrid IDS: Combines data from multiple sensors, frequently network and host-based, in a central analyzer that is better equipped to detect and react to intrusion activity.

4.2.3 Challenges of Intrusion Detection Systems

There are four key challenges that businesses face when managing IDS stems

1. Ensuring Effective Deployment

To ensure a high level of visibility, companies must ensure that their wireless intrusion detection system is optimized and installed correctly. While deploying IDS can be tricky, and if not done properly, it may create vulnerabilities for critical assets.

2. Understanding and Investigating Alerts

IDS alerts give very little information, which, sometimes, is hard to investigate. You may lag with information like what caused the attack or what further actions are required to oppose a threat. Also, investigating the IDS alerts can be time and resource-intensive, which may require additional information to identify the seriousness of the attack.

3. Managing a High Volume of Alerts

Since there is the vast majority of attacks are generated by intrusion detection, it may put the burden on internal teams to identify each one of them. Sometimes, these system alerts are false positives, which are hard to screen. Also, some IDS come pre-loaded with some defined alert signatures that are insufficient for many organizations.

4. Knowing How To Tackle Threats

A common issue that organizations face is the lack of appropriate incident response capability. Identifying a problem is half a thing; knowing how to respond appropriately is a challenging and critical thing. An effective incident response needs an expert who knows how to remediate threats and what procedures are required to address the issue